Transformação Digital

Construindo a Visão 360° do Cidadão Cearense

Guia de Entrada na Interoperabilidade

Primeiros Passos para **novos órgãos** entrarem na **Plataforma de Interoperabilidade**

Incluindo o fluxo de **emissão dos certificados**

Versão 2.0 (março 2026)

íris | Laboratório de Inovação e Dados

CEARÁ GOVERNO DO ESTADO

Transformação Digital

Construindo a Visão 360° do Cidadão Cearense

Este documento tem o objetivo de esclarecer o processo para um órgão ingressar na **plataforma de interoperabilidade**, incluindo acesso aos ambientes de homologação (para testes) e produção (dados reais).

íris | Laboratório de Inovação e Dados

CEARÁ GOVERNO DO ESTADO

Classificação da Informação: Documento
Restrito

- Se você deseja **trocar dados** e incluir novos **serviços digitais** por meio da **interoperabilidade**, é necessário **cadastrar seu órgão na plataforma**.

- Para seu órgão ter acesso ao ambiente de produção é preciso **criar um servidor de segurança**

- Para criar um servidor de segurança são utilizados **dois tipos de certificados SSL**: **autenticação e assinatura**

Classificação da Informação: Documento
Restrito



Enquanto as etapas para gerar os certificados acontecem, é possível **conhecer as funções** da plataforma de interoperabilidade em um **ambiente de homologação.**

Classificação da Informação: Documento
Restrito

Como funciona o ambiente de homologação?

Para usar o **ambiente de homologação** serão emitidos certificados em uma cadeia de homologação (configurado pela Valid). Neste caso, não é necessário passar por todas as etapas do fluxo de emissão.

Ou seja, é possível **testar as funções** da plataforma de interoperabilidade em homologação, enquanto os certificados para uso em produção são emitidos.

Como acessar o ambiente de homologação?

Após configurar o servidor de segurança, será liberado acesso a um **usuário administrador**, que terá permissão para cadastrar novos usuários.

Informações necessárias para criação do usuário administrador:

- Entidade/órgão;
- Nome;
- E-mail;
- Telefone (Celular/Whatsapp).

O que faz o usuário administrador?

- Gerenciamento de usuários
  - Criar;
  - Excluir;
  - Redefinir senha.
- Gestão de certificados
  - Geração de CSR;
  - Importação de certificados.
- Gestão de subsistemas
  - Criar;
  - Registrar;
  - Excluir.

O que é possível fazer no ambiente de homologação?

- Configurar novos serviços
- Consumir serviços de outras entidades
- Validar integrações com o servidor de segurança

⚠️ No ambiente de homologação, deve-se usar serviços vinculados a **bases de dados de teste**.



Para acessar o ambiente em **produção**, é **obrigatório** gerar os certificados SSL.

A seguir, apresentamos quais são os **certificados necessários** e todas as **etapas de criação** deles.

Classificação da Informação: Documento
Restrito

Quais são os certificados necessários?

Para uma nova entidade fazer parte da **plataforma de interoperabilidade** (X-Valid), é necessário criar um **servidor de segurança** para a troca segura de informações.

No servidor de segurança são usados **dois tipos de certificados SSL**:

