



DNS

FORMAÇÃO “ECOSSISTEMA TÉCNICO, JURÍDICO
E ADMINISTRATIVO DE UM CCTLD”

Assis Guerreiro, .PT
Engenheiro de Infraestruturas

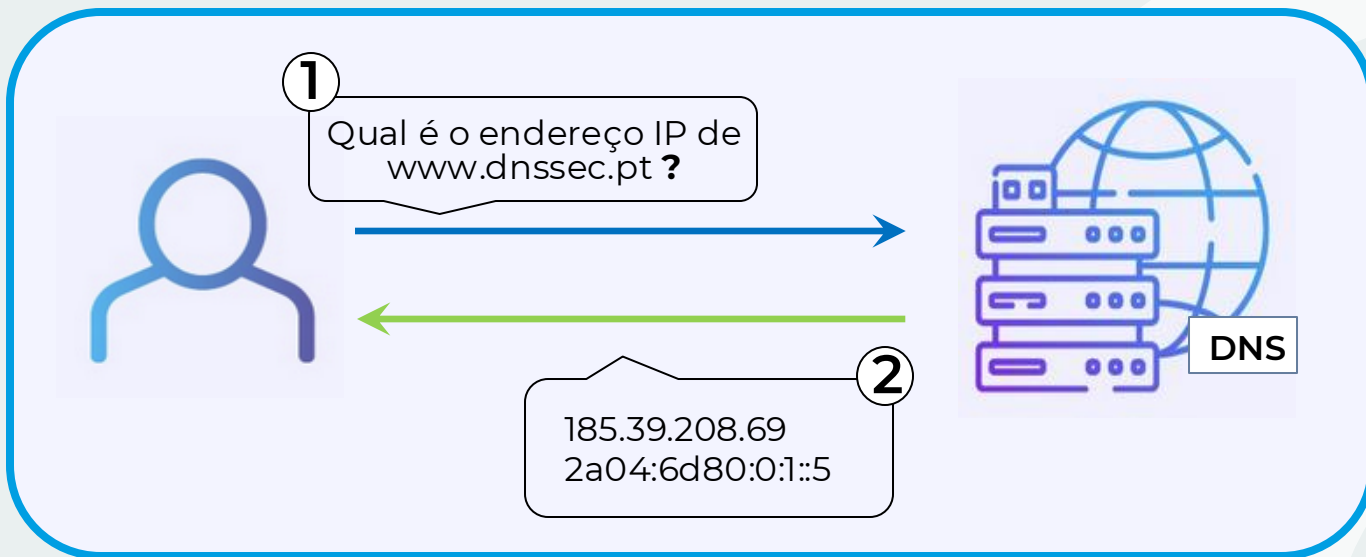
24.09.2025, Moçambique

Agenda

1. O serviço DNS
2. DNS Autoritativo vs DNS Recursivo
3. Gestão DNS num ccTLD
4. Vulnerabilidades
5. Servidores secundários / Anycast
6. DNSSEC
7. Requisitos do protocolo DNS

Domain Name System

Serviço de resolução de nomes de domínios legíveis e fáceis de memorizar em endereços IP e vice-versa.



O Serviço DNS

DNS é fundamental para a Internet!

