Shape

Description automatically generated with medium confidence

**Master in <<** **NAME OF THE MASTER >>**

**Network and Information Systems Security**

**Authors**:

***Name***: Gulit Duarte Costa Fernandes, ***Nº*** 129229

***Name***: Leonel Antonio Domingos Cassul, ***Nº*** 140236

***Name***: Marcos do Nascimento do Espirito Santo, ***Nº*** 129236

***Name***: Adilson Candjara Gomes Wambar, ***Nº*** 128942

***Name***: Quintino Quade Junior , ***Nº*** 131706

***Nome***: Tchancarna Midé 137620

**Date**: 29-10-2025

**Title of the work**: DNSSEC

**Teacher**: Valderi Reis Quietinho Leithardt

**Índice**

[***Glossary*** 3](#_Toc212642234)

[***Introduction*** 3](#_Toc212642235)

[***Development*** 4](#_Toc212642236)

[***Benefícios:*** 20](#_Toc212642237)

[***SIG (Transaction Signature)*** 21](#_Toc212642238)

[TSIG (Transaction Signature) 21](#_Toc212642239)

[***Como funciona:*** 21](#_Toc212642240)

[***Benefícios:*** 21](#_Toc212642241)

[Conclusions 22](#_Toc212642242)

[References 23](#_Toc212642243)

# ***Glossary***

DNS: Sistema de Nomes de Domínio

DNSSEC: Extensões de segurança ao protocolo DNS

IP : Protocolo de Internet

IPv4: IP versão 4

IPv6: IP versão 6

RFCs : Request for Comments:

# ***Introduction***

Nesse trabalho o objetivo é descrever o funcionamento do DNSSEC (é um conjunto de extensões que adicionam segurança ao protocolo DNS (Sistema de Nomes de Domínio)).

# ***Development***

O protocolo do [Sistema de Nomes de Domínio (DNS](https://www.ibm.com/br-pt/topics/dns)) permite que os usuários naveguem pela internet usando nomes de host em vez de endereços IP numéricos. O DNS funciona como uma lista telefônica da internet: ele simplifica o processo de encontrar sites específicos por meio de navegadores.

Quando um cliente DNS faz uma solicitação de DNS usando um nome de host, como www.example.com, uma série de funções conecta essa solicitação ao endereço IP correspondente. Essas funções fornecem a autenticação de endereços IP (IPv4 e IPv6) e tornam o uso da Internet mais acessível, traduzindo nomes de domínio personalizáveis em endereços numéricos complexos.

Para executar essas funções, o protocolo DNS depende de quatro tipos de [servidores DNS](https://www.ibm.com/br-pt/topics/dns-server) que, quando operam corretamente, tornam o processo rápido e seguro. Servidores DNS utilizam [registros DNS](https://www.ibm.com/br-pt/topics/dns-records) registros como A e [registros CNAME](https://www.ibm.com/br-pt/topics/cname?_ga=2.24685690.1703755890.1710244943-168385799.1679007172&_gl=1*1c5ceda*_ga*MTY4Mzg1Nzk5LjE2NzkwMDcxNzI.*_ga_FYECCCS21D*MTcxMDI1MTYyNy40MDUuMS4xNzEwMjUxNzQ5LjAuMC4w), que contêm as informações que orientam o processo de resolução para encaminhar corretamente as solicitações DNS. Esses registros são arquivos em formato de texto chamados de “arquivos de zona”, escritos na sintaxe do DNS.

Os registros de recursos de DNS são armazenados em servidores DNS confiáveis, também conhecidos como servidores de nomes autoritários. Eles contêm informações relacionadas ao domínio, incluindo quanto tempo o servidor manterá os registros DNS em cache, um período conhecido como vida útil (TTL). Esses registros permitem a vinculação de domínios e subdomínios e o roteamento adequado de e-mails, auxiliam na segurança do DNS e muito mais.

***Funcionamento do protocolo DNS[Parte do Leonel Cassule]***

Tal como numa lista telefónica, em que tenho um nome associado ao numero telefónica

Ex:

|  |  |  |
| --- | --- | --- |
| Id | Nome do Contacto | Nº do Telemóvel |
| 01 | Leonel Cassul | +351 960 00 000 |
| 02 | António Domingos | + 244 964 000 000 |
| 03 | Judite Manuel | +55 959 956 99 |

Tabela1.1: Lista Telefónica

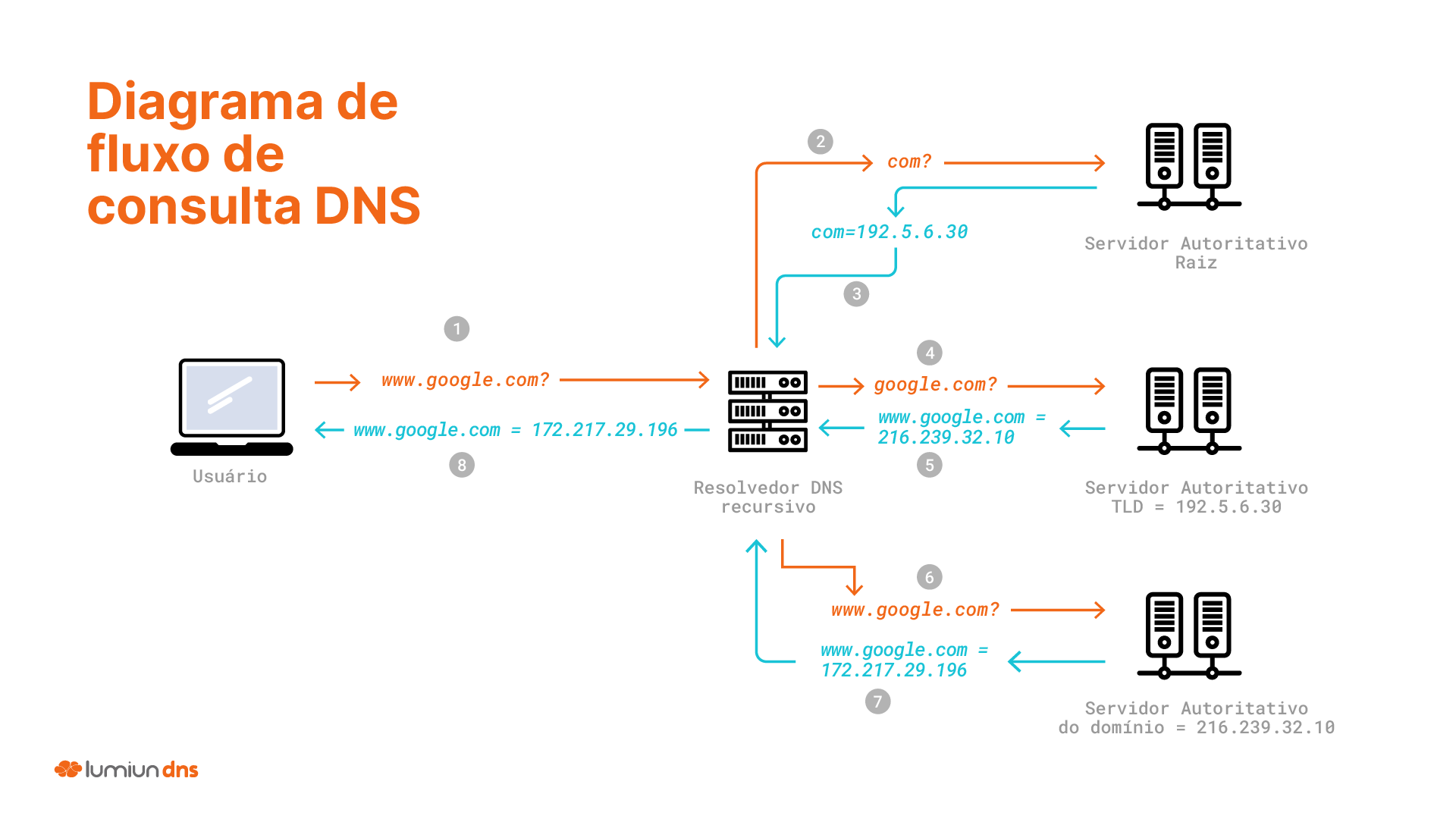
Que torna mais fácil a pesquisa do contacto e a memorização por nome do que por numero, também assim é o funcionamento do Protocolo DNS,

Ao usar um cliente DNS, como seu computador, dispositivo inteligente, qualquer navegador da web ou aplicação para se conectar a um nome de domínio, você aciona o que é conhecido como **consulta recursiva**, solicitação de DNS, pesquisa de DNS ou consulta de DNS.

Quando uma solicitação de registro DNS é feita a partir de um dispositivo como um smartphone, computador ou tablet, um navegador (como o Google Chrome) verifica primeiro o cache do registro. Se **não existir nenhum registro**, um resolvedor no nível do sistema operacional será consultado. Esse componente do sistema operacional, chamado de resolvedor de stub, verifica o registro.

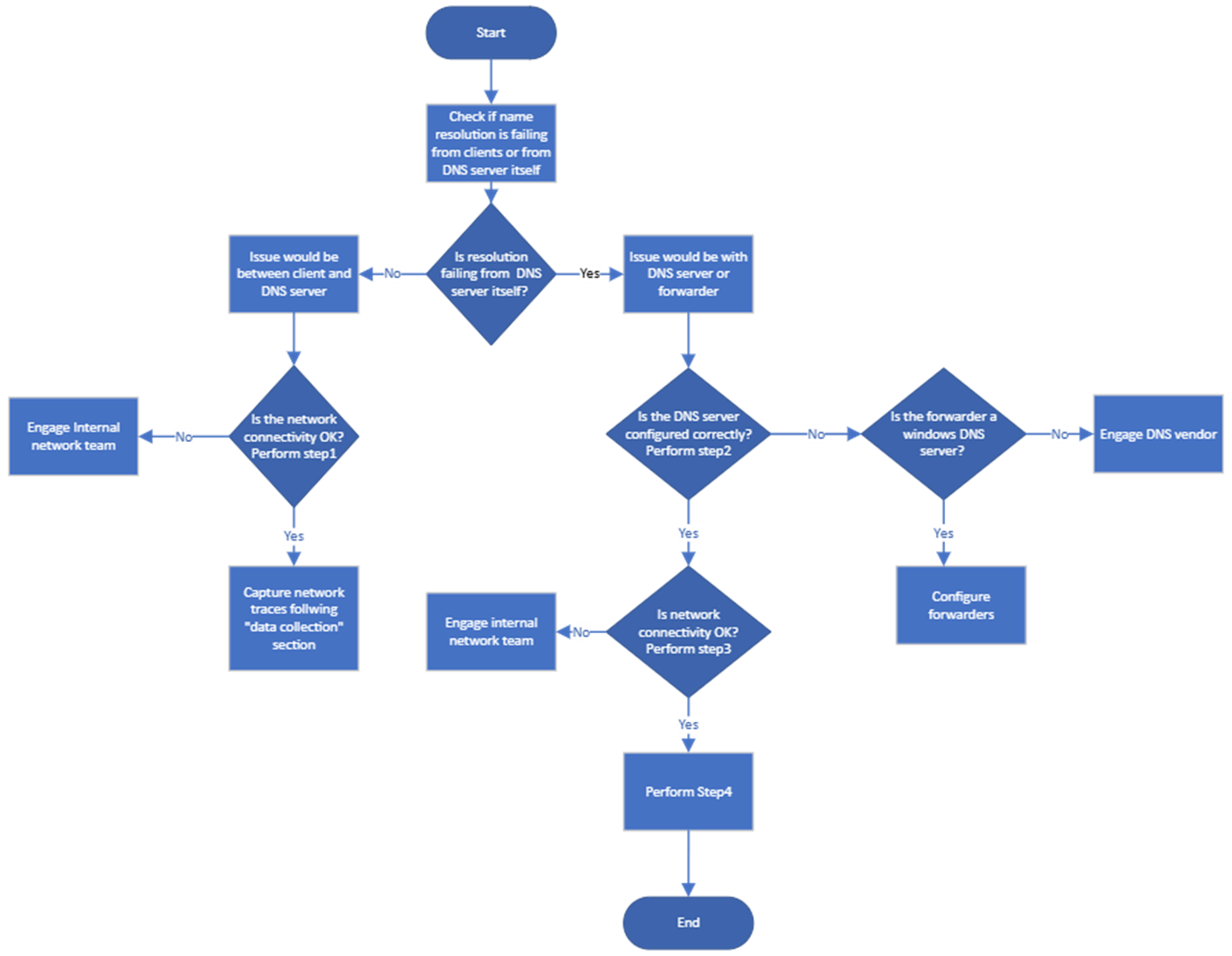
Se o registro solicitado não estiver armazenado em cache no nível local, as consultas de DNS serão direcionadas por meio de uma série de servidores DNS externos que ajudam a resolver a solicitação.  
O primeiro servidor em funcionamento é o servidor **DNS recursivo**, também conhecido como recursor DNS ou resolvedor DNS recursivo, que geralmente é operado por um provedor de serviços de Internet (ISP). Se possível, o resolvedor recursivo usa dados DNS em cache para acessar o site desejado; se esses dados não estiverem disponíveis, ele encaminhará a solicitação para o servidor raiz.

Os servidores raiz, ou servidores DNS raiz, recebem a solicitação e podem roteá-la para um servidor conhecido como domínio de nível superior ou servidor de nomes TLD, com base na extensão do site: .com, .Org ou .net, por exemplo.

Os servidores de nomes TLD recebem solicitações de extensões específicas e as encaminham para o servidor de nomes autoritativo, também conhecido como servidor DNS autoritativo ou servidor de nomes de domínio autoritativo.

O servidor de nomes autoritativo contém informações para a zona DNS que ele gerencia, incluindo informações relacionadas a nomes de domínio específicos armazenados em registros de recursos DNS, e conecta os nomes dos domínios com seus endereços IP correspondentes.

As informações são retornadas ao cliente DNS, completando a resolução de DNS.

Quando o servidor DNS não consegue recuperar uma resposta completa, ele aciona uma consulta DNS iterativa. Os servidores continuarão a enviar a solicitação por meio de servidores diferentes até que um endereço IP seja encontrado ou seja atingido o tempo limite ou algum erro.

***Especificação do protocolo DNS***

***Namespace do domínio***

O namespace do DNS rege os nomes de host do DNS público na internet. O namespace cria uma hierarquia estruturada como uma árvore, e cada nó da árvore tem um rótulo textual e registros de recursos DNS que descrevem o domínio. O nome de domínio é composto pelo **rótulo** junto com o rótulo de suas anotações pai (essas seções são separadas por um ponto, como em "example.com") e é separado em zonas. Cada zona é delegada a uma entidade legal específica para administração e gerenciamento. Essa estrutura permite que os sites recebam nomes exclusivos.

***Sintaxe do nome de domínio***

O nome de domínio cria uma estrutura hierárquica com diferentes níveis. Os nomes de domínio consistem em uma ou mais partes chamadas rótulos e cada parte é separada por um ponto. Os rótulos podem conter até 63 caracteres.

Exemplo: forum.support.example.com

No exemplo acima, ".com" representa o domínio de nível superior, "exemplo" representa o nome do domínio, "suporte" é um subdomínio de "exemplo" e "fórum" é um subdomínio de "suporte".

**Resolvendo uma solicitação DNS**

Um servidor DNS recursivo, também conhecido como recursor DNS ou resolvedor DNS recursivo, se comunica com outros servidores DNS para localizar e retornar um endereço IP. Esse servidor recebe uma consulta DNS e pode conectar o usuário ao site desejado por meio dos dados armazenados em cache. Se os dados do site não forem armazenados em cache, eles enviarão uma solicitação de acompanhamento para os servidores de nomes autoritativos.

O servidor de nomes autoritativo geralmente é a parada final do processo de resolução de uma consulta DNS. Este servidor contém os registros dos recursos de todos os domínios dessa zona. Ocasionalmente, os servidores de nomes autoritativos devem enviar uma solicitação a outro servidor de nomes para encontrar informações sobre subdomínios específicos.

**Formato de mensagem DNS**

As mensagens DNS consistem em consultas e respostas e contêm os seguintes campos:

Um cabeçalho contendo identificação, sinalizadores, o número de perguntas e respostas, o número de registros de recursos de autoridade (RRs) e o número de registros de recursos adicionais.

 Um campo de sinalização que indica o tipo de mensagem e se o servidor de nomes é confiável, o status de uma consulta e se foi recursiva ou truncada.

Uma seção de pergunta com o nome de domínio e o tipo de registro sendo resolvidos.

Uma seção de resposta com os registros de recursos do nome consultado.

***Protocolo de transporte DNS***

O DNS usa o User Datagram Protocol para responder às consultas DNS devido à sua velocidade e baixa sobrecarga. Nas respostas DNS maiores que 512 bytes, ou se um servidor estiver gerenciando transferências de zona (a transferência de registros DNS de servidores DNS primários para secundários) ou tarefas semelhantes, ele usa o protocolo de controle de transmissão (TCP). O TCP permite verificações de integridade dos dados e divide a mensagem em pacotes menores para ajudar a garantir que ela chegue ao seu destino o mais rápido possível.

**Arquivos mestre DNS (arquivos de zona)**

Os arquivos mestres DNS são armazenados em servidores de nomes DNS. São arquivos de texto que definem informações de DNS para uma única zona de DNS, como por exemplo:

Tempo de vida global (TTL): define a quantidade de tempo de armazenamento dos registros em caches DNS locais.

Registro de início de autoridade (SOA): estabelece o servidor de nomes autoritativo primário em relação a uma determinada zona.

Registros de recursos: esses registros são usados para armazenar nomes de host, endereços IP e outras informações em servidores de nomes DNS.

***DNS em escala empresarial***

Em pequena escala, o usuário nem deve perceber que esse processo está acontecendo. Em escala empresarial, entender como o DNS funciona é essencial para manter serviços internos e externos, além de escolher uma [solução de DNS gerenciado](https://www.ibm.com/br-pt/products/ns1-connect?utm_content=SRCWW&p1=Search&p4=43700079202251610&p5=e&gad_source=1&gclid=EAIaIQobChMI3KabyYbShAMVfUpHAR0eWAUJEAAYASAAEgL4PfD_BwE&gclsrc=aw.ds).

Os casos de uso para soluções de DNS gerenciado incluem:

***Multi CDN***

Uma [rede de entrega de conteúdo (CDN)](https://www.ibm.com/br-pt/topics/content-delivery-networks) é uma rede global de servidores que melhora o desempenho de entrega e reduz a [latência](https://www.ibm.com/br-pt/topics/latency). Um sistema multi CDN permite o uso dinâmico de várias CDNs para oferecer o melhor serviço.

***Roteamento geográfico***

As soluções de DNS gerenciado facilitam o roteamento automatizado com base na localização geográfica dos usuários finais, acelerando a rede e o desempenho das aplicações.

***Direção de tráfego de DNS***

O direcionamento de tráfego oferece às organizações o poder de otimizar as conexões com aplicativos, serviços e conteúdos com base nas condições dos dados, cargas e redes de monitoramento de usuários reais (RUM).

***Visão geral do DNSSEC***

O DNSSEC é um conjunto de extensões que adicionam segurança ao protocolo DNS (Sistema de Nomes de Domínio), permitindo que as respostas DNS sejam validadas como genuínas. O DNSSEC fornece autoridade de origem, integridade de dados e negação autenticada de existência. Com o DNSSEC, o protocolo DNS é muito menos suscetível a certos tipos de ataques, particularmente ataques de falsificação de DNS.

**As principais extensões DNSSEC** são especificadas nas seguintes RFCs (Request for Comments):

[RFC 4033](https://datatracker.ietf.org/doc/html/rfc4033): "Introdução e requisitos de segurança DNS"

[RFC 4034](https://datatracker.ietf.org/doc/html/rfc4034): "Registros de recursos para as extensões de segurança DNS"

[RFC 4035](https://datatracker.ietf.org/doc/html/rfc4035): "Modificações de protocolo para as extensões de segurança DNS"

Para obter um resumo das RFCs DNSSEC, consulte [RFC9364](https://www.rfc-editor.org/rfc/rfc9364): DNS Security Extensions (DNSSEC).

***Como funciona o DNSSEC***

As zonas DNS são protegidas com DNSSEC usando um processo chamado assinatura de zona. Assinar uma zona com DNSSEC adiciona suporte à validação sem alterar o mecanismo básico de uma consulta e resposta DNS. Para assinar uma zona com DNSSEC, o servidor DNS autoritativo primário da zona deve suportar DNSSEC.

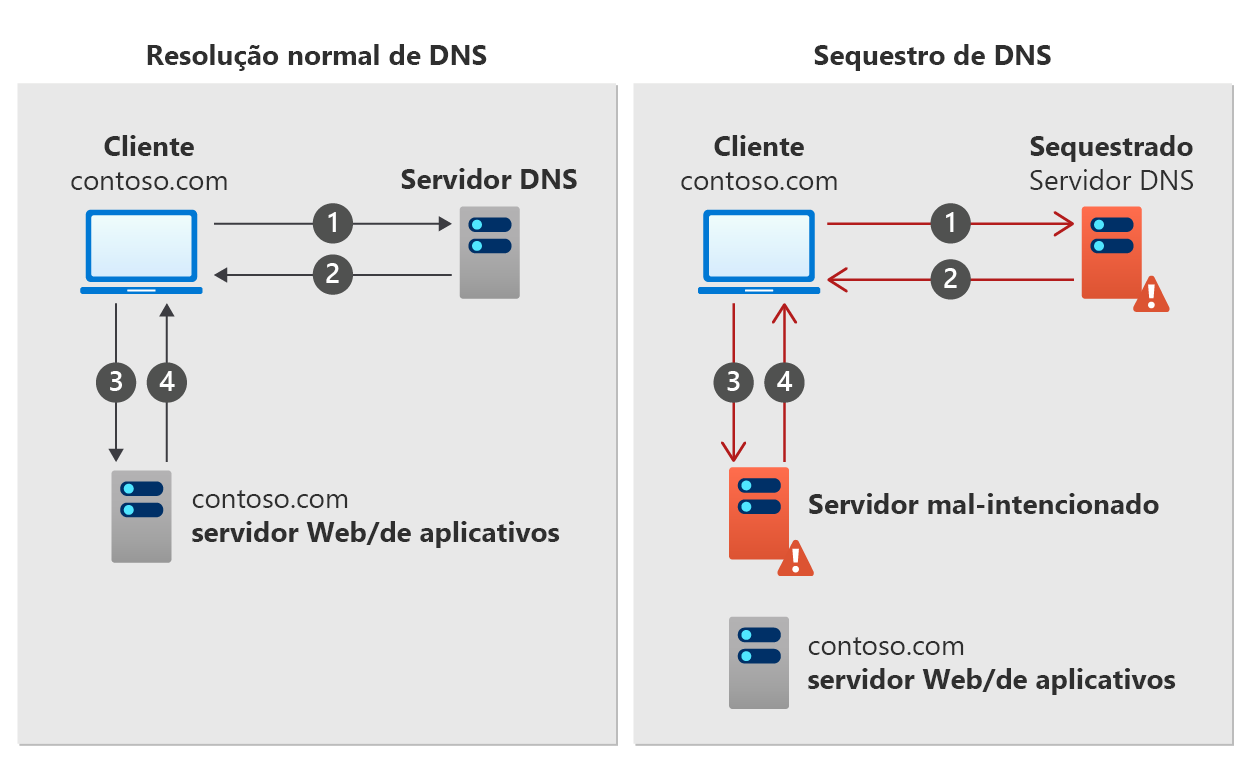
Assinaturas de Registro de Recursos (RRSIGs) e outros registros criptográficos são adicionados à zona quando ela é assinada. A figura a seguir mostra os registros de recursos DNS na zona contoso.com antes e depois da assinatura da zona.



[A validação](https://learn.microsoft.com/pt-pt/azure/dns/dnssec#dnssec-validation) DNSSEC de respostas DNS ocorre usando essas assinaturas digitais com uma cadeia ininterrupta [de confiança](https://learn.microsoft.com/pt-pt/azure/dns/dnssec#chain-of-trust).

 A validação DNSSEC de respostas DNS pode impedir tipos comuns de ataques de sequestro de DNS, também conhecidos como redireccionamento de DNS. O sequestro de DNS ocorre quando um dispositivo cliente é redirecionado para um servidor mal-intencionado usando respostas DNS incorretas (falsificadas). O envenenamento de cache DNS é um método comum usado para falsificar respostas DNS.

Um exemplo de como o sequestro de DNS funciona é mostrado na figura a seguir.



***Resolução DNS normal:***

Um dispositivo cliente envia uma consulta DNS para contoso.com para um servidor DNS.

O servidor DNS responde com um registro de recurso DNS para contoso.com.

O dispositivo cliente solicita uma resposta de contoso.com.

O contoso.com aplicativo ou servidor Web retorna uma resposta ao cliente.

***Sequestro de DNS***

Um dispositivo cliente envia uma consulta DNS para contoso.com para um servidor DNS sequestrado.

O servidor DNS responde com um registro de recurso DNS inválido (falsificado) para contoso.com.

O dispositivo cliente solicita uma resposta para contoso.com do servidor mal-intencionado.

O servidor mal-intencionado retorna uma resposta falsificada para o cliente.

O tipo de registro de recurso DNS falsificado depende do tipo de ataque de sequestro de DNS. Um registro MX pode ser falsificado para redirecionar e-mails de clientes ou um registro A falsificado pode enviar clientes para um servidor Web mal-intencionado.

O DNSSEC funciona para evitar o sequestro de DNS executando a validação em respostas DNS. No cenário de sequestro de DNS mostrado aqui, o dispositivo cliente pode rejeitar respostas DNS não validadas se o domínio contoso.com estiver assinado com DNSSEC. Para rejeitar respostas DNS não validadas, o dispositivo cliente deve impor [a validação](https://learn.microsoft.com/pt-pt/azure/dns/dnssec#dnssec-validation) DNSSEC para contoso.com.

DNSSEC também inclui Next Secure 3 (NSEC3) para evitar a enumeração de zona. A enumeração de zona, também conhecida como caminhada de zona, é um ataque pelo qual o invasor estabelece uma lista de todos os nomes em uma zona, incluindo zonas filhas.

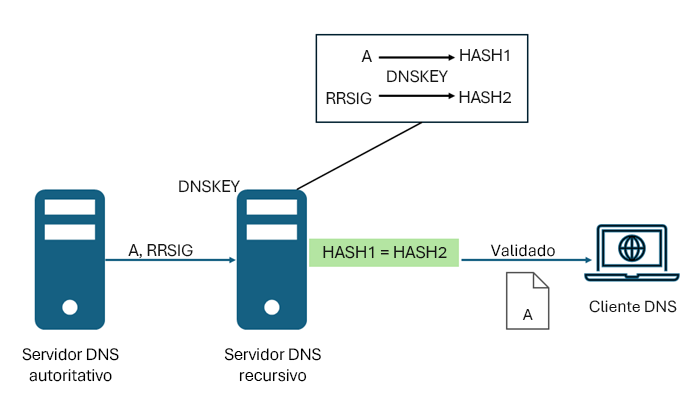
Antes de assinar uma zona com DNSSEC, certifique-se de entender [como o DNSSEC funciona](https://learn.microsoft.com/pt-pt/azure/dns/dnssec#how-dnssec-works). Quando estiver pronto para assinar uma zona, consulte [Como assinar sua zona DNS pública do Azure com DNSSEC.](https://learn.microsoft.com/pt-pt/azure/dns/dnssec-how-to)

***Validação DNSSEC***

Se um servidor DNS reconhece DNSSEC, ele pode definir o sinalizador DNSSEC OK (DO) em uma consulta DNS como um valor de 1. Esse valor informa ao servidor DNS que responde para incluir registros de recursos relacionados ao DNSSEC com a resposta. Esses registros DNSSEC são registros RRSIG (Resource Record Signature) usados para validar que a resposta DNS é genuína.

Um servidor DNS recursivo (não autoritativo) executa a validação DNSSEC em registros RRSIG usando uma âncora de confiança (DNSKEY). O servidor usa uma DNSKEY para descriptografar assinaturas digitais em registros RRSIG (e outros registros relacionados ao DNSSEC) e, em seguida, calcula e compara valores de hash. Se os valores de hash forem os mesmos, ele fornecerá uma resposta ao cliente DNS com os dados DNS solicitados, como um registro de endereço de host

***Veja o diagrama a seguir:***



Se os valores de hash não forem os mesmos, o servidor DNS recursivo responderá com uma mensagem SERVFAIL. Desta forma, servidores DNS capazes de resolver (ou encaminhar) DNSSEC com uma âncora de confiança válida instalada podem proteger contra sequestro de DNS no caminho entre o servidor recursivo e o servidor autoritativo. Essa proteção não exige que os dispositivos cliente DNS reconheçam DNSSEC ou imponham a validação de resposta DNS, desde que o servidor DNS recursivo local (último salto) esteja protegido contra sequestro.

Os dispositivos cliente Windows 10 e Windows 11 não validam [resolvedores](https://learn.microsoft.com/pt-pt/azure/dns/dnssec#dnssec-terminology) de stub com reconhecimento de segurança. Esses dispositivos cliente não executam a validação, mas podem impor a validação do DNSSEC usando a Diretiva de Grupo. [O NRPT](https://learn.microsoft.com/pt-pt/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn593632(v=ws.11)) pode ser usado para criar e impor uma política de validação de DNSSEC baseada em namespace.

***Âncoras de confiança e validação de DNSSEC***

 As âncoras de confiança operam com base na hierarquia de namespace DNS. Um servidor DNS recursivo pode ter qualquer número de âncoras de confiança ou nenhuma âncora de confiança. Âncoras de confiança podem ser adicionadas para uma única zona DNS filho ou qualquer zona pai. Se um servidor DNS recursivo tiver uma âncora de confiança raiz (.), ele poderá executar a validação do DNSSEC em qualquer zona DNS. Para obter mais informações, consulte [Informações](https://www.iana.org/dnssec) sobre o operador da zona raiz.

O processo de validação do DNSSEC funciona com âncoras de confiança da seguinte forma:

Se um servidor DNS recursivo não tiver uma âncora de confiança DNSSEC para uma zona ou o namespace hierárquico pai da zona, ele não executará a validação do DNSSEC nessa zona.

Se um servidor DNS recursivo tiver uma âncora de confiança DNSSEC para o namespace pai de uma zona e receber uma consulta para a zona filha, ele verificará se um registro DS para as zonas filho está presente na zona pai.

Se o registro DS for encontrado, o servidor DNS recursivo executará a validação DNSSEC.

Se o servidor DNS recursivo determinar que a zona pai não tem um registro DS para a zona filho, ele assumirá que a zona filho é insegura e não executa a validação DNSSEC.

Se vários servidores DNS recursivos estiverem envolvidos em uma resposta DNS (incluindo encaminhadores), cada servidor deverá ser capaz de executar a validação DNSSEC na resposta para que haja uma cadeia ininterrupta de confiança.

Os servidores recursivos que têm a validação DNSSEC desabilitada ou não reconhecem DNSSEC não executam a validação.

