

**Declaração de Práticas de Negócios
da Autoridade de Registro
AR AASP
vinculada às cadeias da Autoridade
Certificadora Valid**

1. INTRODUÇÃO

Este documento tem por objetivo divulgar as práticas de negócio adotadas pela AR AASP, credenciada sob as cadeias da AC VALID, no que diz respeito à atividade de Certificação Digital padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

A DPN foi elaborada de acordo com os princípios e critérios da WebTrust para Autoridades de Certificação: <https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/Overview-of-WebTrust-services/Principles-and-criteria>

2. VISÃO GERAL

A Declaração de Práticas de Negócio (DPN) descreve as práticas e os procedimentos empregados pela Autoridade de Registro enquanto credenciadas na Estrutura de Certificação de Digital das Autoridades Certificadoras, suas políticas encontram-se disponíveis no repositório da AC VALID: <https://validcertificadora.com.br/pages/repositorio>

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Para a emissão de certificados digitais ICP-Brasil, é necessário realizar a identificação dos requerentes na solicitação de certificados, e essa identificação é feita por um agente de registro devidamente treinado e contratado por Autoridade de Registro vinculada à AC VALID.

As autoridades de registro atuam na validação, emissão e entrega do certificado digital indicadas neste Manual. Essa atividade pode ser realizada de forma presencial, por videoconferência ou renovação online. Para os casos presenciais e videoconferência, os agentes de registro identificam os solicitantes dos certificados, desde que cumpridos todos os requisitos indicados neste Manual de AR e no Manual Operacional do Agente de Registro, registram essa etapa no sistema disponibilizado pela VALID.

A seguir digitalizam os documentos recebidos do titular, disponibilizando-os em sistema, para as etapas seguintes do processo. A etapa de Verificação e liberação de emissão dos certificados digitais é realizada pela própria VALID, para aqueles casos que não possuem match biométrico, e, em caso de dúvidas, os devolve para que o agente de registro da AR vinculada os corrija e/ou complemente.

Somente depois que todos os documentos forem considerados corretos, a central de verificação libera a emissão do certificado, após a verificação, o agente de registro da AR vinculada orienta o titular na emissão e instalação do seu certificado digital.

4. AQUISIÇÃO DO CERTIFICADO DIGITAL

O interessado poderá requisitar seu certificado digital por meio de e-commerce da AR ou AC VALID (<https://www.validcertificadora.com.br>) ou via televendas (3004-3454 para Capitais e regiões metropolitanas e 0800-725-4565 para as demais localidades).

5. CONTATOS

RESPONSÁVEL PELA AR: André Luiz Ferreira

RAZÃO SOCIAL: Associação dos Advogados de São Paulo

ENDEREÇO: Rua Álvares Penteado n. 151 - Centro

TELEFONE: 11 3291-9200

E- MAIL: andre.ferreira@aasp.com.br

PÁGINA WEB: www.aasp.org.br

6. OBRIGAÇÕES E RESPONSABILIDADES DA AR

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante, realizar a validação biométrica e a validade da solicitação;
- c) presenciar a assinatura do Termo de Titularidade e responsabilidade, pelo Titular do Certificado e pelo Responsável (nos casos de emissão de certificados SSL);
- d) encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável utilizando protocolo de comunicação seguro;
- e) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- f) disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;
- g) identificar e registrar todas as ações executadas;
- h) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil e *WebTrust Principles and Criteria for Registration Authorities*
- i) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas leis aplicáveis;
- j) proceder o reconhecimento das assinaturas e da validade dos documentos de identificação apresentados;
- k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em localidades de atendimento vinculadas credenciadas.
- l) oferecer treinamento aos seus agentes de registro, especialmente quanto ao recolhimento de assinaturas e a validade dos documentos apresentados;
- m) comunicar a AC a qual está vinculada imediatamente, em caso de tentativa ou execução de fraude qualquer de suas instalações técnicas ou localidades de atendimento;
- n) comunicar ao titular de um certificado válido, em prazo anterior, a data de expiração deste, para que seja solicitada a emissão de um novo certificado;

- o) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR.

7. OUTRAS ATIVIDADES DESEMPENHAS PELA AR

Outras atividades complementares realizadas pelas AR's vinculadas à VALID são:

- a) Venda de produtos de certificação digital;
- b) Controle de estoques dos produtos; e
- c) Fornecimento de informações à AC vinculada e aos titulares de certificado digital, quando solicitadas.

8. TITULARES DE CERTIFICADO

Pessoas físicas ou jurídicas, de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das políticas da AC, aplicáveis, podem ser Titulares de Certificado.

Os certificados podem ser utilizados por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações, sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada, e se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

9. AGENDAMENTO DA EMISSÃO

Após conclusão compra do certificado pelo cliente, ainda no e-commerce ou televendas, o cliente deverá realizar o agendamento podendo a emissão ser por videoconferência, presencial ou renovação online.

10. DOCUMENTOS NECESSÁRIOS

A documentação solicitada para emissão do certificado digital será de acordo com o tipo de produto requisitado, podendo o cliente consultar no momento da compra (pelo site ou televendas), sendo todas em sua versão original e/ou digital, em caso de documento digital o mesmo deverá ter barramento eletrônico, tendo a possibilidade de consulta da veracidade do mesmo.

