**FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"**
**Curso Superior de Tecnologia em Segurança da Informação**

Yuri Henrique Diniz

Juan Molina Boldim

# ESTADO ATUAL DA IMPLANTAÇÃO DO DNSSEC

## Um Panorama da Segurança no DNS

**Americana, SP**

**2026**

**FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"**
**Curso Superior de Tecnologia em Segurança da Informação**

Yuri Henrique Diniz

Juan Molina Boldim

# ESTADO ATUAL DA IMPLANTAÇÃO DO DNSSEC

## Um Panorama da Segurança no DNS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do professor Marcus Vinicius Lahr Giraldi

Área de concentração: Segurança da Informação.

**Americana, SP**

**2026**

Yuri Henrique Diniz
Juan Molina Boldim

# ESTADO ATUAL DE IMPLANTAÇÃO DO DNSSEC

## Um panorama de segurança no DNS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em segurança da informação pelo Centro Paula Souza – Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.
Área de concentração: Segurança da Informação.

Americana, 09 de junho de 2026

**Banca Examinadora:**

Marcus Vinicius Lahr Giraldi
Especialista
Fatec de Americana

Henri Alves De Godoy
Doutor
Fatec de Americana

Lídia Regina De Carvalho Freitas Barban
Especialista
Fatec de Americana

## FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

DINIZ, Yuri Henrique

Estado atual da implantação do dnssec: um panorama da segurança no dns. / Yuri Henrique Diniz, Juan Molina Boldim – Americana, 2026.

46f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinicius Lahr Giraldi

1. DNS – rede de computadores 2. Redes de computadores 3. Segurança em sistemas de informação. I. DINIZ, Yuri Henrique, II. BOLDIM, Juan Molina III. GIRALDI, Marcus Vinicius Lahr IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.519DNS
681519
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

## RESUMO

O Sistema de Nomes de Domínio (DNS) é uma infraestrutura essencial da *Internet*, permitindo a tradução de nomes legíveis para endereços IP. Contudo, seu design original, criado em um contexto de confiança acadêmica, não inclui mecanismos de autenticação ou verificação de integridade, tornando-o vulnerável a ataques como *spoofing* e cache *poisoning*. O DNSSEC surgiu como uma extensão criptográfica para resolver essas limitações, adicionando assinaturas digitais, registros específicos — como DNSKEY, RRSIG, DS, NSEC e NSEC3 — e uma cadeia de confiança hierárquica que autentica cada etapa da resolução de nomes. Apesar da sua robustez técnica, a adoção do DNSSEC é historicamente lenta devido à complexidade operacional, ao risco de erros na gestão e rotação de chaves, ao suporte limitado dos *registrars* e ao baixo incentivo econômico para sua implantação. Estudos recentes mostram que, embora haja avanços em automação com CDS/CDNSKEY e o novo mecanismo *Authenticated Bootstrapping*, esses recursos ainda apresentam adoção restrita. Pesquisas também revelam discrepâncias significativas entre TLDs incentivados e não incentivados, além de uma baixa taxa de validação pelos resolvedores, o que limita o impacto prático do DNSSEC para o usuário final. Assim, embora a tecnologia tenha evoluído e ofereça melhorias substanciais de segurança, o fator mais determinante para sua ampliação permanece sendo a existência de incentivos institucionais, regulatórios e econômicos. Desse modo, o futuro do DNSSEC dependerá não apenas do avanço técnico, mas da capacidade de coordenar operações entre *registrars*, registries e operadores, criando um ecossistema favorável à sua adoção em larga escala.



**Palavras-chave:** DNSSEC; DNS; Adoção.

## ABSTRACT

*The Domain Name System (DNS) is a fundamental component of the Internet, enabling the translation of human-readable names into IP addresses. However, its original design, developed in an academic and trusted environment, lacks authentication and integrity mechanisms, making it vulnerable to attacks such as spoofing and cache poisoning. DNSSEC was introduced as a cryptographic extension to address these limitations by adding digital signatures, specific records—such as DNSKEY, RRSIG, DS, NSEC, and NSEC3—and a hierarchical chain of trust that authenticates each stage of name resolution. Despite its technical robustness, DNSSEC adoption has progressed slowly due to operational complexity, risks associated with key management and rollover, limited registrar support, and low economic incentives for deployment. Recent studies show that, although automation mechanisms such as CDS/CDNSKEY and the newer Authenticated Bootstrapping improve operational reliability, their adoption remains limited. Research also highlights substantial disparities between incentivized and non-incentivized TLDs, as well as low validation rates by recursive resolvers, which reduces the practical security benefits for end users. Thus, although the technology has evolved and offers significant security improvements, institutional, regulatory, and economic incentives remain the most decisive factors influencing widespread adoption. Therefore, the future of DNSSEC will depend not only on technical evolution but also on coordinated efforts among registrars, registries, and operators to create an environment conducive to large-scale deployment.*



**Keywords:** *DNSSEC; DNS; Adoption*.

## LISTA DE FIGURAS

## LISTA DE QUADROS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ARPANET | Advanced Research Projects Agency Network |
| CAA | Certification Authority Authorization |
| ccTLD | Country Code Top-Level Domain |
| CDNSKEY | Child DNSKEY |
| CDS | Child DS |
| DMARC | Domain-based Message Authentication, Reporting and Conformance |
| DNS | Domain Name System |
| DNSKEY | Domain Name System Key Record |
| DNSSEC | Domain Name System Security Extensions |
| DO bit | DNSSEC OK bit |
| DoH | DNS over HTTPS |
| Dot | DNS over TLS |
| DS | Delegation Signer |
| ECDSA | Eliptic Curve Digital Signature Algorithm |
| gTLD | Generic Top-Level Domain |
| HSM | Hardware Security Module |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IETF | Internet Engineering Task Force |
| IP | Internal Protocol |
| IPsec | Internet Protocol Security |
| KSK | Key Signing Key |
| MECSA | Measurement of Encrypted Communication Standards Adoption |
| NSEC | Next Secure Record |
| NSEC3 | NSEC3 Hashed Record |
| PKI | Public Key Infrastructure |
| RDP | Remote Desktop Protocol |
| RR | Resource Record |
| RRSIG | Resource Record Signature |
| RSA | Rivest-Shamir-Adleman |

| | |
|---|---|
| SHA | Secure Hash Algorithm |
| SPF | Sender Policy framework |
| SSH | Secure Shell |
| TLD | Top-Level Domain |
| TTl | Time To Live |
| ZSK | Zone Signing Key |

## SUMÁRIO

# 1 INTRODUÇÃO

Em um mundo com um sistema informático tão complexo como a *Internet*, é difícil imaginar como funcionam os tantos subsistemas que fazem parte dela. Existem diversos protocolos, dispositivos, tecnologias de conexão físicas etc. Em um sistema com tantos subsistemas, é complicado manter a segurança dos dados quando eles trafegam sendo processados e armazenados por diversos elementos.

O *Domain Name System* (DNS) é um componente fundamental da *Internet*, responsável por traduzir nomes de domínio em endereços IP. Por sua importância e pelo papel central que exerce no funcionamento das redes, a segurança do DNS é essencial para garantir a confiabilidade da comunicação na *Internet*. Contudo, o DNS foi criado em um período em que a *Internet* não possuía ameaças significativas, e por isso não incorporava mecanismos de autenticação ou proteção contra falsificação de dados. Para corrigir essas limitações, a IETF desenvolveu o *Domain Name System Security Extensions* (DNSSEC), um conjunto de extensões que adiciona verificação criptográfica às respostas do DNS.

A importância do trabalho se dá principalmente por oferecer uma visão ampla do nível de adoção do DNSSEC e apontar razões e dificuldades de sua implementação. Além disso, ele explica o funcionamento tanto do DNS quanto do DNSSEC para enriquecer o entendimento. Sua viabilidade se dá pela existência de artigos que realizaram diversas medições usando diferentes métodos em vários contextos de análise para entender as dificuldades e o estado atual de implantação.

A questão que norteia este trabalho é a dúvida sobre o quão amplamente adotado e bem gerenciado o DNSSEC é na prática.

O objetivo final é realizar uma análise do processo de adoção do DNSSEC nos últimos anos e do seu estado atual de implantação, tendo em vista medições disponíveis por meio de artigos e pesquisas.

O artigo tem como objetivos específicos: fornecer breve fundamentação de como o DNS funciona; explicar como o DNSSEC melhora a segurança; realizar uma análise do seu desenvolvimento e do estado atual; e discorrer sobre as soluções atuais.

A hipótese é que, apesar de ser uma extensão que traz diversas proteções, a adoção dela cresce, porém, lentamente com o passar dos anos. As razões para isso

seriam a alta complexidade do gerenciamento de domínios que fazem uso dela, custo econômico e falta de mão de obra especializada para manter a infraestrutura.

O percurso metodológico deste trabalho é uma análise documental de diversos estudos que medem o grau de implantação do DNSSEC e apontam dificuldades encontradas na sua implementação. Serão extraídos dados tanto qualitativos quanto quantitativos, buscando identificar padrões, desafios comuns e possíveis soluções apontadas pela literatura. Essa análise permite obter um panorama geral do cenário atual de implantação do DNSSEC.

O trabalho está organizado em seis capítulos, sendo o capítulo I a fundamentação teórica geral, o capítulo II o percurso metodológico, o capítulo III conterá a introdução ao DNS, o capítulo IV a fundamentação do DNSSEC, o capítulo V onde os artigos serão discutidos e analisados e o capítulo VI a conclusão.

# 2 PERCURSO METODOLÓGICO

Este trabalho foi desenvolvido por meio de pesquisa bibliográfica, com abordagem qualitativa e caráter exploratório. Inicialmente, foram estudados os fundamentos do DNS e do DNSSEC a partir de obras técnicas e documentos de referência, a fim de estabelecer a base conceitual necessária. Em seguida, realizou-se o levantamento dos estudos que compõem o corpo da análise, utilizando fontes como Google Acadêmico, repositórios de RFCs e relatórios técnicos. Foram selecionados trabalhos publicados principalmente entre 2015 e 2025, priorizando estudos com dados empíricos, medições em larga escala e análises operacionais. O material coletado foi lido, comparado e organizado em temas que estruturaram o desenvolvimento: dificuldades de implantação, papel dos *registrars*, automações, incentivos e panorama de adoção. A partir dessa sistematização, foi possível construir uma síntese crítica sobre os fatores que influenciam o avanço do DNSSEC.

A seguir são apresentados estudos e pesquisas relacionados ao tema deste trabalho. O levantamento realizado foi orientado pela busca de pesquisas científicas e tecnológicas que têm como objetivo medir o grau de adoção de tecnologias de segurança para o ecossistema DNS. A ferramenta que serviu de referência para isso foi o Google Acadêmico, por meio do qual se buscou mapear as pesquisas dessa natureza circunscritas nos últimos anos.