***Cadeia de confiança***

Uma cadeia de confiança ocorre quando todos os servidores DNS envolvidos no envio de uma resposta para uma consulta DNS são capazes de validar que a resposta não foi modificada durante o trânsito. Para que a validação do DNSSEC funcione de ponta a ponta, a cadeia de confiança deve ser ininterrupta. Essa cadeia de confiança se aplica a servidores autoritativos e não autoritativos (recursivos).

***Servidores autorizados***

Os servidores DNS autoritativos mantêm uma cadeia de confiança através da utilização de registos de signatário de delegação (DS). Os registros DS são usados para verificar a autenticidade de zonas filhas na hierarquia DNS.

Para que a validação do DNSSEC ocorra em uma zona assinada, o pai da zona assinada também deve ser assinado. A zona pai também deve ter um registro DS para a zona filho.

Durante o processo de validação, o pai de uma zona é consultado para o registro DS. Se o registro DS não estiver presente, ou os dados do registro DS no pai não corresponderem aos dados DNSKEY na zona filho, a cadeia de confiança será quebrada e a validação falhará.

***Servidores recursivos***

Os servidores DNS recursivos (também chamados de servidores DNS de resolução ou armazenamento em cache) mantêm uma cadeia de confiança através do uso de âncoras de confiança DNSSEC.

A âncora de confiança é um registro DNSKEY, ou registro DS contendo um [hash](https://learn.microsoft.com/pt-pt/dotnet/standard/security/ensuring-data-integrity-with-hash-codes) de um registro DNSKEY. O registro DNSKEY é criado em um servidor autoritativo quando uma zona é assinada e removido da zona se a zona não estiver assinada.

As âncoras de confiança devem ser instaladas manualmente em servidores DNS recursivos.

Se uma âncora de confiança para uma zona pai estiver presente, um servidor recursivo poderá validar todas as zonas filho no namespace hierárquico. Isso inclui consultas encaminhadas. Para dar suporte à validação DNSSEC de todas as zonas DNS assinadas pelo DNSSEC, você pode instalar uma âncora de confiança para a zona raiz.

***Substituição de chaves***

A chave de assinatura de zona (ZSK) em uma zona assinada por DNSSEC é periodicamente substituída (substituída) automaticamente pelo Azure. Não deve ser necessário substituir a chave de assinatura de chave (KSK), mas esta opção está disponível contactando o suporte da Microsoft. A substituição do KSK requer que você também atualize seu registro DS na zona pai.

***Algoritmo de assinatura de zona***

As zonas são assinadas por DNSSEC usando o algoritmo de assinatura digital de curva elíptica (ECDSAP256SHA256).

***Registos de recursos relacionados com DNSSEC***

A tabela a seguir fornece uma breve descrição dos registros relacionados ao DNSSEC. Para obter informações mais detalhadas, consulte [RFC 4034: Registros de recursos para as extensões](https://datatracker.ietf.org/doc/html/rfc4034) de segurança DNS e [RFC 7344: Automatizando a manutenção](https://datatracker.ietf.org/doc/html/rfc7344) de confiança da delegação DNSSEC.

***Exibir registros de recursos relacionados ao DNSSEC***

Os registros relacionados ao DNSSEC não são exibidos no portal do Azure. Para exibir registros relacionados ao DNSSEC, use ferramentas de linha de comando, como Resolve-DnsName ou dig.exe. Essas ferramentas estão disponíveis usando o Cloud Shell ou localmente, se instaladas no seu dispositivo. Certifique-se de definir o sinalizador DO em sua consulta usando a -dnssecok opção em Resolve-DnsName ou a +dnssec opção em dig.exe.

***DNSSEC vs. segurança do DNS***

O DNSSEC e a segurança do DNS são conceitos relacionados no âmbito da segurança da internet, cada um com um foco e um escopo distintos. O DNSSEC refere-se especificamente a um conjunto de extensões de DNS projetadas para fortalecer a segurança do Sistema de Nomes de Domínio. Seu principal objetivo é garantir a integridade e a autenticidade dos registros do DNS por meio de criptografia de chave pública e privada.

A segurança do DNS é um termo mais amplo que engloba uma abordagem abrangente para proteger todo o ambiente do DNS. Embora o DNSSEC seja um componente crucial da segurança do DNS, o escopo da segurança do DNS vai além dos protocolos específicos do DNSSEC. A segurança do DNS lida com uma ampla variedade de ameaças, incluindo ataques do tipo [distributed denial-of-service (DDoS)](https://www.ibm.com/br-pt/topics/ddos) e roubo de domínios, fornecendo uma estratégia abrangente de proteção contra atividades maliciosas que possam comprometer a infraestrutura do DNS.

***Tipos de Registros e Zonas DNS***

**Registros de DNS**

É um conjunto de instruções usado para conectar nomes de domínio com endereços de protocolo da internet (IP) dentro dos servidores DNS. O DNS permite que os usuários naveguem pela internet usando nomes de domínio e URLs personalizáveis em vez de endereços IP numéricos complexos, exemplo lista telefônica da Internet.

**Uma imagem com texto, captura de ecrã, número, software

Os conteúdos gerados por IA podem estar incorretos.**

**Tabela 1:** Zona de DNS e seus registros para o domínio receitips.com.br:fonte (1)

**Zonas de DNS**

É uma entidade lógica distinta dentro do espaço de nomes de domínio do [sistema de nomes de domínio](https://www.ibm.com/br-pt/topics/dns) (DNS), usada para fornecer controle mais detalhado ao administrador, organização ou outra entidade legal responsável por sua administração.

**Ex:** O domínio "exemplo.com" pode existir na mesma zona que os subdomínios "blog.exemplo.com". e "comunidade.exemplo.com".

Os registros e zonas DNS (Sistema de Nomes de Domínio) são essenciais para o funcionamento da internet, permitindo que nomes de domínio sejam convertidos em endereços IP e facilitando a localização de serviços e recursos online.

