

O que é DNS e como ele funciona?

O **DNS (Domain Name System)** é como uma "agenda de contatos" da internet. Ele traduz os nomes dos sites que digitamos (como `www.exemplo.com`) em endereços IP (como `192.0.2.1`), que são os números que os computadores usam para se comunicar entre si.

Por que isso é importante?

Imagine se você tivesse que lembrar o número IP de cada site que visita. Seria como lembrar o número de telefone de todos os seus amigos sem poder usar os nomes deles. O DNS facilita isso, permitindo que você use nomes fáceis de lembrar.

Passo a passo de como o DNS funciona:

1. Você digita um site no navegador

Exemplo: `www.exemplo.com`

2. Seu computador pergunta ao DNS qual é o IP desse site

Ele envia essa pergunta para um servidor DNS.

3. O servidor DNS procura a resposta

Se ele não souber, ele pergunta para outros servidores até encontrar o IP correto.

4. O IP é devolvido para o seu computador

Agora seu navegador sabe para onde ir.

5. Você acessa o site

Com o IP em mãos, seu computador se conecta ao servidor do site e carrega a página.

Resumo

O DNS é essencial para tornar a navegação na internet simples e rápida. Sem ele, teríamos que memorizar números em vez de nomes de sites.

Delegação de Domínios

A **delegação** acontece quando você quer que uma parte do seu domínio seja gerenciada por outro servidor DNS. É como dizer:

“Essa parte do meu site será cuidada por outro responsável.”

Exemplo prático:

Você tem o domínio `empresa.com.br` e quer que o subdomínio `blog.empresa.com.br` seja gerenciado por outro serviço (como um provedor de hospedagem).

Você então **cria registros NS (Name Server)** para `blog.empresa.com.br`, apontando para os servidores DNS do provedor.

Resultado:

Quando alguém acessa `blog.empresa.com.br`, o DNS sabe que precisa perguntar aos servidores do provedor para obter os dados corretos.

Reapontamento de Registros DNS

O **reapontamento** é quando você muda o destino de um registro DNS. Isso pode ser feito por vários motivos, como:

- Mudar o servidor de hospedagem
- Redirecionar o tráfego para outro serviço
- Atualizar o IP de um servidor

Exemplo prático:

Você tem um registro `www.empresa.com.br` que aponta para o IP `192.0.2.1`.

Se você mudar de servidor, pode atualizar esse registro para apontar para `203.0.113.5`.

Tipos comuns de registros que podem ser reapontados:

- **A:** Aponta para um IP
 - **CNAME:** Aponta para outro nome de domínio
 - **MX:** Aponta para servidores de e-mail
 - **TXT:** Usado para validações (como SPF, DKIM)
-

Resumo

- **Delegação:** Você entrega o controle de uma parte do domínio para outro servidor DNS.
- **Reapontamento:** Você muda o destino de um registro DNS para refletir uma nova configuração ou serviço.

O que é DNSSEC?

DNSSEC significa **Domain Name System Security Extensions**.

É uma extensão do DNS tradicional que adiciona **segurança** às consultas DNS, protegendo contra ataques como o *spoofing* ou *cache poisoning*.

Problema que o DNSSEC resolve:

O DNS comum não verifica se a resposta que você recebeu veio de uma fonte confiável. Isso abre brechas para que atacantes enviem respostas falsas, redirecionando você para sites maliciosos.

Como o DNSSEC funciona:

- Ele usa **assinaturas digitais** para garantir que os dados DNS não foram alterados.
 - Quando você consulta um domínio protegido por DNSSEC, o servidor DNS envia junto uma **assinatura criptográfica**.
 - Seu resolvedor DNS verifica essa assinatura usando uma **cadeia de confiança**, que começa na raiz do DNS.
-

O que são registros DS?

O **registro DS (Delegation Signer)** é um tipo especial de registro DNS usado **na delegação segura de domínios** com DNSSEC.

Função do DS:

- Ele **liga** a zona pai (por exemplo, .br) à zona filha (por exemplo, empresa.com.br) de forma segura.
- Contém um **hash da chave pública** usada para assinar os registros DNS da zona filha.
- Permite que a cadeia de confiança do DNSSEC continue da raiz até o seu domínio.

Exemplo prático:

Se você tem o domínio empresa.com.br e quer ativar o DNSSEC:

1. Você gera um par de chaves (pública e privada).
 2. Usa a chave privada para assinar seus registros DNS.
 3. Cria um registro **DS** com o hash da chave pública.
 4. Envia esse DS para o **registro.br** (a zona pai), que o publica.
 5. Agora, qualquer consulta ao seu domínio pode ser verificada até a raiz, garantindo autenticidade.
-

Resumo

- **DNSSEC** protege o DNS contra falsificações, usando criptografia.
- **Registros DS** são essenciais para conectar a segurança entre domínios e subdomínios, mantendo a cadeia de confiança.