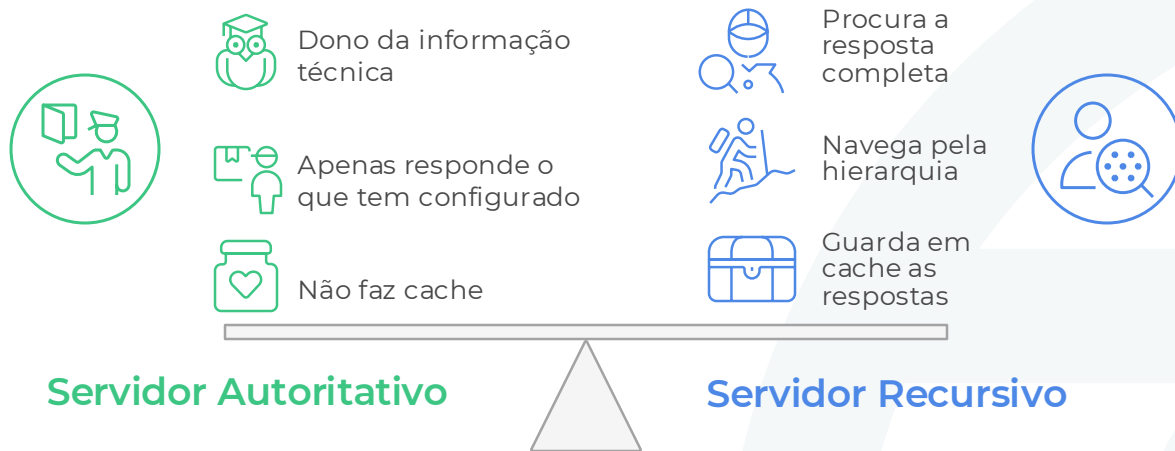


O Serviço DNS



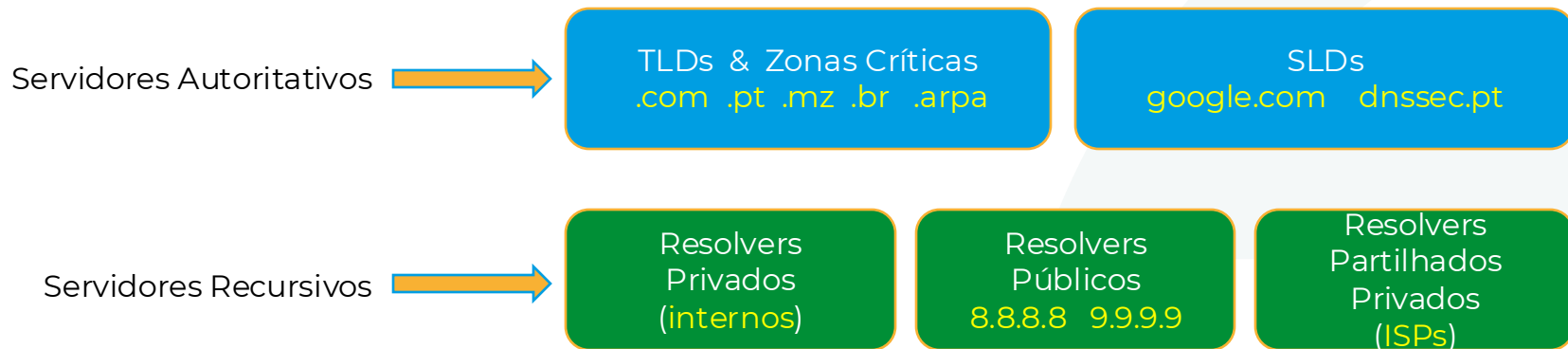
DNS Autoritativo vs DNS Recursivo

Comparando Servidores Autoritativos e Recursivos



DNS Autoritativo vs DNS Recursivo

Classificação de operadores por Servidores Autoritativos e Servidores Recursivos



Gestão DNS num ccTLD

ICANN → ccTLD Registry → Registrars → Titulares → Utilizadores

ccTLD = domínio de topo nacional (.pt, .mz, .br, .ao)

Gerido por entidades nacionais (ex.: Associação DNS.PT)

Responsável por:

-  Registo e gestão de domínios (contactos, faturação)
-  Servidores autoritativos para o ccTLD
-  Publicação da zona na Internet
-  Implementar iniciativas as melhores práticas

Vulnerabilidades

Insecure by design

Protocolo desenvolvido sem requisitos de segurança o que o torna o serviço DNS vulnerável a diversos tipos de ataques, nomeadamente:

DNS Spoofing / DNS Cache Poisoning / DNS Hijacking

-  Falsificação das respostas DNS
-  Redirecionamento para servidores de nomes/sites com fins maliciosos, controlados pelo atacante
-  Respostas para domínios que não existem

