nic.br cgi.br | ceptro.br

WTR PoP-RN

Natal, RN | 20/08/25

Configurando seu DNS e DNSSEC com KINDNS

Wanderson Modesto

ceptro.br nic.br cgi.br

Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons
Atribuição – Não a Obras Derivadas (by-nd)
http://creativecommons.org/licenses/by-nd/3.0/br/legalcode

Você pode:

- **Compartilhar** — copiar, distribuir e transmitir a obra.
- **Fazer uso comercial da obra.**
- Sob as seguintes condições:

Atribuição — Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do **Workshop de IPv6** do CEPTRO.br/NIC.br, e que os originais podem ser obtidos em **http://ceptro.br**. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.

Vedada a criação de obras derivadas — Você não pode modificar essa apresentação, nem criar apresentações ou outras obras baseadas nela.

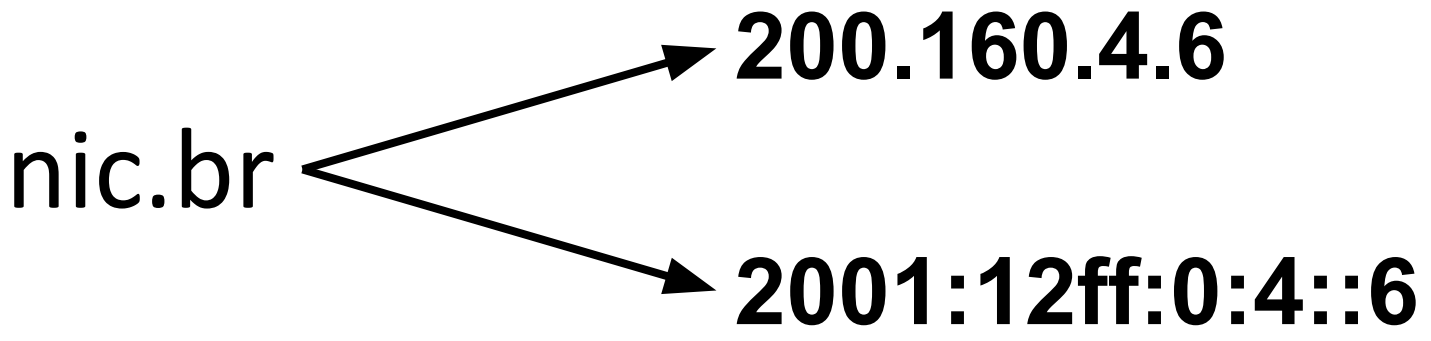
Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

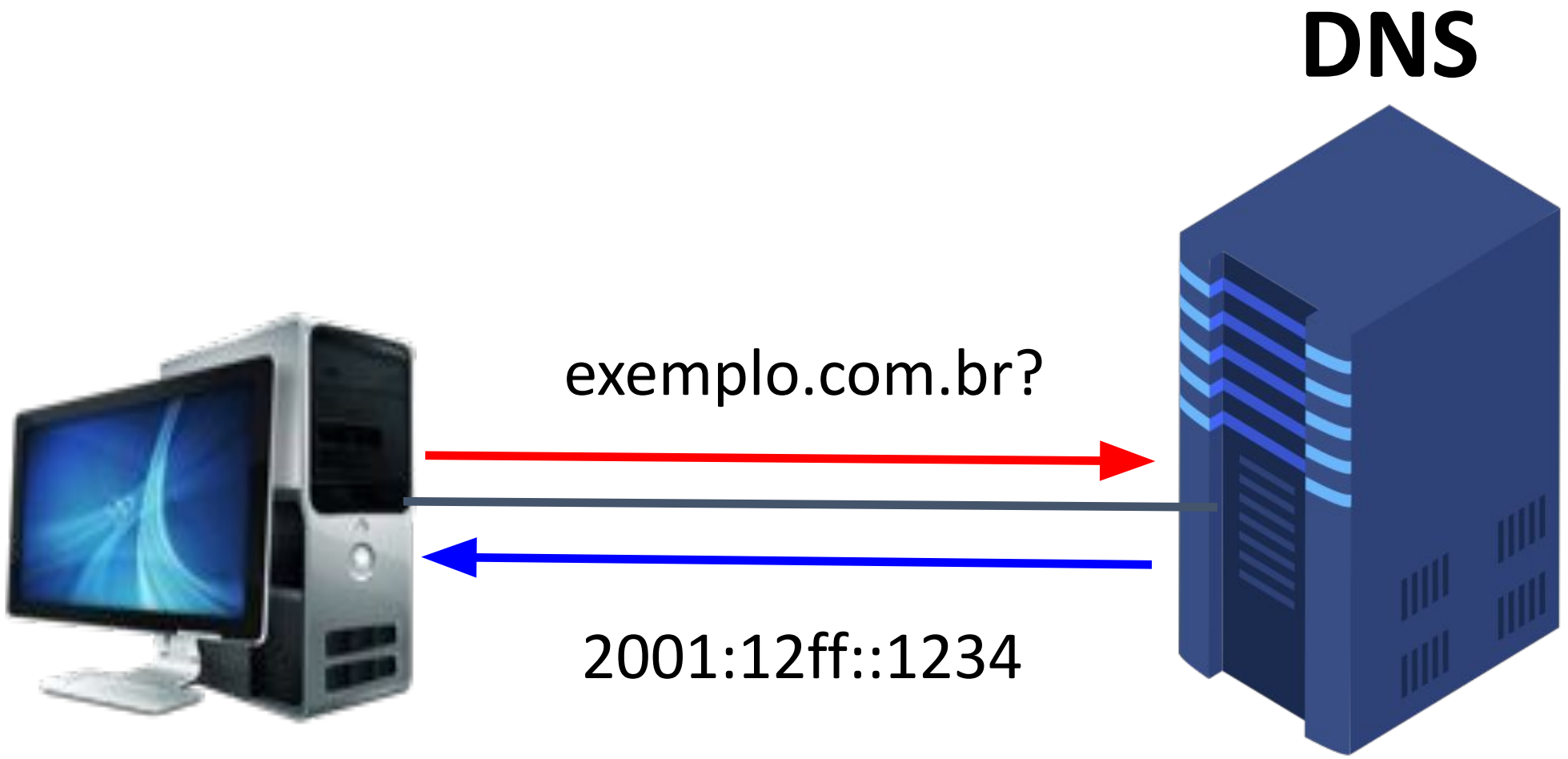
Introdução ao DNS

ceptro.br nic.br cgi.br

DNS

- Especificado pelas RFCs 1034 e 1035
- Domain Name System (DNS)
  - Sistema que associa nomes a endereços IPs



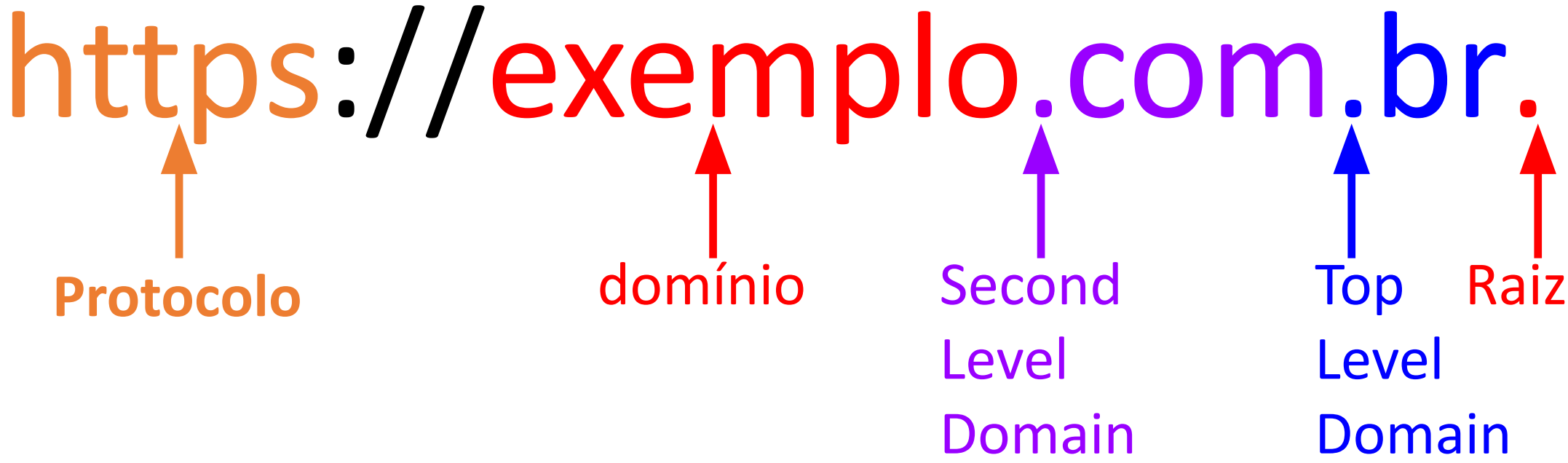

DNS
exemplo.com.br?
2001:12ff::1234

Mas e os nomes de Internet?

- Mas uma só máquina de DNS conseguiria resolver nomes para todos?
  - Problema de **Memória**
    - Todos os registros de domínios do mundo
  - Problema de **Processamento**
    - Responder todas as máquinas do mundo

Problema de memória

- FQDN (Fully Qualified Domain Name)

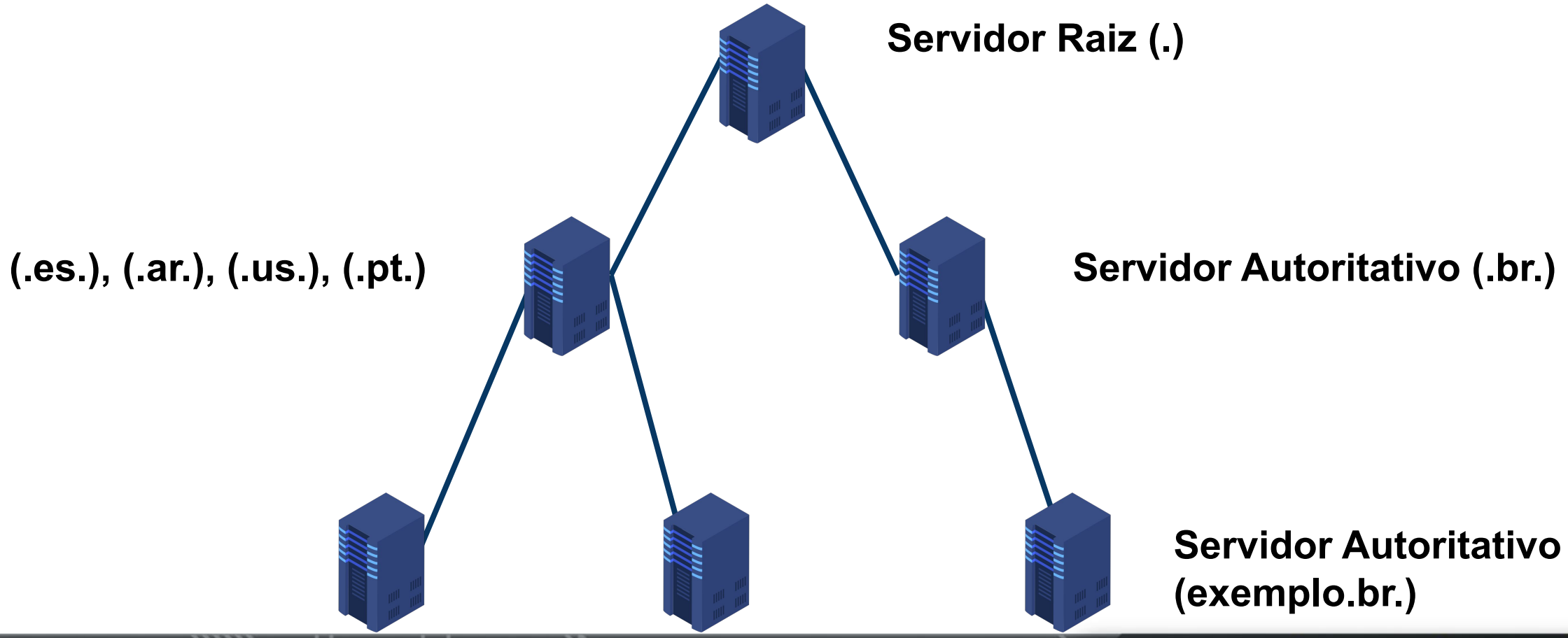


Problema de memória

- Top Level Domain (TLDs)
  - Country-code (ccTLD) - .br, .ar, .py, .uy, .cl, .co
  - Generic (gTLD) - .cheap, .ninja, .bom, .final
  - Test (tTLD) - .테스트, .ИСПЫТАНИЕ, .טעסט
  - Sponsored (sTLD) - .xxx, .museum, .aero, .mil
  - Infrastructure (arpa) - .arpa

Problema de memória

- Base hierárquica e distribuída



Problema de Processamento

- Mas só uma máquina para cada nível da hierarquia?
  - Mais de um servidor Autoritativo!
  - Espelhos dos servidores!

Problema de Processamento

- Servidores raiz
  - Constituído de 13 servidores
  - Centenas de espelhos espalhados pelo mundo

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Lab 0: Setup Inicial

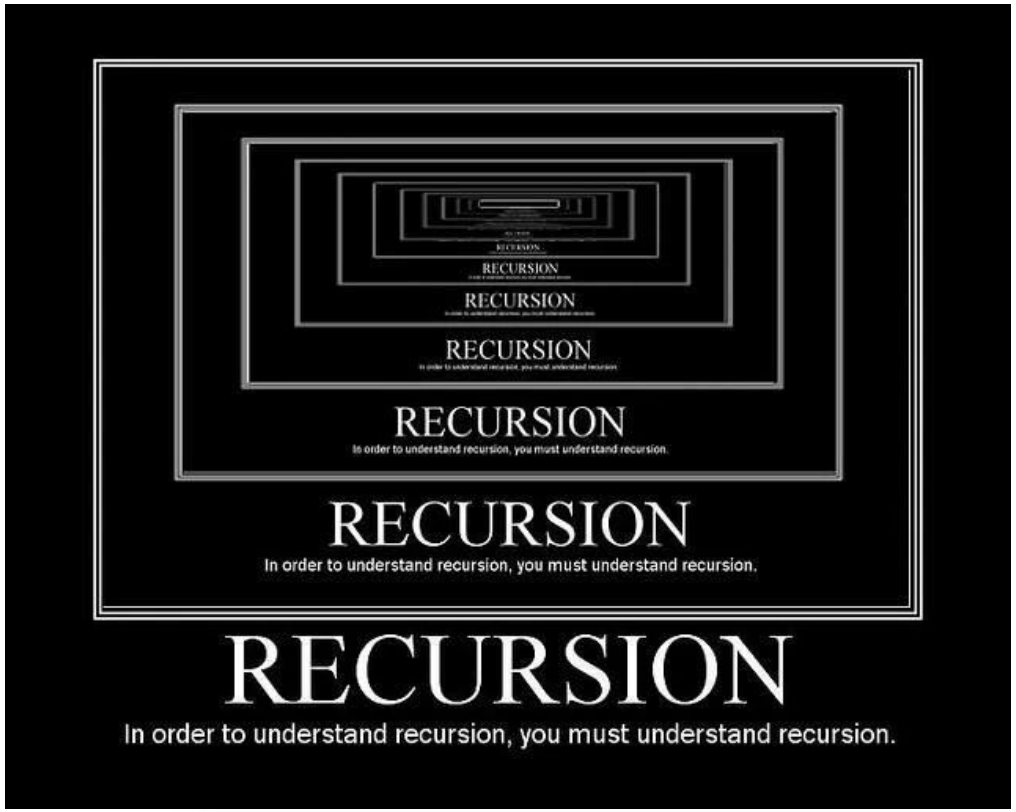
ceptro.br nic.br cgi.br

DNS Recursivo

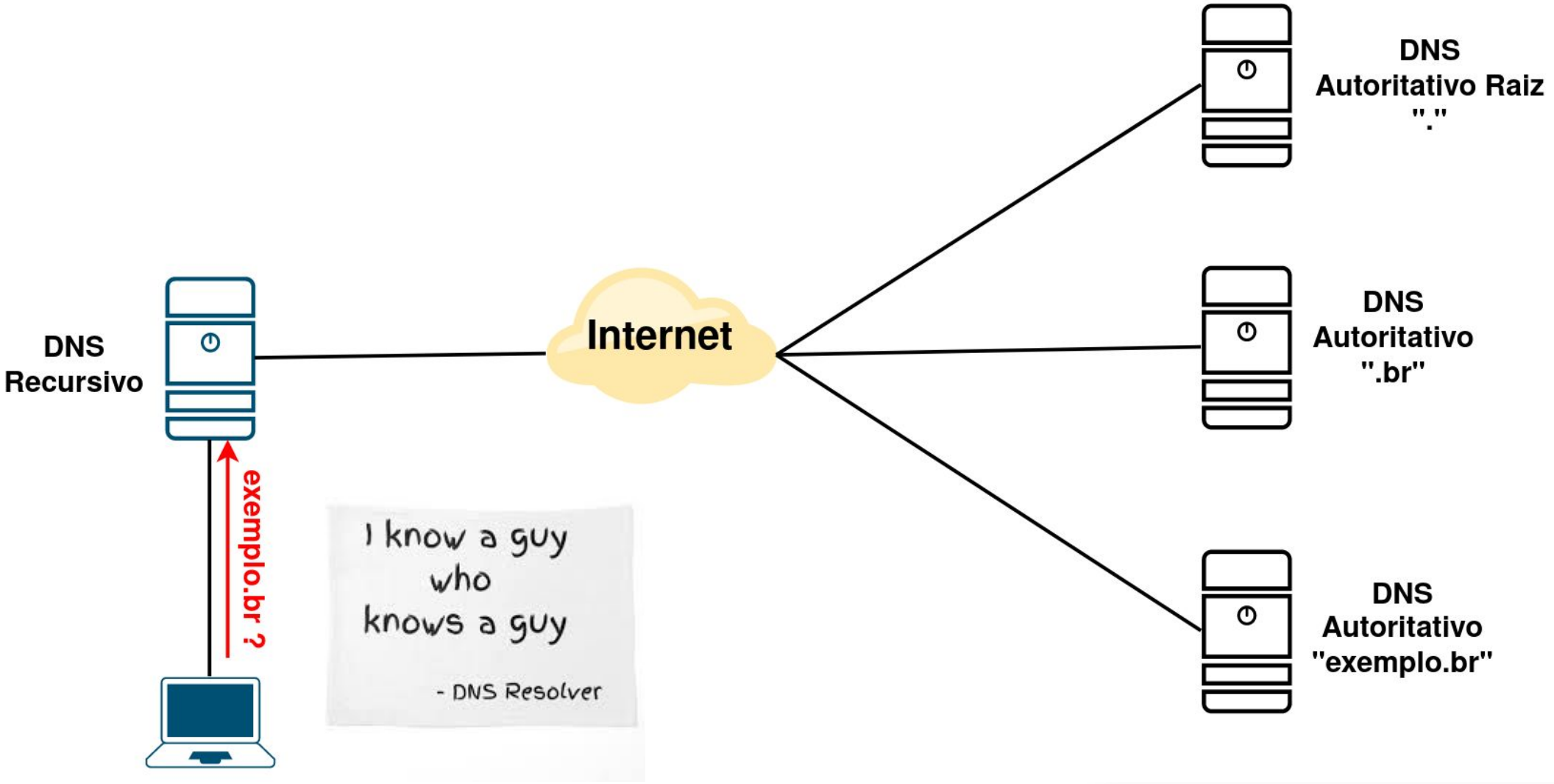
ceptro.br nic.br cgi.br

Problema de Processamento

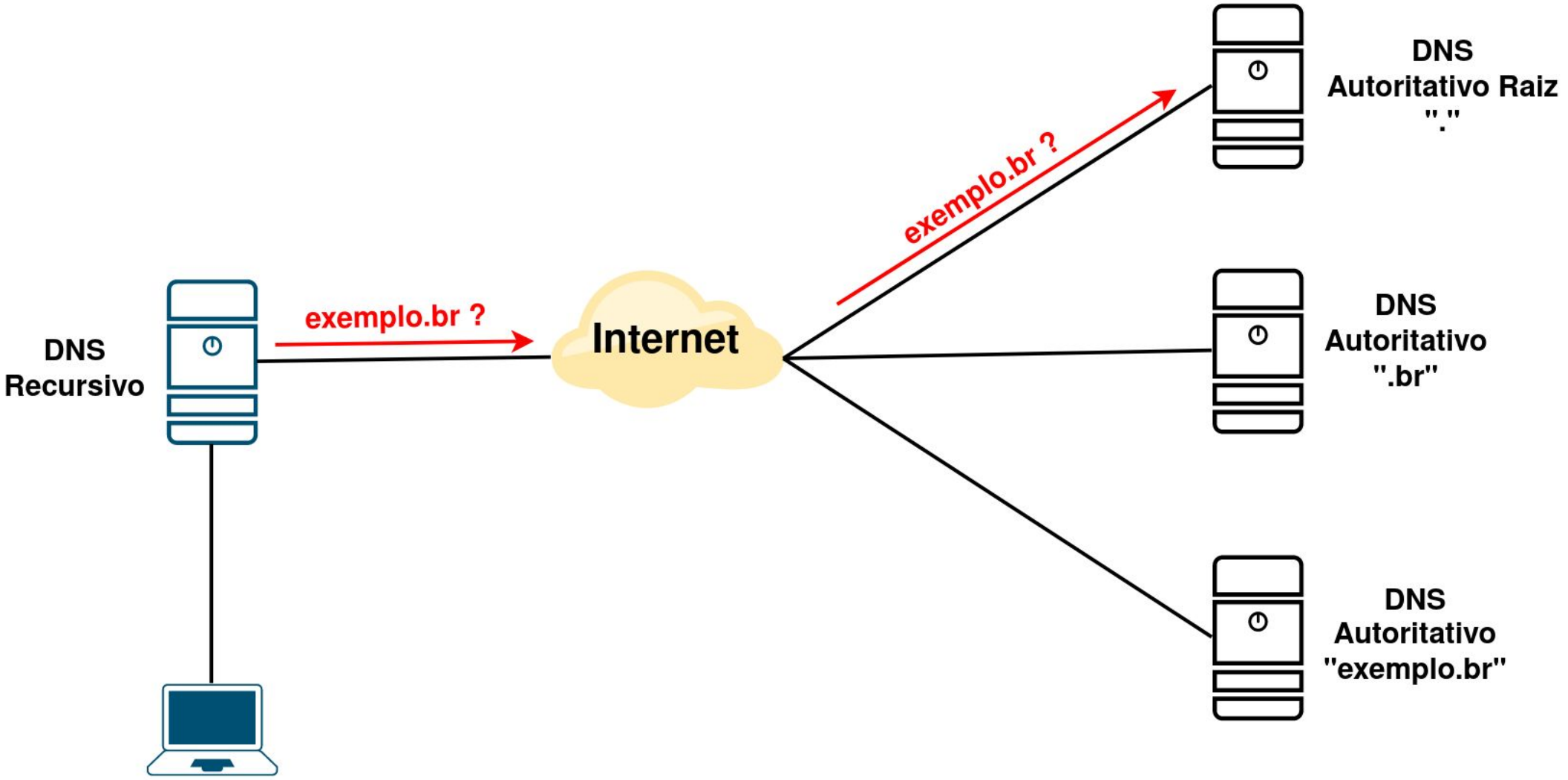
- Perguntas repetidas vindas de várias máquinas?
  - Servidores recursivos!
  - Caches!