A. CERTIFICADO PESSOA FÍSICA DO TIPO A1, A3:

Documento de identificação

B. CERTIFICADO PESSOA JURÍDICA DO TIPO A1, A3:

Documento de identificação dos sócios e responsável pelo uso do Certificado Digital;
Cartão CNPJ da empresa;
Documento societário da empresa (Contrato/Estatuto e Ata de eleição e/ou alteração consolidada);
Procuração (se for o caso).

C. EQUIPAMENTOS / BANCÁRIO / SERVIDORES:

Registro do domínio ou termo de autorização do uso do domínio, assinado;

Documentos para pessoa jurídica; e

CSR/URL/DOMÍNIO com os dados correspondentes da empresa.

Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia, que por força de Lei, equivalem a documentos de identidade em todo território nacional, como por exemplo a CNH, Passaporte, Carteira de Identidade e etc.

11. PROCESSO DA EMISSÃO

O agente de registro (profissional contratado pela AR) atenderá o cliente para verificar se os documentos apresentados não possuem pendências e se estes de fato correspondem à pessoa que se apresenta naquele momento.

Os documentos originais serão digitalizados, para compor o dossiê do processo de emissão do certificado, e será realizada a coleta biométrica da face e digitais do cliente, que também integrarão o referido dossiê.

Tratando-se de certificado de equipamento, será verificado se o solicitante detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço.

Para certificados que façam o uso de CSR será solicitada a assinatura manuscrita ou digital com certificado digital ICP-Brasil do responsável no Termo de Titularidade.

12. PROCESSO DE RENOVAÇÃO

O cliente será contatado quando aproximada a data de expiração de seu certificado digital. No caso de e-CPF será autorizada a renovação online uma única vez, por meio do site da AC VALID, desde que o certificado digital não tenha expirado.

Para qualquer outro tipo de certificado digital; e-CPF que já tenha feito renovação online; ou e-CPF que já tenha expirado o cliente deverá seguir conforme o processo de aquisição inicial de um novo certificado digital.

13. PROCESSO DE REVOGAÇÃO

REVOGAÇÃO OBRIGATÓRIA:

- ✓ Quando constatada emissão imprópria ou defeituosa do mesmo;
- ✓ Quando for necessária a alteração de qualquer informação constante no mesmo;
- ✓ No caso de dissolução da AC VALID; ou
- ✓ No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

QUEM PODE SOLICITAR A REVOGAÇÃO:

- ✓ Por solicitação do titular do certificado;
- ✓ Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
- ✓ Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- ✓ Pela AC VALID;
- ✓ Pela AR;
- ✓ Por determinação do Comitê Gestor da ICP-Brasil ou da AC Raiz.

Para que o certificado seja revogado o solicitante da revogação de um certificado deve ser identificado e todas as ações decorrentes desse processo serão registradas e armazenadas. As justificativas serão documentadas e o processo será concluído com a geração e a publicação de uma Lista de Certificados Revogados – LCR, que contenha o certificado em questão e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC VALID.

Após a revogação do certificado, o solicitante pode solicitar um novo certificado, enviando à AR uma solicitação, na forma, condições e prazo estabelecidos para a solicitação inicial de um certificado.

14. OBRIGAÇÕES DO TITULAR DO CERTIFICADO DIGITAL

Constituem-se obrigações do titular de certificado emitido sob a cadeia AC VALID:

- ✓ Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação e assumir a responsabilidade pelo custo do processo de emissão do certificado;
- ✓ Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos e utilizar obrigatoriamente senha para proteção da chave privada do certificado;
- ✓ Utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na Política de Certificação correspondente;
- ✓ Conhecer os seus direitos e obrigações, contemplados pela Declaração de Política de Certificação da AC VALID, pela Política de Certificação correspondente e por outros documentos aplicáveis da ICP-Brasil;
- ✓ Responsabilizar-se por todos os atos praticados perante a AC VALID utilizando o referido certificado e sua correspondente chave privada;
- ✓ Informar à AC VALID qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

15. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante ou pelo próprio titular no site da VALID para aqueles clientes que possuem a senha de revogação.

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 ou pela confirmação da senha que o próprio cliente criou no momento da emissão do certificado.

16. TRATAMENTO DE DADOS

Todas as informações e documentos obtidos em decorrência dos processos de emissão, renovação e revogação serão armazenados, mantidos em sigilo conforme os padrões de segurança estabelecidos pela ICP-Brasil.

Os dados não serão utilizados para outros fins, salvo em caso de autorização expressa do cliente ou titular do certificado, ou em casos de determinação judicial e outros casos previstos em lei.

17. OUTRAS INFORMAÇÕES

A AC VALID é detentora do selo de padrões internacionais *WebTrust* e replica todos os critérios e processos à sua rede de Autoridades Certificadoras credenciadas, bem como suas Declarações de Práticas de Certificação (DPC), Políticas de Certificados (PC) e sua Política de Segurança (PS).

18. REFERÊNCIAS

- ✓ ITI/ Instituto nacional de tecnologia – DOC-05, DOC-05.02, DOC-05.05 e DOC-03.01:
<https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais>
- ✓ CA/ Browser Forum – WebTrust SM/TM Principles and Criteria for Registration Authorities:
<https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais>