# Declaração de Práticas de Certificação

# da Autoridade Certificadora da Ordem dos Advogados do Brasil - OAB

## DPC da AC OAB

## Versão 6.6- 12/03/2019

# Sumário


**1. INTRODUÇÃO ..... 7**

1.1. VISÃO GERAL ..... 7
1.2. IDENTIFICAÇÃO ..... 7
1.3. COMUNIDADE E APLICABILIDADE ..... 7
*1.3.1. Autoridades Certificadoras ..... 7*
*1.3.2. Autoridades de Registro ..... 7*
*1.3.3. Prestador de Serviço de Suporte ..... 8*
*1.3.3A Prestadores de Serviço de Confiança ..... 8*
*1.3.4. Titulares de Certificado ..... 8*
*1.3.5. Aplicabilidade ..... 8*
1.4. DADOS DE CONTATO ..... 8

**2. DISPOSIÇÕES GERAIS ..... 9**

2.1. OBRIGAÇÕES E DIREITOS ..... 9
*2.1.1. Obrigações da AC OAB ..... 9*
*2.1.2. Obrigações das AR ..... 10*
*2.1.3. Obrigações do Titular do Certificado ..... 10*
*2.1.4. Direitos da Terceira Parte (Relying Party) ..... 10*
*2.1.5. Obrigações do Repositório ..... 11*
2.2. RESPONSABILIDADES ..... 11
*2.2.1. Responsabilidades da AC OAB ..... 11*
*2.2.2. Responsabilidades das AR ..... 11*
2.3. RESPONSABILIDADE FINANCEIRA ..... 11
*2.3.1. Indenizações devidas pela terceira parte(Relying Party) ..... 11*
*2.3.2. Relações Fiduciárias ..... 11*
*2.3.3. Processos Administrativos ..... 11*
2.4. INTERPRETAÇÃO E EXECUÇÃO ..... 12
*2.4.1. Legislação ..... 12*
*2.4.2. Forma de interpretação e notificação ..... 12*
*2.4.3. Procedimentos da solução de disputa ..... 12*
2.5. TARIFAS DE SERVIÇO ..... 12
*2.5.1. Tarifas de emissão e renovação de certificados ..... 12*
*2.5.2. Tarifas de acesso ao certificado ..... 12*
*2.5.3. Tarifas de revogação ou de acesso à informação de status ..... 12*
*2.5.4. Tarifas para outros serviços ..... 12*
*2.5.5. Política de reembolso ..... 12*
2.6. PUBLICAÇÃO E REPOSITÓRIO ..... 13
*2.6.1. Publicação de informação da AC OAB ..... 13*
*2.6.2. Frequência de publicação ..... 13*
*2.6.3. Controles de acesso ..... 13*
*2.6.4. Repositórios ..... 13*
2.7. FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE ..... 13
2.8. SIGILO ..... 14
*2.8.1. Disposições gerais ..... 14*
*2.8.2. Tipos de informações sigilosas ..... 14*
*2.8.3. Tipos de informações não sigilosas ..... 14*
*2.8.4. Divulgação de informação de revogação ou suspensão de certificado ..... 15*
*2.8.5. Quebra de sigilo por motivos legais ..... 15*
*2.8.6. Informações a terceiros ..... 15*
*2.8.7. Divulgação por solicitação do Titular ..... 15*
*2.8.8. Outras circunstâncias de divulgação de informação ..... 15*
2.9. DIREITOS DE PROPRIEDADE INTELECTUAL ..... 16

**3. IDENTIFICAÇÃO E AUTENTICAÇÃO ..... 16**

3.1. REGISTRO INICIAL ..... 16
*3.1.1. Disposições Gerais ..... 16*
*3.1.2. Tipos de nomes ..... 18*
*3.1.3. Necessidade de nomes significativos ..... 18*
*3.1.4. Regras para interpretação de vários tipos de nomes ..... 18*
*3.1.5. Unicidade de nomes ..... 19*
*3.1.6. Procedimento para resolver disputa de nomes ..... 19*
*3.1.7. Reconhecimento, autenticação e papel de marcas registradas ..... 19*
*3.1.8. Método para comprovar a posse de chave privada ..... 19*
*3.1.9. Autenticação da identidade de um indivíduo ..... 19*
*3.1.10. Autenticação da identidade de uma organização ..... 20*
*3.1.11. Autenticação da identidade de equipamento ou aplicação ..... 21*
3.1.12. AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO CF-E-SAT ..... 22
3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL ..... 22
3.3. GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO ..... 23
3.4. SOLICITAÇÃO DE REVOGAÇÃO ..... 23

**4. REQUISITOS OPERACIONAIS ..... 23**

4.1. SOLICITAÇÃO DE CERTIFICADO ..... 23
4.2. EMISSÃO DE CERTIFICADO ..... 23
4.3. ACEITAÇÃO DE CERTIFICADO ..... 23
4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO ..... 24
*4.4.1. Circunstâncias para revogação ..... 24*
*4.4.2. Quem pode solicitar revogação ..... 24*
*4.4.3. Procedimento para solicitação de revogação ..... 24*
*4.4.4. Prazo para solicitação de revogação ..... 25*
*4.4.5. Circunstâncias para suspensão ..... 25*
*4.4.6. Quem pode solicitar suspensão ..... 25*
*4.4.7. Procedimento para solicitação de suspensão ..... 25*
*4.4.8. Limites no período de suspensão ..... 25*
*4.4.9. Frequência de emissão de LCR ..... 26*
*4.4.10. Requisitos para verificação de LCR ..... 26*
*4.4.11. Disponibilidade para revogação ou verificação de status on-line ..... 26*
*4.4.12. Requisitos para verificação de revogação on-line ..... 26*
*4.4.13. Outras formas disponíveis para divulgação de revogação ..... 26*
*4.4.14. Requisitos para verificação de outras formas de divulgação de revogação ..... 26*
*4.4.15. Requisitos especiais para o caso de comprometimento de chave ..... 26*
4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA ..... 27
*4.5.1. Tipos de eventos registrados ..... 27*
*4.5.2. Frequência de auditoria de registros (logs) ..... 28*
*4.5.3. Período de retenção para registros (logs) de auditoria ..... 28*
*4.5.4. Proteção de registro (log) de auditoria ..... 28*
*4.5.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria ..... 28*
*4.5.6. Sistema de coleta de dados de auditoria ..... 28*
*4.5.7. Notificação de agentes causadores de eventos ..... 28*
*4.5.8. Avaliações de vulnerabilidade ..... 28*
4.6. ARQUIVAMENTO DE REGISTROS ..... 29
*4.6.1. Tipos de registros arquivados ..... 29*
*4.6.2. Período de retenção para arquivo ..... 29*
*4.6.3. Proteção de arquivo ..... 29*
*4.6.4. Procedimentos para cópia de segurança (backup) de arquivo ..... 29*
*4.6.5. Requisitos para datação (time-stamping) de registros ..... 29*
*4.6.6. Sistema de coleta de dados de arquivo ..... 29*
*4.6.7. Procedimentos para obter e verificar informação de arquivo ..... 29*
4.7. TROCA DE CHAVE ..... 30