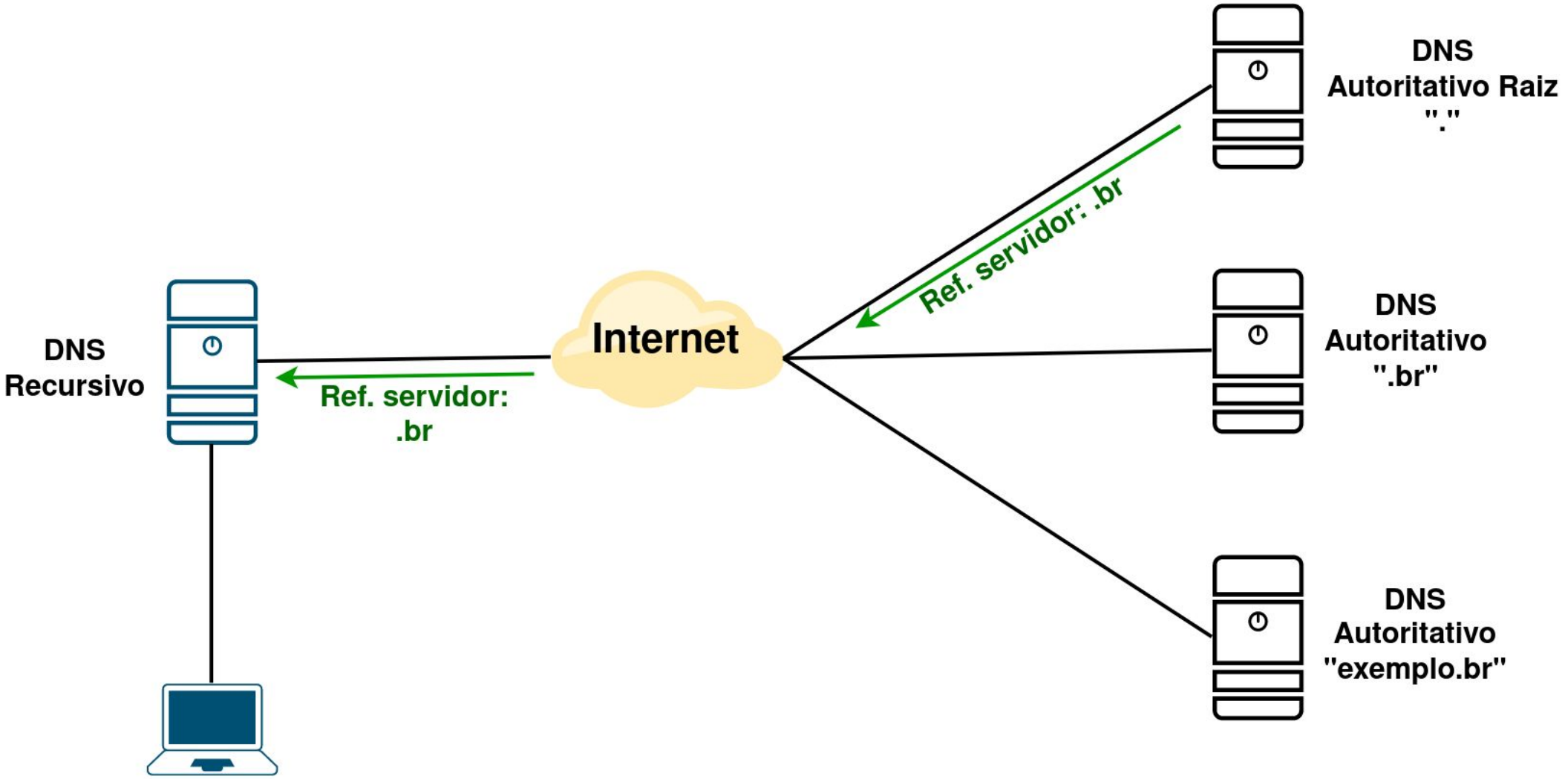
Funcionamento do DNS



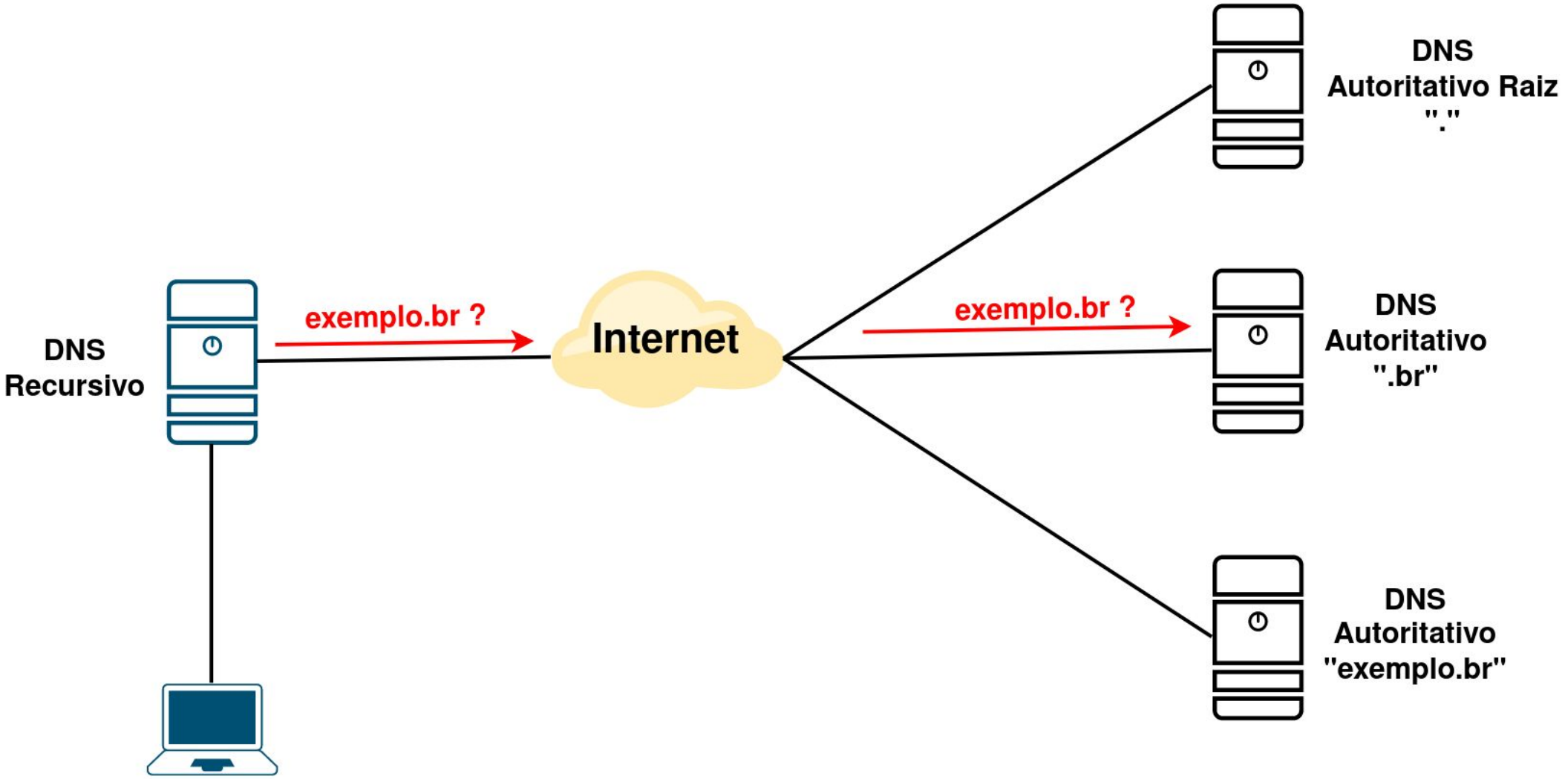
Funcionamento do DNS



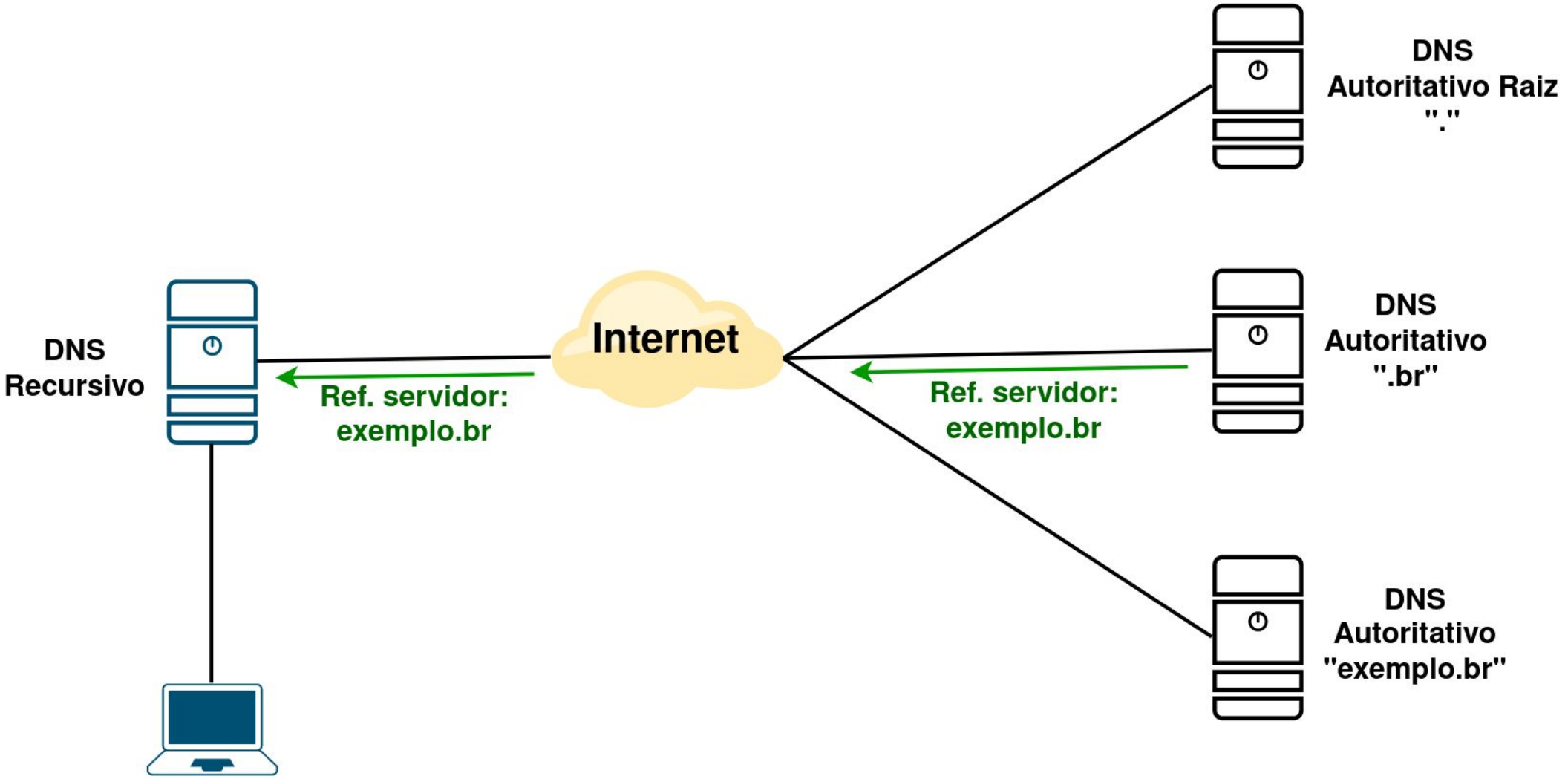
Funcionamento do DNS



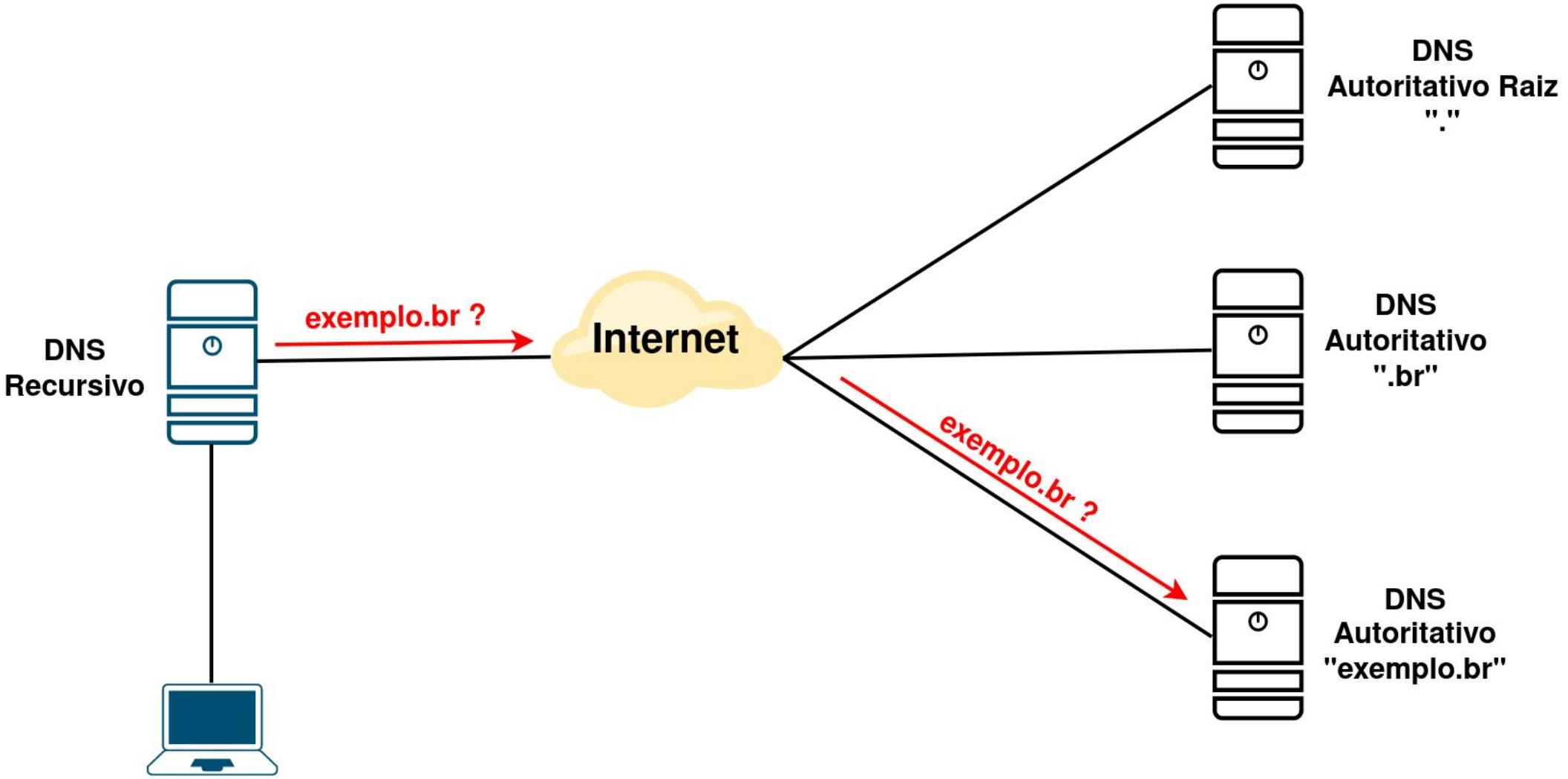
Funcionamento do DNS



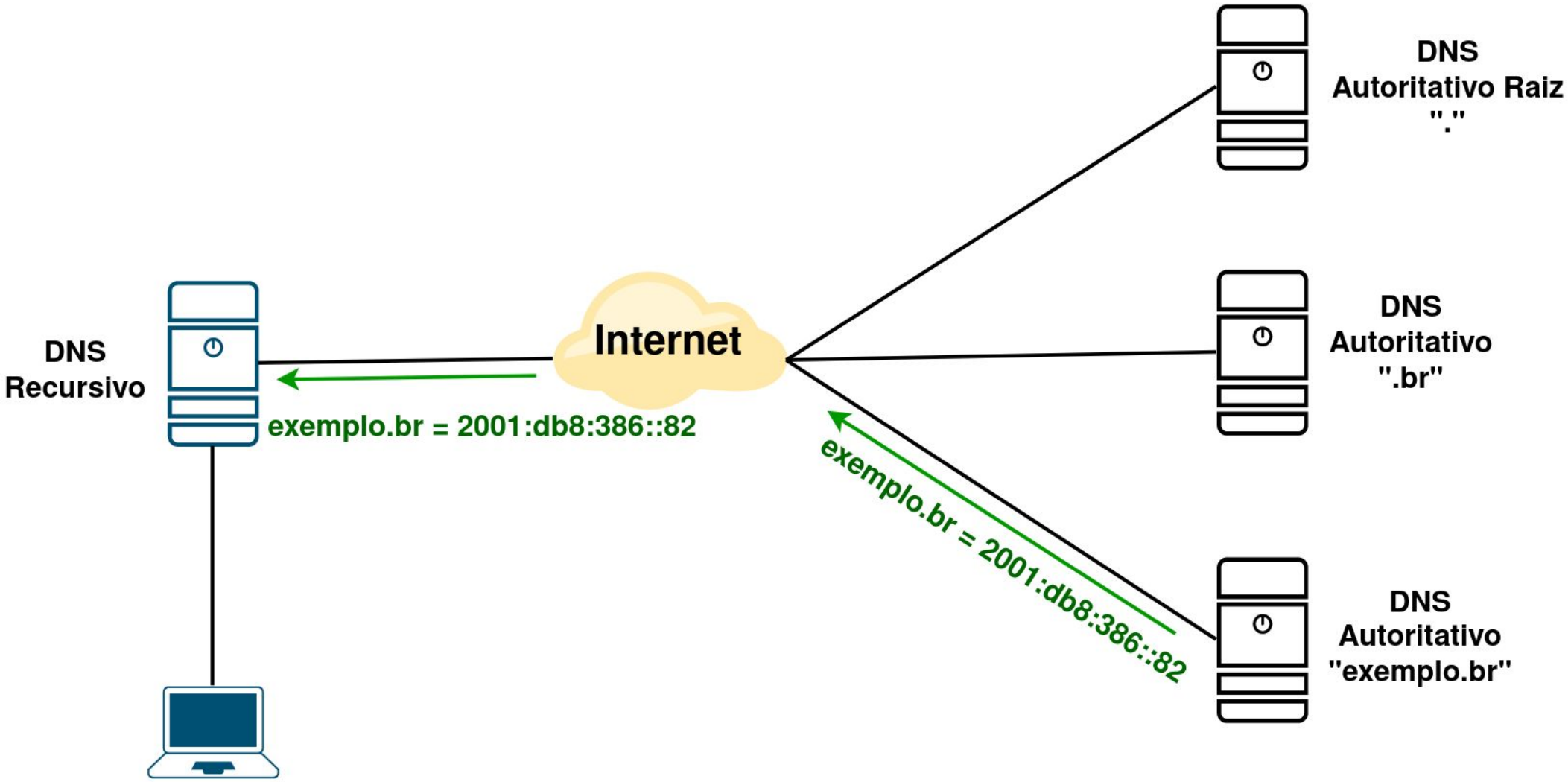
Funcionamento do DNS



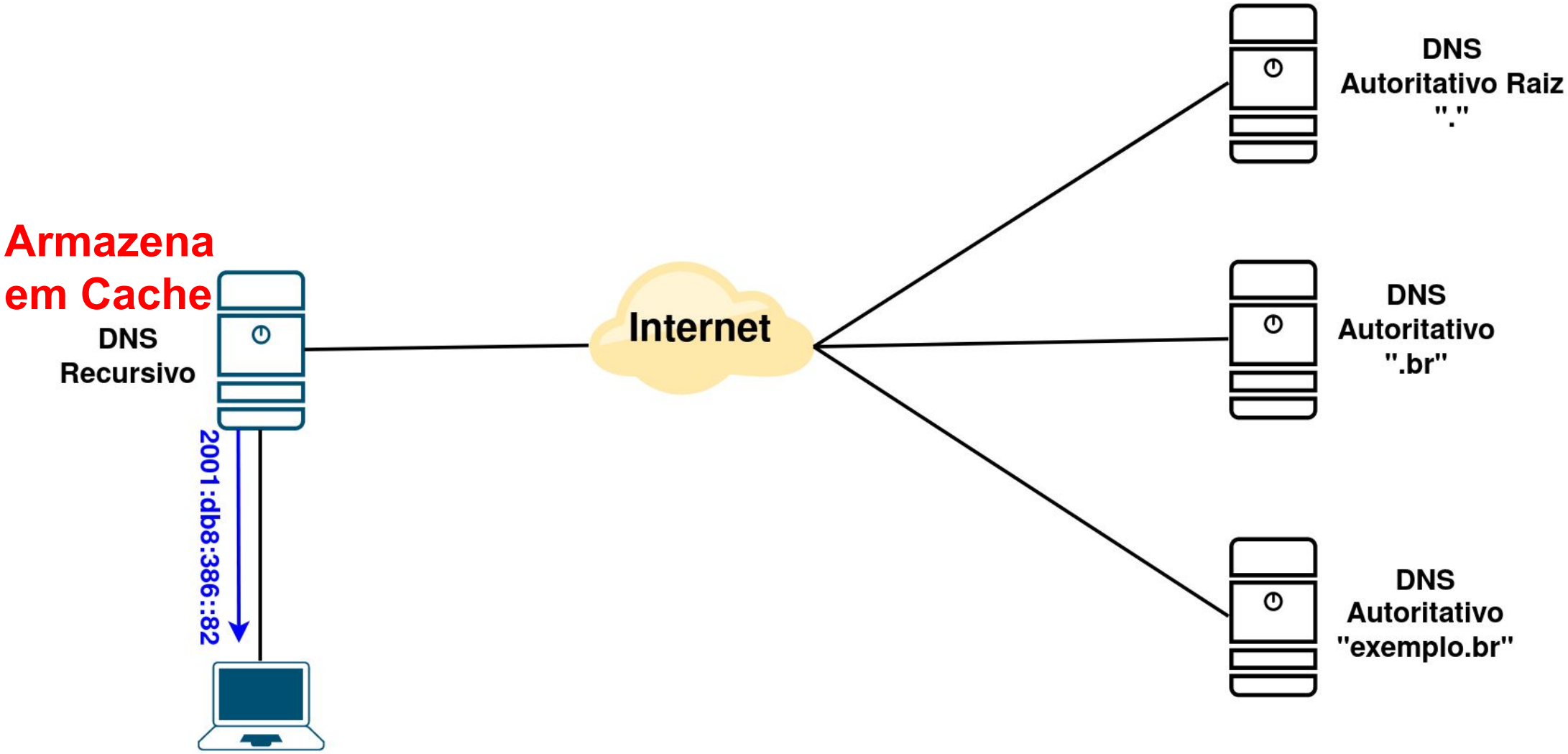
Funcionamento do DNS



Funcionamento do DNS

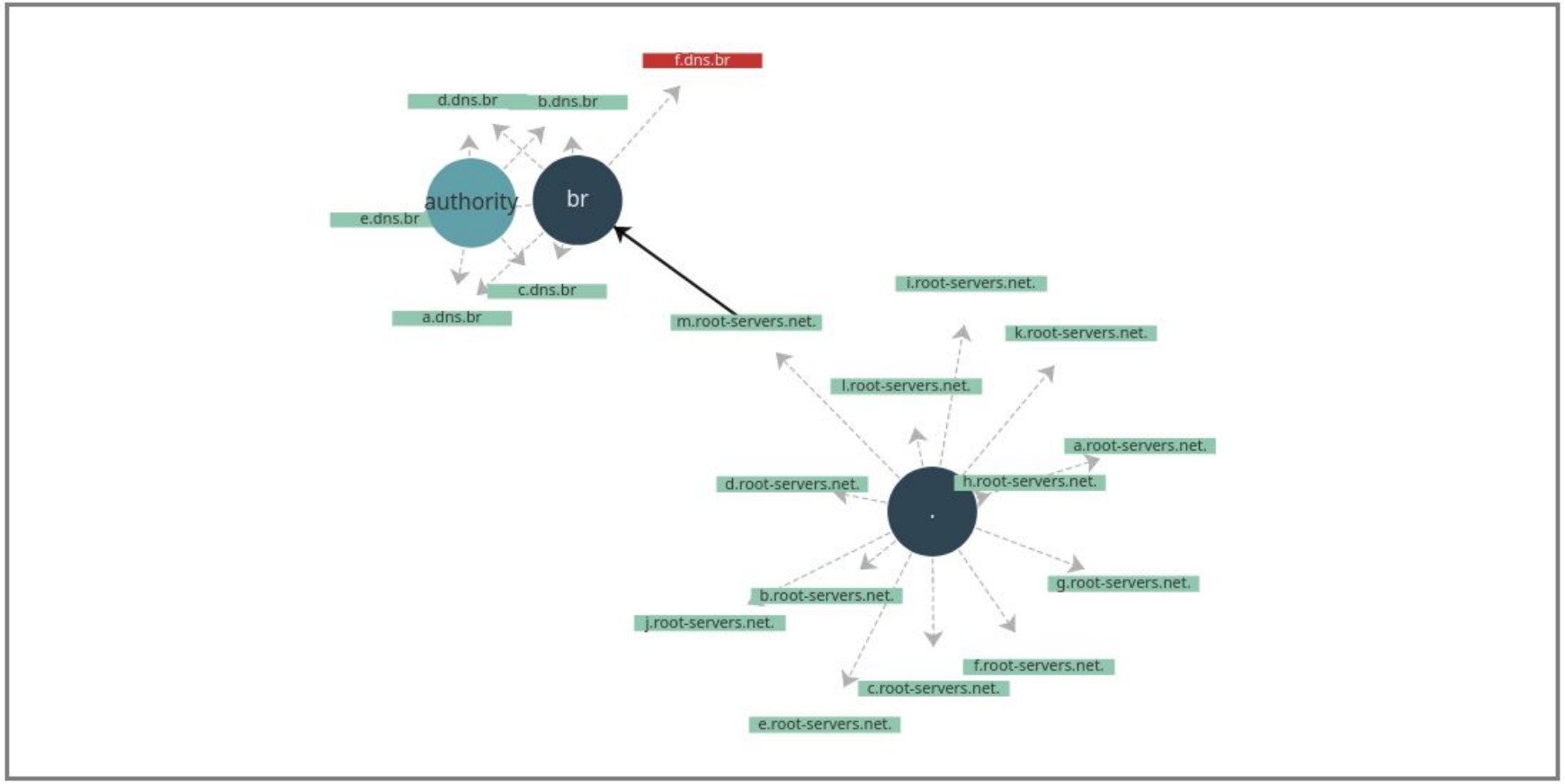


Funcionamento do DNS



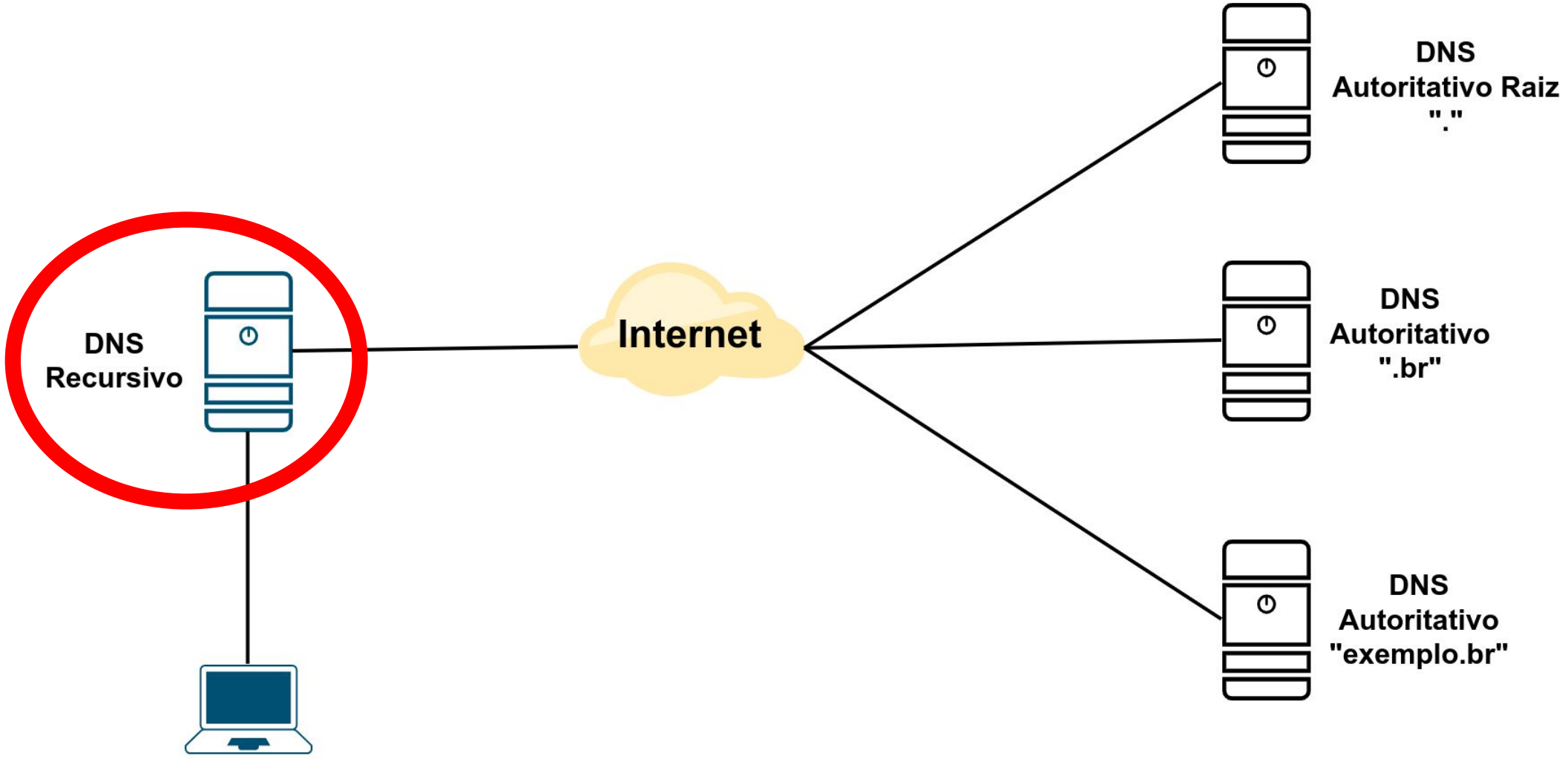
Buddy NS

BuddyNS delegation lab



