V/ Cert

Declaração de Práticas de Certificação

Autoridade Certificadora VALID SSL EV

OID 2.16.76.1.1.144

DPC da AC VALID SSL EV
Versão 4.1
Setembro de 2024

V/ Cert

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
1.0	13/07/2020	N/A	N/A	Criação da Declaração de Práticas de Certificação (DPC) AC VALID SSL EV
1.1	21/12/2020	N/A	Diversos	Ajustes na Declaração de Práticas de Certificação (DPC) - AC VALID SSL EV
1.2	12/01/2021	N/A	Diversos	1.1.3-Inclusão de referência aos documentos CAB/Forum 2.2.1 – Inclusão de referência à verificação de registros CAA antes da emissão. 2.2.2- Inclusão de referências às páginas de publicação de modelos de certificados válidos, expirados e revogados. 4.1 Exclusão da modalidade de validação online para certificados SSL EV. 4.9.9. Inclusão de informações sobre consulta OCSP.
2.0	16/03/2021	Resolução nº177 e nº181	Diversos - 3.2.3.1 e 3.2.3.1.8	Revisão e consolidação do DOC-ICP-05 - Inclui a previsão de batimento biométrico e biográfico, realizado em base oficial nacional, no processo de identificação de requerente de certificado digital ICP-Brasil.
3.0	10/10/2022	Resolução nº 204	1.6 e 4.5.1.2	Adequação para atendimento às resoluções
2.0	02/03/2021	Resolução nº177 e 181	Diversos - 3.2.3.1 e 3.2.3.1.8	Adequação para atender as resoluções
3.0	22/02/2022	Resoluções 196 e 197	Diversos	Adequação para atender as resoluções.
4.0	10/10/2022	Resolução 204	1.6 e 4.5.1.2	Adequação para atender à resolução.
4.1	05/09/2022	N/A	Diversos	Revisão de texto e correção dos links

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. Este documento estabelece os requisitos mínimos, observados obrigatoriamente pela Autoridade Certificadora VALID SSL EV (AC VALID SSL EV), integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução dos seus serviços.

1.1.2. A estrutura desta DPC esta baseada no âmbito da ICP-Brasil adota obrigatoriamente a mesma estrutura empregada no documento "REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [5]". As informações sobre a administração e geração dos tipos de certificados emitidos pela AC VALID SSL EV, são apresentados nas Políticas de Certificado (PCs) que podem ser consultadas no endereço eletrônico: https://validcertificadora.com.br/pages/repositorio-v2

1.1.3. A AC VALID SSL EV segue as atualizações dos documentos do CA/Browser Forum "Baseline Requirements for the Issuance and Management of PubliclyTrusted Certificates" [13]. e "Guidelines For The Issuance And Management Of Extended Validation Certificates" [14]. No caso de qualquer inconsistência entre esse documento e os requisitos do CA/Browser Fórum, estes terão precedência sobre o documento.

1.1.4. A estrutura desta DPC está baseada na RFC 3647.

1.1.5. A AC VALID SSL EV mantém todas as informações da sua DPC sempre atualizadas.

1.1.6. Este documento compõe 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 denominado "Declaração de Práticas de Certificação da Autoridade Certificadora AC VALID SSL EV" (DPC), comumente referido como "DPC da AC VALID SSL EV" identifica procedimentos e práticas empregados no âmbito da ICP-Brasil. O OID (*Object Identifier*) atribuído à esta DPC é o **2.16.76.1.1.144**.

1.2.2 A AC VALID SSL EV, emissora de certificados para usuários finais é exclusiva e separada de acordo com o propósito de uso de chaves de autenticação de servidor (SSL/TLS).

1.3. Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

Esta DPC refere-se exclusivamente à AC VALID SSL EV no âmbito da ICP-Brasil.

1.3.2. Autoridade de Registro

1.3.2.1. No endereço eletrônico https://validcertificadora.com.br/pages/repositorio a Autoridade de Registro (AR) vinculada à AC VALID SSL EV, esta responsável nas competências dos processos de recebimento, validação e encaminhamento das solicitações de emissão e revogação dos certificados digitais e na identificação dos seus solicitantes:

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

1.3.3 Titulares de Certificado

Pessoas físicas ou jurídicas, de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado. Os certificados podem ser utilizados por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações. Em sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

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

1.3.4 Parte 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

No endereço eletrônico (https://validcertificadora.com.br/pages/repositorio-v2) constam 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 à AC VALID SSL EV.

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

A AC VALID SSL EV implementa as seguintes Políticas de Certificado Digital:

POLÍTICA DE CERTIFICADO	NOME	OID
Política de Certificado de Assinatura Digital do tipo A1 da AC VALID SSL EV	PC A1 da AC VALID SSL EV	**2.16.76.1.2.1.110**
Política de Certificado de Assinatura Digital do tipo A3 da AC VALID SSL EV	PC A3 da AC VALID SSL EV	**2.16.76.1.2.3.100**

1.4.2 Uso proibitivo do certificado

Quando cabível, as aplicações para as quais existem restrições ou proibições para o uso desses certificados estão listados nos PCs implementadas.

Não existem restrições ou proibições para o uso dos certificados emitidos por essa AC. Os certificados SSL emitidos sob esta DPC não garantem que o equipamento no qual o certificado foi instalado não esteja isento de defeitos, malware ou vírus

1.5 Política de Administração

1.5.1 Organização administrativa do documento

AC VALID SSL EV

1.5.2 Contatos

Endereço: Alameda Rio Claro, 241 - Bela Vista - São Paulo, SP
CEP: 01332 010
Telefone: +55 11 2575-6800
Página da Web: https://validcertificadora.com.br
E-mail: pki.compliance@valid.com

Para os casos de solicitações de revogação do certificado ou relatos de problemas de certificado (decorrentes de suspeita de comprometimento de chave, uso indevido de certificado ou outros tipos de fraude, comprometimento, uso indevido ou conduta inadequada relacionada a um certificado emitido pela AC VALID SSL EV) podem ser encaminhados para os seguintes contatos:

- SAC - 3004-3454 para São Paulo ou 0800 725 4565 para demais localidades, equipe especializada das (8h as 20h);
- Suporte N2 - https://www.validcertificadora.com.br/, na aba chat ao vivo, em horário comercial das (8h as 19h) ou a qualquer horário pelo https://www.validcertificadora.com.br/faleconosco, temos uma equipe especializada para atendimento destes chamados 24 horas, 7 dias na semana;
- Suporte Comercial SSL/ SSL EV e SSL EV - O cliente poderá entrar em contato com o Consultor Responsável pela venda do certificado SSL / SSL EV ou SSL EV pelo e-mail comercial@valid.com

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Kamila Burunsizian Marciano
Área: Normas e Compliance
Telefone: +55 11 2575-6906 +55 11 2575-6978
E-mail: pki.compliance@valid.com

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.
Os procedimentos de aprovação da DPC da AC VALID SSL EV são estabelecidos a critério do CG da ICP-Brasil.

