

# Como configurar DNSSEC em seu domínio <sup>1</sup>

David Robert Camargo de Campos

Rafael Dantas Justo

<tutorial-dnssec@registro.br>

Registro.br

---

<sup>1</sup>

versão 1.5.0 (Revision)

A última versão deste tutorial pode ser encontrada em: [ftp://ftp.registro.br/pub/doc/configuracao\\_dnssec\\_dominio.pdf](ftp://ftp.registro.br/pub/doc/configuracao_dnssec_dominio.pdf)

- O objetivo deste tutorial é implantar DNSSEC no servidor autoritativo para determinado domínio
- Todas as operações serão executadas no servidor principal (*Master*)

## Requisitos

- Bind 9.7 – <http://www.isc.org/downloads>

## Utilização do comando `dnssec-keygen` para geração de chaves:

```
$ dnssec-keygen -r /dev/urandom -f KSK dominio.com.br
```

Onde, **dominio.com.br** deve ser substituído pelo seu domínio.

- O comando irá gerar dois arquivos com extensões `.key` e `.private`

Mais informações podem ser encontradas no Tutorial de DNSSEC

### Utilização do comando `dnssec-signzone` para assinatura

```
$ dnssec-signzone -S -z -o dominio.com.br db.dominio.com.br
```

Onde, `dominio.com.br` deve ser substituído pelo nome do domínio e `db.dominio.com.br` pelo nome do arquivo de zona.

- O comando irá gerar um novo arquivo de zona com a extensão `.signed`
- O período de validade padrão da assinatura é de 30 dias

Mais informações podem ser encontradas no [Tutorial de DNSSEC](#)

### Alteração da referência para o arquivo de zona

```
zone "dominio.com.br" {  
    type master;  
    file "/etc/namedb/db.dominio.com.br.signed";  
    ...  
};
```

Onde, **dominio.com.br** deve ser substituído pelo nome do domínio e **db.dominio.com.br** deve ser substituído pelo nome do arquivo de zona.

Reiniciar o Bind



Copiar os dados de **KeyTag** e **Digest** do arquivo **dsset-dominio.com.br** para a interface no site do Registro.br.

**Exemplo:** `$ cat dsset-dominio.com.br | head -1`

```
dominio.com.br  IN DS      KeyTag      5  1  Digest
                15469      5EC0184678E0B7DC3AACFFA5D0EB9DBA1F3F6C37
```

- Onde, **dominio.com.br** deve ser substituído pelo nome do domínio

#### DNSSEC

| Record | KeyTag               | Digest               |
|--------|----------------------|----------------------|
| DS 1   | <input type="text"/> | <input type="text"/> |
| DS 2   | <input type="text"/> | <input type="text"/> |

Aguardar nova publicação no site do Registro.br



- 1 Criar chave (dnssec-keygen) (slide 3)
- 2 Assinar a zona (dnssec-signzone) (slide 4)
- 3 Modificar o named.conf (slide 5)
- 4 Reiniciar o BIND (named) no servidores Master
- 5 Adicionar o DS no site do Registro.br (slide 7)
- 6 Aguardar nova publicação

## Servidor Autoritativo

Reassinar a zona antes das assinaturas expirarem

- 1 Incrementar o serial (record SOA) do arquivo de zona original
- 2 Reassinar a zona utilizando o comando `dnssec-signzone`

# Perguntas?

<http://registro.br/tecnologia/dnssec/tutoriais/>

Envie suas dúvidas para [tutorial-dnssec@registro.br](mailto:tutorial-dnssec@registro.br)