https://www.buddyns.com/delegation-lab

DNS Recursivo



DNS Recursivo

- Também conhecido como "Resolver"
- Servidor responsável por encontrar o endereço IP do nome pedido
  - Faz consultas aos servidores autoritativos
- Possui cache das informações consultadas

DNS Recursivo

- 3 formas de operação
  - Privado
  - Privado compartilhado
  - Público

DNS Recursivo Privado

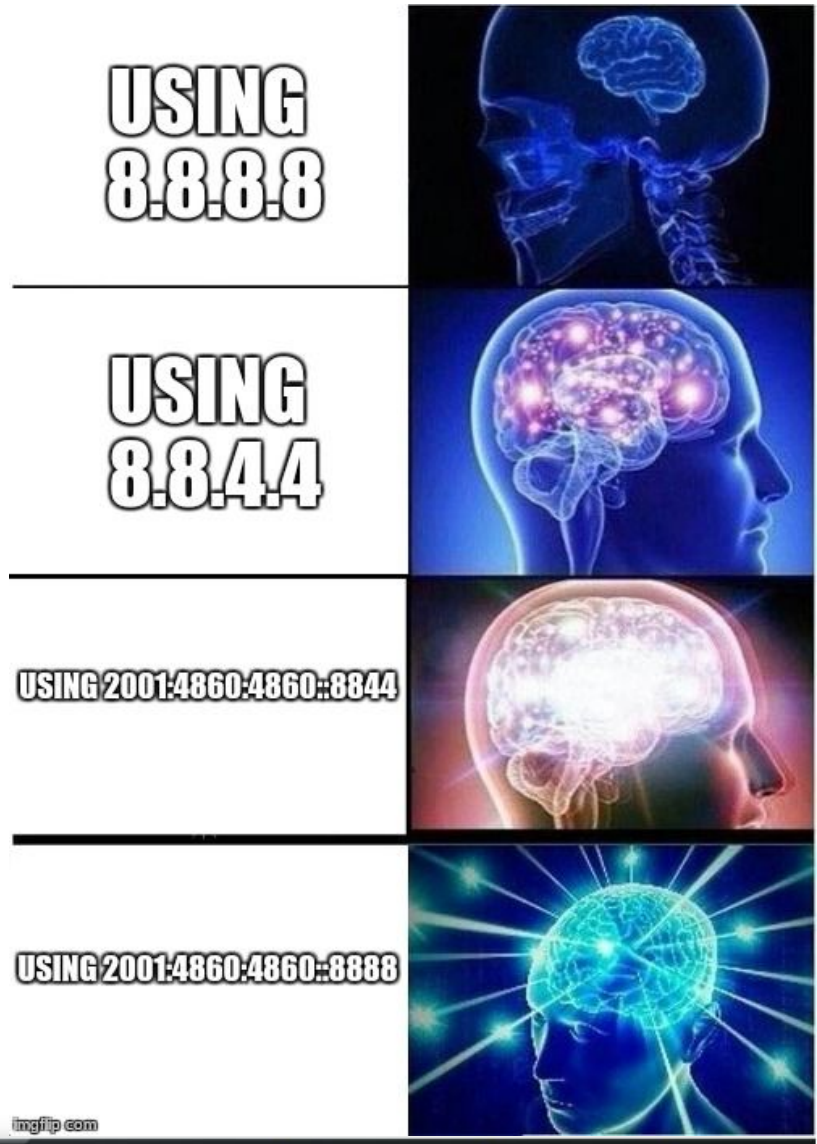
- Serviço restrito apenas a sua rede/empresa
- Não deve permitir consultas da Internet
- Caso de uso mais comum: empresas que queiram ter um servidor recursivo próprio