**Tipos de Registros DNS**

1. **A (Address Record)**:
   * O registro **A** mapeia um nome de domínio para um endereço IPv4.
   * Exemplo: www.exemplo.com pode apontar para 192.0.2.1.
2. **AAAA (IPv6 Address Record)**:
   * O registro **AAAA** é semelhante ao **A**, mas mapeia um nome de domínio para um endereço IPv6.
   * Exemplo: www.exemplo.com pode apontar para 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
3. **CNAME (Canonical Name Record)**:
   * O **CNAME** mapeia um domínio para outro domínio, em vez de um endereço IP.
   * Exemplo: www.exemplo.com pode ser um alias para exemplo.com.
4. **MX (Mail Exchange Record)**:
   * O **MX** especifica o servidor de e-mail responsável pelo recebimento de e-mails para um domínio.
   * Exemplo: exemplo.com pode ter um registro MX apontando para mail.exemplo.com.
5. **NS (Name Server Record)**:
   * O **NS** especifica os servidores de nomes responsáveis por um domínio.
   * Exemplo: exemplo.com pode ter um registro NS apontando para ns1.exemplo.com.
6. **PTR (Pointer Record)**:
   * O **PTR** é usado para resolução reversa de DNS, ou seja, ele mapeia um endereço IP de volta para um nome de domínio.
   * Exemplo: 192.0.2.1 pode apontar para [www.exemplo.com](http://www.exemplo.com).
7. **TXT (Text Record)**:
   * O **TXT** pode conter texto arbitrário e é frequentemente usado para autenticação, como SPF (Sender Policy Framework) e DKIM (DomainKeys Identified Mail) para e-mails.
   * Exemplo: v=spf1 include:\_spf.exemplo.com ~all.
8. **SRV (Service Record)**:
   * O **SRV** especifica informações sobre serviços oferecidos, como um servidor de chat ou de VoIP.
   * Exemplo: \_sip.\_tcp.exemplo.com pode apontar para o servidor de SIP para chamadas VoIP.
9. **SOA (Start of Authority)**:
   * O **SOA** é o primeiro registro de uma zona DNS e define informações importantes sobre a zona, como o servidor mestre e os tempos de atualização.
   * Exemplo: SOA ns1.exemplo.com. hostmaster.exemplo.com. (2023101401 3600 1800 1209600 86400).
10. **CAA (Certification Authority Authorization)**:
    * O **CAA** especifica quais autoridades de certificação (CAs) estão autorizadas a emitir certificados SSL/TLS para um domínio.
    * Exemplo: 0 issue "letsencrypt.org" permite que a Let's Encrypt emita certificados para o domínio.

**Tipos de Zonas DNS**

1. **Zona Direta**:
   * A zona direta é a zona principal para um domínio. Ela mapeia os nomes de domínio para endereços IP (tipicamente via registros A ou AAAA).
   * Exemplo: Para o domínio exemplo.com, a zona direta contém os registros A e MX, entre outros.
2. **Zona Reversa**:
   * A zona reversa permite a resolução de IPs para nomes de domínio (resolução reversa).
   * Normalmente, ela usa registros PTR para mapear endereços IP a domínios.
   * Exemplo: A zona reversa para 192.0.2.1 poderia ter um registro PTR apontando para www.exemplo.com.
3. **Zona Autorizada (Master Zone)**:
   * A zona autorizada contém os registros definitivos para um domínio e é mantida pelo servidor DNS principal.
   * Ela é a fonte de autoridade para os registros de uma zona.
4. **Zona de Caching (Slave Zone)**:
   * Uma zona de cache é uma cópia de leitura das zonas de autoridade. Os servidores DNS secundários armazenam essas zonas para reduzir o tráfego e melhorar a performance de resolução.
   * Os servidores DNS secundários sincronizam periodicamente as zonas de cache com o servidor DNS principal.
5. **Zona de Pesquisa (Forward Lookup Zone)**:
   * A zona de pesquisa permite que um nome de domínio seja mapeado para um endereço IP. Ela inclui os registros como A, AAAA, CNAME, etc.
6. **Zona de Pesquisa Reversa (Reverse Lookup Zone)**:
   * A zona de pesquisa reversa permite que um endereço IP seja mapeado para um nome de domínio. Ela utiliza registros PTR.
   * Usada principalmente para diagnósticos de rede e verificação de identidade de servidores de e-mail.

Uma imagem com texto, captura de ecrã, ecrã, diagrama

Os conteúdos gerados por IA podem estar incorretos.

**Figura 1:** Tipos de zonas DNS :fonte [2]

***Implementação prática com BIND***

A implementação do DNSSEC é fundamental para proteger seu domínio contra-ataques como envenenamento de cache DNS e falsificação de respostas. Em um contexto digital em que a segurança é essencial, um ataque bem-sucedido ao DNS pode comprometer seriamente a reputação de uma marca, tornando a proteção da arquitetura do website indispensável.

O processo de resolução de DNS ocorre antes que o usuário acesse a aplicação do site. Caso a solicitação de DNS seja interceptada por um atacante, o usuário pode ser direcionado a um site falso, projetado para enganar, em vez do site legítimo. Além disso, a complexa arquitetura de cache do protocolo DNS torna difícil a correção rápida de registros corrompidos.

A diagram of a computer network

AI-generated content may be incorrect.Portanto, mesmo que o website possua firewalls robustos, a segurança dos dados e da tecnologia do usuário final permanece vulnerável se a infraestrutura DNS não estiver adequadamente protegida por DNSSEC (Figura).

O DNSSEC (Domain Name System Security Extensions) é uma extensão do DNS que adiciona camadas de segurança para garantir que as respostas do DNS sejam autênticas e não foram alteradas. Ele previne ataques como envenenamento de cache DNS e falsificação de respostas, essenciais para proteger a integridade de domínios na internet.

1. Problema que o DNSSEC resolve

Imagine que você deseja acessar o site do seu banco: meubanco.com. Seu navegador precisa do endereço IP correspondente. Sem DNSSEC, um atacante pode:

* Envenenar o cache do DNS, redirecionando você para um site falso;
* Falsificar a resposta DNS, enviando diretamente um IP malicioso.

Esses ataques podem resultar em roubo de dados sensíveis, como senhas e informações bancárias.

1. Como o DNSSEC impede ataques

DNSSEC utiliza assinaturas digitais para garantir que as respostas do DNS sejam autênticas. O processo é dividido em etapas:

2.1 Chaves criptográficas

* Cada domínio possui uma chave privada (para assinar) e uma chave pública (para validação).
* Exemplo: meubanco.com assina seu registro DNS do tipo A (IP) com sua chave privada, gerando uma assinatura digital.

2.2 Assinatura digital

* Ao consultar o DNS, o usuário recebe o registro (A → 192.168.1.10) e a assinatura digital.

2.3 Validação pelo resolvedor

* O resolvedor DNS verifica a assinatura com a chave pública do domínio.
* Se a assinatura for válida, o IP é retornado ao usuário; caso contrário, a resposta é rejeitada.