4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE ..... 30
*4.8.1. Recursos computacionais, software, e dados corrompidos ..... 30*
*4.8.2. Certificado de entidade é revogado ..... 30*
*4.8.3. Chave da entidade é comprometida ..... 30*
*4.8.4. Segurança dos recursos após desastre natural ou de outra natureza ..... 30*
*4.8.5. Atividades das Autoridades de Registro ..... 31*
4.9. EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS ..... 31
**5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL ..... 32**
5.1. CONTROLES FÍSICOS ..... 32
*5.1.1. Construção e localização das instalações ..... 32*
*5.1.2. Acesso físico nas instalações de AC ..... 32*
*5.1.3. Energia e ar condicionado nas instalações de AC ..... 34*
*5.1.4. Exposição à água nas instalações de AC ..... 35*
*5.1.5. Prevenção e proteção contra incêndio nas instalações de AC ..... 35*
*5.1.6. Armazenamento de mídia nas instalações de AC ..... 35*
*5.1.7. Destruição de lixo nas instalações de AC ..... 36*
*5.1.8. Instalações de segurança (backup) externas (off-site) para AC ..... 36*
*5.1.9. Instalações técnicas de AR ..... 36*
5.2. CONTROLES PROCEDIMENTAIS ..... 36
*5.2.1. Perfis qualificados ..... 36*
*5.2.2. Número de pessoas necessário por tarefa ..... 37*
*5.2.3. Identificação e autenticação para cada perfil ..... 37*
5.3. CONTROLES DE PESSOAL ..... 37
*5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade ..... 37*
*5.3.2. Procedimentos de verificação de antecedentes ..... 38*
*5.3.3. Requisitos de treinamento ..... 38*
*5.3.4. Frequência e requisitos para reciclagem técnica ..... 38*
*5.3.5. Frequência e sequencia de rodízio de cargos ..... 38*
*5.3.6. Sanções para ações não autorizadas ..... 38*
*5.3.7. Requisitos para contratação de pessoal ..... 39*
*5.3.8. Documentação fornecida ao pessoal ..... 39*
**6. CONTROLES TÉCNICOS DE SEGURANÇA ..... 39**
6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES ..... 39
*6.1.1. Geração do par de chaves ..... 39*
*6.1.2. Entrega da chave privada à entidade titular ..... 39*
*6.1.3. Entrega da chave pública para emissor de certificado ..... 39*
*6.1.4. Disponibilização de chave pública da AC para usuários ..... 40*
*6.1.5. Tamanhos de chave ..... 40*
*6.1.6. Geração de parâmetros de chaves assimétricas ..... 40*
*6.1.7. Verificação da qualidade dos parâmetros ..... 40*
*6.1.8. Geração de chave por hardware ou software ..... 40*
*6.1.9. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3) ..... 40*
6.2. PROTEÇÃO DA CHAVE PRIVADA ..... 41
*6.2.1. Padrões para módulo criptográfico ..... 41*
*6.2.2. Controle "n de m" para chave privada ..... 41*
*6.2.3. Recuperação (escrow) de chave privada ..... 41*
*6.2.4. Cópia de segurança (backup) de chave privada ..... 41*
*6.2.5. Arquivamento de chave privada ..... 42*
*6.2.6. Inserção de chave privada em módulo criptográfico ..... 42*
*6.2.7. Método de ativação de chave privada ..... 42*
*6.2.8. Método de desativação de chave privada ..... 42*
*6.2.9. Método de destruição de chave privada ..... 42*
6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES ..... 43
*6.3.1. Arquivamento de chave pública ..... 43*
*6.3.2. Períodos de uso para as chaves pública e privada ..... 43*

6.4. DADOS DE ATIVAÇÃO ..... 43
*6.4.1. Geração e instalação dos dados de ativação ..... 43*
*6.4.2. Proteção dos dados de ativação ..... 43*
*6.4.3. Outros aspectos dos dados de ativação ..... 43*
6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL ..... 44
*6.5.1. Requisitos Técnicos Específicos de Segurança Computacional ..... 44*
*6.5.2. Classificação da segurança computacional ..... 44*
*6.5.3. Controles de Segurança para as Autoridades de Registro ..... 44*
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA ..... 45
*6.6.1. Controles de desenvolvimento de sistema ..... 45*
*6.6.2. Controles de gerenciamento de segurança ..... 45*
*6.6.3. Classificações de segurança de ciclo de vida ..... 45*
*6.6.4. Controles na Geração de LCR ..... 45*
6.7. CONTROLES DE SEGURANÇA DE REDE ..... 46
*6.7.1. Diretrizes Gerais ..... 46*
*6.7.2. Firewall ..... 46*
*6.7.3. Sistema de detecção de intrusão (IDS) ..... 46*
*6.7.4. Registro de acessos não-autorizados à rede ..... 46*
6.8. CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO ..... 47

**7. PERFIS DE CERTIFICADO E LCR ..... 47**

7.1. DIRETRIZES GERAIS ..... 47
7.2. PERFIL DO CERTIFICADO ..... 47
*7.2.1. Número de versão ..... 47*
*7.2.2. Extensões de certificado ..... 47*
*7.2.3. Identificadores de algoritmo ..... 47*
*7.2.4. Formatos de nome ..... 47*
*7.2.5. Restrições de nome ..... 47*
*7.2.6. OID (Object Identifier) de DPC ..... 47*
*7.2.7. Uso da extensão "Policy Constraints" ..... 48*
*7.2.8. Sintaxe e semântica dos qualificadores de política ..... 48*
*7.2.9. Semântica de processamento para extensões críticas ..... 48*
7.3. PERFIL DE LCR ..... 48
*7.3.1. Número(s) de versão ..... 48*
*7.3.2. Extensões de LCR e de suas entradas ..... 48*

**8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO ..... 48**

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO ..... 48
8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO ..... 48
8.3. PROCEDIMENTOS DE APROVAÇÃO ..... 48

**9. DOCUMENTOS REFERENCIADOS ..... 49**

# CONTROLE DE ALTERAÇÕES

| Versão | Data | Resolução que aprovou a alteração | Item Alterado | Descrição da Alteração |
|---|---|---|---|---|
| **6.3** | **10/11/2016** | **Não se aplica** | 6.5.3.2 | adequação do item k) a versão 2.1 do DOC-ICP-03.01. |
| **6.4** | **13/04/2017** | **Não se aplica** | 1.1.3; 1.3.4; 3.1.9.1; 3.1.9.2; 3.1.10.1.1; 3.1.10.3; 3.1.11.1; 6.1.1.2; 6.1.5.2; 6.1.6; 6.1.8; 6.2.1; 6.5.3.2; 6.8; | Criação de certificados do tipo PJ .<br><br>Exclusão da certidão administrativa.<br><br>Inclusão da consulta CNA. |
| **6.5** | **25/10/2017** | **Resolução N°119, de junho de 2017**<br><br>**Resolução N°123, de 06 de julho de 2017**<br><br>**Não se aplica** | 2.7.1,6.1.1.2,6.1.6 6.1.8.1,6.2.1.1. 6.8, 3.1.10.2. | Referência a auditoria WEBTRUST<br><br>Alteração dos Padrões Obrigatório Módulo Criptográfico<br><br>Inclusão da consulta CNSA. |
| | | **Resolução N°130, de 19 de setembro de 2017**<br><br>**RESOLUÇÃO Nº 132, DE 10 DE NOVEMBRO DE 2017**<br><br>**Não se aplica** | 1.3.3.A,1.3.3.A.1,3.1.1.2,3.1.1.2.1,3.1.1.2.2, 3.1.1.2.3, 3.1.1.2.4, 3.1.1.2.5., 3.1.9.2.1, 6.2.4.3 | Procedimentos de validação fora do ambiente físico da AR.<br><br>Inclusão da Nota no item 3.1.9.2.1, decorrente ao Decreto nº. 8727/2016.<br><br>Validade da CNH.<br><br>Inclusão do Prestador de Serviço de Confiança –PSC. |
| **6.6** | **12/03/2019** | **Não se aplica** | 1.1.3; 2.1.3; 3.1.9.1; 3.1.9.2.3; 3.1.10.1.3; 4.3.2; 4.4.1.2 h); 4.4.3.1; 4.4.10.1; 4.4.15.2; 6.2.1.2; 6.2.4.1 | Eliminação de referências a certificados do tipo equipamento |

# Declaração de Práticas de Certificação da Autoridade Certificadora da Ordem dos Advogados do Brasil - OAB

## 1. INTRODUÇÃO

### 1.1. Visão Geral

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

1.1.2. A estrutura desta DPC está baseada no DOC-ICP-05 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Declarações de Prática de Certificação das Autoridades Certificadoras da ICP-Brasil. As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC OAB ou entidades a ela vinculadas possa vir a adotar.