DNS Recursivo Privado Compartilhado

- Serviço restrito apenas a sua rede/empresa e a seus clientes
- Não deve permitir consultas da Internet
- Caso de uso mais comum: provedores de Internet (ISP)

DNS Recursivo Público

- Serviço disponibilizado para toda a Internet
- Caso de uso mais comum: Quem não sabe configurar DNS Recursivo
  - Google (8.8.8.8)
  - Cloudflare (1.1.1.1)
  - OpenDNS



Implementações de DNS Recursivo

- Softwares populares
  - Unbound
  - Bind9
  - PowerDNS
  - outros (https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software)

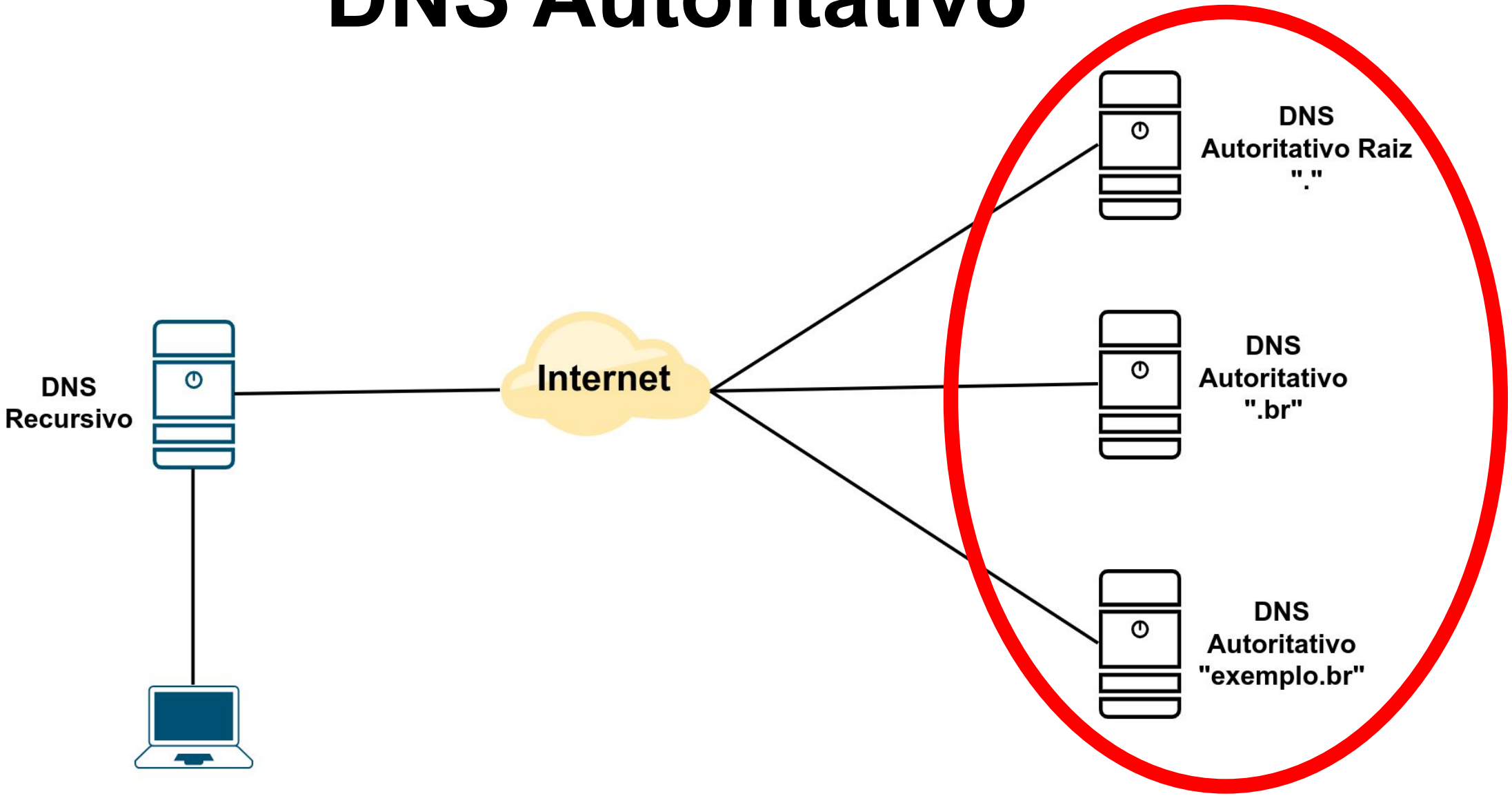
Lab 1: DNS Recursivo

ceptro.br nic.br cgi.br

DNS Autoritativo

ceptro.br nic.br cgi.br

DNS Autoritativo



DNS Autoritativo

- Servidor que possui autoridade sobre determinada parte de um domínio
- Informa ao servidor DNS recursivo as informações perguntadas

DNS Autoritativo

- Respostas possíveis a uma consulta de um recursivo
  - Não sei e não tenho a informação
  - Não sei, mas sei quem sabe
  - Sei, segue a informação

Implementações de DNS Autoritativo

- Softwares populares
  - NSD
  - Bind9
  - PowerDNS
  - outros(https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software)

Resource Record (RR)

- As informações referentes a um domínio em específico são chamados Resource Records (RR)
- Existe uma grande variedade de tipos

https://en.wikipedia.org/wiki/List_of_DNS_record_types

- Lista completa

https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml

Resource Record (RR)

- Entradas RR comuns:
  - SOA - indica onde começa a autoridade da zona
  - NS - indica um servidor de nomes para a zona
  - A - indica um endereço IPv4 ao domínio
  - AAAA - indica um endereço IPv6 ao domínio
  - MX - indica servidor de email para o domínio
  - CNAME - indica um nome alternativo ao domínio

Resource Record (RR)

- Exemplo de **entrada A**

  nic.br IN A 200.160.4.6

- Exemplo de **entrada AAAA**

  nic.br IN AAAA 2001:12ff:0:4::6

Resource Records Set (RRSet)

- Conjunto de todas as entradas RR com o mesmo nome e do mesmo tipo
  - Por exemplo todas as entradas A (IPv4) de um domínio

Lab 2: DNS Autoritativo

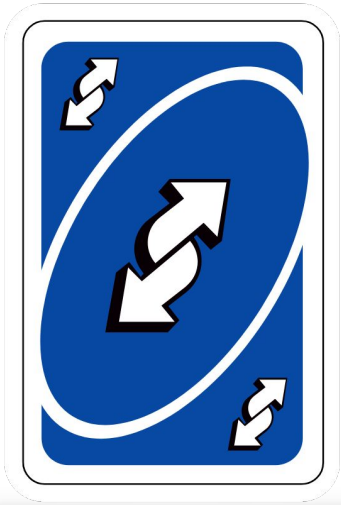
ceptro.br nic.br cgi.br

DNS Reverso

ceptro.br nic.br cgi.br

DNS Reverso

- Consulta DNS direta:
  - "Qual o endereço IP de www.nic.br ?"
- Consulta DNS reversa:
  - "Qual o nome associado ao IP 200.160.4.6?

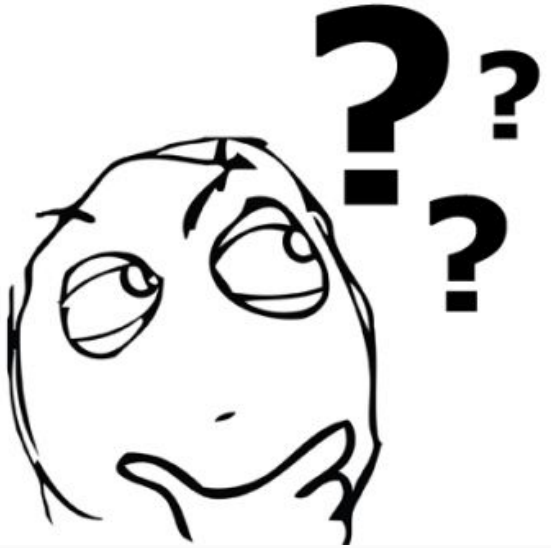


DNS Reverso

- O DNS reverso basicamente é a informação oposta do DNS direto
- Dado determinado IP, que informações temos sobre ele

DNS Reverso

- Qual a utilidade disso?
  - Usamos a resolução do DNS porque é mais fácil entender e decorar nomes do que números
  - Qual a utilidade de um DNS reverso então?



DNS Reverso

- Qual a utilidade disso?
  - Logs
  - Melhor organização
  - Segurança e validação (ex: email, autenticação)
  - Ferramentas monitoramento

DNS Reverso

- Como criar uma entrada reversa?
  - Resource Record **PTR** (domain name pointer)
    - Serve tanto para IPv4 como IPv6

6.4.160.200.in-addr.arpa. IN PTR nic.br.

6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa. IN PTR nic.br.