2.4 Corrente de confiança

* As chaves públicas dos domínios estão vinculadas às chaves de domínios de nível superior e, por fim, à chave raiz do DNS, criando uma hierarquia confiável.

1. Exemplo prático completo
2. O navegador consulta o resolvedor DNS sobre exemplo.com.
3. O resolvedor consulta o servidor autoritativo de exemplo.com.
4. O servidor retorna:
   * A → 203.0.113.10
   * RRSIG → assinatura digital do registro A
5. O resolvedor valida a assinatura usando a chave pública.

Se válida, o navegador recebe o IP correto; se inválida, o acesso é bloqueado.

A screenshot of a phone

AI-generated content may be incorrect.

O DNSSEC é essencial para garantir que usuários acessem sites legítimos e não sejam vítimas de ataques baseados em DNS. Mesmo com firewalls e outras proteções, a validação da infraestrutura DNS protege dados e integridade de usuários finais

***Riscos de incorporar DNSSEC***

Embora o DNSSEC seja uma forma inestimável de aumentar a segurança da rede, ele pode, involuntariamente, introduzir vulnerabilidades críticas. O DNSSEC pode aumentar o risco e amplificar os efeitos de ataques de navegação de serviço distribuída (DDoS), em que um servidor, serviço ou rede é interrompido pelo tráfego de vários dispositivos ao mesmo tempo.

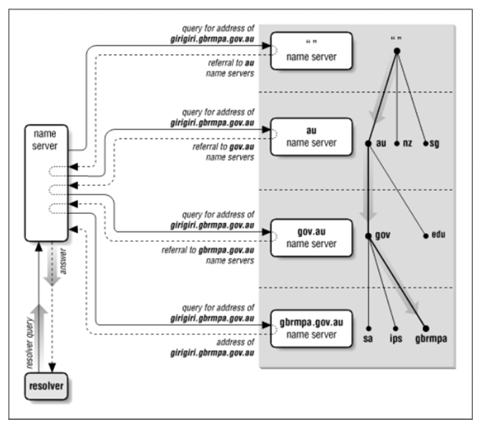
O DNSSEC também aumenta o número de respostas de consulta de DNS, pois a tecnologia requer campos adicionais e informações criptográficas para verificar corretamente os registros. Isso significa que as respostas de alto volume podem permitir que os agentes mal-intencionados tenham um volume de ataque muito maior contra uma zona do que poderiam se o DNSSEC não estivesse em vigor.

***Segurança e boas práticas (dnssec e tsig)***

Bem, como sabemos que o DNSSEC é uma extensão do protocolo DNS que adiciona uma camada de segurança para garantir a **autenticidade** e **integridade** dos dados DNS.

***Como funciona:***

* Utiliza **criptografia de chave pública** para assinar digitalmente os registros DNS.
* Cria uma **cadeia de confiança** desde os servidores raiz até os servidores autoritativos de um domínio.
* Permite que os resolvedores verifiquem se os dados não foram alterados.



### ***Benefícios:***

* + **Autenticidade**: Garante que a resposta vem da fonte legítima.
  + **Integridade**: Assegura que os dados não foram adulterados.
  + **Proteção**: Previne ataques como envenenamento de cache e man-in-the-middle

***Boas práticas:***

* Implementar DNSSEC nos servidores DNS.
* Configurar os servidores para validar assinaturas DNSSEC.
* Proteger rigorosamente as chaves privadas de assinatura.
* Combinar com outras práticas como TLS/SSL e firewalls

## ***SIG (Transaction Signature)***

O TSIG é um protocolo usado para **autenticar transações entre servidores DNS**, especialmente em transferências de zonas.

## TSIG (Transaction Signature)

O TSIG é um protocolo usado para **autenticar transações entre servidores DNS**, especialmente em transferências de zonas.

### ***Como funciona:***

* + - Usa **chaves secretas compartilhadas** para assinar e verificar mensagens entre servidores.
    - Garante que apenas servidores autorizados possam realizar operações como replicação de zonas.

### ***Benefícios:***

* ·          Protege a comunicação entre servidores DNS.
* ·          Evita modificações não autorizadas nas mensagens DNS.

# Conclusions

Durante este trabalho analisamos os seguintes tópicos: Estrutura e Arquitetura do DNS, funcionamento do protocolo DNS, tipos de registos e zonas DNS, Implementação prática com BIND, segurança e Boas Práticas (DNSSEC e TSIG). Portanto o DNSSEC é uma extensão do protocolo DNS, que visa proteger e tornar o funcionamento mais seguro das solicitações que circulam dentro da estrutura do DNS. Em suma, o DNS é um componente essencial da infraestrutura da Internet, combinando eficiência, escalabilidade e segurança. Sua compreensão e correta implementação, aliadas às boas práticas e mecanismos de proteção, são fundamentais para garantir o funcionamento seguro e estável das redes modernas.

# References

*This is a MANDATORY section! It should contain all the bibliographical references that have been used in the paper and should use a standard scientific format, such as APA or IEEE. To help you with this type of citations and references, we suggest you use software such as Mendeley (https://www.mendeley.com) or Zotero (https://www.zotero.org/).*

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user’s data privacy threats and defense mechanisms. *Procedia Computer Science*, *56*, 376–383.

Park, Ah.-J., Kim, H.-Y., & Lim, J.-I. (2015). A framework of device authentication management in IoT environments. *2015 5th International Conference on IT Convergence and Security (ICITCS)*, 1–3.

1. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). DNS Security Introduction and Requirements. RFC 4033. <https://www.rfc-editor.org/rfc/rfc4033>
2. Hoffman, P., & Schlyter, J. (2010). DNS Security (DNSSEC) Operational Practices. RFC 6781. <https://www.rfc-editor.org/rfc/rfc6781>
3. Mockapetris, P. (1987). Domain Names - Implementation and Specification. RFC 1035. <https://www.rfc-editor.org/rfc/rfc1035>
4. <https://www.akamai.com/pt/blog/trends/dnssec-how-it-works-key-considerations>
5. [**https://www.ibm.com/br-pt/think/topics/dns-records**](https://www.ibm.com/br-pt/think/topics/dns-records)
6. [**https://www.ibm.com/br-pt/think/topics/dns-zone**](https://www.ibm.com/br-pt/think/topics/dns-zone)
7. [1] <https://ayltoninacio.com.br/blog/tipos-de-registros-dns>
8. [2]<https://www.com/c/68f9232b-9cb4-832e-9044-f926bee4ac9f>