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AGR	Agente de Registro
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	*International Electrotechnical Commission*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio

PIN	Personal Identification Number
PIS	Programa de Integração Social
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
PUK	PIN Unbloking Key
RFC	*Request For Comments*
RG	Registro Geral
SSL	*Secure Socket Layer*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

2.1.1 A AC VALID SSL EV mantém disponível repositório atendendo as seguintes obrigações:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e a sua LCR/OCSP;
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. As publicações da AC VALID SSL EV podem ser consultadas através do protocolo http.
Somente a AC VALID SSL EV, 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 VALID SSL EV está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e pode ser encontrado na página Web https://validcertificadora.com.br/pages/repositorio-v2

2.1.4 A AC VALID SSL EV deve disponibilizar 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR/OCSP:

- http://icp-brasil.validcertificadora.com.br/ac-validsslev/
- http://icp-brasil2.validcertificadora.com.br/ac-validsslev/

2.2 Publicação de informações dos certificados

2.2.1 As informações descritas abaixo são publicadas e atualizadas em serviço de diretório e/ou em página web da AC VALID SSL EV (https://validcertificadora.com.br/pages/repositorio-v2) A AC VALID SSL EV está em

conformidade com a versão atual do documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" [13]. No caso de qualquer inconsistência entre este documento e esses requisitos, esses têm precedência sobre este documento.

A disponibilidade das informações publicadas pela AC VALID SSL EV em serviço de diretório e/ou página web é de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Antes de emitir certificados SSL, a AC VALID BRASIL SSL EV verifica se há registros CAA para cada extensão dNSName no subjectAltName no certificado a ser emitido, conforme especificado na RFC 6844

2.2.2. As seguintes informações são publicadas em serviço de diretório e/ou em página *web* da AC VALID SSL EV (https://validcertificadora.com.br/pages/repositorio-v2):

a) seus próprio certificado;
b) suas LCRs/OCSP;
c) sua DPC;
d) as PCs que implementa;
e) uma relação, regularmente atualizada, contendo a AR vinculada e seu respectivo endereço; e
f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.
g) links para paginas web separadas com certificados válido, revogado e expirado por ela emitidos para que fornecedores de software ou aplicações realizem testes.
h) paginas da Web de teste que permitem que os fornecedores de software aplicativos testem seus softwares com Certificados de Assinante. Essas páginas de teste Web são acessíveis nos seguintes URLs:

- Certificados Válidos: https://approved.vpki.com.br/
- Certificados Revogados: https://revoked.vpki.com.br/
- Certificados Expirados: https://expired.vpki.com.br/

2.3 Tempo ou Frequência de Publicação

2.3.1. De modo a assegurar a disponibilização sempre atualizada de seus conteúdos:

a) os certificados são publicados imediatamente após sua emissão;
b) a publicação da LCR se dá conforme o item 4.4.9 da PC correspondente;
c) as versões ou alterações desta DPC e da PC são atualizadas na web site da AC VALID SSL EV após aprovação da AC Raiz da ICP-Brasil; e
d) os endereços das AR vinculadas são atualizadas na *web* site da AC VALID SSL EV.

As demais informações mencionadas no item 2.2.2 serão publicadas sempre que sofrerem alterações.

A AC VALID SSL EV revisa sua DPC pelo menos uma vez ao ano e faz as alterações necessárias para que a operação permaneça precisa, transparente e cumprindo com os requisitos. A AC VALID SSL EV monitora de perto as votações que acontecem no Fórum do CA/Browser (https://cabforum.org/ballots/) e as atualizações dos Requisitos e implementações da linha de base, mantendo as operações da AC atualizadas com

relação a esses Requisitos em tempo hábil.

2.4. Controle de Acesso aos Repositórios

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à LCR da AC VALID SSL EV, às PC implementadas e aos endereços das AR vinculadas.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC VALID SSL EV verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros.
A AC reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1 Atribuição de Nomes

3.1.1 Tipos de nomes

3.1.1.1 O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "*Distinguished Name*" do padrão ITU X.500, endereços de correio eletrônico, endereço de página *Web* (URL), ou outras informações que permitam a identificação unívoca do titular.

3.1.1.2 Um certificado emitido para uma AC subsequente não deverá incluir o nome da pessoa responsável.

3.1.2 Necessidade dos Nomes Serem Significativos

3.1.2.1 Os certificados emitidos pela AC VALID SSL EV exigem o uso de nomes significativos que possibilitam de terminar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem, para a identificação dos titulares dos certificados emitidos.

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.4.1. Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados na PC implementada.

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

Esta DPC estabelece que identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado emitido pela AC VALID SSL EV. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo DN.

3.1.6 Procedimento para resolver disputa de nomes

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

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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

3.2 Validação inicial de identidade

Neste item e nos seguintes, a DPC descreve em detalhes os requisitos e procedimentos utilizados pela AR vinculada à AC VALID SSL EV para a realização dos seguintes processos:

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 e 3.2.7:

   i. para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim.

   ii. para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado, 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 VALID SSL EV. 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 VALID SSL EV, por meio dos seus agentes de registro, acompanhará, no ambiente da AC candidata a subsequente, a geração do par de chaves e da solicitação do certificado (Certificate Request PKCS#07) contendo a chave pública correspondente à chave privada gerada. A solicitação é gravada em mídia, que é verificada e guardada em envelope lacrado.

A AR verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, segundo o padrão definido RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

3.2.2 Autenticação da identificação da organização

3.2.2.1Disposições Gerais

3.2.2.1.1 Neste item devem ser definidos os procedimentos empregados pela AR vinculada para a confirmação da identidade de uma pessoa jurídica.

3.2.2.1.2 Sendo o titular do certificado pessoa jurídica, é 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 É feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos::

a) apresentação do rol de documentos elencados no item 3.2.2.2;

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 certificado.

Nota 1: A AR poderá solicitar uma assinatura manuscrita ao responsável pelo certificado em termo específico para a 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 Fica dispensado o disposto no item 3.2.2.1.3, alíneas “b” e “c” caso o responsável

pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

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; ou

b) por videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

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 criada ou autorizada a sua criação 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 representantes legais, quando aplicável;

b) Relativos à sua habilitação fiscal:
   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

Nota 1: Essas confirmações 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 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 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
c) Nome completo do responsável pelo certificado, sem abreviações; e
d) Data de nascimento do responsável pelo certificado.

3.2.2.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de

titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.2.3.2.

3.2.2.4 Responsabilidade decorrente do uso do certificado de uma organização

Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei quanto aos poderes de representação conferidos ao responsável de uso indicado no certificado.

3.2.3 Autenticação da identidade de um indivíduo

A confirmação é realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas abaixo, que asseguraram nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

a) Não se aplica;

b) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; ou

c) Não se aplica.