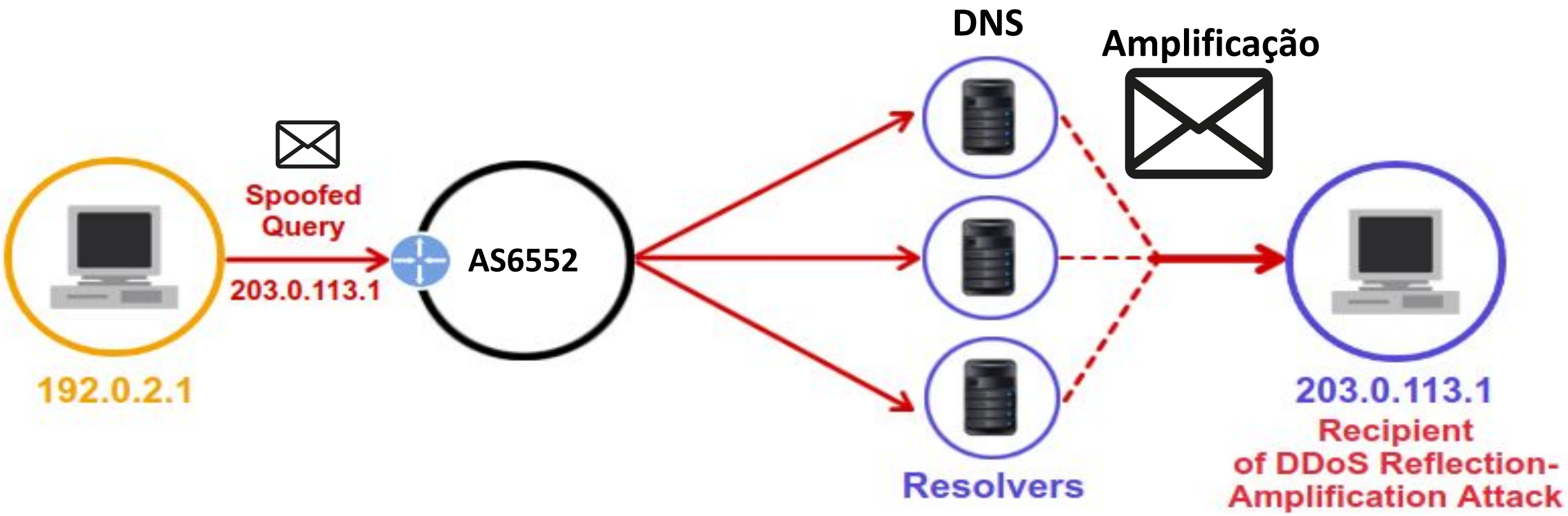
Lab 3: DNS Reverso

ceptro.br nic.br cgi.br

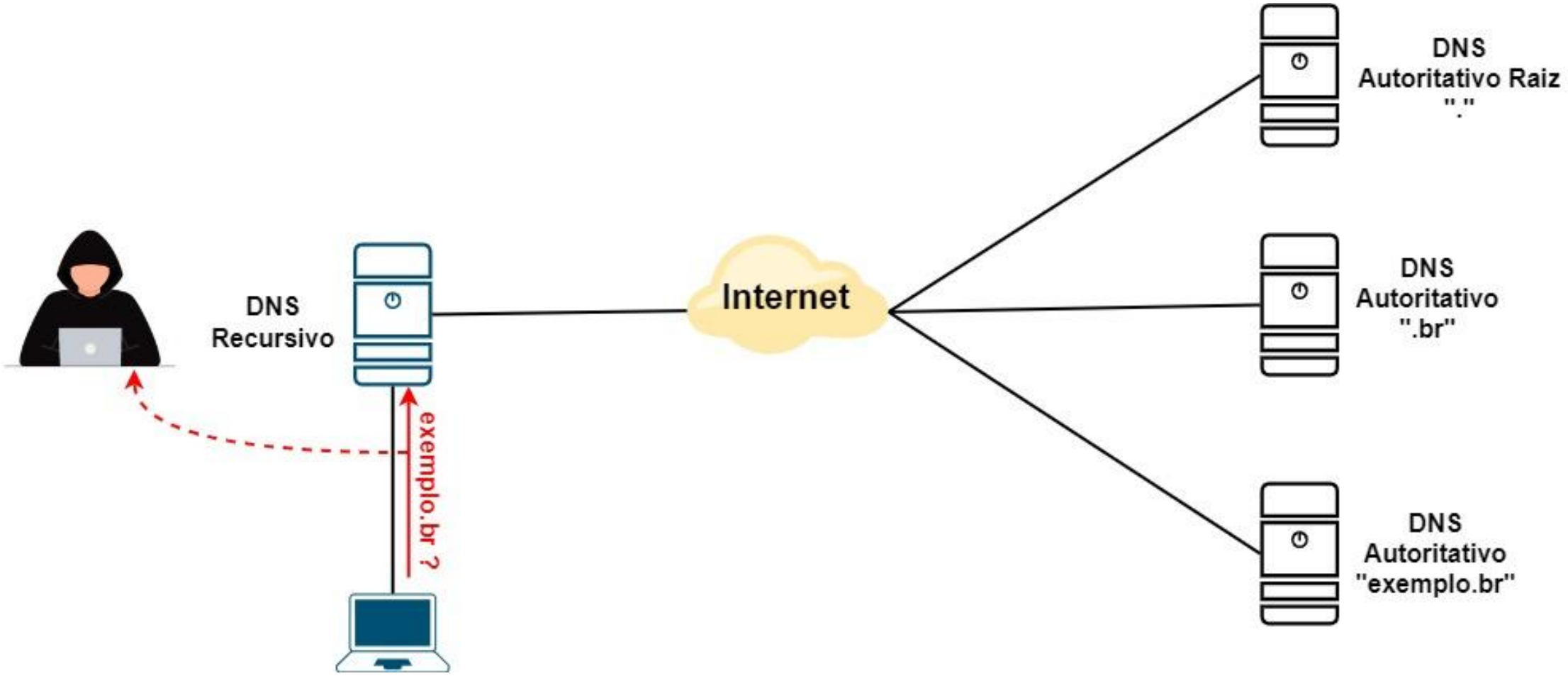
Ataques no DNS

ceptro.br nic.br cgi.br

Ataque Negação de Serviço

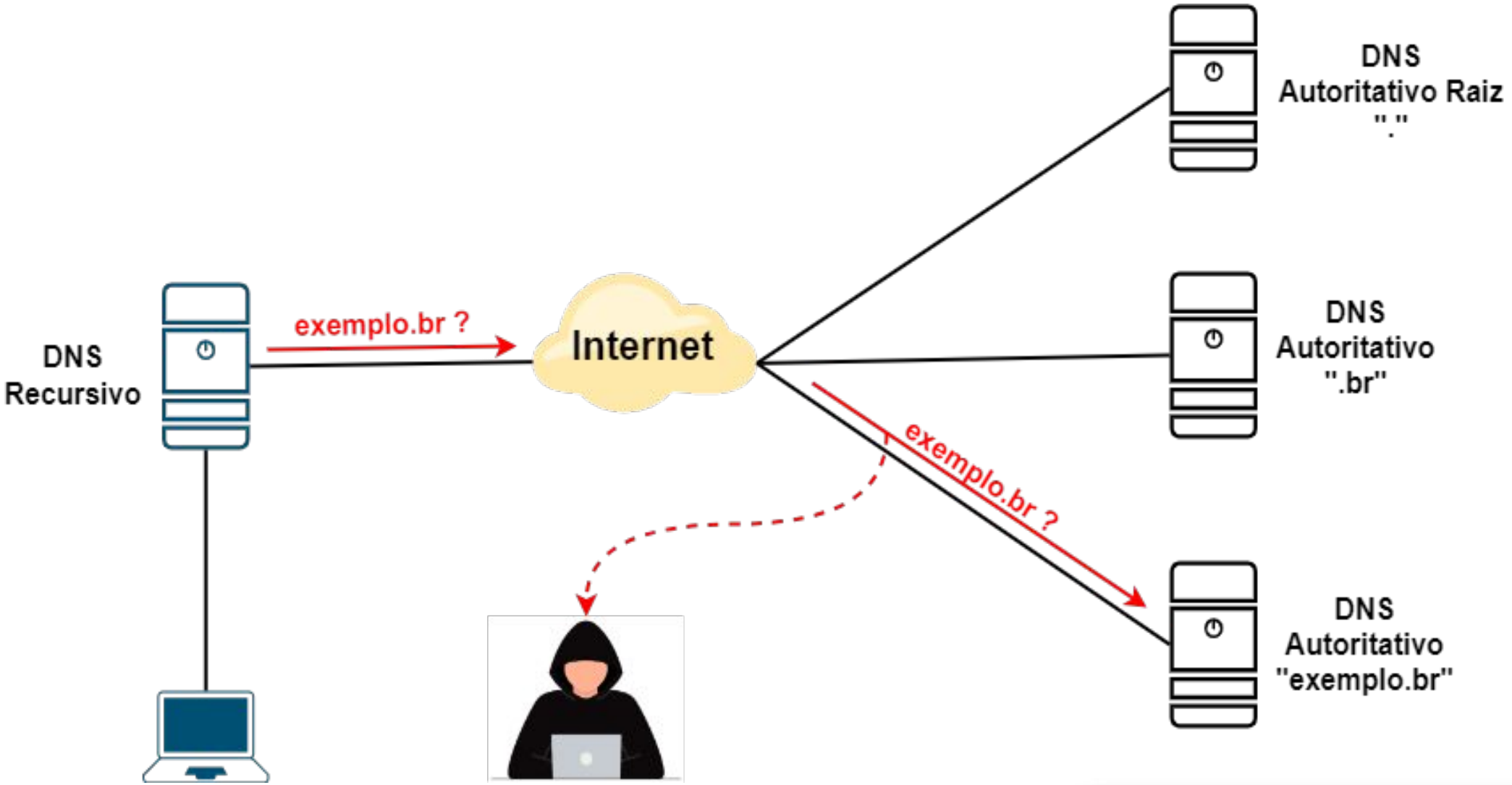


Ataque Man-in-The-Middle

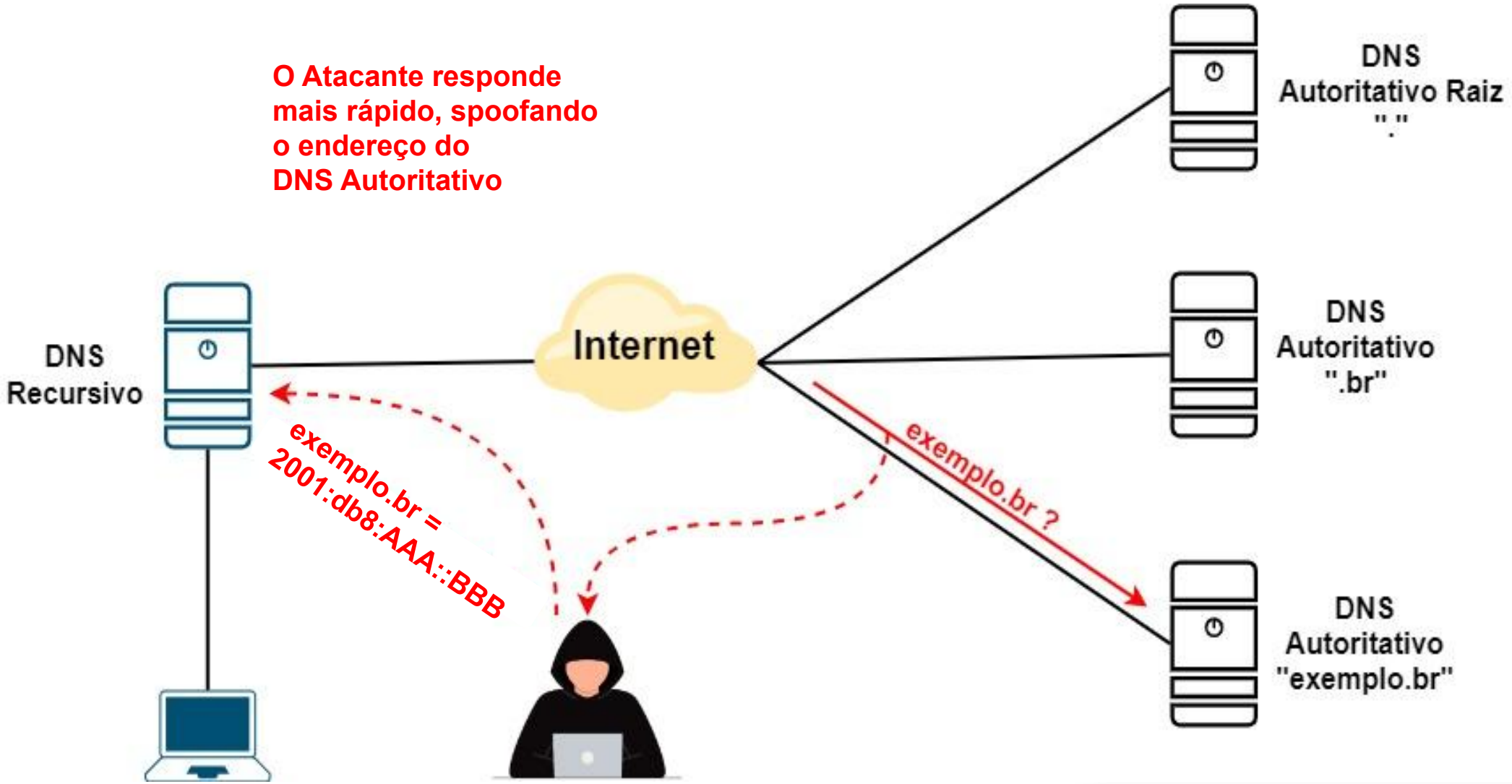


Ataque Man-in-The-Middle

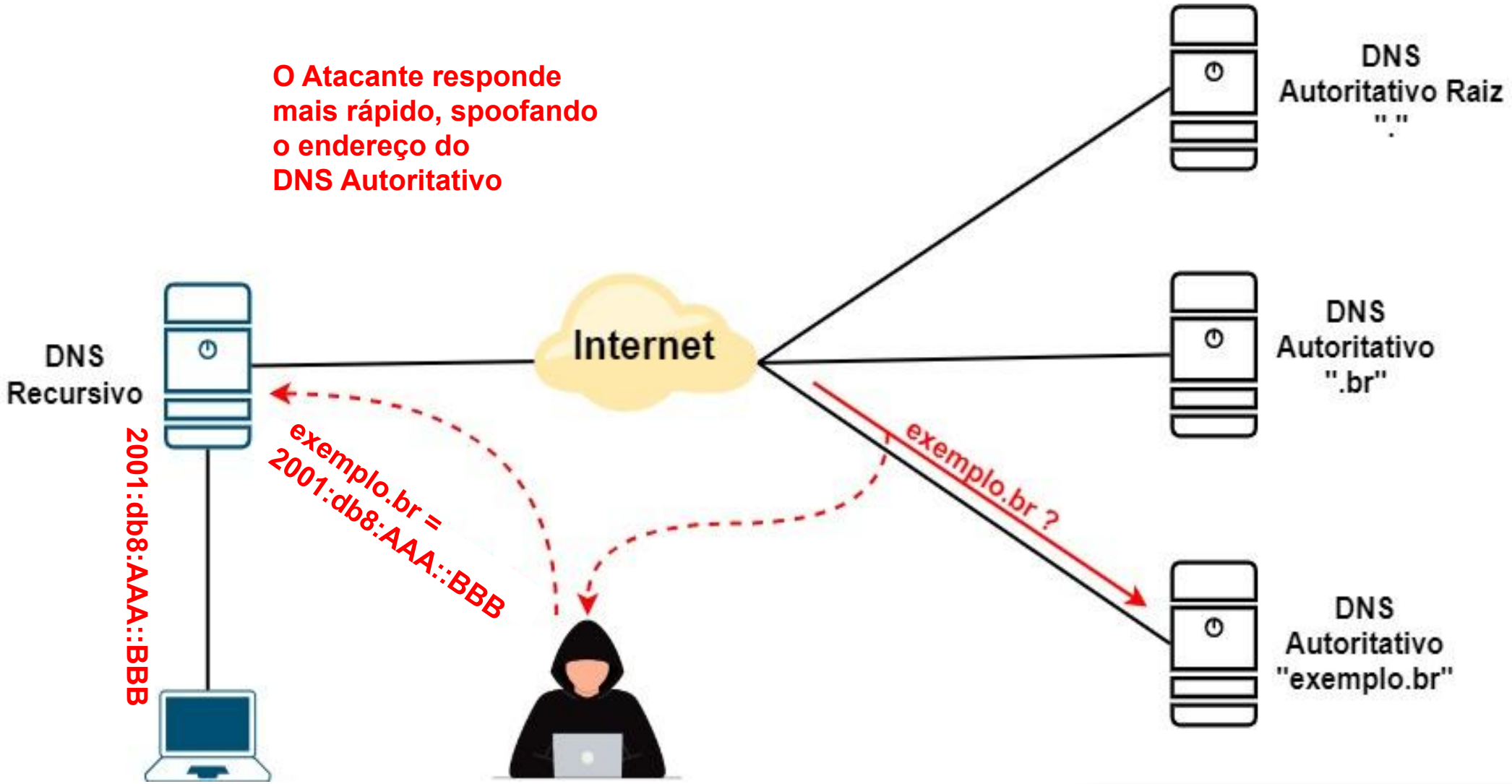
Ataque DNS Poisoning



Ataque DNS Poisoning



Ataque DNS Poisoning

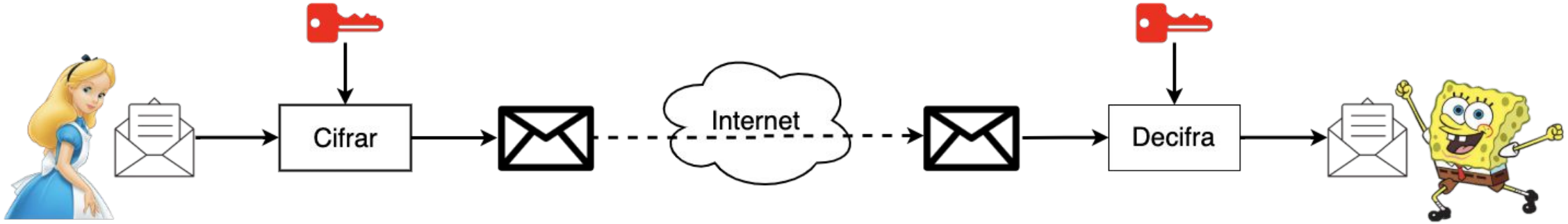


TSIG

ceptro.br nic.br cgi.br

Criptografia Simétrica

- Transformação matemática inversível cujo cálculo depende, no sentido direto (cifração) e no sentido inverso (decifração), de uma mesma informação secreta: a chave criptográfica.
- Provê apenas confidencialidade.