 **Autenticação:** cria canais seguros de comunicação entre os membros.

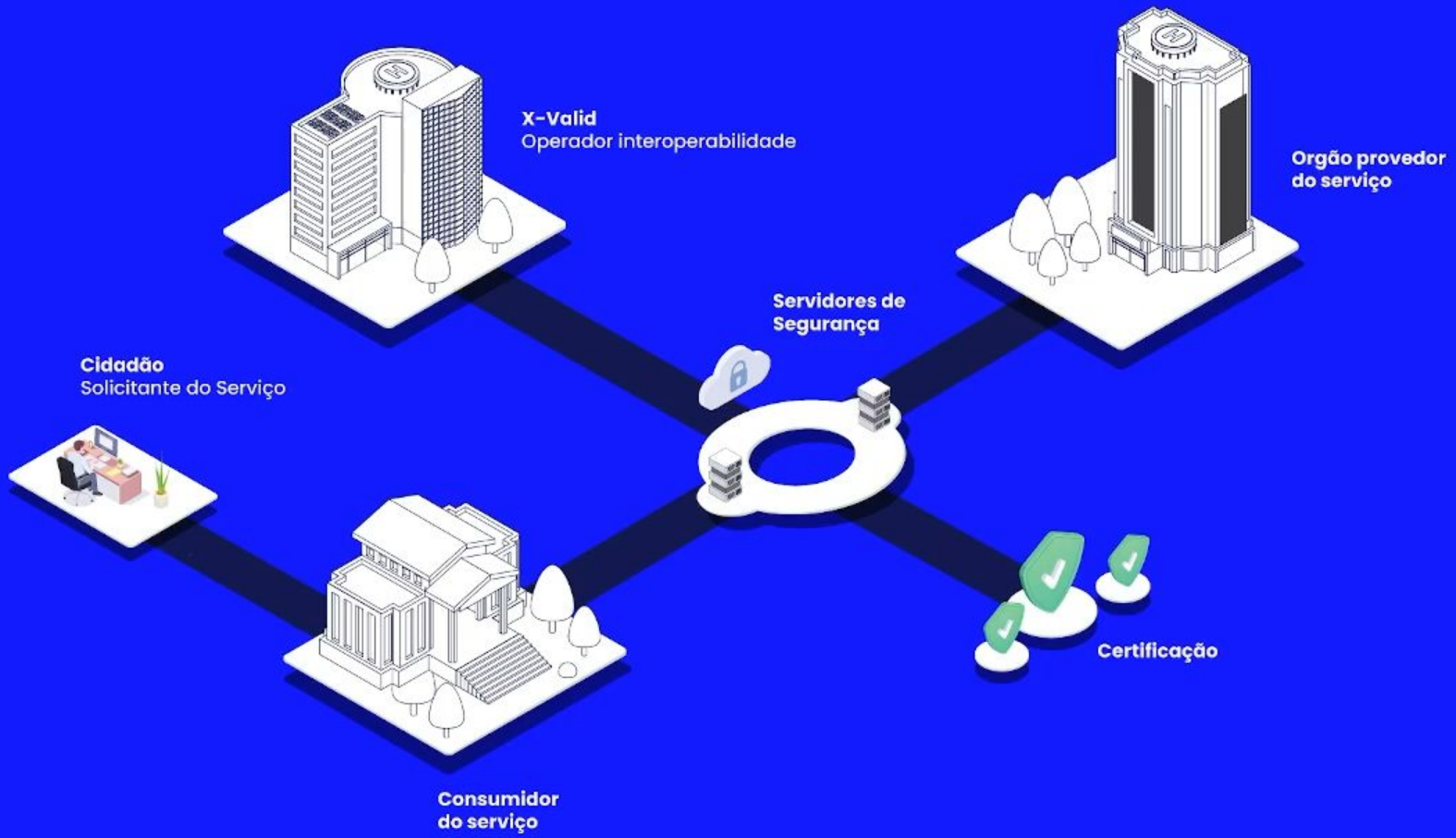
 **Assinatura:** garante auditoria com validade jurídica, pois assina todas as mensagens recebidas e enviadas.

Quem emite e qual a validade dos certificados?

A Infraestrutura de Chaves Públicas Brasileiras (**ICP-Brasil**) é a entidade oficial do Brasil para a emissão de certificados digitais, por meio da **Autoridade Certificadora Valid**.

A ICP-Brasil emite os certificados de autenticação e de assinatura.
A validade máxima do certificado é de **1 ano**.