Chung et al. (2017a) conduzem um estudo longitudinal sobre o ecossistema DNSSEC, analisando a gestão de chaves, assinaturas e registros ao longo de 21 meses para todos os domínios assinados sob os TLDs **.com**, .**net** e **.org**, além de realizarem medições ativas com mais de 59 mil *resolvers*. Os autores identificam problemas recorrentes na configuração das zonas: 31% dos domínios deixam de publicar registros essenciais, 39% utilizam chaves criptográficas consideradas fracas e aproximadamente 70% não realizam rotação de KSKs. No lado dos validadores, apenas 12% dos *resolvers* que solicitam registros DNSSEC efetivamente validam as assinaturas. Conforme Chung et al. (2017), essas falhas operacionais comprometem a eficácia do DNSSEC e reforçam a necessidade de maior automação e práticas sistemáticas de auditoria.

Yajima et al. (2021) realizam um estudo em larga escala para medir a adoção de diversos mecanismos de segurança de DNS, incluindo DNSSEC, DNS Cookies,

SPF, DMARC, MTA-STS, DANE e CAA. Usando dados de 13 servidores-raiz, 276 TLDs e 10 mil domínios populares, os autores investigam o suporte a cada mecanismo e a correlação entre sua complexidade e seu nível de adoção. Os resultados mostram que, enquanto TLDs e servidores-raiz adotam fortemente mecanismos críticos como DNSSEC e DNS Cookies, os domínios comuns apresentam taxas muito baixas de implantação, exceto para SPF. O estudo conclui que mecanismos mais difíceis de configurar apresentam menor adesão e que a adoção geral só deve avançar com ferramentas mais simples e processos automatizados.

O estudo de Elliott e Moxley (2023) “The Sad Story of DNSSEC” analisa se o DNSSEC realmente protege o usuário final ao depender da validação dos *resolvers*. Segundo o estudo, mesmo domínios corretamente assinados frequentemente não resultam em respostas válidas porque a maioria dos *resolvers* públicos não valida as assinaturas. Para chegar a esse resultado, os autores consultaram os 100 domínios mais populares usando 67.177 *resolvers* diferentes, classificando o comportamento de cada um. A análise revelou que apenas cerca de um terço valida corretamente, enquanto mais da metade retorna cadeias quebradas ou respostas inconsistentes. Os autores concluem que, embora o DNSSEC seja tecnicamente sólido, sua eficácia na prática é limitada, pois a validação raramente ocorre no caminho até o usuário.

Roth et al. (2019) investigam como o suporte oferecido pelos *registrars* influencia a implantação correta do DNSSEC. Para isso, combinaram uma análise longitudinal de 51 meses sobre milhões de domínios em TLDs distintos com testes práticos de compra e configuração em 20 *registrars* populares. Os autores identificam que TLDs com incentivos e bom suporte apresentam taxas de adoção muito maiores, enquanto muitos *registrars* ainda exibem interfaces deficientes, falta de automação e erros na publicação de registros DS. A pesquisa mostra que problemas operacionais e não limitações técnicas são o principal obstáculo para a adoção.

O relatório de Kampourakis e Karopoulos (2022) apresenta uma análise abrangente dos níveis de adoção do DNSSEC na União Europeia e no restante do mundo, utilizando dados públicos e medições próprias. Os autores mostram que a distribuição da adoção é bastante desigual entre os Estados-Membros, com países como República Tcheca, Dinamarca e Finlândia superando 70%, enquanto outros permanecem abaixo de 10%. O estudo descreve os requisitos técnicos para implantação correta, destacando a necessidade de DS no *registry*, o suporte do TLD

e a compatibilidade de *resolvers*. Também aborda dificuldades recorrentes, como configurações incompletas que rompem a cadeia de confiança. A partir dessa análise, o relatório oferece uma visão atualizada do ecossistema DNSSEC e da evolução de sua adoção na UE e globalmente.

O artigo de Chung et al. (2017b) investiga por que a adoção do DNSSEC permanece extremamente baixa, apesar de sua padronização e suporte difundido entre TLDs. Utilizando medições em larga escala e experimentos práticos de implantação de DNSSEC em 30 *registrars*, os autores mostram que a principal barreira está nos próprios *registrars*, que oferecem suporte limitado, interfaces confusas e processos inseguros para publicação de registros DS. Apenas uma pequena parcela dos *registrars* habilita DNSSEC por padrão, e muitos aceitam registros DS incorretos ou não autenticam e-mails usados para atualizações, criando riscos de segurança. O estudo revela ainda que mecanismos atuais de transmissão de DNSSEC aos *registrars* são frágeis e propensos a erros humanos. Os resultados indicam que o ecossistema de DNSSEC depende fortemente de poucos *registrars* que o suportam adequadamente, enquanto a grande maioria dificulta sua implantação. O artigo conclui apontando melhorias necessárias para tornar o DNSSEC mais acessível e seguro.

O artigo de Misell et al. (2025) investiga a adoção do novo mecanismo de automação do DNSSEC chamado *Authenticated Bootstrapping* (AB), criado para simplificar a configuração inicial do DNSSEC e reduzir erros operacionais. Para medir seu uso na prática, os autores analisaram um conjunto massivo de domínios, verificando quais implementavam DNSSEC e quais publicavam os registros necessários para automação, como CDS e CDNSKEY. O estudo também avaliou quais operadores de DNS já suportavam o novo método e qual era a taxa de configurações corretas entre os domínios compatíveis. Os resultados mostraram que, embora o AB seja tecnicamente sólido e funcione corretamente nas zonas que o utilizam, sua adoção ainda é extremamente limitada: apenas três provedores implementam o mecanismo, e apenas uma pequena fração das zonas está devidamente assinada com DNSSEC. A conclusão é que a principal barreira não está na automação em si, mas na ainda baixa adoção do DNSSEC de forma geral. Assim, o AB tem grande potencial para facilitar implantações, mas seu impacto real depende de uma adoção mais ampla do DNSSEC e de mais operadores incorporando o suporte ao mecanismo.

O quadro 1 lista a seguir todos os artigos selecionados, ano de publicação e seus respectivos objetivos. Foram selecionados artigos de diferentes anos para avaliar a evolução do DNSSEC ao longo dos anos e como as conclusões evoluíram.

**Quadro 1** - Comparativo de Trabalhos Acadêmicos sobre DNSSEC.

| **Autores** | **Ano** | **Objetivo Principal** |
|---|---|---|
| Chung et al. | 2017a | Analisar e avaliar o ecossistema do DNSSEC de forma longitudinal. |
| Chung et al. | 2017b | Analisar o impacto dos registrars na adoção do DNSSEC. |
| Roth et al. | 2019 | Medir a evolução do suporte dos registrars ao DNSSEC. |
| Yajima et al. | 2021 | Avaliar adoção de múltiplos mecanismos de segurança do ecossistema DNS. |
| Kampourakis e Karopoulos | 2022 | Mapear a implantação do DNSSEC em países da UE. |
| Elliott e Moxley | 2023 | Avaliar a validação DNSSEC por parte dos resolvers |
| Misell et al. | 2025 | Avaliar o nível adoção dos mecanismos de automação CDS/CDSNKEY e Bootstraping |

Fonte: Desenvolvido pelo autor (2025).

# 3 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão apresentados os principais conceitos e tecnologias relevantes para o entendimento do contexto ao redor do DNSSEC. Inclui os fundamentos básicos para se entender o DNS, a origem do DNSSEC, principais componentes e seu funcionamento.

## 3.1 CRIPTOGRAFIA ASSIMÉTRICA

Criptografia Assimétrica é um esquema criptográfico que usa duas chaves complementares. O vínculo apresentado se deve a uma relação matemática, de maneira que, ao criptografar informações com uma delas, só é possível descriptografar utilizando a outra, sendo que o inverso também é verdadeiro. Apesar de ser mais segura, seu desempenho pode ser inferior ao da criptografia simétrica, pois há uma maior complexidade de operações matemáticas envolvidas (BRAGA; DAHAB, 2018).

## 3.2 CHAVE CRIPTOGRÁFICA

Uma chave criptográfica é uma sequência de caracteres utilizada como entrada para criptografar ou descriptografar informações em um algoritmo criptográfico. O nível de segurança das informações criptografadas é fortemente relacionado com o tamanho da chave e da aleatoriedade das chaves geradas (CORRIGAN-GIBBS et al., 2013).

## 3.3 CADEIA DE CONFIANÇA

Uma cadeia de confiança consiste em um conjunto de entidades ligadas por confiança transitiva, a partir de uma entidade raiz cuja confiabilidade é assumida a priori. É transitiva de maneira que uma entidade confia em uma segunda; se essa segunda confia em uma terceira, logo a primeira também confia nessa última. A base fundamental da cadeia é uma entidade raiz que se supõe confiável, de forma que, por consequência, o comprometimento dela representa a perda de toda a cadeia. Pode-se usar como exemplo a cadeia de confiança em sistemas de infraestrutura de chaves públicas, que dependem da capacidade de atribuir a cada entidade suas

responsabilidades de um jeito seguro e de anular certificados que não são mais confiáveis (CHUAT et al., 2019).

## 3.4 DNS

O DNS é um dos componentes fundamentais do funcionamento da *Internet* e essa seção busca oferecer uma introdução com base na obra de Tanenbaum e Wetherall (2021). O DNS tem como função principal a resolução de nomes legíveis por pessoas, como **www.google.com**, em endereços IPs que são de fato utilizados por dispositivos na rede. Essa conversão é importante, pois para pessoas é mais fácil lembrar de nomes, porém os dispositivos trabalham melhor com endereços numéricos. O DNS funciona, portanto, como uma base de dados que armazena a relação entre nomes de domínio e endereços IPs.

Na época da ARPANET, essa relação de nomes e endereços era mantida em um arquivo único, convencionalmente chamado de hosts.txt, e cada máquina tinha uma cópia desse arquivo para resolver nomes localmente. Porém, com o crescimento exponencial do número de dispositivos conectados e de domínios utilizados, tornou-se necessária uma nova abordagem e, em 1983, foi criado o DNS. O DNS trouxe um sistema escalável, distribuído e capaz de lidar com quantidades grandes de nomes de forma dinâmica.

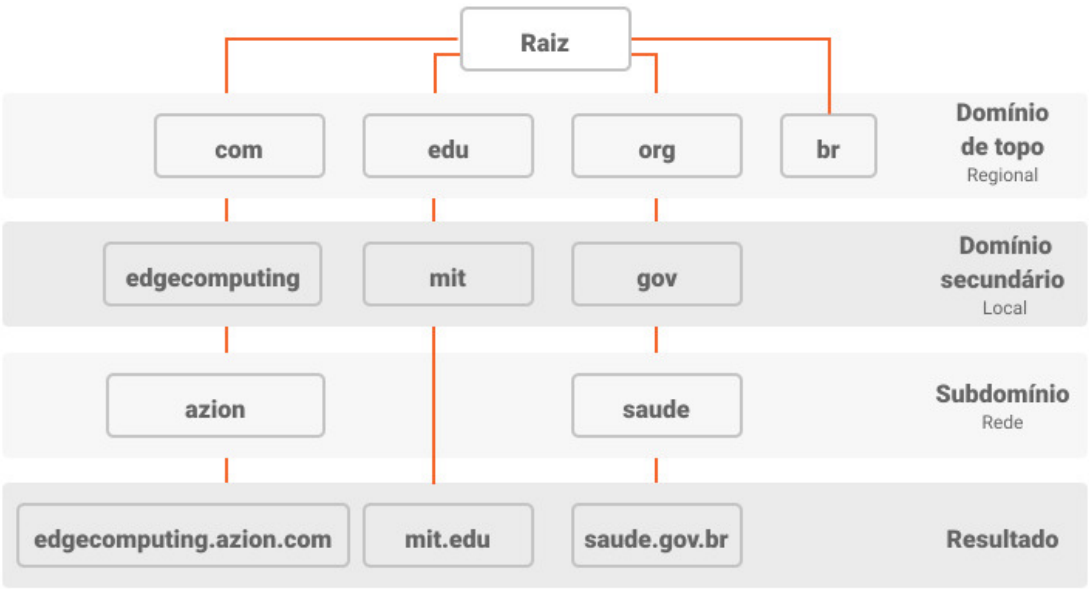
No DNS, as relações são armazenadas na forma de registros de recurso chamados de *Resource Records*. Cada registro contém uma relação entre um nome e um valor, além de outros dados complementares. Existem diferentes tipos de registros, sendo que cada tipo associa dados de natureza distinta a um dado nome. Os tipos mais conhecidos e utilizados são:

a) A: associa um nome de domínio a um endereço IPv4.
b) AAAA: associa um nome de domínio a um endereço IPv6.
c) CNAME: cria um alias para outro nome de domínio.
d) MX: define os servidores responsáveis pelo recebimento de e-mails para o domínio.
e) NS: indica quais servidores são autoritativos para aquele domínio.
f) TXT: armazena informações de texto, muitas vezes usadas para verificações e políticas de segurança.

Esses registros são divididos entre os domínios de forma hierárquica. No topo fica a zona raiz, representada nos endereços por um ponto final (“.”), que, por convenção, é omitido, sendo, por exemplo, ocultado em navegadores. No nível abaixo

ficam os domínios de topo os TLDs (Top-Level Domains), como **.com**, **.org**, **.br**, **.net**, entre vários outros. Cada um desses domínios é administrado por uma autoridade responsável. Abaixo de cada TLD estão os domínios de segundo nível, como google.com. A partir desse nível, os domínios podem ser subdivididos em subdomínios, refletindo a estrutura interna da empresa ou organização. A figura 1 mostra a estrutura dos domínios do DNS começando da raiz.

**Figura 1** - Hierarquia de domínios




Fonte: Azion. “O que é DNS”. Disponível em: https://www.azion.com/pt-br/learning/dns/o-que-e-dns/. Acesso em: 21 nov. 2025.

O fluxo básico de uma resolução de nome pode ser exemplificado quando um usuário digita um endereço de um site em seu navegador. O sistema operacional primeiramente verifica se o registro com a resposta está em cache. Caso não esteja, uma consulta é enviada ao servidor DNS local, que pode ser da empresa, operado e administrado pelo provedor de *Internet* ou por serviços públicos. Ao receber a consulta, o servidor DNS local realiza uma série de consultas a servidores DNS, começando dos domínios superiores até os inferiores em busca do registro para aquele nome.

Essa busca ocorre em etapas. Primeiramente, o servidor DNS local consulta um dos servidores raiz em busca dos servidores responsáveis pelo TLD indicado no endereço. Os servidores raiz não armazenam todos os registros, porém conseguem indicar quais servidores são responsáveis por cada TLD. O próximo passo é o servidor local consultar um dos servidores do TLD, que responde com a localização dos servidores autoritativos do domínio. E, finalmente, o servidor local obtém o registro final do servidor autoritativo do domínio.

Para não realizar consultas repetitivas o DNS tem mecanismos de cache para otimizar, melhorando assim o desempenho e reduzindo tráfego. Cada registro contém um valor chamado de TTL ou *Time-to-Live*, definido pelo administrador da zona, que determina quanto tempo o registro pode ficar armazenado em cache, seja na cache local em um computador doméstico ou em um resolvedor. Depois que o TTL expira, o registro é descartado, sendo considerado desatualizado. Esse mecanismo reduz os acessos aos servidores e melhora o desempenho, porém pode causar problemas quando há atualizações de registros, já que o registro atualizado demora justamente o tempo do TTL para se propagar.

Outro detalhe importante do funcionamento do DNS é a diferença entre servidores que são autoritativos e os que não são. Um servidor autoritativo tem posse das informações oficiais de um domínio, sendo comumente configurado e mantido pelo proprietário ou por um provedor de hospedagem. Já os servidores não autoritativos são os intermediários que podem agilizar o processo de resolução, respondendo com registros em cache. Respostas de cache, por sua vez, não são consideradas autoritativas, pois a informação nelas pode, mesmo que por um período curto, diferir das encontradas nos servidores autoritativos.

Em resumo, o DNS foi projetado para ser um serviço distribuído, ou seja, os dados não se concentram em um único servidor, também hierárquico; os servidores são organizados do mais geral para o mais específico e resiliente, não apresentando um único ponto de falha.

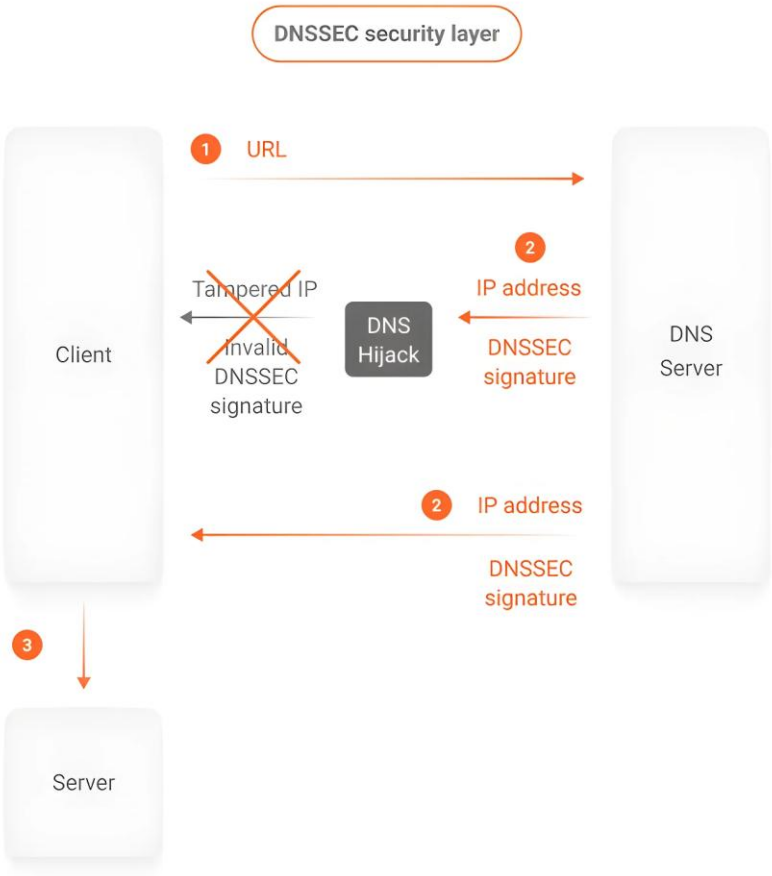
## 3.5 PROBLEMAS DE SEGURANÇA

Apesar de resolver problemas administrativos e de escalabilidade, a arquitetura original do DNS, concebida para uma *Internet* acadêmica e de confiança, traz desafios de segurança em vista do cenário atual de ameaças cibernéticas. Desafios esses

resolvidos por meio de tecnologias complementares, assegurando que o sistema continue funcionando de maneira correta, eficiente e confiável. Uma dessas tecnologias é o DNSSEC, desenvolvido para autenticar as respostas DNS. Essa seção tem o intuito de oferecer uma introdução ao DNSSEC e baseia-se na obra DNSSEC Mastery, de Lucas (2021).

O DNSSEC surge mais precisamente como um conjunto de extensões de segurança para o DNS, sendo criado para lidar com as vulnerabilidades presentes na arquitetura original do sistema no que tange à ausência de autenticação e verificação de integridade das respostas. No DNS tradicional, quando um usuário realiza uma consulta, o DNS retorna um endereço IP ou outra informação vinculada ao nome consultado, porém não há garantia de que essa resposta veio de um servidor de nomes legítimo ou que não foi alterada em trânsito. Essas vulnerabilidades já são exploradas por ataques bem conhecidos, como o *DNS Spoofing* e *Cache Poisoning*. Em ambos os casos, o invasor injeta informações falsas no resolvedor, redirecionando o usuário para servidores maliciosos. A Figura 2 mostra o processo de como o DNSSEC válida e dessa forma protege contra esses dois tipos de ataques.

**Figura 2** - Funcionamento da validação DNSSEC




Fonte: Azion. “O que é DNSSEC”. Disponível em: https://www.azion.com/pt-br/learning/dns/o-que-e-dnssec/. Acesso em: 21 nov. 2025.

O DNSSEC foi desenvolvido para lidar com esses casos, incluindo assinaturas digitais aos registros DNS. Isso permite que o resolvedor autentique as respostas que recebe por meio da validação dessas assinaturas usando uma chave pública, confirmando a autenticidade e integridade dos dados. A criptografia de chave pública é uma tecnologia que provê autenticidade não só para o DNSSEC, mas é amplamente usada também em diversas outras aplicações seguras na *Internet*, como HTTPS, SSH, IPsec, RDP etc.

Apesar de trazer autenticidade e integridade às respostas, o DNSSEC não garante confidencialidade. Isso significa que, caso alguém capture uma resposta em trânsito na rede, o conteúdo pode ser lido, revelando assim quais domínios estão sendo acessados. Por esse motivo, é comum o DNSSEC ser implementado em conjunto com outras tecnologias, como o *DoH* (DNS sobre HTTPS) ou *DoT* (DNS

sobre TLS), que encapsulam as respostas em canais criptográficos, adicionando dessa maneira privacidade à comunicação.

Resumindo, o DNSSEC é uma evolução fundamental para a segurança do DNS. Ele traz uma solução ao problema fundamental de segurança do DNS original por meio da verificação de assinaturas criptográficas, criando uma fundação confiável para comunicações seguras. No entanto, já que não proporciona privacidade, é recomendada sua implementação em conjunto com outras tecnologias que complementam essa barreira de proteção.

## 3.6 FUNCIONAMENTO DO DNSSEC

O DNSSEC é baseado na arquitetura original do DNS, mas a incrementa com uma camada robusta de autenticação por meio de assinaturas digitais. Para entender o seu funcionamento de maneira plena, é necessário examinar como ele organiza as chaves, como a relação de confiança é estabelecida entre diferentes níveis da hierarquia e como isso tudo altera a dinâmica de resolução de nomes em relação ao DNS clássico. Essa seção explica em detalhes o funcionamento do DNSSEC tendo como base a obra DNSSEC Mastery (2021).