Transaction Signatures (TSIG)

- Definido pela RFC 2845
- Sistema de criptografia de chave simétrica (mesma senha nos dois servidores)
- Utilizado principalmente para transferência de dados de domínios/zonas de forma segura

Transaction Signatures (TSIG)

- Utilizado para transferir os dados entre os espelhos dos servidores DNS Autoritativos
- Dentro de sua rede, deve ser utilizado para proteger a comunicação entre o servidor DNS autoritativo primário e secundário

DNSSEC

ceptro.br nic.br cgi.br

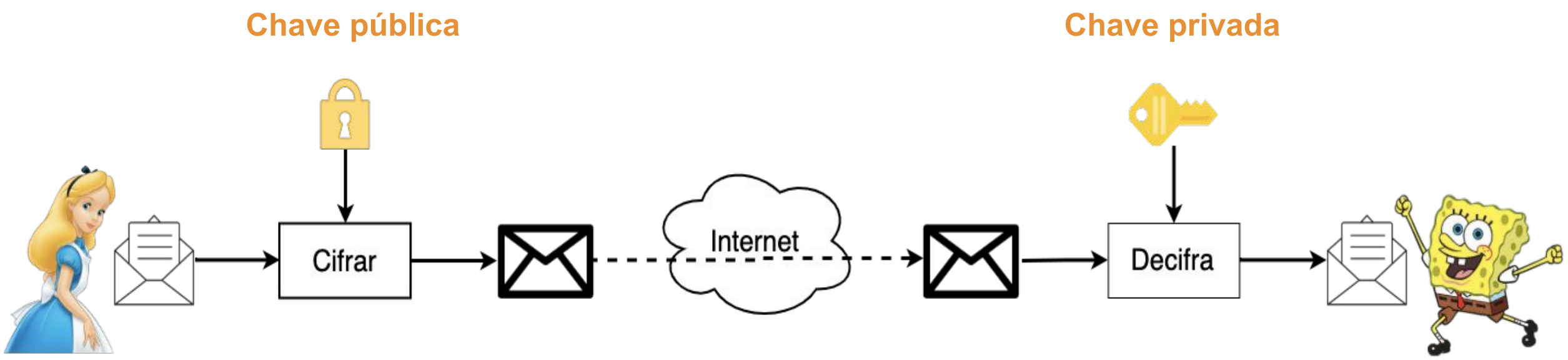
Criptografia Assimétrica

- Formada por duas chaves criptográficas distintas e relacionadas
  - Chave pública: amplamente conhecida
  - Chave privada: segredo do seu dono

- Transformações feitas usando uma chave somente podem ser invertidas com o uso da outra chave.

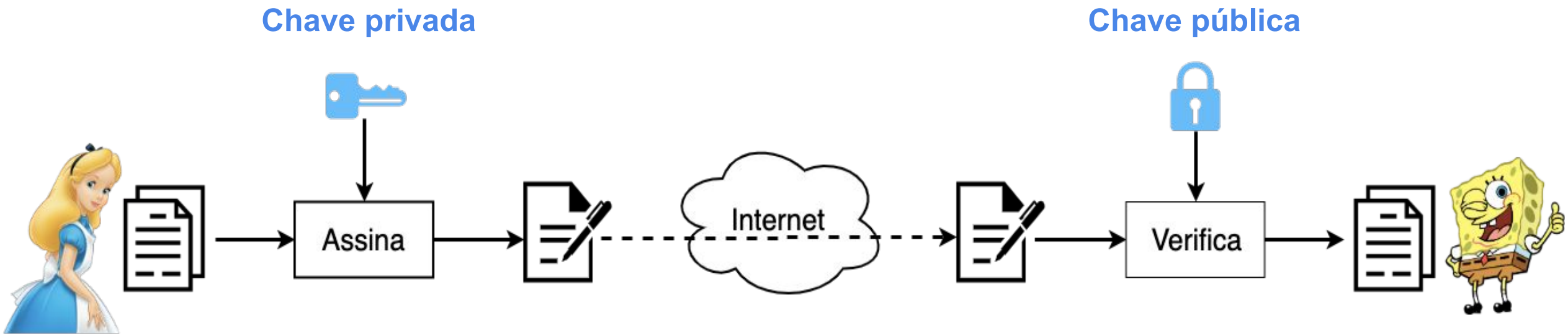
Criptografia Assimétrica

- Cifração: confidencialidade



Criptografia Assimétrica

- Assinatura digital:
  - integridade, autenticidade e irretratabilidade



DNSSEC

- RFC 9364
- DNSSEC
  - **DNS SEC**urity extensions
  - Forma de tornar as consultas DNS mais seguras

DNSSEC

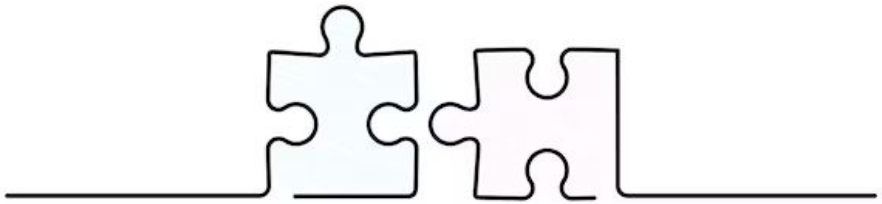
- O que o DNSSEC garante?
  - Autenticidade da origem
  - Integridade
  - A não existência de um nome

DNSSEC

- O que o DNSSEC não garante?
  - Confidencialidade
  - Proteção contra ataques de negação de serviço

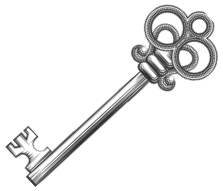
DNSSEC

- Duas partes
  - **Parte 1 -** Criptografia para **assinar a Zona**
    - Chaves ZSK
    - Opera com os dados no servidor autoritativo
  - **Parte 2** - Criptografia para **assinar a chave**
    - Chaves KSK
    - Opera na cadeia de confiança



DNSSEC

- Novos Resource Records
  - **DNSKEY** - contém uma chave pública

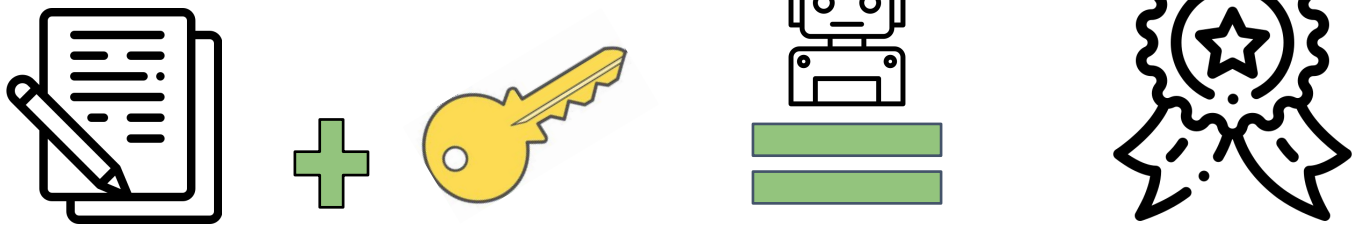



  - **RRSIG** - contém uma assinatura criptográfica


  - **DS** - contém o hash de um registro DNSKEY

Parte 1 - Chaves ZSK

- ZSK - Zone Signing Key (**256**)
  - Chave Pública 
  - Chave Privada 
- Assina o RRSet (Conjunto de RR mesmo nome e tipo)



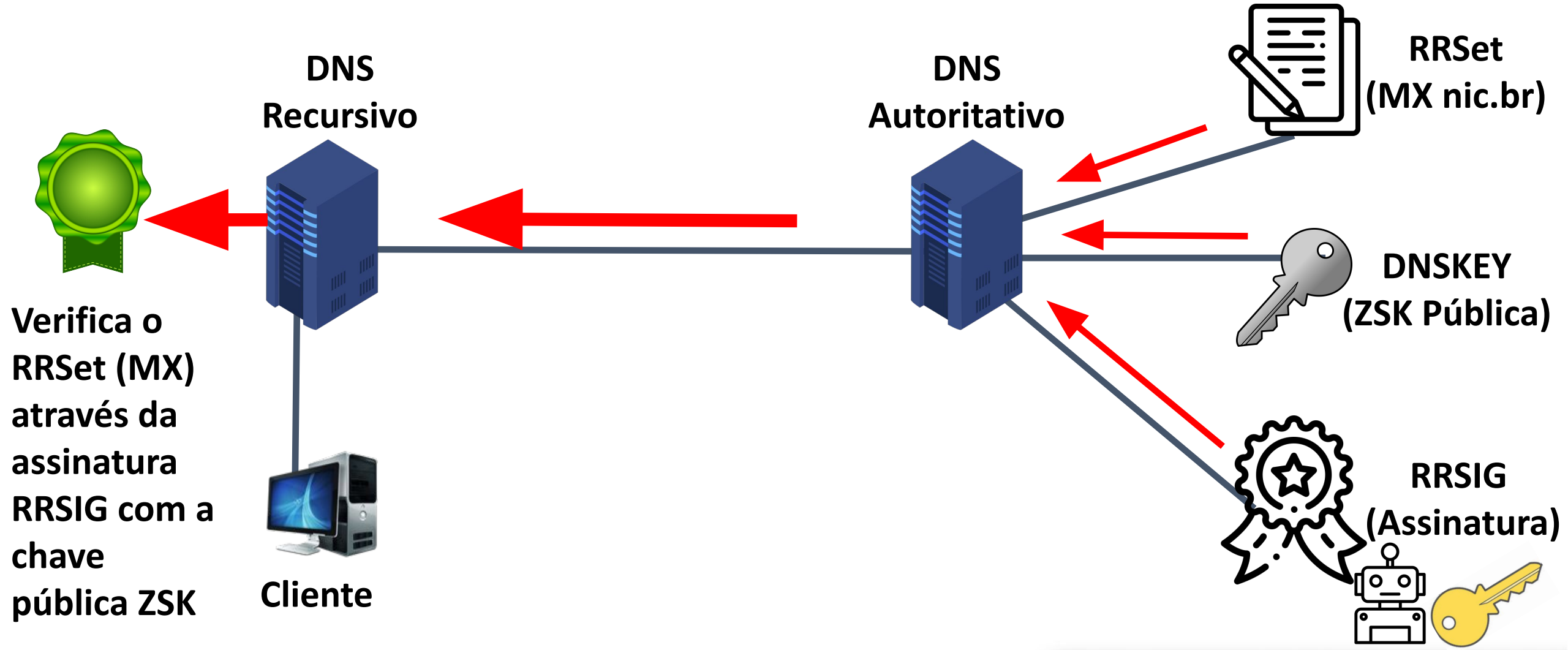
RRSet (MX nic.br)

ZSK Privada

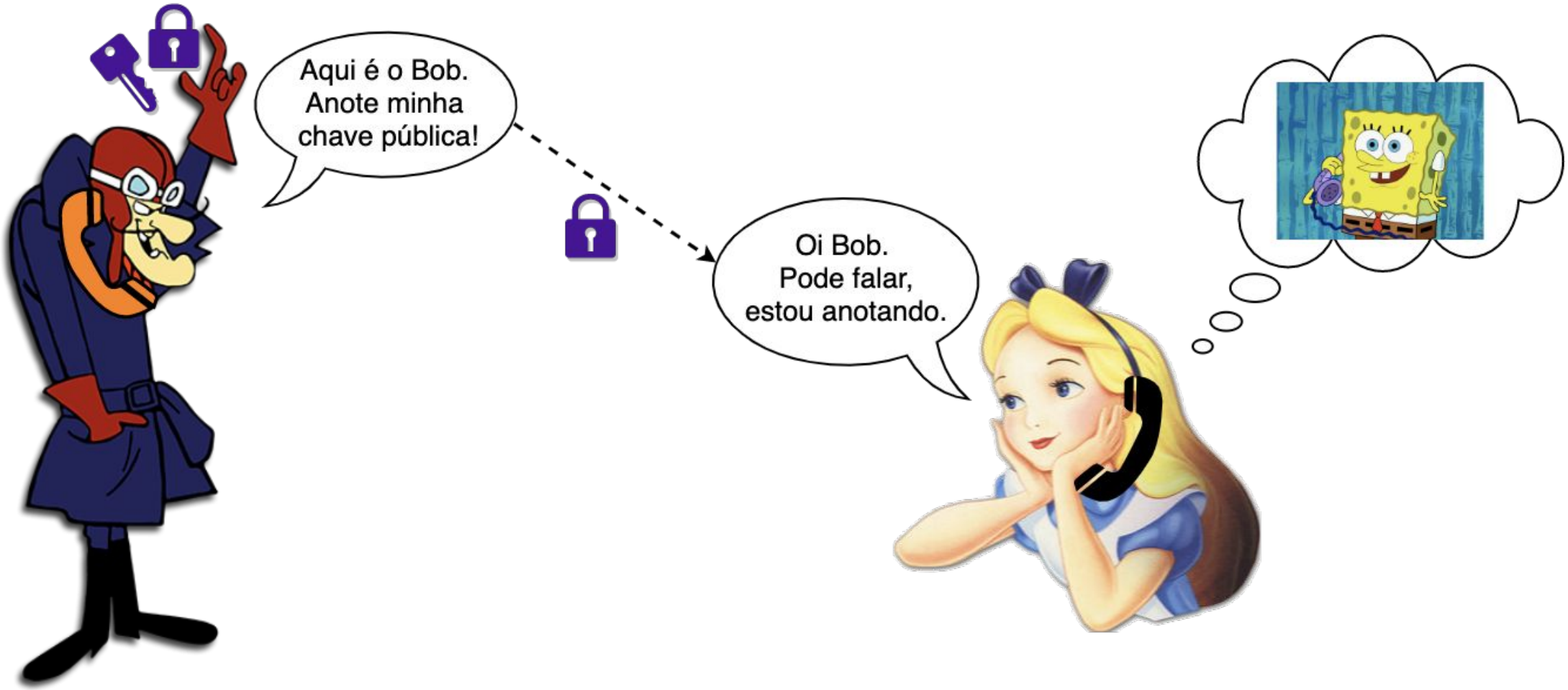
Algoritmo

RRSIG (Assinatura RRSet MX)

Parte 1 - Chaves ZSK



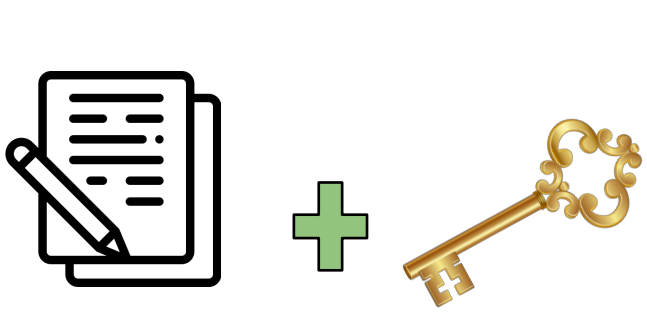
Como garantir a credibilidade de uma chave pública?