3.2.3.1 Documentos para efeitos de identificação de um indivíduo

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) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

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.

3.2.3.1.1 Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a apresentação de qualquer dos documentos elencados no item 3.2.3.1 e a etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

3.2.3.1.2 Os documentos digitais deverão ser verificados por meio de barramentos ou

aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado. Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 3.2.3.1.3.

3.2.3.1.3 Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados:

a) por agente de registro distinto do que realizou a etapa de identificação;

b) pela AR ou AR própria da AC ou ainda AR própria do PSS da AC; e

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

3.2.3.1.4 A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente, e as normas editadas pelo Comitê Gestor da ICP-Brasil.

3.2.3.1.5 Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Não se aplica.

3.2.3.1.8. A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

3.2.3.1.8.1 Não se aplica.

3.2.3.2 Informações contidas no certificado emitido para um indivíduo

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

a) nome completo, sem abreviações;
b) data de nascimento;
c) Cadastro de Pessoa Física (CPF).

3.2.3.2.1.1. Não se aplica.

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

a) número de Identificação Social - NIS (PIS, PASEP ou CI);
b) número do Registro Geral - RG do titular e órgão expedidor;
c) número do Cadastro Específico do INSS (CEI);
d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor; e

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

3.2.3.2.3 Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original.

3.2.3.2.3.1 Não se aplica.

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

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

3.2.4 Informações não verificadas do titular do certificado

Não se aplica.

3.2.5 Validação das autoridades

Não se aplica.

3.2.6 Critérios para interoperação

Não se aplica.

3.2.7 Autenticação da identidade de equipamento ou aplicação

3.2.7.1. Disposição Gerais

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

3.2.7.1.2. Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade na forma do item 3.2.3 e esta assinará o termo de titularidade de que trata o item 4.1.

3.2.7.1.3. Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, na forma do item 3.2.2.

3.2.7.1.4. Fica dispensada a observância do disposto no item 3.2.3.1 para certificados cujo titular seja pessoa física, caso a solicitação seja assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e cujos dados biométricos já tenham sido devidamente coletados.

3.2.7.1.5. Fica dispensada a observância do item 3.2.2.1.3 alíneas “b” e “c” para certificados cujo titular seja pessoa jurídica nos seguintes casos:

a) quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e responsável, e cujos dados biométricos deste último tenham sido devidamente coletados; ou
b) quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo

A3 ou superior, cuja titularidade é da mesma pessoa física responsável legal da organização e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.2.7.2.1. Para certificados de equipamento ou aplicação que utilizem URL na identificação do titular, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço. Nesse caso deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

Para certificados do tipo Multidomínio, IP ou URL, é necessário prova de controle da aplicação sobre a URL pretendida pela inclusão de um arquivo ou um valor randômico na aplicação.

A prova de controle será feita pelo método – Alteração Acordada no Site – que segue o item 3.2.2.4.6 (Agreed-Upon Change to Website) para certificados do tipo URL, Curinga e Multidomínio, e segue o item 3.2.2.5.1 para certificados do tipo IP do documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" [13].

3.2.7.2.2. Não se aplica.

3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação

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

a) URL ou nome da aplicação;

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

c) data de nascimento do responsável pelo certificado;

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

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

3.2.7.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade e responsabilidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.2.3.2.

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

Não se aplica.

3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica

3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT

Não se aplica.

3.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR

Não se aplica.

3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico

Não se aplica.

3.2.8 Procedimentos complementares

3.2.8.1 A AC VALID SSL EV 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, bem como os documentos do CA/Browser Forum aplicáveis.

3.2.8.2 Todo o processo de identificação do titular do certificado são registrados com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. O sistema biométrico da ICP-BRASIL solicita aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.8.2.1 Não se aplica.

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

3.2.8.3.1. Não se aplica.

3.2.8.3.2. Não se aplica.

3.2.8.3.3. Não se aplica.

3.2.8.4 A AC VALID SSL EV devem disponibilizar, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

3.2.8.4.1. Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, fica dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 3.2.3.1.

3.2.8.4.2 Não se aplica.

3.2.9 Procedimentos específicos

Não se aplica.

3.3 Identificação e autenticação para pedidos de novas chaves

3.3.1 No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC VALID SSL EV para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

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

a) doção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;

b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;

c) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;

d) solicitação por meio eletrônico dada nas alíneas ‘b’ e ‘c’, acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação da AC-Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;

e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou

f) por meio de mecanismo automatizado de gerenciamento de certificado do tipo SSL/TLS (ACME), conforme disposto no item 3.3.2.1.

3.3.2.1 Para certificados de equipamento ou aplicação que utilizem URL, a AC poderá implementar mecanismos automatizado de gerenciamento de certificado (ACME) de forma a preservar a posse ou propriedade da URL (domínio) e a identificação do solicitante, seja pessoa física ou jurídica. O processo automatizado implica as seguintes etapas:

a) o solicitante submete uma requisição de certificado (PKCS#10) da URL desejada;

b) a requisição deverá ser acompanhada do certificado da URL solicitada, ainda válido, e o conjunto (requisição + certificado da URL) deve ser assinado com certificado ICP-Brasil, no mínimo do tipo A3, de pessoa física ou jurídica do responsável pelo domínio. Se o responsável pelo domínio for pessoa física, o signatário deve ser o mesmo contido no campo otherName (OID 2.16.76.1.3.2) que identifica o responsável pelo certificado da URL. Se o responsável pelo domínio for pessoa jurídica, o signatário deve ser um certificado de pessoa jurídica cujo CNPJ seja o mesmo contido no campo otherName (OID 2.16.76.1.3.3) que identifica o titular do certificado da URL;

c) o aplicativo de AR valida a assinatura e a requisição e, caso esteja em conformidade, encaminha desafio de prova de domínio e o termo de titularidade;

d) o solicitante responde o desafio e assina o termo de titularidade com o mesmo certificado utilizado no item “b”, acima;

e) confirmado atendimento pleno do desafio e da assinatura do termo de titularidade, o aplicativo de AR poderá emitir o certificado e encaminhá-lo ao solicitante; e

f) todas as evidências do processo acima devem constar no dossiê do certificado.

3.3.3. Não existem procedimentos específicos nas PC implementadas.

3.3.4 Não se aplica.

3.4. Identificação e autenticação para novas chaves após a revogação

A solicitação de revogação de certificado é realizada através de declaração assinada pelo(s) representante(s) legal(is) com firma(s) reconhecida(s).
A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC VALID SSL EV 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

Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC VALID SSL EV e pela AR a ela vinculada para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital e contemplam:

a. A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
b. O uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados;
c. Um termo de titularidade assinado pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4], contemplando os itens previstos no Acordo de Assinante.
d. O atendimento via videoconferência será realizado atendendo os critérios mencionados abaixo:
    - Clientes que possui suas biometrias coletada em uma validação presencial; - Certificados vencidos;
    - Clientes que possui um e-mail que tenha acesso;
    - Clientes que possui uma web-cam e internet.