No contexto do DNSSEC, a implementação de novas funcionalidades para garantir a autenticação e a integridade das respostas exigiu a criação de novos tipos de registro, que não existiam no DNS originalmente. Esses novos tipos são essenciais para a validação confiável durante a resolução de nomes. Cada um desempenha um papel importante, formando um conjunto de mecanismos que se conectam para criar a cadeia de confiança do DNSSEC.

Um dos registros mais relevantes é o DNSKEY. Ele é usado para armazenar chaves públicas que correspondem aos seus pares privados utilizados para assinar registros na zona. Cada zona, como exemplo.com, possui dois pares de chaves, a *Zone Signing Key* (ZSK) e a *Key Signing Key* (KSK). O registro DNSKEY guarda as versões públicas dessas chaves e permite que os resolvedores validem as assinaturas digitais em registros RRSIG. A diferença principal entre elas é que a ZSK assina os conjuntos de registros da zona, como A, MX ou CNAME, enquanto a KSK assina apenas o próprio DNSKEY, garantindo a integridade da ZSK. Essa separação torna a administração mais simples e reforça a segurança, já que a KSK muda com menos frequência e pode ser protegida com mais cuidado.

Outro registro essencial é o RRSIG, que armazena a assinatura digital de um conjunto de registros DNS. Quando uma consulta é feita para um registro *A*, por exemplo, o servidor autoritativo envia não só o valor solicitado, mas também um RRSIG com a assinatura dessa informação. Essa assinatura é criada com a chave privada correspondente à chave pública disponível no DNSKEY. O resolvedor usa essa chave pública para verificar o RRSIG e garantir que os dados não foram alterados. Um ponto importante é que o RRSIG está ligado a um *RRset*, um conjunto de registros que correspondem ao mesmo nome, ao mesmo tipo e à mesma classe.

A conexão entre as zonas na hierarquia do DNSSEC é feita por meio do registro DS (*Delegation Signer*). Esse registro fica na zona pai, como o TLD **.com**, e contém um *hash* da chave pública KSK da zona filha, por exemplo, **exemplo.com**. Com isso, o resolvedor consegue confirmar que a chave pública informada pela zona filha realmente corresponde ao *hash* publicado na zona pai. Essa ligação mantém a continuidade da cadeia de confiança do DNSSEC, que vai desde a raiz até o domínio consultado. Sem o registro DS, não haveria essa ponte de verificação entre as zonas, e a validação perderia sua confiabilidade.

Quando um nome de domínio ou registro não existe, o DNSSEC usa os registros NSEC e NSEC3 para garantir respostas negativas seguras. No DNS tradicional, uma resposta NXDOMAIN não é autenticada, o que abre brechas para falsificações. O NSEC foi criado para listar explicitamente os nomes presentes em uma zona e provar que um nome específico não existe. Por exemplo, se o resolvedor perguntar por **teste.exemplo.com** e esse nome não estiver cadastrado, o servidor pode responder com um NSEC mostrando que os nomes vizinhos são **site1.exemplo.com** e **site2.exemplo.com**, comprovando que “teste” não se encaixa nessa faixa. O problema é que isso revela todos os nomes existentes, o que permite ataques de enumeração de zona. Para reduzir esse risco, surgiu o NSEC3, que funciona de forma parecida, mas armazena apenas *hashes* criptográficos dos nomes, evitando a exposição direta e mantendo a prova de inexistência de forma segura.

Esses mecanismos fazem com que o DNSSEC ofereça um nível de segurança que o DNS tradicional não possui. Ao mesmo tempo, trazem mais complexidade e exigem cuidados extras na administração. A rotação de chaves, especialmente da KSK, precisa ser feita com atenção para evitar que os registros DS e DNSKEY fiquem fora de sincronia, o que poderia tornar o domínio inacessível. Além disso, a presença

de RRSIGs e DNSKEYs nas respostas aumenta o tamanho dos pacotes DNS, o que pode causar fragmentação em pacotes UDP e o uso de TCP, o que pode exigir ajustes em redes e *firewalls*.

Em resumo, os registros usados pelo DNSSEC, como DNSKEY, RRSIG, DS, NSEC e NSEC3, formam a base da validação criptográfica do sistema. Cada um tem uma função específica, que inclui armazenar chaves, assinar dados, ligar zonas de forma segura e comprovar a inexistência de registros. Quando são bem configurados e administrados, esses recursos tornam o DNS mais resistente a ataques de falsificação e ajudam a construir uma *Internet* mais segura e confiável.

## 3.7 GESTÃO DE CHAVES CRIPTOGRÁFICAS

A gestão de chaves criptográficas é um dos pontos mais importantes para manter o DNSSEC funcionando de forma segura. Todo o sistema de autenticação e integridade depende da geração, do armazenamento, da distribuição e da renovação corretas dessas chaves. Um simples erro de configuração ou uma falha de sincronização pode invalidar toda a cadeia de confiança e deixar o domínio inacessível, mesmo que os servidores continuem funcionando normalmente. Por isso, entender o ciclo de vida das chaves e seguir boas práticas é essencial para qualquer administrador que implemente o DNSSEC. Essa seção explica como a gestão de chaves funciona e sua importância com base na obra DNSSEC Mastery (2021).

Como explicado na seção anterior, no DNSSEC existem dois tipos principais de chaves, a ZSK e a KSK. A ZSK é usada para assinar todos os conjuntos de registros de uma zona, como os registros A, AAAA, MX e CNAME. Como ela lida com um volume maior de dados e é usada com mais frequência. Já a KSK tem a função de assinar o registro DNSKEY que contém a ZSK, servindo como elo de confiança entre a zona e o registro DS na zona pai. A razão de não se utilizar um único par é que isso aumentaria o risco de comprometimento, já que zonas podem armazenar muitos registros e esses, por sua vez, podem mudar com frequência, o que exige o uso extensivo da chave privada. Ao expor tantas assinaturas da mesma chave em diferentes conjuntos de dados, o sistema se torna muito suscetível a ataques de análise criptográfica. Uma zona DNSSEC então mantém dois pares: o usado para assinar e validar registros, que é trocado com frequência, justamente pelo motivo

acima, e outro trocado mais raramente para ainda assim garantir a estabilidade das relações de confiança.

A geração dessas chaves deve seguir padrões criptográficos reconhecidos, garantindo que os algoritmos e tamanhos escolhidos estejam de acordo com as recomendações mais recentes da IETF. Algoritmos como RSA com SHA-*256* e ECDSA são os mais usados, pois oferecem um bom equilíbrio entre segurança e desempenho. Normalmente, utiliza-se RSA de 2048 bits para ZSK e 2048 ou 4096 bits para KSK. Esse processo deve ser feito em ambientes controlados, de preferência com o uso de HSMs (*Hardware Security Modules*) ou outros dispositivos seguros, para evitar que a chave privada seja exposta em sistemas vulneráveis.

Depois de gerar as chaves, é preciso planejar como elas serão distribuídas. As versões públicas da ZSK e da KSK são incluídas nos registros DNSKEY da zona. Já o *hash* da KSK deve ser publicado na zona pai por meio do registro DS, para que os resolvedores possam confirmar a autenticidade da cadeia de confiança. Esse processo exige uma boa coordenação entre o operador da zona e o registrar, pois qualquer diferença entre os dados locais e os da zona pai pode causar falhas na resolução de nomes.

A rotação de chaves é uma parte essencial do ciclo de vida do DNSSEC. Nenhuma chave deve ser usada por tempo indeterminado, já que o uso prolongado aumenta o risco de comprometimento. No caso da ZSK, essa troca costuma ser mais frequente, acontecendo normalmente a cada poucos meses. Já a KSK, por ter uma função mais sensível, pode ser trocada em intervalos de um a vários anos, mas o processo precisa ser feito com muito cuidado, seguindo etapas bem definidas para evitar falhas. Os dois métodos principais de *rollover* são: o *Double Signature*, em que a chave antiga e a nova assinam os registros durante um período de transição, e o *Pre-publishing*, que publica as duas chaves no DNSKEY ao mesmo tempo, permitindo que os resolvedores atualizem suas referências antes da remoção da anterior.

Para tornar esse processo mais simples e menos sujeito a erros, foi criada a automação de troca de chaves, descrita na RFC 8078. Essa especificação define dois novos tipos de registros: CDS e CDNSKEY. Usados para os servidores autoritativos e os registradores coordenarem automaticamente a atualização dos registros DS na zona pai, usando métodos seguros de autenticação. Dessa forma, a rotação das KSKs

fica mais confiável e menos dependente de ações manuais, o que é essencial em operações com vários participantes e prazos curtos.

Além dos aspectos técnicos, também existem políticas de segurança e boas práticas que todo operador de DNSSEC deve seguir. É importante manter registros detalhados das chaves, com datas de criação, troca e expiração, além das informações sobre os algoritmos usados. Testes periódicos ajudam a confirmar se a validação DNSSEC está funcionando corretamente. O acompanhamento constante das métricas de resolução e dos logs de validação permite detectar rapidamente qualquer problema na cadeia de confiança.

Em resumo, o gerenciamento do ciclo de vida das chaves no DNSSEC exige equilíbrio entre segurança e disponibilidade. A geração, distribuição e troca corretas das ZSKs e KSKs, aliadas ao uso de mecanismos automáticos, garantem que a infraestrutura permaneça estável e confiável. Ignorar qualquer uma dessas etapas pode comprometer a integridade de um domínio e reduzir a confiança dos usuários na *Internet*. Assim, cuidar das chaves não é apenas uma tarefa técnica, mas um elemento essencial para a segurança global da rede.

## 3.8 VALIDAÇÃO POR PARTE DOS RESOLVEDORES

A implementação do DNSSEC no lado autoritativo representa apenas uma parte da tarefa completa. Para que a validação ocorra completamente, é necessário que os *resolvers* recursivos consigam suportar e estar configurados para validar as respostas. Quando o *resolver* recebe uma resposta assinada, ele irá buscar o DNSKEY correspondente, além de verificar a assinatura pela cadeia de confiança que começa na raiz. Caso a assinatura dê inválida ou o registro DS estiver ausente, o resolver retorna um erro e a resposta é descartada automaticamente. Essa seção expõe o processo de validação com base na obra DNSSEC Mastery (2021).

O processo de resolução é mais complexo no DNSSEC, já que cada zona exige validação. Um resolvedor configurado para usar DNSSEC começa a sua busca nos servidores raiz normalmente. Porém, os servidores raiz nesse caso, além de responderem com os registros NS para o domínio de TLD, entregam também o registro DS e o RRSIG. Os resolvedores já têm posse das chaves públicas dos servidores raiz, logo, para validar essa resposta, simplesmente verificam o RRSIG;

caso seja valido, confiam nos registros NS e DS. O registro DS contém o *hash* da chave pública da zona filha; o resolvedor o usa para verificar a identidade dela.

Na prática, provedores de *Internet* e administradores de redes corporativas precisam permitir a validação em seus resolvedores internos. Essa configuração pode ser geralmente feita facilmente, bastando ativar a opção de validação no arquivo de configuração do BIND, por exemplo. Depois de habilitada, qualquer resposta inválida será rejeitada automaticamente, protegendo os usuários contra ataques de falsificação de DNS.