V/Cert


X-Valid
Operador interoperabilidade
Orgão provedor do serviço
Servidores de Segurança
Cidadão
Solicitante do Serviço
Certificação
Consumidor do serviço

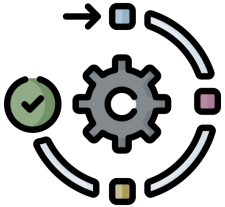
Fluxo de Emissão de Certificado Digital

íris | Laboratório de Inovação e Dados

CEARÁ GOVERNO DO ESTADO

Fluxo de Emissão de Certificado Digital

12 Etapas



1. Envio dos documentos obrigatórios;
2. Análise dos documentos;
3. Geração das CSRs no Servidor de Segurança;
4. Agendamento do atendimento;
5. Atendimento on-line;
6. Geração do termos de titularidade e responsabilidade;
7. Assinatura dos termos;
8. Validação dos termos;
9. Emissão do certificado;
10. Importação no Servidor de Segurança;
11. Solicitação de registro do Certificado de Autenticação;
12. Aprovação do registro do Certificado de Autenticação.

1. Envio dos documentos obrigatórios

Quem deve executar essa etapa?

O órgão que deseja fazer parte da plataforma ou que deseja renovar o seu certificado.

Quais os documentos obrigatórios para Pessoa Jurídica?

📄Ato Constitutivo, sendo Estatuto ou Contrato Social em vigor, registrado em órgão competente;

📄Documento de eleição de seus administradores;

📄Cartão do CNPJ (emitido pelo site da Receita Federal no máximo há 5 dias).

Representante legal (titular do órgão)

🪪 Carteira Nacional de Habilitação (CNH original e colorida);

📱 Telefone celular;

📩 E-mail para envio do link da vídeo chamada.

Para onde enviar os documentos? sac.xvalid@valid.com

2. Análise de Documentos



Quem deve executar essa etapa?

Valid Certificadora.

Como acontece?

Nesta etapa, o time especializado da Valid analisa detalhadamente e valida os documentos enviados, para garantir que todas as normativas exigidas pelo ICP-Brasil sejam atendidas.

3. Geração das CSRs no Servidor de Segurança

Quem deve executar essa etapa?

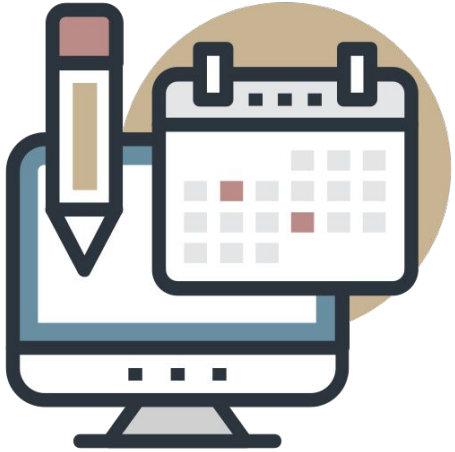
A **Valid** ou o administrador do servidor de segurança.

Como acontece?

O administrador deve acessar o servidor de segurança para gerar duas CSRs, sendo uma para autenticação e outra para assinatura. No menu **Gerenciamento**, clicar na opção **Chaves e Certificados**. Em seguida, clicar no botão **+ Gerar Chave e CSR** e seguir os passos:

1. Escolher o uso da chave: Autenticação ou Assinatura
2. Escolher o tipo de chave: RSA (2048)
3. Escolher o serviço de certificação: AC VALID SSL EV
4. Inserir o nome da chave: Pode adicionar o nome do órgão
5. Escolher o formato: PEM (base64)
6. Clicar no botão **GERAR**

4. Agendamento do Atendimento



Quem deve executar essa etapa?

Valid Certificadora

Como acontece?

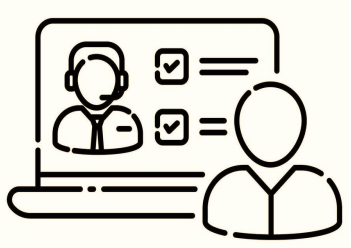
A Valid entra em contato com o **representante legal** do órgão para agendar o atendimento.