1.1.3. A AC OAB está certificada em nível imediatamente subsequente ao da AC Certisign certificada pela AC Raiz da ICP-Brasil. O certificado da AC OAB contém a chave pública correspondente à sua chave privada, utilizada para assinar certificados de assinatura geral e proteção de e-mail (S/MIME): de assinatura A3 (para pessoas físicas, jurídicas e aplicação para assinatura de resposta OCSP) e para assinar a sua Lista de Certificados Revogados (LCR), conforme regulado pelo DOC-ICP-01.02 - Requisitos Adicionais para Aderência aos Programas de Raízes Confiáveis [12].

1.1.4. Para regulamentar usos específicos dos certificados emitidos pela a AC OAB são publicadas Políticas de Certificado disponíveis em página web (http://icp-brasil.certisign.com.br/repositorio/ac-oab/index.htm).

### 1.2. Identificação

Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora da Ordem dos Advogados do Brasil - OAB e referida como "DPC da AC OAB", cujo OID (*object identifier*) é 2.16.76.1.1.36.

### 1.3. Comunidade e Aplicabilidade

#### 1.3.1. Autoridades Certificadoras

Esta DPC refere-se à AC OAB, no âmbito da ICP-Brasil.

#### 1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC OAB para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC OAB (https://www.certisign.com.br/certisign/repositorios/icp-brasil/autoridades-registro/ac-oab):

a) relação de todas as AR credenciadas, com informações sobre as PC que implementam.
b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
d) relação de AR que tenham se descredenciado da cadeia da AC OAB, com respectiva data do descredenciamento;

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC OAB mantém as informações acima sempre atualizadas.

### 1.3.3. Prestador de Serviço de Suporte

1.3.3.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC OAB e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC OAB (http://icp-brasil.certisign.com.br/repositorio/ac-oab/index.htm).

1.3.3.2. PSS são entidades utilizadas pela AC e/ou suas AR para desempenhar atividade descrita nesta DPC ou nas PC e se classificam em três categorias, conforme o tipo de atividade prestada:
a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC OAB mantém as informações acima sempre atualizadas.

### 1.3.3A Prestadores de Serviço de Confiança

1.3.3A.1 A relação de todos os Prestadores de Serviço de Confiança – PSC vinculados diretamente a AC OAB é publicada em serviço de diretório e/ou em página web da AC OAB (http://icp-brasil.certisign.com.br/repositorio/ac-oab/index.htm).

1.3.3A.2. PSC são entidades utilizadas pelas AC, ou a própria AC, descritas nesta PC ou na DPC implementada pela AC e se classificam em três categorias, conforme o tipo de atividade prestada:
a) armazenamento de chaves privadas dos usuários finais; ou
b) serviço de assinatura digital, verificação da assinatura digital; ou
c) ambos.

### 1.3.4. Titulares de Certificado

Pessoas físicas, jurídicas, advogados, estagiários, funcionários e consultores estrangeiros habilitados e registrados na OAB podem ser titular de Certificado. Advogados e estagiários desde que possuam a situação de REGULAR OU LICENCIADA na consulta ao Cadastro Nacional dos Advogados - CNA (pessoa física) e pessoa jurídica situação ATIVA no Cadastro Nacional de Sociedades de Advogados - CNSA (pessoa jurídica).

No caso de certificado emitido para pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

### 1.3.5. Aplicabilidade

A AC OAB implementa as seguintes Políticas de Certificado Digital:

Para Certificados de Assinatura Digital:

• Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora OAB, PC A3 da AC OAB, OID 2.16.76.1.2.3.28

Nas PC correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC OAB e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

## 1.4. Dados de Contato

Empresa: Ordem dos Advogados do Brasil – Conselho Federal

Endereço: SAS Qd. 05 - Lt. 01 - Bl. M - Brasília - DF

CEP: 70070-939

Área: Gerência de Tecnologia da Informação

Contato: Antônio de Pádua Canavieira

Telefone: (61) 21939615

Telefone:(61) 2193-9600

E-mail: antonio@oab.org.br

## 2. DISPOSIÇÕES GERAIS

### 2.1. Obrigações e Direitos

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhados nas PC implementadas pela AC OAB.

#### 2.1.1. Obrigações da AC OAB

a) operar de acordo com esta DPC e com as PC que implementa;
b) gerar e gerenciar seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC Certisign, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado.
e) notificar os usuários quando ocorrer suspeita de comprometimento da chave privada da AC OAB, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AR 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 sua LCR e quando aplicável, disponibilizar consulta online de situação do certificado (OCSP Online Certificate Status Protocol);
k) publicar em sua página web esta DPC da AC OAB e as PC que implementa;
l) publicar em sua página web as informações descritas no item 2.6.1.2 desta DPC;
m) publicar em sua página web informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas nesta DPC da AC OAB, nas PC e Política de Segurança (PS) da AC OAB 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 pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
u) informar à terceira parte 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, mensalmente, a quantidade de certificados digitais emitidos;
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado; e
x) obedecer estritamente a esta DPC da AC OAB e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil.

### 2.1.2. Obrigações das AR

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar as solicitações de emissão ou de revogação de certificados à AC OAB utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
d) informar aos respectivos titulares de certificado a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pela AC OAB aos seus respectivos solicitantes;
f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC OAB e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]
h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP -Brasil;
i) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;
k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas ;
l) obedecer estritamente a esta DPC e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil; e
m) notificar os titulares, com antecedência mínima de 30 (trinta) dias, a expiração da validade dos certificados.

### 2.1.3. Obrigações do Titular do Certificado

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações contemplados por esta DPC, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;
e) informar à AC OAB o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
f) apresentação dos originais e fornecimento de cópias autênticas dos documentos que forem exigidos para emissão do certificado;
g) verificar, no momento da aceitação do certificado, a veracidade e exatidão das informações contidas no seu certificado e notificar a AC, solicitando a imediata revogação do certificado que contiver inexatidões ou erros; e
h) obedecer estritamente a esta DPC e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil e as obrigações contratuais assumidas perante à AC e AR.

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

### 2.1.4. Direitos da Terceira Parte (Relying Party)

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

2.1.4.2. Constituem-se direitos da terceira parte:
a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
b) verificar, a qualquer tempo, a validade do certificado.

Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
a) não constar da LCR da AC emitente;
b) não estiver expirado; e

c) sua validade puder ser verificada através de certificado válido da AC emitente.

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

#### 2.1.5. Obrigações do Repositório

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC OAB e sua LCR;
b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
c) implementar os recursos necessários para a segurança dos dados nele armazenados; e
d) disponibilizar verificação on-line do status do certificado ou outro mecanismo de atualização de status aprovado pela ICP-Brasil, quando aplicável por força de contratação específica.

### 2.2. Responsabilidades

#### 2.2.1. Responsabilidades da AC OAB

2.2.1.1. A AC OAB responde pelos danos a que der causa.

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

2.2.1.3. Não se aplica.

#### 2.2.2. Responsabilidades das AR

A AR é responsável pelos danos a que der causa.

### 2.3. Responsabilidade Financeira

#### 2.3.1. Indenizações devidas pela terceira parte(Relying Party)

A terceira parte responde perante a AC OAB e ARs vinculadas apenas pelos prejuízos a que der causa com a prática de ato ilícito, nos termos da legislação vigente.

#### 2.3.2. Relações Fiduciárias

A AC OAB ou sua AR vinculada indeniza integralmente os prejuízos que, comprovadamente, der causa, quando o Titular do Certificado for pessoa física.

As indenizações da AC OAB e de suas AR vinculadas cobrem perdas e danos decorrentes de comprometimento da chave privada da AC OAB, de erro na identificação do titular, de emissão defeituosa do certificado ou de erros ou omissões da AC OAB ou das AR vinculadas.

#### 2.3.3. Processos Administrativos

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

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC OAB, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente;
b) nos casos de erro na identificação, o titular do certificado não pode requerer qualquer indenização quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular à AC OAB ou às ARs vinculadas;
c) nos casos de erro na transcrição, o titular do certificado não pode requerer qualquer indenização quando houver aceitado o certificado.

## 2.4. Interpretação e Execução

### 2.4.1. Legislação

Esta DPC é regida pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-Brasil, bem como pelas demais leis em vigor no Brasil.