## 3.9 CADEIA DE CONFIANÇA

De acordo com a obra DNSKEY Mastery (2021) um elemento essencial é a cadeia de confiança. A cadeia se inicia na zona raiz, que é supervisionada pela ICANN (*Internet Corporation for Assigned Names and Numbers*), a entidade responsável pelo par KSK da zona. Esse par é conhecido como *Trust Anchor*, e sua chave pública é o ponto inicial de confiança da cadeia, estando presente nos resolvedores com DNSSEC habilitado. A zona raiz assina os registros DS que apontam para as chaves públicas das zonas imediatamente abaixo na hierarquia, nesse caso os TLDs como **.com**, **.net**, **.br**, etc. Por sua vez, cada TLD publica sua DNSKEY e assina um registro DS para cada domínio que delega, vinculando-o à sua KSK. Assim se constrói uma sequência de assinaturas que vai da raiz até o domínio consultado.

Em uma consulta DNSSEC para **www.google.com**, por exemplo, o servidor autoritativo retorna o registro A com o endereço IP, o RRSIG que assina esse registro, o DNSKEY com a chave pública da zona. O resolvedor segue a cadeia de validação verificando o RRSIG com o DNSKEY, confirmando o DNSKEY com o DS da zona pai e repetindo o processo até chegar à raiz. Se alguma assinatura não corresponder ou se um registro estiver faltando, a validação falha e a resposta é desconsiderada.

## 3.10 PROCESSO BÁSICO DE IMPLANTAÇÃO

Com base na obra DNSSEC Mastery (2021) essa seção busca discutir de maneira breve o processo de implantação do DNSSEC. Antes de começar a implementação, é importante verificar se a infraestrutura atual suporta o DNSSEC. Quando se trata de hardware, não há grandes exigências, mas os servidores autoritativos que fazem a assinatura digital dos registros precisam ter recursos

suficientes para lidar com respostas maiores e com o processamento extra gerado pelas assinaturas. Isso inclui ter uma CPU com desempenho maior e mais memória, principalmente em ambientes com alto volume de tráfego.

No aspecto de software, é importante que o servidor DNS utilizado tenha suporte nativo ao DNSSEC. Entre as soluções mais conhecidas estão o BIND, o KnotDNS e o PowerDNS. O BIND oferece suporte completo ao DNSSEC, incluindo a geração de chaves, a assinatura de zonas e a rotação automática. O KnotDNS, desenvolvido pelo NIC.cz, se destaca pelo alto desempenho e pela eficiência na assinatura de zonas grandes. Já o PowerDNS é valorizado pela flexibilidade e pela facilidade de integração com banco de dados, sendo muito usado por provedores que gerenciam diversos domínios.

O processo de configuração do DNSSEC em uma zona pode variar conforme o software utilizado, mas segue uma lógica parecida na maioria dos casos. O primeiro passo é gerar a ZSK e KSK. É importante que essa geração use algoritmos seguros, como RSA-SHA256 ou ECDSA, seguindo os tamanhos de chave recomendados. Depois disso, a chave pública correspondente deve ser publicada no registro DNSKEY da zona, garantindo que as assinaturas digitais possam ser corretamente validadas, protegendo as informações do domínio.

Após a criação das chaves, o próximo passo será assinar a zona. Esse processo cria registros RRSIG para cada grupo de registros existentes, conectando-os à ZSK utilizada. Agora a KSK assina o registro DNSKEY, certificando que a ZSK possa ser autenticada.

Depois da assinatura, é necessário publicar o registro DS na zona pai. Esse registro possui a *hash* da KSK, que é fundamental para estabelecer a cadeia de confiança entre a zona configurada e sua zona pai. A exposição do DS normalmente é feita pelo painel do registrador de domínios, e qualquer falha durante esse processo resultará na quebra da validação.

Após a implantação, é importante conduzir testes que validam se a implementação está correta e se a cadeia de confiança está funcionando conforme o esperado. Ferramentas como o comando dig podem ser usadas para receber os registros da zona e eles serem validados manualmente ou, até mesmo, se for o caso, utilizar um resolver ao invés de um cliente para fazer esses testes.

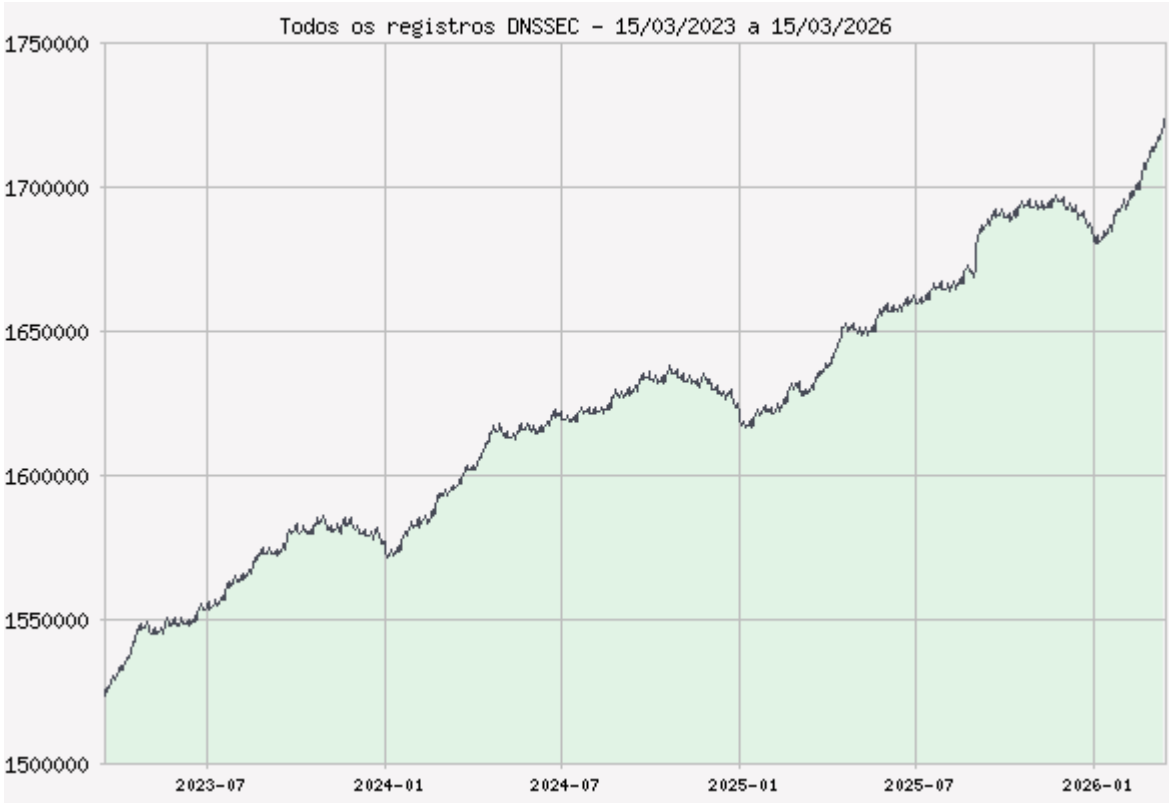
A fim de obter mais dados nos testes, ferramentas online como o DNSViz disponibilizam gráficos da cadeia de confiança, facilitando a identificação de problemas, como registros DS incorretos ou assinaturas expiradas. Outro recurso útil é o Verisign DNSSEC Debugger, que realiza uma verificação automatizada de um domínio, apresentando falhas de configuração.

Além das ferramentas mencionadas, validadores como o Unbound-host podem ser utilizados para verificar a autenticidade das assinaturas em consultas individuais. Além dos testes, o monitoramento contínuo dos logs também é fundamental para descobrir erros de validação e tomar ações corretivas o mais rápido possível.

# 4 PANORAMA DE ADOÇÃO DO DNSSEC

Com o objetivo de compreender de forma ampla a trajetória e o nível de adoção do DNSSEC, esta seção reúne e organiza as principais evidências presentes na literatura selecionada. Inicialmente, são apresentados individualmente os estudos utilizados como base, destacando suas contribuições e perspectivas sobre o tema. Em seguida, são analisados os fatores apontados por esses trabalhos que ajudam a explicar o comportamento observado no ecossistema DNS. Por fim, é discutido o estado atual da adoção do DNSSEC à luz dos estudos mais recentes, oferecendo uma visão consolidada do cenário contemporâneo e dos desafios ainda presentes. Como exemplo a figura 3 apresenta a evolução do DNSSEC dentre os domínios **.br**.

**Figura 3** – Evolução do DNSSEC dentre os domínios .br




Fonte: REGISTRO.BR. Estatísticas de domínios. Disponível em: https://registro.br/dominio/estatisticas/. Acesso em: 17 mar. 2026.

## 4.1 PRINCIPAIS RESULTADOS DOS TRABALHOS

Para fundamentar a análise sobre a adoção do DNSSEC, foram selecionados seis trabalhos que investigam diferentes dimensões dessa tecnologia, desde seus princípios de funcionamento até os desafios práticos enfrentados por administradores e organizações. Esses estudos permitem compreender tanto os avanços proporcionados pelo DNSSEC quanto as dificuldades que ainda limitam sua implementação em larga escala. Nesta seção, apresenta-se uma síntese dos principais pontos abordados por cada um dos trabalhos escolhidos, com o objetivo de contextualizar a discussão e evidenciar as contribuições que servem de base para este projeto.

A obra The Sad Story of DNSSEC, por Elliott e Moxley (2023), é uma análise desenvolvida a partir da ótica da experiência do usuário em 2023. Nela, os autores consultam os 100 domínios mais populares do Tranco por meio de um grande conjunto de 67.177 *resolvers*, que foram obtidos de uma base *crowd-sourced*, e classificam as respostas por categoria. Com base no conjunto de domínios selecionados e nas respostas recebidas por meio de cada resolvedor, os autores foram capazes de determinar quais resolvedores implementam de maneira adequada o DNSSEC. Os resultados do experimento revelam que apenas 33% dos resolvedores acessíveis publicamente implementam DNSSEC corretamente e que o restante ou implementa a extensão incorretamente (57%) ou apresenta comportamento inconsistente. A conclusão dada no estudo é de grande relevância, pois revela uma grande lacuna de adoção não só do lado dos operadores de sites, mas também dos que operam *resolvers*. E que até a data do estudo o DNSSEC não apresentava benefícios substanciais, já que para acessar boa parte dos sites os usuários teriam que aceitar registros que não foram validados (ELLIOTT; MOXLEY, 2023).