Daniel Kaminsky 2008

<http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

Vulnerabilidades

2008: ICANN Domain Hijacking

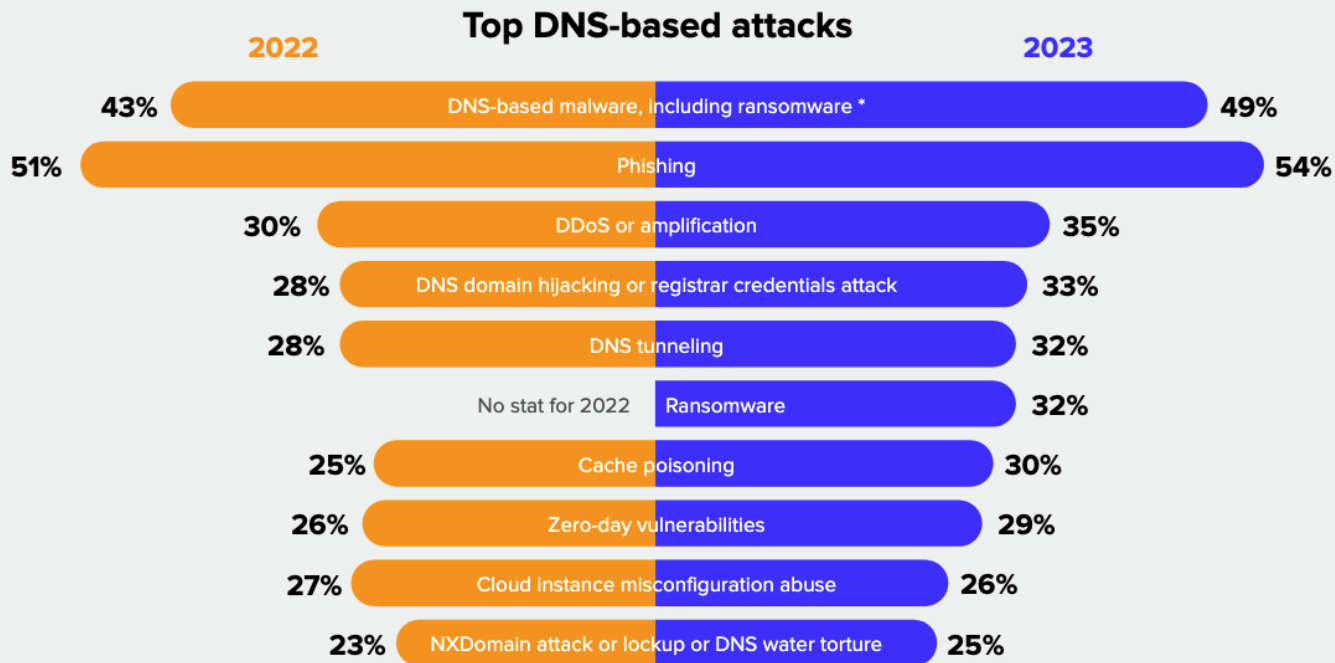
The Internet Corporation for Assigned Names and Numbers (ICANN) is the governing body that supports the DNS. In June 2008, [ICANN fell victim to a DNS hijacking attack](#) that redirected traffic intended for ICANN's websites to a malicious site containing political propaganda. The incident was an embarrassment for ICANN because of its prominent role in the security and stability of the internet.

2013: New York Times and Twitter Hijacking

A more prominent example of DNS hijacking emerged in August 2013, when the domains of the [New York Times, Twitter \(now known as X\), and other organizations were hijacked](#), sending their website visitors to malicious websites. Like the ICANN hijacking five years earlier, this attack, perpetrated by the "Syrian Electronic Army," was carried out by compromising a domain-name registrar and changing the name servers associated with the targeted organizations.