### 2.4.2. Forma de interpretação e notificação

2.4.2.1. Na hipótese de uma ou mais disposições desta DPC ser, por qualquer razão, considerada inválida, ilegal, ou conflituosa com norma da ICP-Brasil, a inaplicabilidade não afeta as demais disposições, sendo esta DPC interpretada, então, como se não contivesse tal disposição e, na medida do possível, interpretada para manter a intenção original da DPC. Nesse caso, o Grupo de Práticas e Políticas da AC OAB examinará a disposição inválida e proporá à nova redação ou retirada da disposição afetada, na forma do item 8 desta DPC.

2.4.2.2. As notificações ou qualquer outra comunicação necessária, relativas às práticas descritas nesta DPC, são feitas através de mensagem eletrônica assinada digitalmente, com chave pública certificada pela ICP-Brasil, ou por escrito e entregue à AC OAB.

2.4.2.3. A DPC da AC OAB na ICP-Brasil, não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

### 2.4.3. Procedimentos da solução de disputa

2.4.3.1. Em caso de conflito entre esta DPC da AC OAB, as PC que implementa ou outros documentos que a AC OAB adotar, prevalece o disposto nesta DPC. O contrato para emissão de certificados poderá criar obrigações específicas, limitar o uso dos certificados ou restringir valores de transações comerciais, desde que respeitados os direitos previstos nesta DPC.

2.4.3.2. Esta DPC da AC OAB não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3.3. Casos omissos deverão ser encaminhados para apreciação da AC Raiz.

## 2.5. Tarifas de Serviço

### 2.5.1. Tarifas de emissão e renovação de certificados

Variável conforme definição interna Comercial.

### 2.5.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

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

### 2.5.4. 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.

### 2.5.5. 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 OAB, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC OAB, será emitido gratuitamente outro certificado em substituição.

## 2.6. Publicação e Repositório

### 2.6.1. Publicação de informação da AC OAB

2.6.1.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC OAB (http://icp-brasil.certisign.com.br/repositorio/ac-oab/index.htm), obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC OAB 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.

2.6.1.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC OAB (http://icp-brasil.certisign.com.br/repositorio/ac-oab/index.htm):

a) seus próprio certificado;
b) suas LCR;
c) esta DPC;
d) as PC que implementa;
e) uma relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;
f) uma relação, regularmente atualizada, das AR vinculadas que tenham celebrado acordos operacionais com outras AR da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e
g) uma relação, regularmente atualizada, dos PSS vinculados.

### 2.6.2. Frequência de publicação

Certificados são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme o item 4.4.9 da PC correspondente. As versões ou alterações desta DPC e da PC, assim como os endereços das instalações técnicas das AR vinculadas, são atualizadas no web site da AC OAB após aprovação da AC Raiz da ICP-Brasil.

### 2.6.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC OAB, às PC implementadas e aos endereços das instalações técnicas das AR vinculadas.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos ou desta lista 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.

### 2.6.4. Repositórios

O repositório da AC OAB 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 (http://icp-brasil.certisign.com.br/repositorio/ac-oab/index.htm).

As publicações da AC OAB podem ser consultadas através do protocolo http.

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

2.6.4.1 A AC OAB disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR.

## 2.7. Fiscalização e Auditoria de Conformidade

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

com suas respectivas DPC, PC, Política de Segurança e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pela WebTrust.

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

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

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

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

## 2.8. Sigilo

### 2.8.1. Disposições gerais

2.8.1.1. AC OAB gera e mantém sua chave privada, sendo responsável pelo seu sigilo. A divulgação ou utilização indevida da sua chave privada é de sua inteira responsabilidade.

2.8.1.2. O titular de certificados digitais de assinatura digital e de sigilo emitidos para pessoas físicas é responsável pela geração, manutenção e sigilo de suas respectivas chaves privadas bem como pela divulgação ou utilização indevida dessas chaves.

2.8.1.3. No intuito de preservar o sigilo da sua chave privada o titular pelo certificado deve tomar todas as medidas para a proteção da mesma.

O sigilo da chave privada do certificado é garantido através de senha de acesso à chave privada. Esta senha será definida pelo usuário no momento da instalação do certificado. A criação e utilização dessa senha para acesso à aplicação são de responsabilidade do usuário.

O Titular pelo Certificado deve observar procedimentos básicos de segurança, tais como:

1) Nunca fornecer a senha a terceiros;
2) Utilizar senha de, no mínimo, 8 caracteres;
3) Não utilizar senha fraca ou óbvia, conforme definido na Política de Segurança da AC OAB, item 5.1.1.11;
4) Montar senha com caracteres numéricos e alfanuméricos;
5) Memorizar a senha e não escrevê-la.
6) Guardar a mídia principal e cópia de segurança em lugar seguro.

### 2.8.2. Tipos de informações sigilosas

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

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

### 2.8.3. Tipos de informações não sigilosas

As informações consideradas não sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC OAB;
b) informações corporativas ou pessoais que constem no certificados ou em diretórios públicos;

c) a PC correspondente;
d) esta DPC;
e) versões públicas de Políticas de Segurança;
f) resultados finais de auditorias; e
g) Termo de Titularidade ou solicitação de emissão do certificado.

A AC OAB 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 OAB 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 OAB ou a AR a ela vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

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

### 2.8.4. Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. Informações sobre revogação de certificados emitidos pela AC OAB são fornecidas em sua LCR ou através de OCSP, quando aplicável.

2.8.4.2. A razão para a revogação de certificado é informada ao titular do certificado e será tornada pública, desde que autorizada a divulgação pelo mesmo.

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

### 2.8.5. Quebra de sigilo por motivos legais

A AC OAB fornecerá, mediante ordem judicial ou por determinação legal, documentos, informações ou registros sob sua guarda.

### 2.8.6. Informações a terceiros

Nenhum documento, informação ou registro sob a guarda da AC OAB é fornecido a qualquer pessoa, exceto quando a pessoa que requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para fazê-lo.

### 2.8.7. Divulgação por solicitação do Titular

2.8.7.1. O titular de certificado e seu representante legal têm acesso a quaisquer dos seus próprios dados e identificações e podem autorizar a divulgação de seus registros.

2.8.7.2. Autorizações podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado do mesmo tipo ou superior emitido na ICP-Brasil;
b) por solicitação escrita, com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização numa das formas acima, exceto nos casos do item 2.8.5.

### 2.8.8. Outras circunstâncias de divulgação de informação

Não se aplica.

### 2.9. Direitos de Propriedade Intelectual

A Certisign Certificadora Digital S.A. ou sua licenciante VeriSign, Inc., quando aplicável, detém todos os direitos de propriedade intelectual sobre as idéias, conceitos, técnicas e invenções, processos e/ou obras, incluídas ou utilizadas nos produtos e serviços fornecidos por AC OAB nos termos dessa DPC.

Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

O titular de certificado emitido pela AC OAB concede à AC Certisign e à AC OAB o direito de publicar e divulgar em página web, a chave pública contida no certificado, correspondente à chave privada que esta sob sua posse.

## 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

### 3.1. Registro Inicial

#### 3.1.1. Disposições Gerais

3.1.1.1. Neste item e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pelas AR vinculadas a AC OAB para a realização dos seguintes processos:

a) **Validação da solicitação de certificado** – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:

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

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

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

iv. as etapas descritas acima podem ser realizadas por um ou mais agentes de validação.

b) **Verificação da solicitação de certificado** - confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:
i. por agente de registro distinto do que executou a etapa de validação;

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

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

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

3.1.1.2. Excepcionalmente, o processo de validação poderá ser realizado fora do ambiente físico da AR, através de procedimento de validação externa, mediante o deslocamento do Agente de Registro

da AR até o interessado na obtenção do certificado, observadas as hipóteses, a forma e as condições abaixo dispostas, vedada a criação de instalações físicas destinadas a tal fim, qualquer que seja a denominação utilizada, tais como, mas não limitada a, ponto de atendimento, posto de validação, parceiro, canal, agente credenciado ou agência autorizada.

3.1.1.2.1. As AR poderão adotar o procedimento de validação externa nas seguintes hipóteses:

I. Para pessoas com deficiência ou com mobilidade reduzida, conforme definido pela Lei nº 13.146, de 6 de julho de 2015, devidamente comprovado por documento hábil;

II. Para pessoas Politicamente Expostas – PEP, conforme definido na Resolução nº 16, de 28 de março de 2007, do Conselho de Controle de Atividades Financeiras COAF/MF, devidamente comprovado por documento hábil;

III. Para pessoas que se encontrem cumprindo pena ou detidas em estabelecimento prisional;

IV. Para pessoas com incapacidade física momentânea ou por motivo de saúde, em qualquer caso devidamente justificado e comprovado por documento hábil, estejam impedidas ou impossibilitadas de se deslocar até a instalação física da AR;

V. Para atender contratos firmados com entidades públicas cujos os editais de licitação tenham sido publicados até a data de publicação desta Resolução;

VI. Outras pessoas não citadas anteriormente, mediante solicitação expressa de validação externa pelo titular do certificado, limitado a 15% (quinze por cento) do total de certificados emitidos pela AR no mês imediatamente anterior.

Nota 1: O disposto na alínea VI, aplica-se a partir do mês subsequente à entrada em operação da AR, vedada a validação externa com base no referido dispositivo, no mês do início de sua operação.

Nota 2: Considera-se como total de certificados emitidos pela AR no mês imediatamente anterior, para fins da alínea VI, o volume de certificados emitidos pela AR, informado na documentação encaminhada ao ITI na forma e no prazo previsto pela Instrução Normativa no 14, de 28 de novembro de 2016

Nota 3: Acaso a AR não tenha emitido certificados no mês anterior ou não tenham sido prestadas as informações na forma ou no prazo exigidos, ficará a AR impossibilitada de emitir novos certificados com fulcro na alínea VI, somente podendo voltar a emiti-los no mês imediatamente subsequente, desde que prestadas as informações de forma tempestiva.

Nota 4: Para o cálculo da quantidade limite disposto na alínea VI, em caso de resultado fracionário, admitir-se-á o arredondamento para a unidade superior.

3.1.1.2.2. A validação externa será realizada no domicílio do titular do certificado digital, nas hipóteses previstas nos incisos I, II e IV, do item 3.1.1.2.1, ou no local que este se encontre, na hipótese do inc. III, do mesmo item.

3.1.1.2.3. Para fins do item anterior, considera-se domicílio do titular do certificado digital, o seu domicílio civil, na forma do disposto no Código Civil, Lei nº 10.406, de 10 de janeiro de 2002.

3.1.1.2.4. O local no qual a validação externa será realizada deverá ser informado no Formulário de Validação Externa, a que se refere a alínea "d" do item 3.1.1.2.5.

3.1.1.2.5. A validação fora do ambiente físico da AR deve atender ainda as seguintes condições:

a) utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR;

b) adotar aplicativo de georreferenciamento que permita rastrear o computador móvel utilizado na validação externa, sendo que a localização do equipamento deve ficar disponível no sistema da AR em que o agente de registro deva estar cadastrado previamente;

c) adotar equipamentos de coleta e verificação biométrica do titular e do agente de registro, em atendimento aos padrões da ICP-Brasil;

d) preencher o Formulário de Validação Externa, adendo ADE-ICP-05.D, o qual deverá ser assinado pelo agente de registro e pelo titular do certificado, preferencialmente assinados digitalmente;

e) em se tratando de dossiês físicos do titular de certificado, esses devem ser enviados para a Instalação Técnica em até 5 (cinco) dias úteis; e

f) Utilização de equipamento específico, destinado exclusivamente para fins de validação externa, vedada a utilização, para tal fim, das estações de trabalho ou outros equipamentos empregados na instalação técnica.

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

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

3.1.1.4.1. Não se aplica.
3.1.1.5. Não se aplica.
3.1.1.6. Não se aplica.

3.1.1.7. A AC OAB disponibiliza, 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 DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

3.1.1.8. Não se aplica.

### 3.1.2. Tipos de nomes

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

3.1.2.2. Não se aplica.

### 3.1.3. Necessidade de nomes significativos

Os certificados emitidos pela AC OAB exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem.

### 3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

### 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 OAB.

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 OAB 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 são executados de acordo com a legislação em vigor.

### 3.1.8. Método para comprovar a posse de chave privada

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. A RFC 2510 é utilizada como referência para essa finalidade. O método de verificação utilizado é – Proof of Possession (POP) of Private Key – conforme o item 2.3 da RFC 2510.

### 3.1.9. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos pessoais de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

#### 3.1.9.1. Documentos para efeitos de identificação de um indivíduo

Deve ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de um indivíduo solicitante de certificado:

a) Cédula de Identidade ou Passaporte, se brasileiro;

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

c) Passaporte, se estrangeiro não domiciliado no Brasil;

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

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

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

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

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

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

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

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

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

Os documentos que possuem data de validade precisam estar dentro do prazo, à exceção da CNH que permanece válida como documento de identificação mesmo que sua data de validade esteja expirada.

#### 3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:
a) nome completo, sem abreviações; [1]
b) data de nascimento;[2]
c) Cadastro de Pessoa Física (CPF);
d) números de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente, no caso de advogado, estagiário e consultor estrangeiro;
e) número de inscrição do funcionário, no caso de certificados emitidos para funcionário.

**Nota:** Na hipótese de pessoa física travesti e transexual abrangida pelo Decreto nº. 8727/2016, tanto o nome civil quanto o nome social que constarem no documento de identificação, deverão ser preenchidos no certificado.

3.1.9.2.2. Não é necessário o preenchimento dos 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 Especifico do INSS (CEI);
d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor.

3.1.9.2.3. Para tanto, o titular deve apresentar a documentação respectiva aos campos cujo preenchimento é obrigatório, caso a caso, em sua versão original. É mantido arquivo com as cópias de todos os documentos utilizados.

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

O resultado da consulta ao Cadastro Nacional de Advogados – CNA (http://cna.oab.org.br/) dever ser validada pelo agente de registro contra as informações prestadas:
a) número de habilitação ou identificação profissional emitido pela OAB, no caso de certificados de advogado, estagiário e consultor estrangeiro;
b) número de habilitação ou identificação funcional emitido pela OAB, no caso de certificados para funcionário.

O cartão CPF pode ser substituído por consulta à página da Receita Federal, sendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

### 3.1.10. Autenticação da identidade de uma organização

#### 3.1.10.1. Disposições Gerais

3.1.10.1.1. Neste item são definidos os procedimentos empregados pelas AR vinculadas para a confirmação da identidade de uma pessoa jurídica.

[1] No campo Subject, como parte do Common Name, que compõe o Distinguished Name
[2] No campo Subject Alternative Name, nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.1**

3.1.10.1.2. Em 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.

3.1.10.1.3. Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.1.10.2;
b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1.
**NOTA 01**: A AC OAB e as AR a ela vinculada poderá solicitar uma assinatura manuscrita ao titular ou responsável pelo uso do certificado para comparação com o documento de identidade ou contrato social

#### 3.1.10.2. Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:

i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;
ii. se entidade privada:
1. ato constitutivo, devidamente registrado no órgão competente; e
2. documentos da eleição de seus administradores, quando aplicável, registrado no órgão competente;
iii. consulta do número de inscrição no Cadastro Nacional de Sociedade de Advogados –CNSA (http://cnsa.oab.org.br/).

b) Relativos a sua habilitação fiscal:

i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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

#### 3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.10.3.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:
a) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), 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.
3.1.10.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.1.9.2.

### 3.1.11. Autenticação da identidade de equipamento ou aplicação

#### 3.1.11.1. Disposições Gerais

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

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

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

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

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

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

d) presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade de que trata o item 4.1.1, ou outorga de procuração atribuindo poderes para solicitação de certificado para aplicação e assinatura do respectivo termo de titularidade.

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

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

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

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

a) URL ou nome da aplicação[3];

b) nome completo do responsável pelo certificado, sem abreviações[4];

c) data de nascimento do responsável pelo certificado[5];

d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[6], se o titular for pessoa jurídica;

e) Cadastro Nacional de Pessoa Jurídica (CNPJ)[7], se o titular for pessoa jurídica

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

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

Não se aplica.

## 3.2. Geração de novo par de chaves antes da expiração do atual

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

3.2.2. O processo descrito acima é conduzido segundo uma das seguintes possibilidades:

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

b) A solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física.

3.2.3. Não se aplica.

[3] No campo Subject, como parte do Common Name, que compõe o Distinguished Name

[4] No campo Subject Alternative Name, **OID 2.16.76.1.3.2**

[5] No campo Subject Alternative Name, nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.4**

[6] No campo Subject Alternative Name, **OID 2.16.76.1.3.8**

[7] No campo Subject Alternative Name, **OID 2.16.76.1.3.3**

### 3.3. Geração de novo par de chaves após expiração ou revogação

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

3.3.2. Não se aplica.

### 3.4. Solicitação de Revogação

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

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 OAB está descrito no item 4.4.3.1 desta DPC.

## 4. REQUISITOS OPERACIONAIS

### 4.1. Solicitação de Certificado

4.1.1. Para atender à solicitação de emissão de certificados a AC OAB exige que a AR tenha provido:

a) a comprovação de atributos de identificação constantes do certificado e o recebimento dos documentos obrigatórios exigidos para identificação dos titulares e responsáveis, conforme item 3.1;
b) a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de nível A3;
c) um termo de titularidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico.

4.1.2. Não se aplica.
4.1.3. Não se aplica.
4.1.4. Não se aplica.

### 4.2. Emissão de Certificado

4.2.1. A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento 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, por e-mail, da emissão e do método para a retirada do certificado.

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

### 4.3. Aceitação de Certificado

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

4.3.2. A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, na primeira utilização da chave privada correspondente. O prazo para aceitação do certificado está definido no item 4.4.4 desta DPC.

4.3.3. Não se aplica.

## 4.4. Suspensão e Revogação de Certificado

### 4.4.1. Circunstâncias para revogação

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

4.4.1.2. O certificado é obrigatoriamente revogado:

a) quando constatada emissão imprópria ou defeituosa do mesmo;
b) quando for necessária a alteração de qualquer informação constante no mesmo;
c) no caso de extinção, dissolução ou transformação da AC OAB;
d) no caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;
e) no caso de falecimento do titular - pessoas físicas;
f) no caso de mudança na razão ou denominação social do titular – aplicações e pessoas jurídicas;
g) no caso de extinção, dissolução ou transformação do titular do certificado – aplicações e pessoas jurídicas; ou
h) no caso de falecimento ou demissão do responsável – aplicações e pessoas jurídicas.

4.4.1.3. A AC OAB revoga, no prazo definido no item 4.4.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil.

O CG da ICP-Brasil ou AC Raiz determina a revogação do certificado da AC OAB quando essa deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

### 4.4.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) por solicitação do titular do certificado;
b) por solicitação do responsável pelo certificado, no caso de certificado de aaplicações e pessoas jurídicas;
c) por solicitação da empresa ou órgão, no caso de certificado fornecido por essa empresa ou órgão para seus empregados, funcionários, servidores, parceiros ou fornecedores;
d) pela AC OAB;
e) pela AR que tiver recebido a solicitação;
f) por determinação do CG da ICP-Brasil ou da AC Raiz.

### 4.4.3. Procedimento para solicitação de revogação

4.4.3.1. 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 OAB ou pela AR Responsável.

A revogação é realizada através de Formulário on-line contendo o motivo da solicitação de revogação mediante o fornecimento de dados e da frase de identificação indicada na solicitação de emissão do Certificado.

Caso o Titular ou o Responsável - no caso de certificados de pessoas jurídicas ou aplicações - não recorde a frase de identificação ou quando a revogação é solicitada diretamente pelo Titular sem a participação do Responsável, o Formulário de revogação é impresso e assinado e entregue na AR Responsável.

Caso o Titular não recorde a frase de identificação, o Formulário de revogação é impresso e assinado e entregue na AR Responsável.

4.4.3.2. 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 OAB;
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 OAB, quando aplicável.

4.4.3.3. O prazo máximo para conclusão do processo final de revogação do certificado pela AC OAB, após a conclusão do processo de aceite e registro da solicitação de revogação é de 12 (doze) horas.

4.4.3.4. Não se aplica.

4.4.3.5. A AC OAB responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido da solicitação de sua revogação e a emissão da LCR correspondente, na forma do item 2.3.2.

4.4.3.6. Não se aplica.

### 4.4.4. Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.4.1 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.

4.4.4.2. Não se aplica.

### 4.4.5. Circunstâncias para suspensão

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

### 4.4.6. Quem pode solicitar suspensão

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

### 4.4.7. Procedimento para solicitação de suspensão

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

### 4.4.8. Limites no período de suspensão

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

### 4.4.9. Frequência de emissão de LCR

4.4.9.1. Neste item é definida a frequência para a emissão de LCR referente a certificados de usuários finais.

4.4.9.2. A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 horas.

4.4.9.3. Não se aplica.
4.4.9.4. Não se aplica.

### 4.4.10. Requisitos para verificação de LCR

4.4.10.1. A verificação da validade do certificado na respectiva LCR é obrigatória, antes do mesmo ser utilizado. A AC OAB suporta requisições OCSP em conformidade com a RFC 6960. A validade da resposta OCSP está limitada ao momento de consulta.

4.4.10.2. Também é obrigatória a verificação da autenticidade da LCR/OCSP, por meio das verificações da assinatura da AC OAB e/ou Certificado OCSP Responder e do período de validade da LCR/OCSP.

### 4.4.11. Disponibilidade para revogação ou verificação de status on-line

A AC OAB suporta os processos de revogação de certificados de forma on-line quando aplicável por força de contratação específica.

A AC OAB 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 OAB, por meio do protocolo OCSP (On-line Certificate Status Protocol).

### 4.4.12. Requisitos para verificação de revogação on-line

Não se aplica.

### 4.4.13. Outras formas disponíveis para divulgação de revogação

Não se aplica.

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

Não se aplica.

### 4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. 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.

4.4.15.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente 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.

## 4.5. Procedimentos de Auditoria de Segurança

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

### 4.5.1. Tipos de eventos registrados

4.5.1.1. A AC OAB 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 OAB;
c) mudanças na configuração dos sistemas AC OAB 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 OAB 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.

4.5.1.2. A AC OAB 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.

4.5.1.3. As informações registradas pela AC OAB são todas as descritas nos itens acima.

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

4.5.1.5. A documentação relacionada aos serviços da AC OAB é armazenada, eletrônica ou manualmente, em local único, de forma estruturada para facilitar o acesso e consulta nos processos de auditoria, para atender a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.1.6. As AR vinculadas à AC OAB registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

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

4.5.1.7. A AC OAB define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

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

A periodicidade com que os registros de auditoria da AC OAB 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.

### 4.5.3. Período de retenção para registros (logs) de auditoria

A AC OAB mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 4.6.

### 4.5.4. Proteção de registro (log) de auditoria

4.5.4.1. 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.

4.5.4.2. 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.

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

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

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

### 4.5.6. Sistema de coleta de dados de auditoria

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

### 4.5.7. Notificação de agentes causadores de eventos

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

### 4.5.8. Avaliações de vulnerabilidade

Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC OAB, são analisados detalhadamente e, dependendo de sua gravidade, registrados em

separado. Ações corretivas decorrentes são implementadas pela AC OAB e registradas para fins de auditoria.

## 4.6. Arquivamento de Registros

### 4.6.1. Tipos de registros arquivados

a) solicitações de certificados;
b) solicitações e justificativas 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 OAB; e
g) informações de auditoria previstas no item 4.5.1.

### 4.6.2. Período de retenção para arquivo

a) as LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade são retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. O prazo de retenção já em curso, quando da alteração desta alínea, será reiniciado; e
c) as demais informações, inclusive os arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

### 4.6.3. Proteção de arquivo

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

### 4.6.4. Procedimentos para cópia de segurança (backup) de arquivo

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

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

4.6.4.3. A AC OAB verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

### 4.6.5. Requisitos para datação (time-stamping) 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.

### 4.6.6. Sistema de coleta de dados de arquivo

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

### 4.6.7. Procedimentos para obter e verificar informação de arquivo

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

## 4.7. Troca de chave

4.7.1. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico, disponibilizado pela AR Responsável, por onde é encaminhado o processo de fornecimento de novo certificado.