O estudo de Roth et al. (2019) tinha como foco os *registrars*, que são organizações responsáveis por vender domínios ao público. O trabalho se propôs a avaliar a evolução do suporte ao DNSSEC por parte dos *registrars*, já que trabalhos anteriores apontaram como uma das principais razões para a implantação lenta do DNSSEC a falta de suporte adequado. Do ponto de vista metodológico, os autores combinaram duas abordagens: (i) uma análise de longo prazo (51 meses, comparando a 21 meses em pesquisas anteriores) de todos os domínios de segundo nível em cinco TLDs da *Internet* (**.com**, **.net**, **.org**, .**se** e **.nl**), utilizando dados do

projeto Open INTEL; e (ii) testes práticos, comprando domínios nos 20 sites de registro mais populares para verificar o seu suporte ao DNSSEC. A análise de longo prazo revelou que entre os anos de 2015 e 2019 houve um aumento marginal no número de domínios com registros DNSKEY publicados nos TLDs **.com** e **.net**. Já os domínios sob os TLDs **.nl** e **.se** apresentaram uma evolução substancial. O estudo apontou como razão para esse fenômeno o apoio operacional e os incentivos econômicos oferecidos pelos registries desses TLDs. Em relação ao avanço dos *registrars*, de 2016 a 2019 dois novos *registrars* (NameBright e Google) passaram a oferecer suporte ao DNSSEC em seus próprios servidores e mais cinco (Alibaba, NetworkSolutions, Bluehost, register.com e Google) habilitaram suporte no caso de servidores externos. No entanto, o estudo aponta que, apesar dessa evolução, alguns registradores ainda não implementam e gerenciam a estrutura do DNSSEC de maneira adequada nem oferecem uma interface confiável a seus usuários. O estudo concluiu que, apesar da evolução considerável, ainda existem desafios operacionais não solucionados, principalmente por parte dos *registrars* (ROTH et al., 2019).

Por fim, Yajima et al. (2021) realizaram uma análise ampla sobre mecanismos de segurança no DNS para autoritativos (DNSSEC, DNS Cookies, CAA etc.), cobrindo 13 servidores-raiz, 276 TLDs e 10 mil domínios populares. A coleta de dados foi realizada por meio de requisições que testaram se os servidores autoritativos implementavam as tecnologias. Em razão do objetivo do estudo, foram escolhidos critérios simples que não distinguem entre implantações adequadas e inadequadas, apenas determinam se um servidor em questão faz uso da tecnologia. Seus resultados revelaram que mecanismos de segurança usados para combater ameaças à comunicação DNS, como o DNSSEC e DNS Cookies, tiveram grande adoção por parte dos servidores-raiz e dos TLDs, porém a taxa entre os 10 mil domínios foi baixa, sendo de apenas 7,67% para o DNSSEC e 17,40% para o DNS Cookies. Além de revelar o nível de adoção, o estudo analiticamente correlacionou as taxas com o custo e a complexidade de operação das tecnologias. Como esperado, tecnologias mais custosas e complexas tendem a ter uma taxa mais baixa, como é o caso do DNSSEC. Por fim, o estudo aponta como um fator-chave para aumentar a presença e incentivar a configuração adequada dessas tecnologias o desenvolvimento de ferramentas que facilitem a implantação e cita como exemplo o caso do HTTPS com Let’s Encrypt, uma ferramenta que ajudou muito no seu crescimento (YAJIMA et al., 2021).

No trabalho de Chung et al. (2017a), é mostrada a análise feita ao longo de muito tempo sobre a saúde operacional do ecossistema do DNSSEC, além de ser um dos estudos mais influentes sobre o assunto. Por 21 meses, os autores acompanharam todos os domínios assinados sob **.com**, **.**net e **.org**, além de realizarem medições ativas com mais de 4 mil *resolvers* para analisar seu comportamento de validação. Dentre as buscas feitas, os resultados mostram a prevalência da má gestão, já que 31% dos domínios assinados esqueciam de publicar os registros necessários para validação, cerca de 30% dos domínios assinados não tinham DS na zona pai, resultando na quebra da cadeia de confiança, 1,7% falharam em fornecer RRSIG para SOA e 0,6% traziam RRSIG errados. Na chave pública, os autores relatam 39% de KSKs fracas (1024-bit RSA, abaixo do recomendado) e mais de 90% de ZSKs fracas, além de 70% dos domínios nunca rotacionarem a KSK no período, indo contra as melhores práticas de segurança. Agora, pelos clientes, mesmo que 82% dos *resolvers* analisados sinalizassem interesse por DNSSEC, apenas 12%, aproximadamente, de fato validavam as respostas. Feita a junção, os resultados indicam que o principal obstáculo para a adoção não é apenas “ligar a assinatura”, mas operar corretamente todo o PKI do DNSSEC de ponta a ponta, em que a automação parece ser mais importante para reduzir o erro humano (CHUNG et al., 2017a).

O relatório de Kampourakis e Karopoulos (2022) mostra uma atualização detalhada sobre a adoção de DNSSEC na União Europeia e no restante do mundo, trazendo um diferencial importante quando reunidos dados de fontes públicas e incluídas medições próprias feitas com a ferramenta MECSA. Como destaque, o estudo aponta que, no primeiro trimestre de 2022, cerca de 40% dos usuários nos países da União Europeia utilizavam validadores, ou seja, verificavam respostas assinadas, enquanto a média global ficava em torno de 27%. O estudo destaca as grandes diferenças dentro do bloco europeu, mostrando que os países mais avançados, como República Tcheca, Dinamarca, Finlândia, Luxemburgo e Suécia, ultrapassam 70%, enquanto um grupo intermediário formado por Estônia, Alemanha e Países Baixos está entre 50% e 70%. Já os países com menor adoção, como Hungria, Malta e Romênia, ficam abaixo de 10%, seguidos de outro grupo entre 10% e 30%, que inclui Áustria, Bulgária, Croácia, Chipre, Grécia, Irlanda, Itália, Lituânia, Eslováquia, Eslovênia e Espanha. O relatório também analisa o cenário do DNS

criptografado, abordando o uso de DoT, DoH e DoQ, e mostra que o tráfego em texto claro ainda é muito maior, cerca de mil vezes mais. Indica ainda que o DoT representa aproximadamente 0,4% e é aproximadamente sete vezes mais usado que o DoH, com um aumento pequeno a partir de 2020, quando alguns navegadores passaram a ativar o DoH por padrão. Embora não substituam o DNSSEC, essas iniciativas de privacidade ajudam a construir prioridades técnicas e políticas públicas relacionadas à segurança e proteção de dados na *Internet* (KAMPOURAKIS; KAROPOULOS, 2022).

O estudo de Misell et al. (2025) Measuring the Deployment of DNSSEC Bootstrapping Using Authenticated Signals apresenta uma análise em larga escala sobre o estado atual do DNSSEC e, especialmente, sobre a adoção dos novos mecanismos de automação propostos pelo IETF para facilitar sua implantação. Os autores partem do diagnóstico de que, apesar de existir há quase três décadas, o DNSSEC ainda enfrenta obstáculos significativos para alcançar ampla adoção na *Internet*, em grande parte devido à necessidade de coordenação entre operadores de zona, registradores e registros. Com base em um conjunto de mais de 287 milhões de zonas analisadas, o trabalho busca entender como mecanismos de automação, especialmente CDS/CDNSKEY e o recém-padronizado *Authenticated Bootstrapping* (AB), podem reduzir as barreiras históricas de implantação. Os resultados mostram que a adoção do DNSSEC permanece limitada: apenas 5,5% das zonas estão corretamente assinadas, enquanto cerca de 93% permanecem totalmente sem DNSSEC. Além disso, aproximadamente 640 mil zonas apresentam falhas de validação, e outras 3,1 milhões configuram-se como *secure islands*, isto é, zonas assinadas, mas sem DS registrado no TLD, situação que poderia ser resolvida por mecanismos de automação. O estudo revela ainda que a adoção de CDS/CDNSKEY, pré-requisito para o *bootstrapping* automático, também é modesta: apenas 3,7% das zonas publicam CDS, com maior prevalência entre operadores menores ou regionalmente incentivados (MISELL et al., 2025).

O artigo de Chung et al. (2017b) investiga os motivos estruturais que explicam a baixa adoção do DNSSEC, apesar de sua padronização consolidada e do amplo suporte entre TLDs. Os autores demonstram que o principal gargalo na cadeia de implementação não se encontra no nível dos domínios ou do protocolo, mas sim nos *registrars*, responsáveis por intermediar a publicação dos registros DS nos TLDs. Por

meio de experimentos controlados, incluindo a compra e configuração de domínios em 20 dos *registrars* mais populares, o estudo revela que a maioria dessas empresas oferece suporte limitado, interfaces confusas, ausência de automação e, em alguns casos, procedimentos inseguros para envio de chaves. Apenas três *registrars* suportam DNSSEC quando também operam o DNS, e somente um deles o habilita automaticamente. Nos casos em que o DNSSEC depende da interação entre o registry, o registrar e um *DNS operator* externo, os obstáculos tornam-se ainda mais evidentes. Somente 11 *registrars* permitem a configuração manual de registros DS, e poucos realizam qualquer forma de validação técnica antes de publicá-los, aumentando a probabilidade de erros operacionais. O estudo identifica ainda uma forte concentração: a maior parte dos domínios assinados provém de um número reduzido de *registrars*, indicando que boas práticas não se disseminam de forma homogênea no mercado. Além das barreiras técnicas e operacionais, os autores observam que a adoção é sensível a incentivos econômicos e institucionais. TLDs como **.se** e **.nl** apresentaram taxas significativamente maiores após a introdução de descontos para domínios assinados, reforçando que fatores externos podem influenciar mais a adoção do que melhorias técnicas isoladas (CHUNG et al., 2017b).

## 4.2 DISCUSSÃO

Embora o DNSSEC tenha sido projetado para fortalecer a segurança do ecossistema DNS, sua trajetória de implantação ao longo dos anos revela um avanço mais lento do que inicialmente esperado. A distância entre o potencial da tecnologia e sua adoção prática indica a presença de desafios estruturais, operacionais ou até mesmo organizacionais que influenciaram e influenciam seu desenvolvimento na *Internet*.

Diversos estudos foram conduzidos para medir a evolução do DNSSEC na prática, porém, devido às diferentes metodologias e diferentes contextos de análise, foram levantados diferentes fatores que podem explicar a evolução lenta da sua implementação.

Com base nos trabalhos selecionados, foi possível identificar um conjunto de fatores recorrentes que influenciam direta ou indiretamente a adoção do DNSSEC. Esses elementos emergem tanto das análises técnicas quanto das avaliações

operacionais realizadas pelos autores, revelando padrões, obstáculos e motivações comuns entre diferentes cenários de implementação.

## 4.3 FATORES ECONÔMICOS E INCENTIVOS

Dois fatores determinantes levantados pelos estudos foram os incentivos econômicos e institucionais. Segundo a pesquisa de Roth et al. (2019), a presença de incentivos diretos, como descontos fornecidos por registries e suporte técnico especializado, aumenta muito as taxas de adoção. Nos ccTLDs **.nl** e **.se**, como exemplo, mais de 54% dos domínios estão assinados, em contraste com menos de 1,1% em gTLDs como **.com**, **.net** e **.org**, onde não se encontram incentivos claros ou programas estruturados. Em nível nacional, o relatório de Kampourakis e Karopoulos (2022) corrobora o mesmo fundamento: países que apresentam políticas sólidas e metas já definidas para a implantação do DNSSEC em domínios governamentais apresentam taxas de validação acima dos 70%, enquanto regiões sem coordenação constitucional permanecem abaixo dos 30%. Outra análise, inclusive citada por esse mesmo estudo, que apoia essa interpretação é a análise da APNIC, que destaca que economias como Suécia, Islândia e Arábia Saudita avançaram graças a iniciativas como capacitação técnica, subsídios a *registrars* e diretrizes nacionais claras para implantação (SUEMATSU, 2020). Por meio desses dados, é possível analisar que, embora a decisão de ativação do DNSSEC seja tecnicamente viável, sua adoção depende fortemente de pressões de mercado, alinhamento regulatório e apoio institucional.