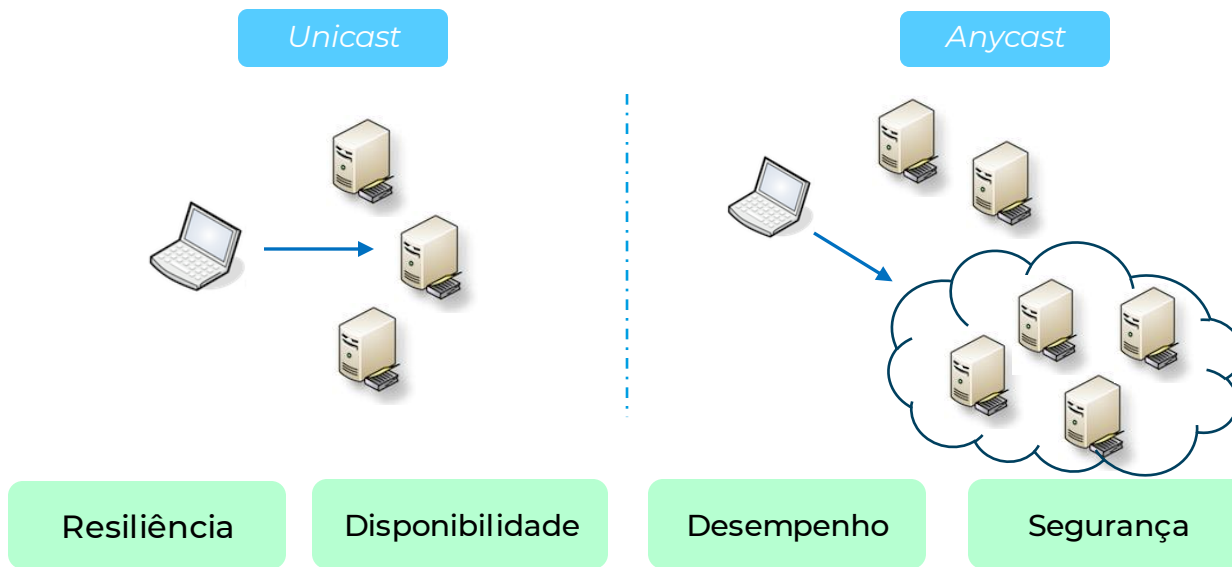
<https://controld.com/blog/biggest-dns-attacks/>