    A AC VALID SSL EV adequou o sistema atual para atendimento a essa modalidade, seguindo requisitos descrito no DOC-ICP-05.05, sendo assim, os clientes deverão atender os requisitos descrito acima para ter o acesso emissão do certificado via videoconferência; e
e. Não se aplica.

Nota 1: O termo de titularidade para certificados de usuários finais com propósito de uso EV SSL segue o padrão adotado no documento EV SSL.

Nota 2: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento, aplicação, codesign e outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

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. Não se aplica.

4.1.1.2. Não se aplica.

4.1.1.3. Não se palica.

4.1.1.4. Não se aplica.

4.1.2 Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1. Responsabilidades da AC.

4.1.2.1.1 A AC VALID SSL EV responde pelos danos a que der causa.

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

4.1.2.1.3 Não se aplica.

4.1.2.2. Obrigações da AC

As obrigações da AC VALID SSL EV são as abaixo relacionadas:

a) operar de acordo com a sua DPC e com as PCs que implementa;

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

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados os certificados de AR a ela vinculadas e de usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas 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 e as PCs aprovadas que implementa;

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 DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

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

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

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

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção, 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 sua AR, 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 à AC VALID SSL EV utilizam de seus serviços; e

y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente deregistro 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 Obrigações das ARs

As obrigações da AR vinculada à AC VALID SSL EV são abaixo relacionadas:

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC VALID SSL EV utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC VALID SSL EV e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como Princípios e Critérios

WebTrust para AR [5];

f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2 e 3.2.3; e
h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR [5].

4.2. Processamento de Solicitação de Certificado

A AC VALID SSL EV divulga em sua Política de Certificado (PC) e/ou Declaração de Práticas de Certificação (DPC) sob a seção 4.2 sua política ou prática sobre processamento de Registros DNS CAA (Autorização de Autoridade de Certificação) para Nomes de Domínio Totalmente Qualificados que é consistente com os Requisitos de Linha de Base SSL, e especifica o conjunto de Nomes de Domínio do Emissor que a AC reconhece nos registros "issue" ou "issuewild" da CAA como permitindo que ela emita.
A AC VALID SSL EV mantém controles para fornecer garantia razoável de que registra todas as ações tomadas, se houver, são consistentes com sua prática de processamento.

4.2.1. Execução das funções de identificação e autenticação

A AC VALID SSL EV e AR 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 Não se aplica.

4.2.2.2 A AC VALID SSL EV e AR 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

A AC VALID SSL EV cumpre os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1 Ações da AC durante a emissão de um certificado

4.3.1.1 A emissão de certificado depende do correto preenchimento de formulário de solicitação, da assinatura do "Termo de Titularidade", no caso de certificados de pessoas jurídicas, ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e Titular é notificado da emissão e do método para a retirada do certificado.

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

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

O Titular é notificado da emissão e do método para a retirada do certificado.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

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

a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;

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

c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.2. A aceitação de todo certificado emitido é declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

4.4.1.3. Não se aplica.

4.4.2 Publicação do certificado pela AC

O certificado da AC VALID SSL EV é publicado 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

O titular do certificado para usuário final emitido pela AC VALID SSL EV deve operar de acordo com esta Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) aplicáveis, estabelecidas 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 VALID SSL EV deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC VALID SSL EV constantes dos termos de titularidade de que trata o item 4.1 são os abaixo relacionados:

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, código de ativação (PIN) 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 VALID SSL EV qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

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
Não se aplica.

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
Não se aplica

4.7.2 Quem pode requisitar a certificação de uma nova chave pública
Não se aplica

4.7.3 Processamento de requisição de novas chaves de certificado
Não se aplica

4.7.4 Notificação de emissão de novo certificado para o titular
Não se aplica

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada
Não se aplica

4.7.6 Publicação de uma nova chave certificada pela AC
Não se aplica

4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades
Não se aplica

4.8 Modificação de certificado
Não se aplica

4.8.1 Circunstâncias para modificação de certificado
Não se aplica

4.8.2 Quem pode requisitar a modificação de certificado
Não se aplica

4.8.3 Processamento de requisição de modificação de certificado
Não se aplica

4.8.4 Notificação de emissão de novo certificado para o titular
Não se aplica.

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado
Não se aplica.

4.8.6 Publicação de uma modificação de certificado pela AC
Não se aplica.

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

Não se aplica.

4.9 Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.1.1. O titular e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independentemente de qualquer circunstância.

4.9.1.2. O certificado deve ser obrigatoriamente revogado:

a) Quando constatada emissão imprópria ou defeituosa dele;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) Não se aplica;
d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora;

4.9.1.3. A AC VALID SSL EV define ainda que:

a) A AC VALID SSL EV deve revogar, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e

b) O CG da ICP-Brasil ou AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas 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. AC VALID SSL EV que emite certificados SSL suporta requisições OCSP em conformidade com a RFC 6960 e/ou RFC5019 e requisitos do CAB Fórum. Para certificados SSL, a resposta OCSP tem validade mínima de um dia e máxima de uma semana, sendo que a próxima atualização estará disponível a cada quatro dias.

4.9.1.4.2. A AC VALID SSL EV provê garantias que uma LCR possa ser baixada em não mais do que três segundos por uma linha de telefone analógica, sobre uma condição normal de rede.

4.9.1.5. A autenticidade da LCR/OCSP é também confirmada por meio das verificações da assinatura da AC VALID SSL EV 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 do titular do certificado;

b) Por solicitação do responsável pelo certificado, no caso de certificado de pessoas jurídicas;

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

d) Pela AC VALID SSL EV;

e) Por uma AR vinculada; ou

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

g) Não se aplica;

h) Não se aplica;

i) Não se aplica;

j) Não se aplica.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. Uma solicitação de revogação é necessária para que AR responsável inicie o processo de revogação. O solicitante da revogação habilitado pode solicitar facilmente e a qualquer tempo a revogação de certificado, evitando assim a utilização indevida do certificado.

Instruções para a solicitação de revogação do certificado são obtidas em página web disponibilizada pela AC VALID SSL EV ou pela AR Responsável.

4.9.3.2. Como diretrizes gerais:

a) O Solicitante da revogação de um certificado é identificado;

b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC VALID SSL EV;

c) As justificativas para a revogação de um certificado são registradas;

d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado e com a atualização do status do certificado na resposta OCSP à base de dados da AC VALID SSL EV, quando aplicável.

4.9.3.3. O prazo máximo admitido para a conclusão do processo de revogação de certificado, após orecebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 24 (vinte e quatro) horas.