Durante o atendimento, será realizada uma **vídeo chamada** para verificações de legitimidade, atendendo as normativas da ICP-Brasil.

5. Atendimento On-line

Quem deve executar essa etapa?

Valid Certificadora e Representante Legal do Órgão



Como acontece?

No horário agendado, o **representante legal** receberá um **e-mail com um *link*** para entrar na vídeo chamada. O *link* é válido por somente **15 minutos**, então é muito importante a pontualidade no atendimento.

Durante o atendimento, a Valid pedirá para o representante legal criar uma senha. Esta senha será solicitada depois para emitir o certificado.

Guarde a senha com segurança! Se você perder ou esquecer a senha, será necessário fazer uma nova vídeo chamada.

6. Geração dos termos de titularidade e responsabilidade



Quem deve executar essa etapa?

Valid Certificadora.

Como acontece?

Quando o atendimento online terminar, a Valid irá gerar um **Termo de Titularidade e Responsabilidade**.

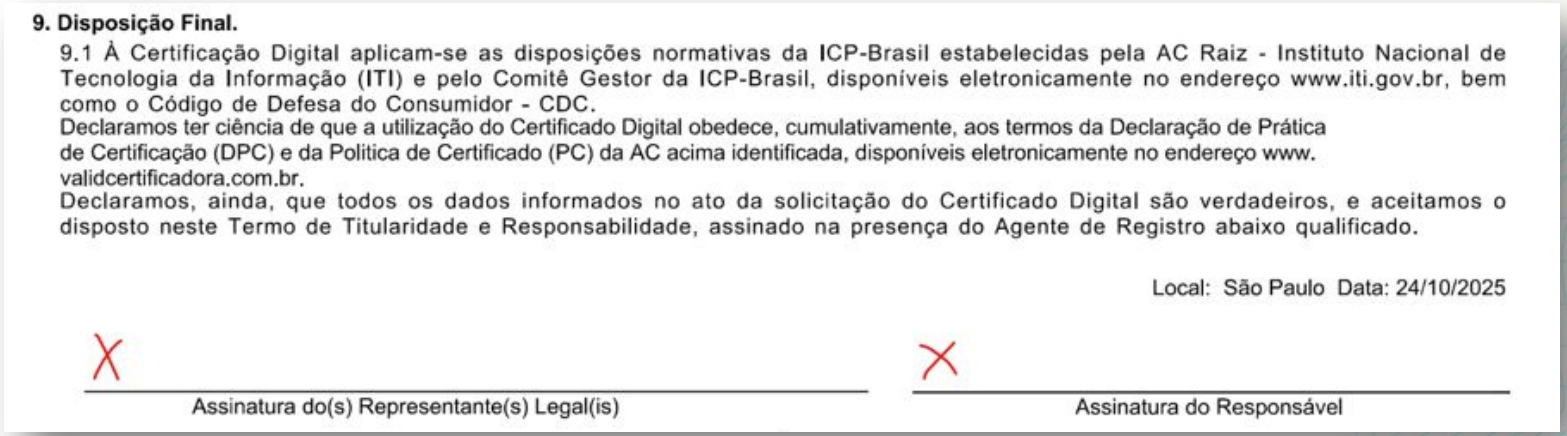
Este Termo será enviado para o **e-mail** do representante legal para **assinatura**.

7. Assinatura dos termos

Quem deve executar essa etapa? Representante legal do órgão

Como acontece?

Quando receber o termo, o representante legal deverá assinar o documento nos campos **Assinatura do Representante Legal** e **Assinatura do Responsável**.



9. Disposição Final.

9.1 À Certificação Digital aplicam-se as disposições normativas da ICP-Brasil estabelecidas pela AC Raiz - Instituto Nacional de Tecnologia da Informação (ITI) e pelo Comitê Gestor da ICP-Brasil, disponíveis eletronicamente no endereço www.iti.gov.br, bem como o Código de Defesa do Consumidor - CDC.