Vulnerabilidades

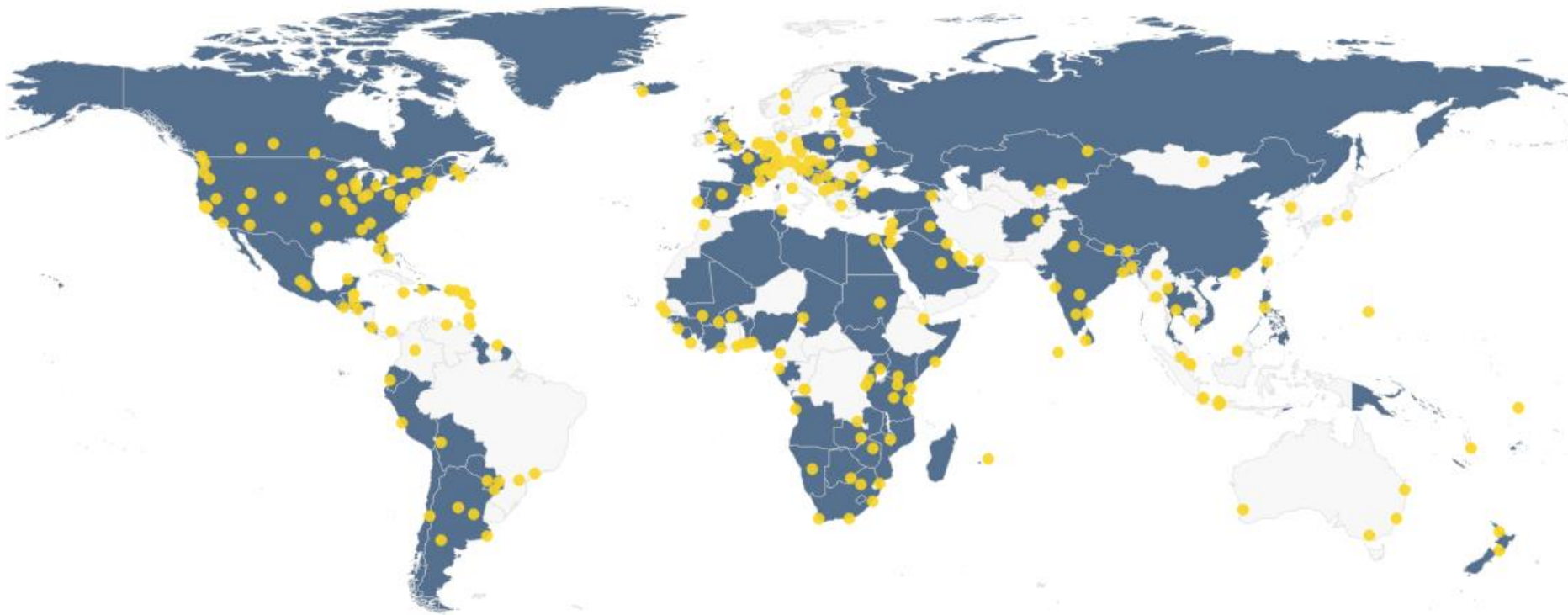


Servidores secundários / Anycast

Os servidores autoritativos secundários são fundamentais.



Servidores secundários / Anycast

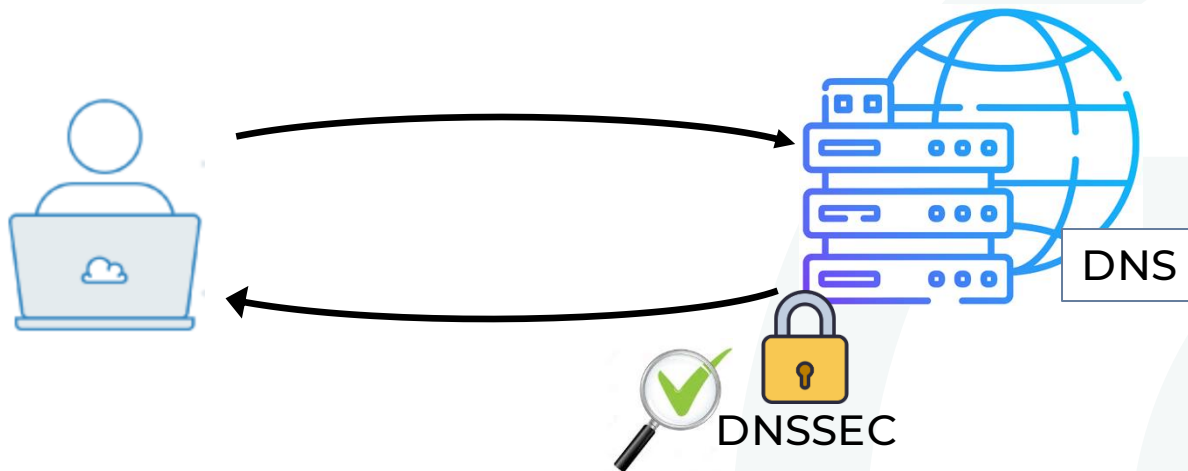


<https://www.pch.net/services/anycast>

DNSSEC

Domain Name System Security Extensions

Extensões de segurança do protocolo DNS criadas para responder a ataques de Cache Poisoning / DNS Spoofing



DNSSEC

Autenticidade – origem da informação DNS é a suposta

Integridade – a informação DNS não é alterada em trânsito, desde que foi assinada na origem

Proof of Non-Existence – resposta autenticada da não existência de um domínio



DNSSEC

Características

-  Evolução do serviço DNS
-  Transparente para utilizadores e sistemas
-  Serviço DNS interoperável com/sem DNSSEC
-  Não utiliza certificados digitais (PKI)
-  Gestão tendencialmente automática