4.9.3.4. Não se aplica.

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

4.9.3.6. Não se aplica.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC.

O prazo para aceitação do certificado pelo seu titular é de 7 (sete) dias, dentro do qual a

revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

4.9.4.2. Não existem procedimentos específicos nas PC implementadas.

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 VALID SSL EV 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 frequência de emissão de LCR referente a certificados de usuários finais pela AC VALID CODESIGNG é de 1 hora.

4.9.7.2 A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 (seis) horas.

4.9.7.3 Não se aplica.

4.9.7.4 Não existem procedimentos específicos nas PC implementadas.

4.9.7.5 Para certificados emitidos pela AC VALID SSL EV as frequências de emissão de LCR são implementadas e descritas em suas PCs, no item correspondente, em conformidade com os requisitos do CAB Fórum.

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 VALID SSL EV suporta os processos de revogação de certificados de forma on-line quando aplicável por força de contratação específica.

A AC VALID SSL EV suporta verificação da situação de estado de certificados de forma on-line quando aplicável por força de contratação específica.

A verificação da situação de um certificado deverá ser feita diretamente na AC VALID SSL EV, por meio do protocolo OCSP (On-line Certificate Status Protocol).

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação on-line de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.9.12.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR Responsável, assinando formulário de solicitação de revogação, observado o item 4.4.3 desta DPC. Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

4.9.13. Circunstâncias para suspensão

Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de usuários finais.

4.9.14. Quem pode solicitar suspensão

A AC VALID SSL EV pode solicitar suspensão quando aprovado pelo Comitê Gestor.

4.9.15. Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão serão definidos em documento interno da AC VALID SSL EV.

4.9.16. Limites no período de suspensão

Os períodos de suspensão serão estabelecidos em documento interno da AC VALID SSL EV.

4.10. Serviços de status de certificado

4.10.1. Características operacionais

A AC VALID SSL EV deve fornecer um serviço de status de certificado na forma de um ponto de distribuição da LCR no 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 Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], este item da DPC descreve os requisitos e os procedimentos que serão

adotados nos casos de extinção ou encerramento dos serviços da AC VALID SSL EV, de uma AR, PSS ou PSBios a ela vinculados.

4.11.2 No caso de encerramento das atividades como AC da ICP-Brasil, a AC VALID SSL EV 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 VALID SSL EV:

a) Comunicará publicamente a extinção dos serviços da AC VALID SSL EV, através de publicação em jornal de grande circulação.

b) Revogará todos os certificados gerados pela AC VALID SSL EV nos prazos estipulados nas PC implementadas 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 VALID SSL EV extinta seguindo o procedimento descrito na DPC Item 6.2.9.

f) Transferirá os dados e gravações da AC VALID SSL EV para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.

g) Transferirá as chaves públicas dos certificados emitidos pela AC VALID SSL EV 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 VALID SSL EV. 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 VALID SSL EV.

i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas

No caso de falência, extinção da AR ou encerramento das atividades como AR vinculada a AC VALID SSL EV a AR deverá seguir os seguintes requisitos e procedimentos:

a) Comunicará publicamente a extinção dos serviços de AR vinculada AC VALID SSL EV, através de publicação em jornal de grande circulação e

b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados.

No caso de encerramento das atividades como PSS vinculada a AC VALID SSL EV, a AC VALID SSL EV, 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; e

b) Manterá a guarda de toda a documentação comprobatória em seu poder.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

A AC VALID SSL EV não executa práticas de custódia e recuperação de chaves.

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

A AC VALID SSL EV não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes estão descritos os controles de segurança implementados pela AC VALID SSL EV e pela AR vinculadas para executar, de modo seguro, suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros. Os requisitos estipulados no CA/Browser Forum Network, estão também incorporados nas descrições a seguir.

5.1 Controles Físicos

5.1.1. Construção e Localização das Instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC VALID SSL EV não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não existem ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. As instalações para equipamentos de apoio, tais como máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro.
As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada.
Existem sistemas de aterramento e de proteção contra descargas atmosféricas.
Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2 Acesso físico

A AC VALID SSL EV possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a POLÍTICA DE SEGURANÇA DA ICPBRASIL [8] 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 VALID SSL EV, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

5.1.2.1.2. O primeiro nível – ou nível 1 – Situa-se após a primeira barreira de acesso às instalações da AC VALID SSL EV. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC VALID SSL EV transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC VALID SSL EV é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido no ambiente onde estão instalados os equipamentos utilizados na operação da AC VALID SSL EV , em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC VALID SSL EV.

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

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

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

5.1.2.1.8. O quarto nível - ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC VALID SSL EV, 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. Na AC VALID SSL EV, existem ambientes de quarto nível para abrigar e segregar:

a) Equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores - (Data Center);

b) Equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia).

c) Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

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

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre obedece às seguintes especificações:

a) Confeccionado em aço; e
b) Possui tranca com chave.

5.1.2.1.14. O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC VALID SSL EV estão armazenados nesses depósitos

5.1.2.2. Sistema físico de detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por 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 fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são

monitoradas por sistema de notificação de alarmes. 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 VALID SSL EV 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 VALID SSL EV está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC VALID SSL EV e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC VALID SSL EV

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

5.1.3.3 Existem tubulações, dutos, calhas, quadros e caixas – de passagem, distribuição e 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, telefonia e 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 às 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 "*nobreaks*" 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. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

5.1.6. Armazenamento de mídia

A AC VALID SSL EV 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 documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

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

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

5.1.8.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC VALID SSL EV 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.

5.1.8.2. 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.

5.2. CONTROLES PROCEDIMENTAIS

5.2.1. Perfis qualificados

5.2.1.1. A AC VALID SSL EV pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida dos certificados digitais, de forma a garantir a segurança da atividade de certificação e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo..

5.2.1.2. A AC VALID SSL EV estabelece 4 perfis distintos para sua operação, atribuídos às seguintes áreas:

- **Gerência de Operações Data Center:**
  - **Supervisão Operacional:**

    - configuração e manutenção do hardware e do software da AC;

    - gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC;

    - controle de acesso lógico dos funcionários à rede AC;

- gerenciamento dos operadores da AC;

- controle de acesso ao sistema de certificação.

➢ **Supervisão de PKI:**

- administração e controle dos componentes criptográficos da AC;

- verificação dos registros de acesso aos diferentes níveis de proteção das chaves privadas das AC (logs);

- elaboração das cerimônias de geração de chaves de AC;

- armazenamento dos registros de auditoria do sistema de certificação;

- utilização de criptografia para segurança de acesso ao aplicativo de certificação;

- autorização e concessão de acesso às instalações físicas e autorização de acessos lógicos ao sistema de certificação;

- **Gerência de Segurança:**

  - implementação da Política de Segurança da AC;

  - verificação dos registros de auditoria;

  - supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC;

  - acompanhamento das auditorias de segurança realizadas por terceiros;

  - verificação do cumprimento desta DPC;

  - Autorização e concessão de acesso às instalações físicas e autorização de acessos lógicos ao sistema de certificação;

  - Utilização de criptografia para a segurança da base de dados de registro de auditoria do sistema de certificação.