Outro contribuinte para o avanço lento é a comparação de custos versus benefícios. Na pesquisa de Yajima et al. (2021), é mostrado que tecnologias que têm um custo de implantação mais baixo e que oferecem resultados mais imediatos e visíveis são principalmente escolhidas para implantação, como é o caso do SPF e do DMARC, que causam a redução do SPAM. Por outro lado, o DNSSEC resolve problemas que são menos perceptíveis aos usuários comuns, como é o caso de ataques de envenenamento de cache e falsificação de respostas. Logo, como esses eventos são raramente vistos no dia a dia, o incentivo à implementação acaba sendo baixo, e muitos preferem não investir por não achar uma operação justificável.

## 4.4 DIFICULDADE DE IMPLEMENTAÇÃO

Mesmo assim, em ambientes com incentivos, a complexidade operacional continua sendo uma barreira significativa. Chung et al. (2017a) identificaram que uma parte relevante dos domínios assinados ainda cometia erros de implantação e gerenciamento: utilização de chaves de tamanhos inadequados, prática inadequada de *rollover*, assinaturas expiradas e até mesmo a presença de chaves compartilhadas por múltiplos domínios. Essa última prática mencionada é principalmente arriscada, já que o comprometimento de uma única chave pode afetar centenas de milhares de domínios de uma só vez. Roth et al. (2019) destacam como alternativa o uso de automações para automatizar processos, podendo diminuir erros humanos, mas também alertam para o uso inadequado dessas automações, que podem gerar problemas se forem mal aplicadas. Um exemplo marcante de falha operacional citada é o incidente envolvendo o registrador Binero, em que a remoção simultânea dos registros DS de mais de 130 mil domínios deixou praticamente toda a base sem proteção por quase dois meses. Embora o estudo não declare explicitamente a causa, o padrão em larga escala com retirada e reintrodução sincronizada de chaves sugere fortemente que algum mecanismo de automação mal configurado estava envolvido. Isso mostra que só automatizar não basta: é preciso ter processos bem definidos, fazer auditorias regulares e manter um monitoramento constante para evitar incidentes.

## 4.5 SUPORTE DOS REGISTRARS

Outro fator importante é o suporte por parte dos *registrars; eles* desempenham um papel central na adoção do DNSSEC porque são os únicos que podem inserir o registro DS no domínio pai, etapa essencial para estabelecer a cadeia de confiança. Quando o registrar não oferece suporte adequado, como interfaces incompletas, ausência de validação ou necessidade de processos manuais suscetíveis a erros, a implantação se torna complexa. Chung et al. (2017b) mostram que muitos *registrars* simplesmente não suportavam DNSSEC ou exigiam procedimentos complicados, o que levava a baixas taxas de ativação e a altas proporções de domínios parcialmente implantados (sem DS). Roth et al. (2019) reforçam esse cenário ao demonstrar que, embora o suporte tenha melhorado ao longo dos anos, ainda há casos de *registrars* que publicam DNSKEYs sem carregar os DS correspondentes, deixando os domínios

invalidados. Assim, o nível de suporte dos *registrars,* incluindo automação, validação e facilidade de uso, afeta diretamente tanto a adoção quanto a qualidade da implantação do DNSSEC.

## 4.6 O PRINCIPAL FATOR

Entre todos os fatores analisados, os incentivos econômicos e institucionais se destacam como o fator mais decisivo para impulsionar a adoção do DNSSEC. Os dados mostram que, sempre que há estímulos estruturados, sejam financeiros, regulatórios ou organizacionais, as taxas de assinatura aumentam de forma significativa. Tanto Roth et al. (2019) quanto o relatório de Kampourakis e Karopoulos (2022), estudos que fazem uma análise geral de adoção, corroboram essa tese, como mencionado anteriormente. Até mesmo estudos centrados em problemas técnicos reforçam essa conclusão: Chung et al. (2017a) documentam falhas operacionais e má gestão generalizada, mas mostram que esses problemas persistem principalmente onde faltam mecanismos institucionais de incentivo ou auditoria contínua. Já Elliott e Moxley (2023) revelam que, apesar de anos de padronização, a validação permanece mínima justamente porque, sem pressão econômica ou regulatória, *resolvers* e operadores não priorizam o DNSSEC. Mesmo iniciativas modernas de automação, embora reduzam custos operacionais, ainda mostram adoção limitada, o que reforça que a ausência de incentivos externos continua sendo a barreira predominante segundo Misell et al. (2025). Em conjunto, os estudos convergem ao demonstrar que, mais do que avanços técnicos ou melhorias de suporte, é o alinhamento institucional e econômico que efetivamente altera o cenário e determina onde o DNSSEC avança de forma consistente. Em resumo, os fatores apresentados revelam que a adoção do DNSSEC não avança de forma lenta por um motivo singular, mas sim pela junção de desafios econômicos, operacionais e estruturais que se somam na prática. Incentivos insuficientes reduzem o interesse inicial; a complexidade técnica desencoraja mesmo aqueles que desejam adotar; e a falta de suporte por parte dos *registrars* dificulta todo o processo operacional. O resultado é um ecossistema em que esforços individuais, mesmo que importantes, dificilmente se traduzem em segurança efetiva de ponta a ponta.

## 4.7 ESTADO ATUAL

Em contraste com as dificuldades observadas, os estudos mais recentes apontam que a adoção do DNSSEC segue em crescimento. Mesmo com a ampliação contínua do volume de domínios registrados, a proporção de zonas assinadas tem se elevado de forma consistente. Esse cenário suscita questionamentos sobre o real estado atual de implementação do DNSSEC e sobre quais perspectivas podem ser delineadas para os próximos anos.

Os dois estudos mais recentes analisados retratam um cenário no qual a adoção do DNSSEC ainda permanece limitada, embora com nuances importantes entre a perspectiva do usuário do estudo de Elliott e Moxley (2023) e a visão estrutural do ecossistema DNS do estudo de Misell et al. (2025). Em ambos os casos, a conclusão geral é de que o DNSSEC ainda está longe de alcançar ampla implantação, apesar de progressos técnicos e padronizações recentes.

Do ponto de vista do usuário, o estudo de Elliott e Moxley (2023) evidencia que, mesmo nos casos em que os domínios implementam DNSSEC corretamente, a proteção não se materializa porque a maioria dos *resolvers* públicos não valida as assinaturas. Em uma análise envolvendo mais de 24 mil *resolvers* públicos, apenas cerca de um terço apresentou comportamento consistente com validação adequada, enquanto mais da metade retornou respostas incorretas ou indicativos de cadeias quebradas, mesmo para domínios válidos. Isso demonstra que, na prática, a garantia criptográfica oferecida pelo DNSSEC raramente alcança o usuário, pois grande parte da infraestrutura recursiva ignora ou interpreta incorretamente os registros de segurança.

Já o estudo de Misell et al. (2025) amplia essa visão ao avaliar mais de 287 milhões de zonas DNS. Ele revela que apenas 5,5% das zonas estão corretamente assinadas, enquanto mais de 93% permanecem completamente sem DNSSEC. Além disso, cerca de 3,1 milhões de zonas aparecem como *secure islands*, ou seja, zonas assinadas que não possuem o registro DS correspondente no TLD, impedindo sua validação. Embora o estudo mostre avanços em mecanismos de automação como CDS, CDNSKEY e o recém-padronizado *Authenticated Bootstrapping*, sua adoção ainda é baixa e restrita a poucos operadores, o que limita o impacto desses recursos no ecossistema global. Apenas três provedores (Cloudflare, deSEC e Glauca Digital)

implementam o *bootstrapping* autenticado, ainda que o façam de forma praticamente correta em 99,9% dos casos observados.

A combinação desses resultados revela um padrão claro: o principal obstáculo atual não é a falta de tecnologia ou padronização, mas sim a ausência de adoção coordenada. No lado autoritativo, a grande maioria das zonas ainda não utiliza DNSSEC, e mesmo onde ele é adotado, erros de configuração, ausência de DS ou falta de automação dificultam o estabelecimento de cadeias de confiança completas. No lado dos *resolvers*, a ausência de validação efetiva significa que, mesmo quando a cadeia está correta, os usuários continuam desprotegidos, o que, por sua vez, reduz incentivos para os proprietários de domínios investirem em DNSSEC.

Em síntese, os estudos de 2023 e 2025 apontam que o estado atual do DNSSEC é marcado por baixa adoção, validação inconsistente e benefícios limitados ao usuário final, ainda que avanços significativos em automação e padronização ofereçam um caminho promissor para o futuro. Entretanto, tais avanços só terão impacto real se acompanhados de maior adesão por parte de registradores, operadores e *resolvers*, além de incentivos claros para adoção em larga escala.

## 4.8 AUTOMAÇÕES

Um dos fatores para a lenta adoção do DNSSEC, como citado anteriormente, é justamente a dificuldade de implementação. Para reduzir essa barreira, duas tecnologias tornaram-se centrais nas propostas atuais de automação: os registros CDS/CDNSKEY e o mais recente mecanismo de *Authenticated Bootstrapping* (AB).

## 4.9 CDS E CDNSKEY

Os registros CDS e CDNSKEY foram padronizados com o objetivo de permitir que o próprio operador DNS informe ao registro quais DS *records* devem ser instalados ou atualizados no domínio pai. Isso diminui drasticamente a necessidade de interação manual do usuário final (RFC 8078, 2017).

Em um cenário tradicional, quando um operador habilita DNSSEC ou troca suas chaves, o responsável pelo domínio deve copiar manualmente o novo *hash* (DS) para o painel do registrador. Esse processo é fonte comum de erros operacionais, de acordo com Roth et al. (2019), erros esses como DS inválidos ou expirados, problemas amplamente documentados em medições globais.

Essa tecnologia traz vantagens como: *rollover* automático de chaves e redução de erros humanos. Além disso, já é uma tecnologia bem madura tecnicamente e, de acordo com Misell et al. (2025), entre os domínios que publicam CDS, 99,7% apresentam registros consistentes entre todos os servidores autoritativos.