DNSSEC



Servidores Autoritativos

Assinam registos



Servidores Recursivos

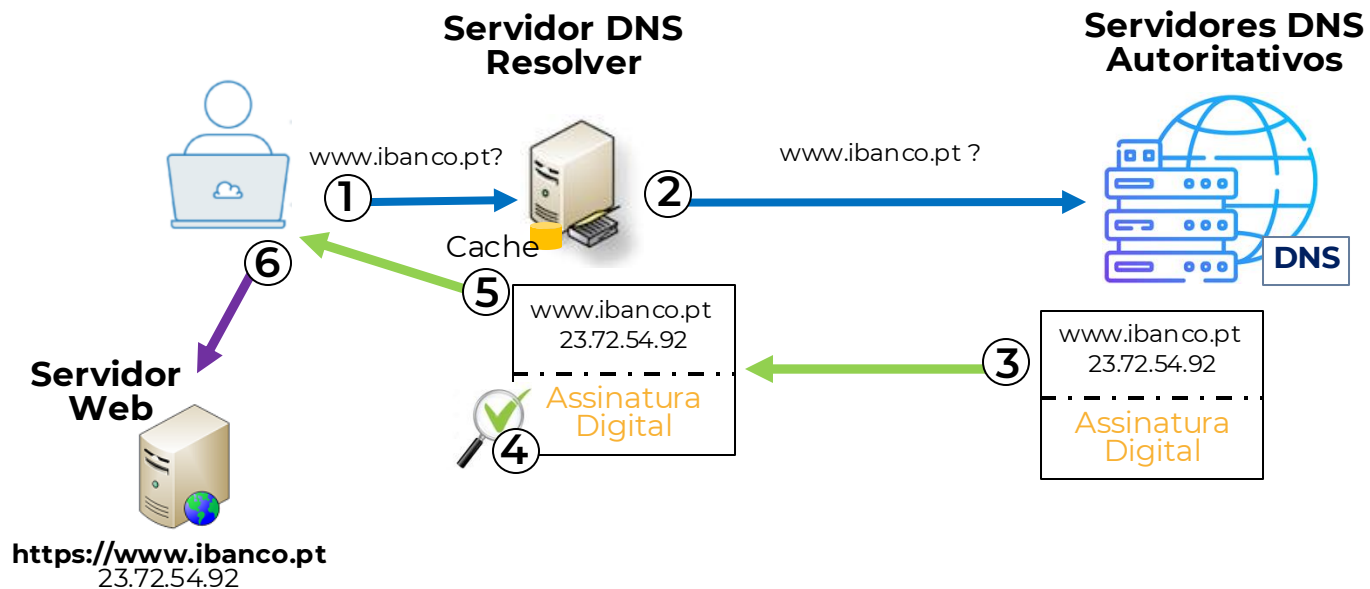
Validam registos

Criptografia de chave pública (assimétrica)



DNSSEC

Resolução DNS com validação DNSSEC



DNSSEC

Troubleshooting de situações mais comuns

-  Assinaturas expiradas
-  Correspondência DS / KSK (filho)
-  Correspondência assinaturas/chaves
-  Assinaturas com TTL superior a sua validade
-  Ferramentas de análise