- **Gerência Operação:**

  - Gerenciamento e controle dos processos de validação, verificação, emissão e revogação de certificados.

5.2.1.3. Os operadores do sistema de certificação da AC VALID SSL EV recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal (Política de Segurança da AC VALID SSL EV), com base nas necessidades de cada perfil.

5.2.1.3.1. A AC VALID SSL EV realiza um exame, para emissão de certificados em cadeia do tipo SSL EV, nos operadores do sistema de certificação da AC VALID SSL EV, de acordo com os princípios e critérios WebTrust aplicáveis.

5.2.1.4. A AC VALID SSL EV possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à AC VALID SSL EV no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

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

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

5.2.3. Identificação e autenticação para cada perfil

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

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

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

a) são diretamente atribuídos a um único operador (funcionário da AC VALID SSL EV devidamente qualificado);
b) não são compartilhados;
c) são restritos às ações associadas ao perfil para o qual foram criados.

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

5.2.4. Funções que requerem separação de deveres

A AC VALID SSL EV deve impor a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. CONTROLES DE PESSOAL

Todos os empregados da AC VALID SSL EV, das AR e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

a) Os termos e as condições do perfil que ocupam;
b) O compromisso de observar as normas, políticas e regras aplicáveis da AC VALID SSL

EV;

c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC VALID SSL EV envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC VALID SSL EV e na Política de Segurança da ICP-Brasil [8].

5.3.2. Procedimentos de Verificação de Antecedentes

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

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

5.3.2.2 Não se aplica.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC VALID SSL EV e da AR vinculada, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC VALID SSL EV e da AR vinculada;
b) sistema de certificação em uso na AC VALID SSL EV;
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 VALID SSL EV e da AR vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC VALID SSL EV e no sistema das AR.

5.3.5. Frequência e sequência de rodízios de cargos

Não estabelecido.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por

pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC VALID SSL EV suspenderá o seu acesso ao sistema de certificação e tomará as medidas administrativas e legais cabíveis.

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

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

5.3.6.3. Concluído o processo administrativo, a AC VALID SSL EV encaminhará suas conclusões à AC Raiz.

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

a) advertência;
b) suspensão por prazo determinado; ou
c) impedimento definitivo de exercer funções no âmbito da AC VALID SSL EV e da ICP- Brasil.

5.3.7. Requisitos para contratação de pessoal

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

5.3.8. Documentação disponibilizada ao pessoal

5.3.8.1. A AC VALID SSL EV disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

a) esta DPC da AC VALID SSL EV;
b) as PC correspondentes;
c) a Política de Segurança da ICP-Brasil;
d) documentação operacional relativa às suas atividades; e
e) contratos, normas e políticas relevantes para suas atividades.

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

5.4. Procedimentos de Log de Auditoria

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC VALID SSL EV com o objetivo de manter um ambiente seguro.

5.4.1. Tipos de Eventos Registrados

5.4.1.1. A AC VALID SSL EV registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) Iniciação e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC VALID SSL EV;
c) Mudanças na configuração dos sistemas AC VALID SSL EV 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 do sistema;
g) Geração de chaves próprias da AC VALID SSL EV ou de chaves de seus usuários finais;
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. A AC VALID SSL EV, emissora de certificados SSL, deve ter capacidade de auditar esses tipos certificados em até seis por cento dos emitidos..

5.4.1.2. A AC AC VALID SSL EV também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

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

5.4.1.3. As informações registradas pela AC VALID SSL EV são todas as descritas nos itens acima.

5.4.1.4. Os registros de auditoria, eletrônicos ou manuais, contêm a data e a hora do evento registrado e a identidade do agente que o causou.

5.4.1.5. A documentação relacionada aos serviços da AC VALID SSL EV é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6. A AC VALID SSL EV 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 obrigatoriamente incluídos em arquivos de auditoria:

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

5.4.1.6.1 Não se aplica.

5.4.1.7. A AC VALID SSL EV a que esteja vinculada a AR define, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2. Frequência de Auditoria de Registros

A periodicidade com que os registros de auditoria da AC VALID SSL EV são analisados pelo pessoal operacional é de uma semana. Todos os eventos significativos são 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 de Auditoria

A AC VALID SSL EV mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os 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 VALID SSL EV, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.5. Procedimentos para Cópia de Segurança (Backup) de Registros de Auditoria

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC VALID SSL EV têm cópias de segurança semanais, feitas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas ao

departamento de segurança.

5.4.6. Sistema de Coleta de Dados de Auditoria (Interno ou Externo)

O sistema de coleta de dados de auditoria interno à AC VALID SSL EV é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7. Notificação de Agentes Causadores de Eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC VALID SSL EV, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8. Avaliações de Vulnerabilidade

Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC VALID SSL EV, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC VALID SSL EV e registradas para fins de auditoria.

5.5. Arquivamento de Registros

Nos itens seguintes da DPC está descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC VALID SSL EV e pela AR a ela vinculada.

5.5.1. Tipos de Registros Arquivados

Os tipos de registros arquivados são:

a) Solicitações de certificados;
b) Solicitações de revogação de certificados;
c) Notificações de comprometimento de chaves privadas;
d) Emissões e revogações de certificados;
e) Emissões de LCR;
f) Trocas de chaves criptográficas da AC VALID SSL EV; e
g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de Retenção para Arquivo

Os períodos de retenção por tipo de registro arquivado são:

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;
b) Os dossiês dos titulares devem ser retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e
c) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de Arquivo

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

5.5.4. Procedimentos de cópia de arquivo

5.5.4.1. A AC VALID SSL EV estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC VALID SSL EV, 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 VALID SSL EV verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para Datação de Registros

Informações de data e hora nos registros baseiam-se no horário *Greenwich Mean Time* (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero.

Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

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 VALID SSL EV em seus procedimentos operacionais são automatizados e 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 VALID SSL EV, 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. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico. A AC VALID SSL EV fornece novo certificado a usuario final utilizando o mesmo procedimento utilizado para emissão do certificado inicial.

A AC VALID SSL EV comunica o titular do certificado, 13 (treze) meses antes da expiração do certificado, junto com instruções para a solicitação de um novo certificado.

