2. Geração da requisição de certificado

O Certificate Signing Request (CSR) é um arquivo de texto criptografado contendo as informações para a solicitação do Certificado Digital. O CSR contém as informações da Instituição (nome, departamento, cidade, estado, país) e a URL onde o certificado SSL será utilizado (Common Name).

Para obter certificados digitais para os serviços computacionais é necessário:

- Chave Privada RSA 2048 bits;
- Uma requisição de certificado CSR;
- Compatibilidade com SHA-256.

A ferramenta OpenSSL é usada para criar a Chave Privada (arquivo .key) e a Solicitação de Assinatura de Certificado (arquivo .csr). Ambas devem ser geradas conforme os comandos abaixo.

- Geração da chave privada:

```
openssl genpkey -algorithm RSA -out exemplo.ifsertao-pe.edu.br.key -pkeyopt
rsa_keygen_bits:2048
```

- Geração da requisição de certificado CSR:

```
openssl req -new -key exemplo.ifsertao-pe.edu.br.key -out exemplo.ifsertao-pe.edu.br.csr
```

O comando anterior requisitará as informações da Instituição para a Solicitação de Assinatura de Certificado. Os campos devem ser preenchidos conforme o servidor que receberá a certificação, no caso do exemplo abaixo, um servidor web identificado pelo domínio **exemplo.ifsertao-pe.edu.br** (campo Common Name):

```
Country name (2 letter code) [xx]: BR
State or province name (full name) []: Pernambuco
```

```
Locality name (eg, City) [Default City]: Cidade
Organization Name (eg, company) [Default Company Ltd]: IFSertaoPE
Organizational Unit Name (eg, section) [ ]: Campi
Common Name (eg your name or your server's hostname) []: exemplo.ifsertao-pe.edu.br
Email Address: []: email.solicitante@ifsertao-pe.edu.br
A challenge password []:
An optional company name []:
```

Observar o seguinte no preenchimento dos campos anteriores:

- Os seguintes caracteres não são aceitos: < > ~ ! @ # $ % ^ * / \ ( ) ?.,&;
- O campo "Common Name" deve ser o nome completo (o domínio) do serviço cadastrado no DNS, ou seja, a exata URL onde o certificado vai ser utilizado;
- O campo "Organization Name" deve ser o nome oficial da Instituição, igual ao existente no cartão do CNPJ;
- Os campos "A challenge password" e "An optional company name" podem ficar em branco.

O arquivo .csr será gerado, sendo possível conferir os dados informados na requisição utilizando o comando:

```
openssl req -inform PEM -in exemplo.ifsertao-pe.edu.br.csr -text
```

É recomendado armazenar os arquivos **exemplo.ifsertao-pe.edu.br.key** e **exemplo.ifsertao-pe.edu.br.csr** em um local seguro, mantendo backup deles.

Revision #2
Created 9 September 2020 12:55:05
Updated 12 May 2026 21:57:23 by Tiago Siqueira Freire