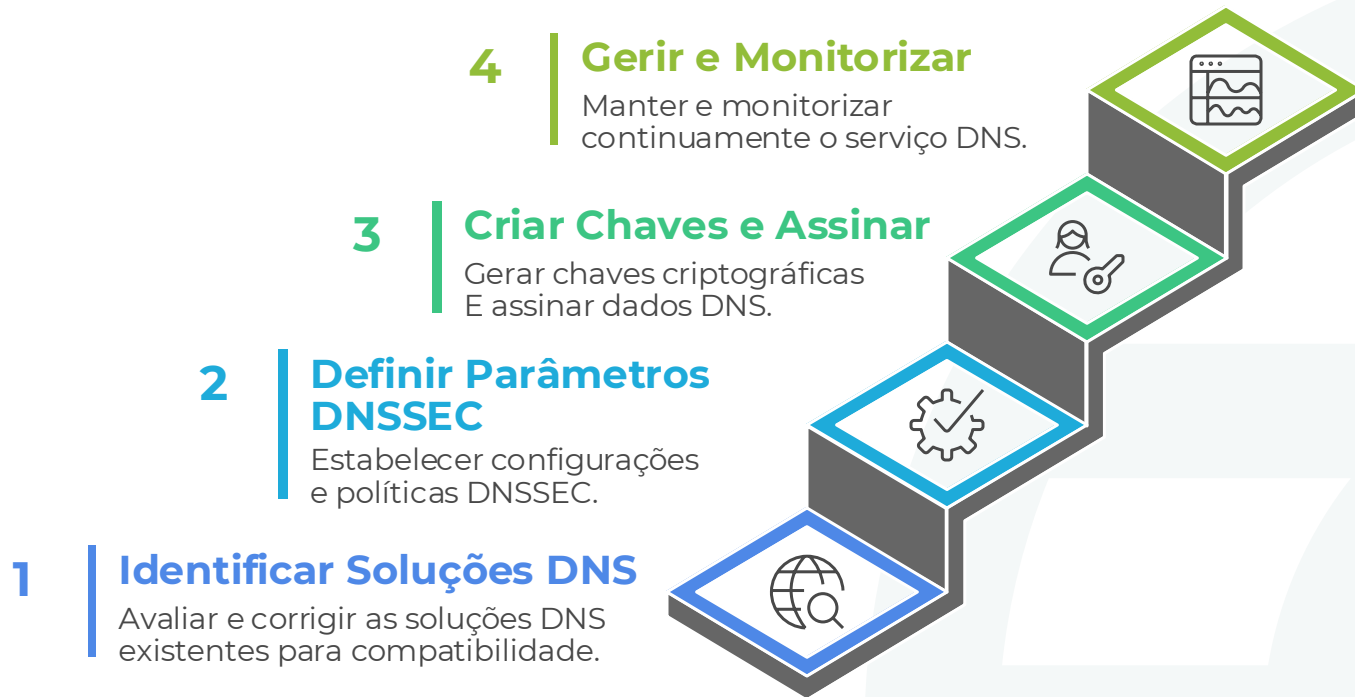
DNSVIZ - <https://dnsviz.net/>

Verisign Labs DNSSEC Analyzer

<https://dnssec-analyzer.verisignlabs.com/pt.pt>

DNSSEC

Macro etapas da implementação DNSSEC



Requisitos do protocolo DNS

TLDs & Zonas Críticas

Ter pelo menos 3 a 4 servidores autoritativos, com soluções de Anycast

A integridade da informação DNS é fundamental

Implementação de DNSSEC e seguir as melhores práticas de gestão

A transferência entre servidores autoritativos deve ser segura e limitada

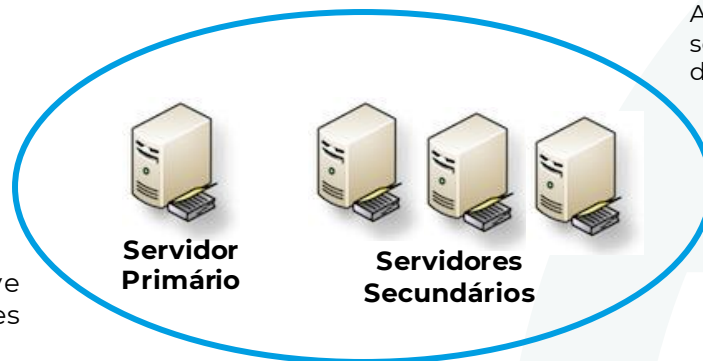
A zona do TLD deve conter apenas delegações

Utilizar a metodologia de primário escondido.

Os servidores autoritativos e recursivos devem estar separados

Deve existir diversidade na infraestrutura operacional: Rede, Geográfica e Software

A infraestrutura DNS deve ser monitorizada





LusNIC
Associação de ccTLDs
de língua portuguesa

Coalition for
Digital Africa



OBRIGADO!

lusnic@lusnic.org