A comunicação de expiração e solicitação de renovação é realizada através de e-mail.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

Nos itens seguintes da DPC estão descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC VALID SSL EV, estabelecido conforme a 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 VALID SSL EV possui 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 um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

5.7.1.2. Os procedimentos previstos no PCN da AR vinculada para recuperação, total ou parcial das atividades da AR, contém 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;
f) Teste e atualização dos planos;

5.7.2. Recursos Computacionais, Software, e/ou Dados Corrompidos

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da AC VALID SSL EV, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que ele pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

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 VALID SSL EV o Gerente de Segurança, juntamente com a Supervisão de PKI da AC VALID SSL EV, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC VALID SSL EV 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 VALID SSL EV, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com a Supervisão de PKI da AC VALID SSL EV, 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 VALID SSL EV estiver encerrando suas atividades

5.7.4. Capacidade de Continuidade de Negócio Após Desastre

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infraestrutura, responsável pela contingência, notifica o Gerente de Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

a) Garantir a integridade física das pessoas que se encontram nas instalações da AC VALID SSL EV;
b) Monitorar e controlar o foco da contingência;
c) Minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

5.8. Extinção da AC

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPC define as medidas de segurança implantadas pela AC VALID SSL EV 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 VALID SSL EV e pela AR vinculada 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 criptográficas da AC VALID SSL EV é gerado pela própria AC VALID SSL EV, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

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

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

O par de chaves da AC VALID SSL EV é gerado em módulo criptográfico de hardware no padrão FIPS 140-2 nível 3 e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V11), conforme definido no DOC-ICP01.01.

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

6.1.1.4. O processo de geração do par de chaves da AC VALID SSL EV é feito por hardware.

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

6.1.1.6. Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC VALID SSL EV são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável. A DPC da AC VALID SSL EV informa que a geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado

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

6.1.3.2. Não se aplica.

6.1.4. Entrega de Chave Pública da AC às Terceiras Partes

A AC VALID SSL EV disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web: https://validcertificadora.com.br/pages/repositorio-v2

6.1.5. Tamanhos de chave

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

6.1.5.2. Não se aplica.

6.1.6. Geração de Parâmetros de Chaves Assimétricas e Verificação da Qualidade dos Parâmetros

6.1.6.1. Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [9].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.7.1 Os certificados de assinatura emitidos pela AC VALID SSL EV têm ativados os bits digitalSignature, keyEncipherment ou keyAgreement. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC VALID SSL EV, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

6.1.7.2 A chave privada AC VALID SSL EV é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2. Proteção da Chave Privada e Controle de Engenharia do Módulo Criptográfico

A AC VALID SSL EV implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas.

A chave privada da AC VALID SSL EV é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

Os titulares de certificados emitidos pela AC VALID SSL EV, 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 e Controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC VALID SSL EV adota o padrão FIPS 140-2 nível 3 (Com Luna 7, Homologado ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V10), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [9].

6.2.1.2. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação INMETRO. Cada PC implementada descreve os padrões do módulo criptográfico a ser utilizado pela entidade titular de certificado.

6.2.2. Controle "n de m' para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de *hardware* que armazena a chave privada da AC VALID SSL EV é dividida em 8 (oito) partes e distribuídas por 8 (oito) custodiantes designados pela AC VALID SSL EV (m).

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

6.2.3. Recuperação (*escrow*) de chave privada

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

6.2.4. Cópia de segurança de chave privada

6.2.4.1. O titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2.A AC VALID SSL EV mantém cópia de segurança de sua chave privada.

6.2.4.3. Não se aplica.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo 3DES – 112 bits ou AES – 128 ou 256 bits, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1.A AC VALID SSL EV 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 VALID SSL EV gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico 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

A ativação das chaves privadas das AC VALID SSL EV é coordenada pela Supervisão de PKI, onde 3 de um grupo de 10 funcionários com perfis qualificados da AC VALID SSL EV, detentores de partição da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica.

Esses funcionários são identificados pelo crachá funcional emitido pela AC VALID SSL EV contendo fotografia, nome, e departamento do funcionário.

6.2.9. Método de desativação de chave privada

A chave privativa da AC VALID SSL EV, instalada em ambiente de produção dos sistemas de certificação, localiza-se em nível de segurança 4, onde só é permitido o acesso ao ambiente em duplas devidamente autorizadas pelo sistema de controle de acesso da AC VALID SSL EV.

Dentro deste ambiente, somente funcionários qualificados do departamento de operações têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação do sistema, após a sua devida identificação e autorização feita através de mecanismos nativos do sistema operacional.

Esses funcionários são identificados pelo crachá funcional emitido pela AC VALID SSL EV contendo fotografia, nome, e departamento do funcionário.Método de destruição de chave privada

6.2.10. Método de Destruição de Chave Privada

A Supervisão de PKI da AC VALID SSL EV, de posse da chave privada original e suas cópias de segurança a serem destruídas, acompanhado do Gerente de Segurança e do representante legal da AC VALID SSL EV, titular do certificado, conduz cerimônia especifica, em ambiente de nível 4 de segurança, para reinicialização das mídias de armazenamento das chaves privadas, não deixando informações remanescente sensíveis nessas mídias.

O Gerente de Segurança e Supervisão de PKI são identificados pelo crachá funcional emitido pela AC VALID SSL EV contendo fotografia, nome, e departamento do funcionário. O representante legal da AC VALID SSL EV é identificado através de cédula de identidade ou passaporte, se estrangeiro.

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. Arquivamento de chave pública

As chaves públicas da própria AC VALID SSL EV e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas e sistemas de OCSP permanecem armazenadas 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. A chave privada da AC VALID SSL EV bem como as chaves privadas dos titulares dos certificados por ela emitidos deverão ser utilizadas apenas durante o período de validade do certificado correspondente. As correspondentes chaves públicas poderão ser utilizadas durante todo o período determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Cada PC implementada pela AC VALID SSL EV define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL [7].

6.3.2.4 A validade admitida para certificados da AC VALID SSL EV é limitada à validade do certificado da AC que o emitiu, desde que mantido o padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4. Dados de ativação

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC VALID SSL EV são únicos e aleatórios.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação.

6.4.2.1.A AC VALID SSL EV garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Não se aplica.

6.4.3. Outros aspectos dos dados de ativação

Não aplicável.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A geração do par de chaves da AC VALID SSL EV é realizada em ambiente próprio para a condução de Cerimônia de Geração de Chaves. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos de segurança computacional dos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC VALID SSL EV são descritos em cada PC implementada.

6.5.1.3.O ambiente computacional da AC VALID SSL EV relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes funções::

a) controle de acesso aos serviços e perfis da AC VALID SSL EV;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC VALID SSL EV;
c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
d) geração e armazenamento de registros de auditoria da AC VALID SSL EV;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) mecanismos para cópias de segurança (*backup*).

6.5.1.4. Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção, tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC VALID SSL EV, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC VALID SSL EV. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Equipamento incorporado à AC VALID SSL EV 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 VALID SSL EV segue as recomendações Common Criteria.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. A AC VALID SSL EV implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela AR Vinculada 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. de acesso (login) e de saída do sistema (logoff);

v. tentativas 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
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 Não se aplica.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC VALID SSL EV utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC VALID SSL EV utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos..

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

6.6.2. Controle de gerenciamento de segurança

6.6.2.1. A AC VALID SSL EV verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência..

6.6.2.2. Uma metodologia formal de gerenciamento de configuração deverá ser usada para a instalação e a contínua manutenção do sistema de certificação da AC.

6.6.3. Controle de segurança de ciclo de vida

Não aplicável.

6.6.4. Controles na Geração de LCR

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

6.7. CONTROLES DE SEGURANÇA DE REDE

6.7.1. Diretrizes Gerais

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

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

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

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

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

6.7.2. Firewall

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

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

6.7.3. Sistema de detecção de intrusão (IDS)

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

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

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

6.7.4. Registro de acessos não autorizados à rede

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

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIL DO CERTIFICADO, LCR e OCSP

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC VALID SSL EV 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. O conteúdo e perfis dos certificados emitidos nas cadeias CS seguem os estabelecidos nos documentos CS Guidelines.

7.1.1. Número(s) de versão

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

7.1.2. Extensões de certificados

Não se aplica.

7.1.3. Identificadores de Algoritmo

Não se aplica.

7.1.4. Formatos de nome

Não se aplica.

7.1.5. Restrições de nome

Não se aplica.

7.1.6. OID (Object Identifier) de DPC

O OID desta DPC é 2.16.76.1.1.144.

7.1.7. Uso da extensão "*Policy Constraints*"

Não se aplicável

7.1.8. Sintaxe e semântica dos qualificadores de política
Não se aplica.

7.1.9. Semântica de processamento para extensões críticas.
Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número (s) de versão
As LCR geradas pela AC VALID SSL EV 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 VALID SSL EV e sua criticalidade.

7.2.2.2. As LCR da AC VALID SSL EV obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões de LCR:

a) Authority Key Identifier, não crítica: contém o hash SHA-1 da chave pública da AC VALID SSL EV;

b) CRL Number, não crítica: contém um número sequencial para cada LCR emitida pela AC VALID SSL EV.

7.3. Perfil de OCSP

7.3.1. Número (s) de versão
Os serviços de respostas OCSP da AC VALID SSL EV implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP
Os serviços de respostas OCSP da AC VALID SSL EV estão em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias 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

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. Relação do Avaliador com a Entidade Avaliada

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, PCs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios WebTrust aplicáveis.

8.4.2. A AC VALID SSL EV 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 ICPBRASIL [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 VALID SSL EV (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC VALID SSL EV 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 VALID SSL EV 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].

8.6. Comunicação dos resultados

A AC VALID SSL EV 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].

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 VALID SSL EV, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC VALID SSL EV, será emitido gratuitamente outro certificado em substituição.

9.2 Responsabilidade Financeira

A responsabilidade da AC VALID SSL EV 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 entidades finais

Conforme item 4 desta DPC.

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 VALID SSL EV será divulgado.

9.3.2 Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

a) os certificados e a LCR/OCSP emitidos pela AC VALID SSL EV;

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

c) a PC correspondente;

d) esta DPC;

e) versões públicas da Política de Segurança;

f) resultados de auditorias; e

g) Termo de Titularidade ou solicitação de emissão do certificado.

A AC VALID SSL EV e a AR a ela vinculada tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) estejam na posse legítima da AC VALID SSL EV ou da AR a ela vinculada 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 VALID SSL EV ou a AR a ela vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

9.3.2.1 Certificados, LCR/OCSP, 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 VALID SSL EV também são considerados documentos não confidenciais:

a) qualquer PC aplicável;

b) qualquer DPC;

c) versões públicas de Política de Segurança – PS; e

d) a conclusão dos relatórios da auditoria.

9.3.2.3. A AC VALID SSL EV também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados 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 possui 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 VALID SSL EV 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. Os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, terão as atribuições de geração, manutenção e 9.3.3 Responsabilidade em proteger a informação confidencial.

9.3.3.4. Não se aplica.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A AC VALID SSL EV 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 VALID SSL EV será tratado, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709, 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 usuários finais são fornecidas na LCR/OCSP da AC VALID SSL EV.

9.4.4 Responsabilidade para proteger a informação privadas

A AC VALID SSL EV 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 VALID SSL EV poderão ser utilizadas ou divulgadas a terceiros mediante o fornecimento de consentimento pelo titular de certificado e representante legal, conforme legislação aplicável.

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

Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil e apresentação do documento de identificação; ou

b) por meio de pedido escrito com firma reconhecida e apresentação do documento de identificação.

9.4.6 Divulgação em processo judicial ou administrativo

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC VALID SSL EV será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

As informações privadas ou confidenciais sob a guarda da AC VALID SSL EV 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

Não se aplica.

9.4.8 Informações a terceiros

Como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC VALID SSL EV 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

A AC VALID SSL EV declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

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

9.6.1.2 Precisão da informação

A AC VALID SSL EV 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 processo AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.3 Identificação do requerente

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

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviço

A AC VALID SSL EV mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios das LCRs.

9.6.1.6 Revogação

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos 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

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 do titular de certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela AC VALID SSL EV, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2 A AC VALID SSL EV deve informar 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 As terceiras partes devem:

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 VALID SSL EV é considerado válido quando:

i. tiver sido emitido pela AC VALID SSL EV;

ii. não constar como revogado pela AC VALID SSL EV;

iii. não estiver expirado; e

iv. puder ser verificado com o uso do certificado válido da AC.

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

9.6.5 Representações e garantias de outros participantes

Não se aplica.

9.7 Representações e garantias de outros participantes

Não se aplica.

9.8 Limitações de responsabilidades

A AC VALID SSL EV 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 VALID SSL EV 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 os 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 VALID SSL EV mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web http://icp-brasil.validcertificadora.com.br/ac-validsslev/dpcacvalidsslev.pdf

9.12.3. Circunstâncias na qual o OID deve ser alterado

Não se aplica.

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 VALID SSL EV 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 VALID SSL EV 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 VALID SSL EV e AR e outras entidades citadas. Havendo conflito entre esta PC 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

Não se aplica.

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
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[1]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[4]	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 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for HighVolume Environments, september 2007
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.
[14] WebTrust Principles and Criteria for Registration Authorities
[15] WebTrust Principles and Criteria for Certification Authorities
[16] WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES –PUBLICLY TRUSTED SSL EV CERTIFICATES Version 1.0.1
Disponível:
https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-

assurance/overview-of-webtrust-services/principles-and-criteria
[17] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted [18]
Certificates Versão 1.6.6
[19] CA/Browser Forum Guidelines for The Issuance and Management of Extended Validation SSL EV Certificates versão 1.4
[20] Baseline Requirements for the Issuance and Management of Publicly Trusted SSL EV Certificates versão 1.2
Disponível: https://cabforum.org/baseline-requirements-documents/