## 4.10 AUTHENTICATED BOOTSTRAPPING (AB)

Em 2024, o RFC 9615 padronizou o *Authenticated Bootstrapping*, considerado atualmente a solução mais promissora para permitir configuração automática e segura do DNSSEC, inclusive na fase inicial. O operador publica cópias autenticadas dos CDS/CDNSKEY em zonas de sinalização (*signaling zones*) que já são protegidas por DNSSEC, criando uma cadeia de confiança verificável antes mesmo de o domínio estar assinado. Esse processo elimina o problema histórico da falta de autenticação inicial e permite, pela primeira vez, ativação totalmente automática do DNSSEC, com segurança equivalente à de um *rollover* normal. (RFC 9615, 2024)

Segundo Misell et al. (2025), apenas três operadores (Cloudflare, deSEC e Glauca Digital) implementam AB atualmente, mas 99,9% das zonas que publicam as sinalizações o fazem corretamente, indicando maturidade técnica e boa viabilidade operacional.

## 4.11 EXPECTATIVAS FUTURAS

Apesar dos avanços recentes em automação, os estudos analisados indicam que, na prática, o fator que se mostra mais determinante continua sendo a presença de incentivos econômicos e institucionais. Quando registries e governos implementam políticas claras, oferecem benefícios financeiros, monitoram ou estabelecem metas de implantação, as taxas de adoção aumentam de forma visível e consistente. Em contraste, regiões e TLDs sem incentivos estruturados tendem a permanecer com níveis reduzidos de assinatura e validação. Tendo como exemplo a diferença apontada por Roth et al. (2019), em que os TLDs **.nl** e **.se** que ofereciam incentivos tinham mais da metade dos seus domínios de segundo nível assinados, enquanto os TLDs **.com**, **.net** e **.org** tinham apenas um pouco mais de 1%. Ou seja, novas tecnologias complementares ajudam, já que reduzem a complexidade, porém, em cenários sem incentivos claros e amplos, o ganho permanece mínimo.

No caso do *Authenticated Bootstrapping*, por ser ainda uma tecnologia muito recente, é incerto o impacto que poderá trazer. Já os registros CDS/CDNSKEY foram propostos há mais de uma década e não se mostraram ser essa grande solução, tendo em vista que o crescimento do DNSSEC permanece lento. Dessa forma, ainda que as automações reduzam erros, simplifiquem operações e eliminem barreiras técnicas, é a existência de incentivos externos que tem demonstrado maior capacidade de transformar o cenário de maneira significativa.

Em resumo, de acordo com as evidências encontradas, pode-se observar que o futuro do DNSSEC dependerá não apenas da evolução tecnológica, mas principalmente da capacidade do ecossistema institucional em adotar políticas que incentivem sua implementação. Embora mecanismos como CDS/CDNSKEY e o *Authenticated Bootstrapping* representem avanços relevantes, tais soluções mostram-se insuficientes quando não há estímulos externos que promovam sua adoção em larga escala. Dessa forma, o progresso efetivo do DNSSEC tende a emergir da convergência entre automações consolidadas e incentivos econômicos, regulatórios ou organizacionais capazes de orientar *registrars*, *registries* e operadores a priorizar a segurança do DNS. Caso essas estratégias sejam ampliadas, há potencial para que o DNSSEC se torne um elemento fundamental bem mais presente na infraestrutura de segurança da *Internet*. Contudo, na ausência de incentivos, é provável que o ritmo de adoção permaneça lento e fragmentado, reproduzindo as dificuldades observadas ao longo dos últimos anos.

# 5 CONCLUSÃO

A análise desenvolvida ao longo deste trabalho permitiu entender de forma ampla o cenário atual da adoção do DNSSEC e os principais desafios que ainda impedem sua expansão. A partir da revisão teórica e dos estudos analisados, ficou evidente que, embora o DNSSEC seja uma solução sólida contra ataques de falsificação no DNS, sua implantação continua enfrentando dificuldades em diferentes partes da infraestrutura da *Internet*.

Primeiro, ficou claro que o DNS tradicional possui limitações importantes, já que não oferece autenticação ou verificação de integridade das respostas. O DNSSEC foi criado justamente para corrigir essas falhas, adicionando assinaturas digitais e criando uma cadeia de confiança baseada em chaves criptográficas. No entanto, a tecnologia só funciona corretamente quando todas as etapas do processo estão bem configuradas, desde a assinatura da zona até a validação feita pelos resolvedores.

Com base nos estudos revisados, foi possível perceber que a adoção do DNSSEC ainda é desigual. Em alguns países e TLDs onde existem incentivos, suporte técnico e políticas públicas bem definidas, a taxa de implantação é bem maior. Por outro lado, muitos domínios e registradores populares ainda não suportam a extensão, e mesmo entre os que suportam, erros de configuração continuam comuns, como ausência de registro DS, chaves fracas, assinaturas expiradas e problemas na cadeia de confiança.

Outro ponto importante observado nos estudos é que a validação no lado do cliente ainda é muito baixa. Muitos resolvedores públicos não validam as assinaturas do DNSSEC, o que impede que os usuários recebam de fato a proteção oferecida pelo DNSSEC. Isso significa que, mesmo quando um domínio está configurado corretamente, a segurança não é garantida se o resolvedor não realizar a verificação das assinaturas.

Com tudo isso, a hipótese inicial do trabalho foi parcialmente confirmada: o DNSSEC realmente avança em um ritmo lento. As razões dadas na hipótese de fato fazem parte do conjunto de fatores que influenciam o estado atual de adoção do DNSSEC. Porém, o fator mais relevante observado foi justamente os incentivos econômicos e institucionais e não a alta complexidade do gerenciamento de domínios,

custo econômico ou falta de mão de obra especializada para manter a infraestrutura, mesmo que esses fatores sejam relevantes.

Diante dessas observações, conclui-se que o DNSSEC é uma ferramenta fundamental para aumentar a segurança do DNS, mas sua evolução depende de mais do que sua eficácia técnica. Para que extensão seja adotado em maior escala, é necessário incentivar boas práticas, melhorar o suporte dos *registrars*, investir em automação para reduzir erros humanos, simplificar as etapas de configuração e promover capacitação técnica. Só com a participação conjunta de operadores, provedores, governos, pesquisadores e da comunidade técnica será possível construir um ecossistema DNS mais seguro, confiável e preparado para o futuro.

# 6 REFERÊNCIAS BIBLIOGRÁFICAS


ARANHA, Diego de Freitas. **Serviço de nomes e roteamento para redes de anonimização de tráfego**. 2007. 147 f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Computação, Universidade Estadual de Campinas – UNICAMP, Campinas, 2007. Disponível em:https://www.researchgate.net/publication/292156696_Servico_de_nomes_e_roteamento_para_redes_de_anonimizacao_de_trafego. Acesso em: 11 jun. 2025.

**BRAGA, Alexandre Melo; DAHAB, Ricardo**. Criptografia assimétrica para programadores – evitando outros maus usos da criptografia em sistemas de software. In: SOCIEDADE BRASILEIRA DE COMPUTAÇÃO (Org.). Minicursos do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – SBSeg 2018. Porto Alegre: SBC, 2018. p. 50–99.

**CHUAT, Laurent et al**. SoK: delegation and revocation, the missing links in the Web's chain of trust. 2019. Disponível em: https://arxiv.org/pdf/1906.10775.pdf. Acesso em: 11 jun. 2025.

**CHUNG, T.; et al**. A longitudinal, end-to-end view of the DNSSEC ecosystem. In: USENIX SECURITY SYMPOSIUM, 26., 2017, Vancouver. Proceedings […]. S.l.: USENIX, 2017a. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-chung.pdf. Acesso em: 26 jun. 2025.

**CHUNG, Taejoong; VAN RIJSWIJK-DEIJ, Roland M.; CHOFFNES, David; LEVIN, Dave; MAGGS, Bruce; MISLOVE, Alan; WILSON, Christo**. Understanding the role of registrars in DNSSEC deployment. In: ACM INTERNET MEASUREMENT CONFERENCE (IMC), 2017, London. Proceedings […]. p. 369–383. 2017b. Disponível em: https://www.cs.umd.edu/~dml/papers/dnssec_imc17.pdf. Acesso em: 22 nov. 2025.

**CORRIGANGIBBS, Henry; MU, Wendy; BONEH, Dan; FORD, Bryan**. Ensuring highquality randomness in cryptographic key generation. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY – CCS, 20., 2013, Berlin. Proceedings. New York: ACM Press, 2013. p. 685696. Disponível em: https://people.csail.mit.edu/henrycg/files/academic/papers/ccs13ensuring-full.pdf. Acesso em: 11 jun. 2025.

**ELLIOTT, A.; MOXLEY, J**. The sad story of DNSSEC: Exploring the real-world deployment of Domain Name System Security Extensions. In: SECURING THE INTERNET INFRASTRUCTURE, 2023, Atlanta. Proceedings […]. ACM, 2023. Disponível em: https://alexkelliott.github.io/dnssec/TheSadStoryOfDNSSEC.pdf. Acesso em: 26 jun. 2025.

IETF. **RFC 8078: Managing DS records from the parent via CDS/CDNSKEY**. 2017. Disponível em: https://www.rfc-editor.org/rfc/rfc8078. Acesso em: 26 jun. 2025.

IETF. **RFC 9615: Authenticated bootstrapping using DNS. 2024**. Disponível em: https://www.rfc-editor.org/rfc/rfc9615. Acesso em: 26 jun. 2025.

KAMPOURAKIS, G.; KAROPOULOS, G. **Internet standards: Domain Name System Security Extensions (DNSSEC) standards – an analysis of uptake in the EU**. European Commission, Joint Research Centre. Luxembourg: Publications Office of the European Union, 2022. DOI: 10.2760/975868.

LUCAS, M. W. **DNSSEC Mastery**. Michigan: Tilted Windmill Press, 2021. E-book Kindle.

**MISELL, Q.; STEURER, Florian; ZIRNGIBL, Johannes; FELDMANN, Anja; FIEBIG, Tobias**. Measuring the Deployment of DNSSEC Bootstrapping Using Authenticated Signals. In: ACM Internet Measurement Conference, 2025, Madison. Proceedings […]. New York: ACM, 2025. p. 1–8. DOI: 10.1145/3730567.3764501. Acesso em: 22 nov. 2025.

MORAES, CRISTINE DO C.S.B. **Template para trabalho de conclusão de curso da Faculdade de Tecnologia de Americana**. Americana, SP: FATEC, 2013

RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3**. RFC 8446. IETF, 2018. Disponível em: https://www.rfc-editor.org/rfc/rfc8446.html. Acesso em: 8 jun. 2025.

**ROTH, S.; VAN RIJSWIJK-DEIJ, R.; CHUNG, T**. Tracking registrar support for DNSSEC: It's slowly getting better. In: INTERNET MEASUREMENT CONFERENCE (IMC '19), 2019, Amsterdam. Proceedings […]. ACM, 2019. DOI: 10.1145/3355369.3355596. Acesso em: 26 jun. 2025.

TANENBAUM, Andrew S.; WETHERALL, David J. *Computer Networks*. 6. ed. Hoboken: Pearson, 2021.

**YAJIMA, T.; et al**. Measuring adoption of DNS security mechanisms with cross-sectional approach. In: IEEE GLOBAL COMMUNICATIONS CONFERENCE (GLOBECOM 2021), 2021, Madrid. Proceedings […]. IEEE, 2021. DOI: 10.1109/GLOBECOM46510.2021.9685960.