Declaramos ter ciência de que a utilização do Certificado Digital obedece, cumulativamente, aos termos da Declaração de Prática de Certificação (DPC) e da Politica de Certificado (PC) da AC acima identificada, disponíveis eletronicamente no endereço www.validcertificadora.com.br.

Declaramos, ainda, que todos os dados informados no ato da solicitação do Certificado Digital são verdadeiros, e aceitamos o disposto neste Termo de Titularidade e Responsabilidade, assinado na presença do Agente de Registro abaixo qualificado.

Local: São Paulo Data: 24/10/2025

X _____

Assinatura do(s) Representante(s) Legal(is)

X _____

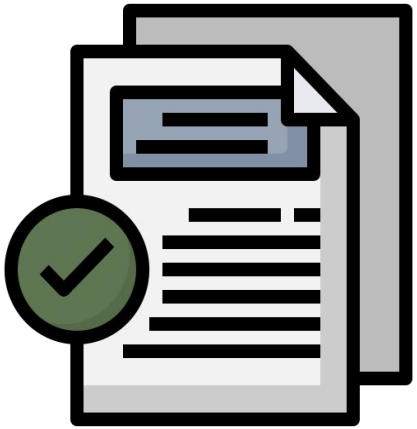
Assinatura do Responsável

📆 O termo tem validade de **7 dias** e **deve ser assinado dentro deste período**.

✍️ A assinatura pode ser digital utilizando um **certificado digital** de pessoa física, ou através do **GOV.BR**, por exemplo.

📩 O documento assinado deve ser **devolvido como resposta ao e-mail** que o representante legal recebeu.

8. Validação dos Termos



Quem deve executar essa etapa?

Valid Certificadora.

Como acontece?

O time da Valid Certificadora valida o documento recebido e libera o certificado para emissão, se estiver tudo de acordo com as exigências legais.

O representante legal receberá **um e-mail** informando o passo a passo final para emitir o certificado.

9. Emissão do certificado



Quem deve executar essa etapa?

O representante legal ou a equipe do órgão que está entrando agora no sistema (com conhecimento da senha de emissão).

Como acontece?

Ao acessar o link enviado no e-mail, uma tela será aberta e será necessário informar o **ticket** (consta no e-mail) e a **senha**. Assim, é possível seguir as etapas indicadas no sistema até a emissão do certificado.

9. Emissão do certificado



O certificado ficará salvo no computador em um **arquivo .cer**.

Este arquivo deve ser enviado para os administradores responsáveis pelo cadastro do Servidor de Segurança.

Observação: o arquivo consiste apenas na chave pública do certificado. A chave privada está protegida no servidor de segurança.

10. Importação no Servidor de Segurança

Quem deve executar essa etapa?

A **Valid** Certificadora ou o administrador do servidor de segurança.

Como acontece?

O certificado emitido deve ser importado para o servidor de segurança em questão.



11. Solicitação de Registro do Certificado de Autenticação



Quem deve executar essa etapa?

A **Valid** Certificadora ou o administrador do servidor de segurança.

Como acontece?

Para registrar um Certificado de Autenticação, primeiro o certificado deve ser importado. Após, é necessário solicitar o registro.

12. Aprovação do registro do Certificado de Autenticação



Quem deve executar essa etapa?

A Valid Certificadora.

Como acontece?

O administrador da plataforma receberá a solicitação de registro. Ele deve avaliar os dados contidos e realizar a aprovação.

Desta forma, o servidor de segurança estará apto e seguro para ser utilizado em produção ✅

Para trocar dados com outras entidades, o órgão deverá seguir o normativo de **Governança de Compartilhamento de Dados** (Decreto nº 37.059/2026 e da Resolução nº 01/2026)

Classificação da Informação: Documento
Restrito

Transformação Digital

Construindo a Visão 360° do Cidadão Cearense

íris | Laboratório de Inovação e Dados

CEARÁ
GOVERNO DO ESTADO

Classificação da Informação: Documento
Restrito