A AR que recebeu e validou o pedido de emissão do certificado envia uma comunicação ao titular do certificado, 30 (trinta) dias antes da data de expiração do mesmo, junto com instruções para a solicitação de um novo certificado.

A comunicação de expiração, junto com as instruções para a solicitação de um novo certificado é realizada através de e-mail enviado ao titular do certificado.

4.7.2. Não se aplica.

## 4.8. Comprometimento e Recuperação de Desastre

A AC OAB possui um Plano de Continuidade de Negócios testado anualmente para garantir a continuidade de seus serviços críticos.

### 4.8.1. Recursos computacionais, *software*, e 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 OAB, 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 o mesmo 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.

### 4.8.2. Certificado de entidade é revogado

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

### 4.8.3. Chave da entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC OAB, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com a Supervisão de PKI da AC OAB, 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 OAB estiver encerrando suas atividades – DPC Item 4.9.

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

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 OAB;
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.

#### 4.8.5. Atividades das Autoridades de Registro

As AR vinculadas à AC OAB possuem um Plano de Continuidade de Negócios testado anualmente para garantir a recuperação, total ou parcial das atividades das AR, contendo, no mínimo as seguintes informações:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios;
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. Atenção especial é dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;
d) documentação dos processos e procedimentos acordados;
e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
f) teste e atualização dos planos.

### 4.9. Extinção dos serviços de AC, AR ou PSS

4.9.1. Observado o disposto no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], este item descreve os requisitos e procedimentos adotados nos casos de extinção dos serviços da AC OAB ou de uma AR ou PSS a ela vinculados.

4.9.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC OAB 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 OAB:

a) Comunicará publicamente a extinção dos serviços da AC OAB, através de publicação em jornal de grande circulação.
b) Revogará todos os certificados gerados pela AC OAB 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 OAB extinta seguindo o procedimento descrito na DPC Item 6.2.9.
f) Transferirá os dados e gravações da AC OAB para a Autoridade Certificadora sucessora, aprovada pela AC Raiz. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.
g) Transferirá as chaves públicas dos certificados emitidos pela AC OAB 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 OAB. 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 OAB.
i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

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

a) Comunicará publicamente a extinção dos serviços de AR vinculada AC OAB, através de publicação em jornal de grande circulação.
b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados;
c) Ficará responsável pela guarda dos documentos, dados e registros relativos aos pedidos de emissão de certificados para a AC OAB, devendo fornecê-los sempre que solicitada pelo

Titular, ou pela AC OAB. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.

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

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

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

# 5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

## 5.1. Controles Físicos

### 5.1.1. Construção e localização das instalações

5.1.1.1. A localização e o sistema de certificação da AC OAB 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 nas instalações de AC

A AC OAB possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e os requisitos que seguem.

#### 5.1.2.1 Níveis de acesso

5.1.2.1.1. A AC OAB possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC OAB;

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC OAB. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC OAB transitam devidamente identificadas e acompanhadas.

Nenhum tipo de processo operacional ou administrativo da AC OAB é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC OAB em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo,

som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC OAB. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC OAB.

Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível.

Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa 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: identificação individual, por meio de cartão eletrônico, e identificação biométrica.

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

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC OAB tais como emissão e revogação de certificados e emissão de LCR e a disponibilidade à resposta a consulta OCSP. 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, é exigido, 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 sendo ocupado.

5.1.2.1.9. No quarto nível, todas as paredes, piso e 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 as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas foram sanadas por normas internacionais pertinentes.

5.1.2.1.11. Na AC OAB, 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).

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

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

a) confeccionado em aço;
b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da AC OAB são armazenados nesses depósitos.

#### 5.1.2.2 Sistemas físicos 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 são armazenadas por um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) trimestralmente, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados 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 o critério mínimo de ocupação deixa de ser satisfeito, devido à saída de um ou mais empregados, 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 estão localizados em ambiente de nível 3 e são permanentemente monitorados por guarda armado. As instalações do sistema de monitoramento estão sendo monitoradas, por sua vez, por câmera de vídeo que permite acompanhar as 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 são implantados pela AC OAB para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os mecanismos e procedimentos de emergência são verificados, semestralmente, por meio de simulação de situações de emergência.

### 5.1.3. Energia e ar condicionado nas instalações de AC

5.1.3.1. A infraestrutura do ambiente de certificação da AC OAB 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 OAB e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC OAB.

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

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

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

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

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

### 5.1.4. Exposição à água nas instalações de AC

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

### 5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

5.1.5.1. Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente 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 OAB não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só abre quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC OAB, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

### 5.1.6. Armazenamento de mídia nas instalações de AC

A AC OAB atende às normas NBR 11.515 e NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados ").

### 5.1.7. Destruição de lixo nas instalações de AC

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

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

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

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

### 5.1.9. Instalações técnicas de AR

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

## 5.2. Controles Procedimentais

### 5.2.1. Perfis qualificados

5.2.1.1. A AC OAB 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 OAB estabelece 4 perfis distintos para sua operação, atribuídos às seguintes áreas:

*A AC 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.

- 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 de 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 OAB 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 OAB), com base nas necessidades de cada perfil.

5.2.1.4. A AC OAB 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 OAB 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 OAB, 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 OAB requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC OAB podem ser executadas por um único empregado.

#### 5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC OAB tem sua identidade e perfil verificados antes de:

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

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

a) são diretamente atribuídos a um único empregado;
b) não são compartilhados; e
c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC OAB adota padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

### 5.3. Controles de Pessoal

Todos os empregados da AC OAB, das AR e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de titularidade:

a) os termos e as condições do perfil que ocupam;
b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
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 OAB e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme estabelecido 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 das entidades, todo o pessoal da AC OAB e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido, pelo menos, a:

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

5.3.2.2. Não se aplica.

### 5.3.3. Requisitos de treinamento

Todo o pessoal da AC OAB e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC OAB e das AR vinculadas;
b) sistema de certificação em uso na AC OAB;
c) procedimentos de recuperação de desastres e de continuidade do negócio;
d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma dos itens 3.1.9, 3.1.10 e 3.1.11; e
e) outros assuntos relativos a atividades sob sua responsabilidade.

### 5.3.4. Frequência e requisitos para reciclagem técnica

O pessoal da AC OAB e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre mudanças tecnológicas nos sistemas da AC OAB.

### 5.3.5. Frequência e sequencia de rodízio 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, ser realizada por pessoa encarregada de processo operacional da AC OAB ou de uma AR vinculada, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas e legais cabíveis.

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

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

5.3.6.3. Concluído o processo administrativo, a AC OAB encaminha suas conclusões à AC Raiz.

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

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

#### 5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC OAB e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

#### 5.3.8. Documentação fornecida ao pessoal

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

a) A DPC da AC OAB;
b) a PC correspondente;
c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
d) documentação operacional relativa a suas atividades; e
e) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela AC OAB e é mantida atualizada.

## 6. CONTROLES TÉCNICOS DE SEGURANÇA

### 6.1. Geração e Instalação do Par de Chaves

#### 6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da AC OAB é gerado pela própria AC OAB, após ter sido credenciada e autorizada a funcionar no âmbito da ICP-Brasil.

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

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

O par de chaves da AC OAB é gerado em módulo criptográfico de hardware no padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no DOC-ICP-01.01.

Somente os titulares dos certificados emitidos pela AC OAB geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC OAB.

6.1.1.3. Cada PC implementada pela AC OAB define o meio utilizado para armazenamento da chave privativa, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

#### 6.1.2. Entrega da chave privada à entidade titular

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. A AC OAB entrega cópia de sua chave pública para a AC Certisign em formato PKCS #10. Essa entrega é feita por representante legal constituído da AC OAB, em cerimônia especifica, em data e hora previamente estabelecida.

6.1.3.2. Os usuários finais enviam suas chaves públicas a AC OAB por meio eletrônico em formato PKCS#10, através de uma sessão segura fixada pelo Secure Socket Layer (SSL).

Os procedimentos específicos aplicáveis estão detalhados nas PC implementadas.

### 6.1.4. Disponibilização de chave pública da AC para usuários

A AC OAB disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, através endereço Web:
http://icp-brasil.certisign.com.br/repositorio/certificados/AC_OABG2.p7c (para cadeia V2) e
http://icp-brasil.certisign.com.br/repositorio/certificados/AC_OAB_G3.p7c (para cadeia V5) .

### 6.1.5. Tamanhos de chave

6.1.5.1. Cada PC implementada pela AC OAB 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. O tamanho mínimo das chaves criptográficas associadas aos certificados da AC OAB é de RSA 4096 bits (cadeias V2 e V5) conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

### 6.1.6. Geração de parâmetros de chaves assimétricas

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

### 6.1.7. Verificação da qualidade dos parâmetros

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

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

6.1.8.1. As chaves da AC OAB são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

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

6.1.9.1. Os certificados de assinatura emitidos pela AC OAB têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC OAB, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

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

## 6.2. Proteção da Chave Privada

A AC OAB implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas. Controles Lógico e Procedimental estão descritos no item 5.2. Controle de acesso físico está descrito no item 5.1.2.

A chave privada da AC OAB 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 OAB, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado da suas chaves privadas.

### 6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC OAB adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [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 AC OAB exige controle múltiplo para utilização da sua chave privada.

6.2.2.2. É necessária a presença de pelo menos 3 (três) de um grupo de 10 (dez) funcionários de confiança, com perfis qualificados para a utilização da chave privada da AC OAB.

### 6.2.3. Recuperação (escrow) de chave privada

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

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

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

6.2.4.2. A AC OAB mantém cópia de segurança de sua chave privada.

6.2.4.3. A AC OAB, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC.

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. Não são arquivadas chaves privadas de assinatura digital.

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

### 6.2.7. Método de ativação de chave privada

A ativação das chaves privadas das AC OAB é coordenada pela Supervisão de PKI, onde 3 de um grupo de 10 funcionários com perfis qualificados da AC OAB, 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 OAB contendo fotografia, nome, e departamento do funcionário.

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

### 6.2.8. Método de desativação de chave privada

A chave privativa da AC OAB, 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 OAB.

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 OAB contendo fotografia, nome, e departamento do funcionário.

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

### 6.2.9. Método de destruição de chave privada

A Supervisão de PKI da AC OAB, 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 OAB, 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 OAB contendo fotografia, nome, e departamento do funcionário. O representante legal da AC OAB é identificado através de cédula de identidade ou passaporte, se estrangeiro.

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

## 6.3. Outros Aspectos do Gerenciamento do Par de Chaves

### 6.3.1. Arquivamento de chave pública

As chaves públicas da AC OAB e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

### 6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC OAB são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

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

6.3.2.4. A validade admitida para certificados da AC OAB é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo 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. Cada PC implementada descreve os requisitos específicos aplicáveis.

### 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 OAB são únicos e aleatórios.

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

### 6.4.2. Proteção dos dados de ativação

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

### 6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

## 6.5. Controles de Segurança Computacional

### 6.5.1. Requisitos Técnicos Específicos de Segurança Computacional

6.5.1.1. A geração do par de chaves da AC OAB 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 do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC OAB são descritos em cada PC implementada.

6.5.1.3. O ambiente computacional da AC OAB 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 OAB;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC OAB;
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 OAB;
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 mecanismos de segurança física.

6.5.1.5. As informações sensíveis contidas nos equipamentos são retiradas dos equipamentos para manutenção.

Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controladas. Ao retornar às instalações da AC OAB, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade da AC OAB, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em caráter permanente. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Equipamentos utilizados pela AC OAB são preparados e configurados como previsto na Política de Segurança da AC OAB ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

### 6.5.2. Classificação da segurança computacional

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

### 6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

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

a) controle de acesso lógico ao sistema operacional;
b) exigência de uso de senhas fortes;
c) diretivas de senha e de bloqueio de conta;
d) logs de auditoria do sistema operacional ativados, registrando:
    i. iniciação e desligamento do sistema;

ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
iii. mudanças na configuração da estação;
iv. tentativas de acesso (login) e de saída do sistema (logoff);
v. tentativas não autorizadas de acesso aos arquivos de sistema;
vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

e) antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
f) firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
h) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

## 6.6. Controles Técnicos do Ciclo de Vida

A AC OAB desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

### 6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC OAB 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 OAB 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 OAB proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC OAB.

### 6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC OAB 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. A AC OAB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

### 6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

### 6.6.4. Controles na Geração de LCR

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

## 6.7. Controles de Segurança de Rede

### 6.7.1. Diretrizes Gerais

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

6.7.1.2. Nos servidores do sistema de certificação da AC OAB, 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 OAB.

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

### 6.7.3. Sistema de detecção de intrusão (IDS)

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

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

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

### 6.7.4. Registro de acessos não-autorizados à rede

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

### 6.8. Controles de Engenharia do Módulo Criptográfico

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

## 7. PERFIS DE CERTIFICADO E LCR

### 7.1. Diretrizes Gerais

7.1.1. Nos seguintes itens desta DPC são descritos os aspectos dos certificados e LCR emitidos pela AC OAB.

7.1.2. As seguintes PCs:

• Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora OAB, PC A3 da AC OAB, OID 2.16.76.1.2.3.28

Implementadas pela AC OAB especificam o formato dos certificados gerados e das correspondentes LCR. Nessas PCs são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1.3. Não se aplica.

### 7.2. Perfil do Certificado

Os certificados emitidos pela AC OAB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

#### 7.2.1. Número de versão

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

#### 7.2.2. Extensões de certificado

Não se aplica.

#### 7.2.3. Identificadores de algoritmo

Não se aplica.

#### 7.2.4. Formatos de nome

Não se aplica.

#### 7.2.5. Restrições de nome

Não se aplica.

#### 7.2.6. OID (Object Identifier) de DPC

O OID desta DPC é 2.16.76.1.1.36.

#### 7.2.7. Uso da extensão "Policy Constraints"

Não se aplica.

#### 7.2.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

#### 7.2.9. Semântica de processamento para extensões críticas

Não se aplica.

### 7.3. Perfil de LCR

#### 7.3.1. Número(s) de versão

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

#### 7.3.2. Extensões de LCR e de suas entradas

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

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

a) "**Authority Key Identifier"**, não crítica, contém o hash SHA-1 da chave pública da AC OAB que assina a LCR. As suítes de assinatura utilizadas na ICP-Brasil, baseiam-se no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];

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

## 8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

### 8.1. Procedimentos de mudança de especificação

Alterações nesta DPC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC OAB. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização do CG da ICP-Brasil.

Esta DPC é atualizada sempre que uma nova PC implementada pela AC OAB o exigir.

### 8.2. Políticas de publicação e notificação

A AC OAB mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web:
http://icp-brasil.certisign.com.br/repositorio/dpc/AC_OAB/DPC_AC_OAB.pdf .

### 8.3. Procedimentos de aprovação

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

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

## 9. DOCUMENTOS REFERENCIADOS

9.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

| Ref. | Nome do documento | Código |
|---|---|---|
| [2] | CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL | DOC-ICP-09 |
| [3] | CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL | DOC-ICP-08 |
| [6] | CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTODAS ENTIDADES INTEGRANTES DA ICP-BRASIL | DOC-ICP-03 |
| [7] | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL | DOC-ICP-04 |
| [8] | POLÍTICA DE SEGURANÇA DA ICP-BRASIL | DOC-ICP-02 |

9.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

| Ref. | Nome do documento | Código |
|---|---|---|
| [1] | CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL | DOC-ICP-03.01 |
| [9] | PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL | DOC-ICP-01.01 |
| [10] | PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL | DOC-ICP-05.02 |
| [11] | REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP BRASIL – SISTEMA BIOMÉTRICO DA ICPBRASIL | DOC-ICP-05.03 |
| [12] | REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS | DOC-ICP-01.02 |

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

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