Parte 2 - Chaves KSK

- KSK - Key Signing Key (**257**)
  - Chave Pública
  - Chave Privada

- Assina o RRSet de **chaves (ZSK pública e KSK pública)**



RRSet (DNSKEY)

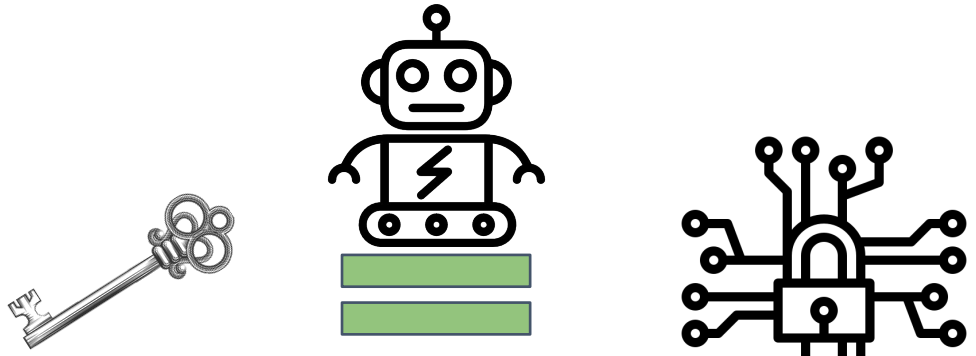
KSK Privada

Algoritmo

RRSIG (Assinatura RRSet DNSKEY)

Parte 2 - Chaves KSK

- Mas e aí quem válida a chave pública do KSK?
- Cadeia de confiança entre servidores autoritativos
- Utiliza o RR DS que é um registro de Hash

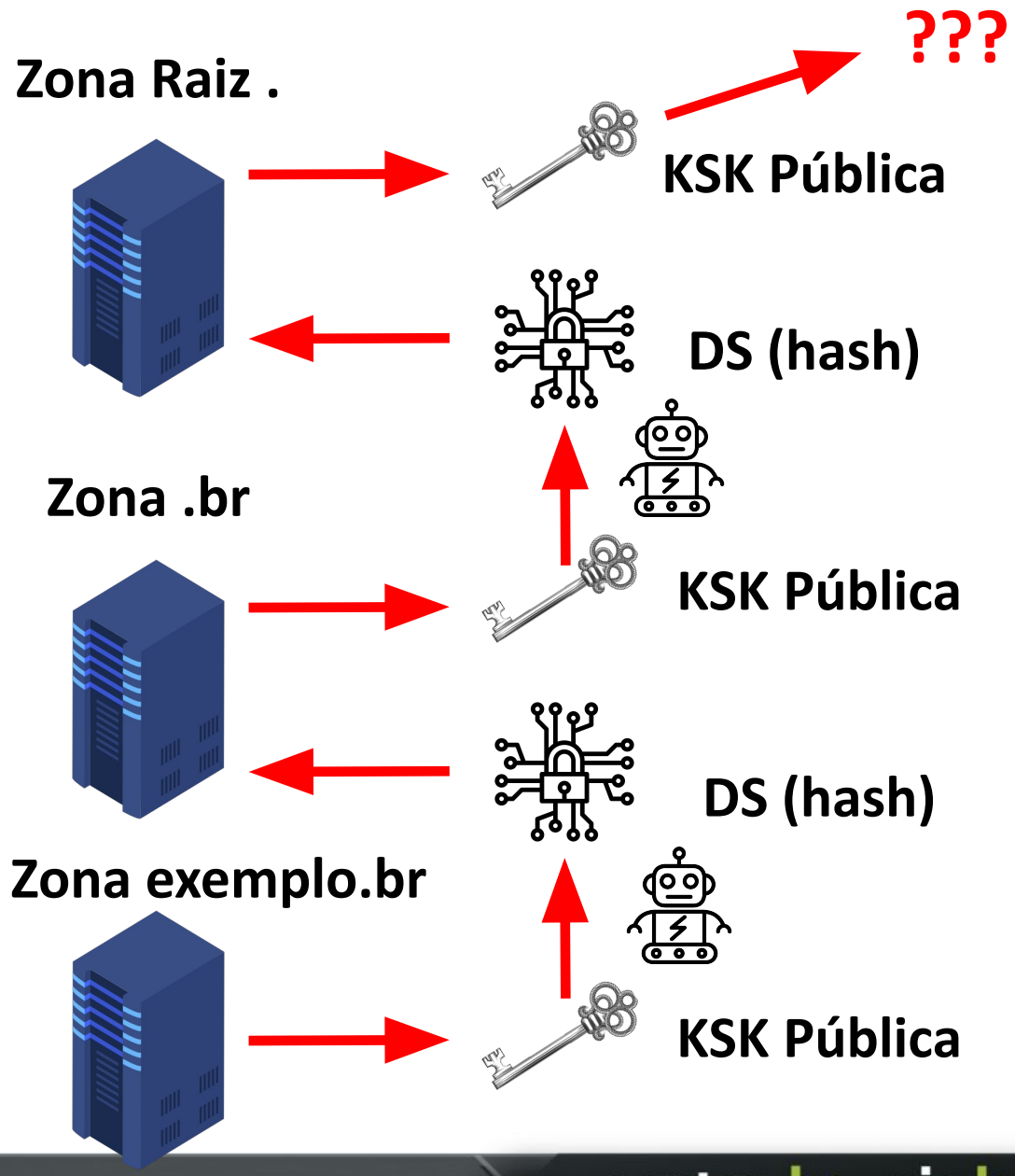


KSK Pública

Algoritmo

DS (hash)

- O DS cria a cadeia de confiança
- O DS é armazenado no servidor autoritativo acima
- E a raiz? Quem garante a autenticidade de sua chave?



Parte 2 - Chaves KSK

- Cerimônia de Assinatura da Zona Raiz - Root Signing Ceremony
- Conjunto de pessoas selecionadas
- Transmitido pela Internet

Verifica a chave pública KSK é igual a já pré cadastrada e válida com a sua assinatura RRSIG

Zona Raiz .

RRSet (DNSKEY - KSK e ZSK)

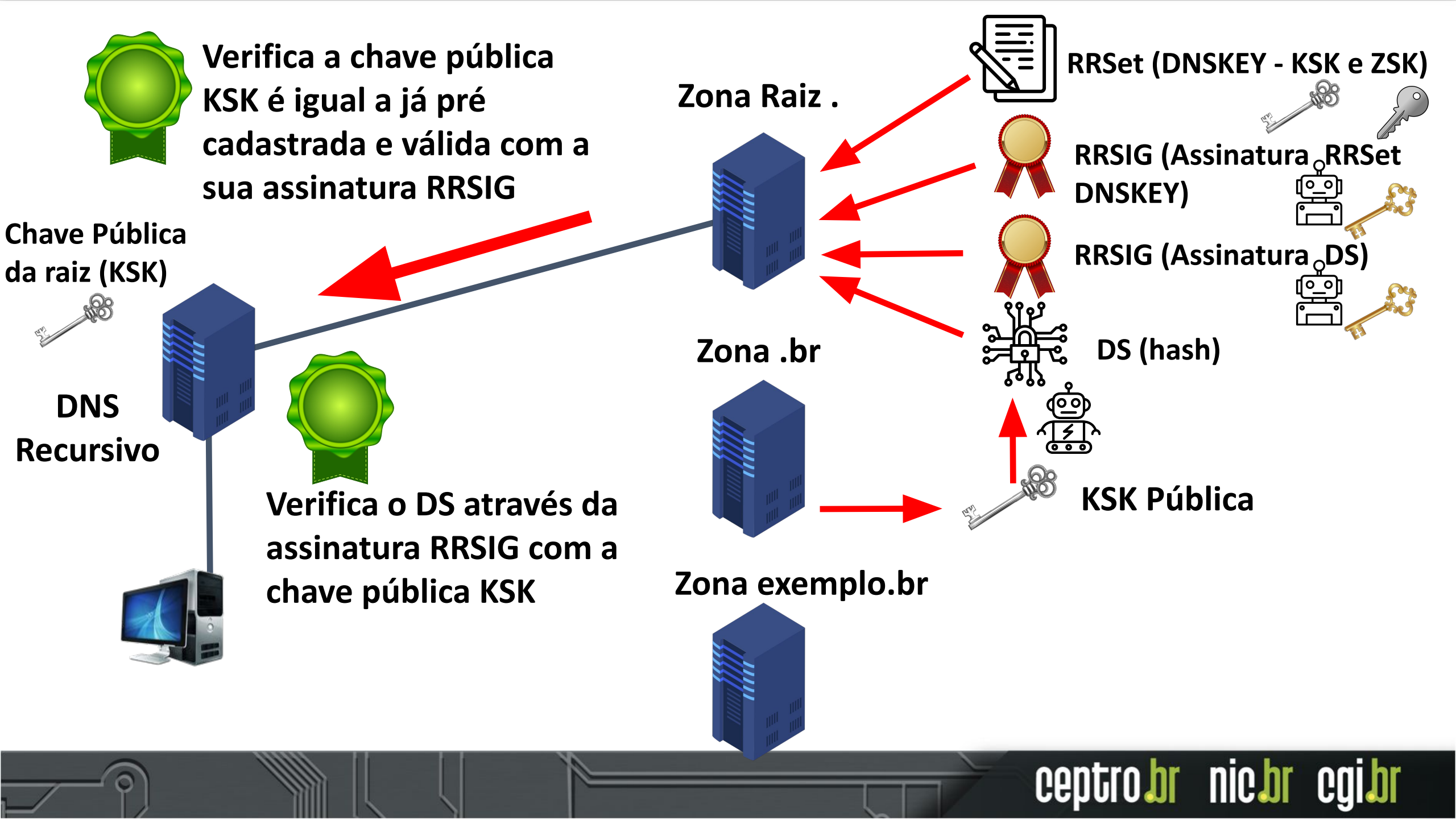
RRSIG (Assinatura RRSet DNSKEY)

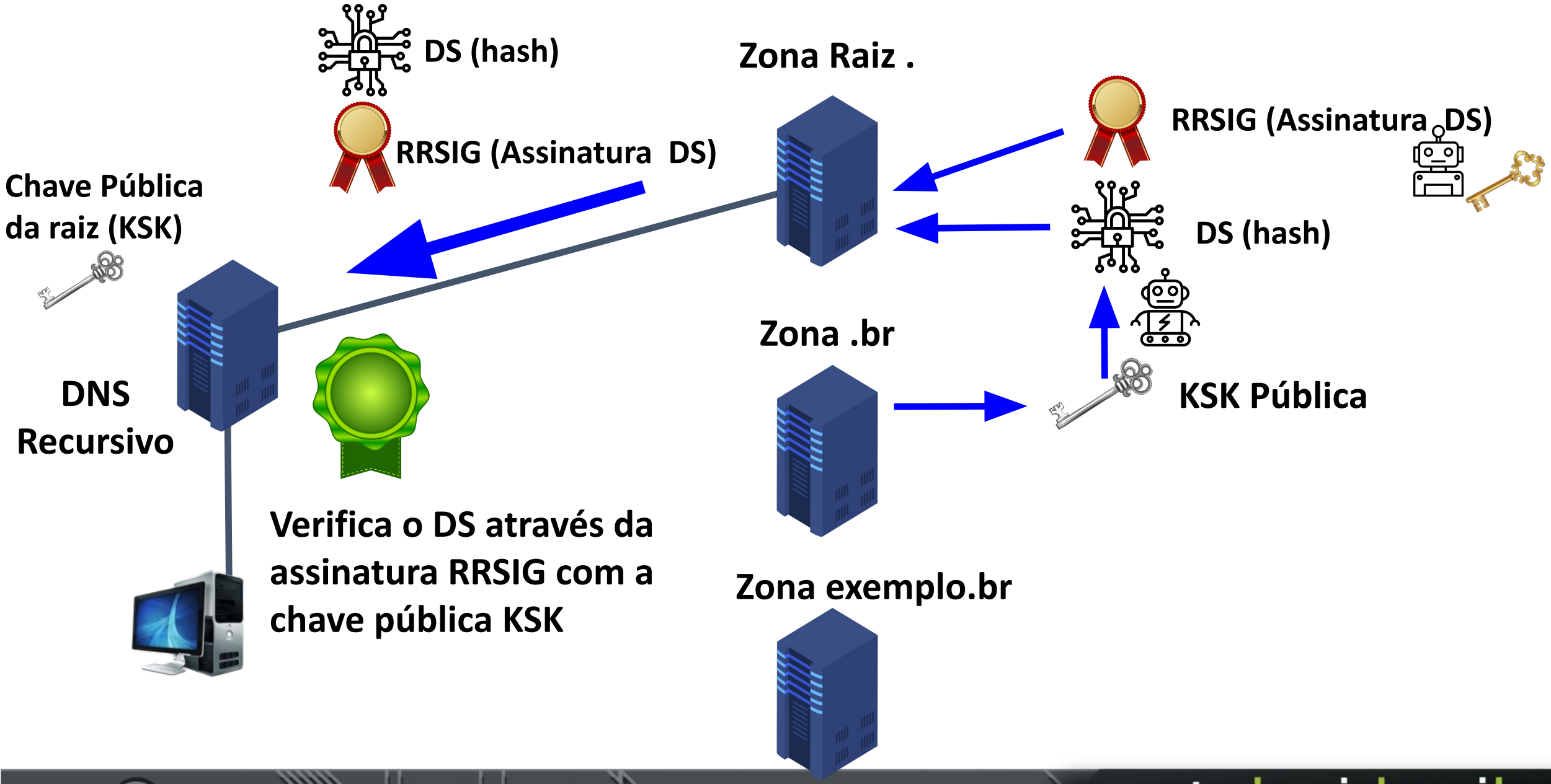
Chave Pública da raiz (KSK)

DNS Recursivo

Zona .br

Zona exemplo.br


Verifica a chave pública KSK é igual a já pré cadastrada e válida com a sua assinatura RRSIG
Chave Pública da raiz (KSK)
DNS Recursivo
Verifica o DS através da assinatura RRSIG com a chave pública KSK
Zona Raiz .
Zona .br
Zona exemplo.br
RRSet (DNSKEY - KSK e ZSK)
RRSIG (Assinatura RRSet DNSKEY)
RRSIG (Assinatura DS)
DS (hash)
KSK Pública


DS (hash)
RRSIG (Assinatura DS)
Chave Pública da raiz (KSK)
DNS Recursivo
Verifica o DS através da assinatura RRSIG com a chave pública KSK
Zona Raiz .
RRSIG (Assinatura DS)
DS (hash)
Zona .br
KSK Pública
Zona exemplo.br

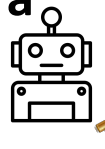
Verifica a chave pública KSK com DS (hash) enviado pelo autoritativo acima

Verifica o RRSet DNSKEY através da assinatura RRSIG com a chave pública KSK

Zona Raiz .

RRSet (DNSKEY - KSK e ZSK)

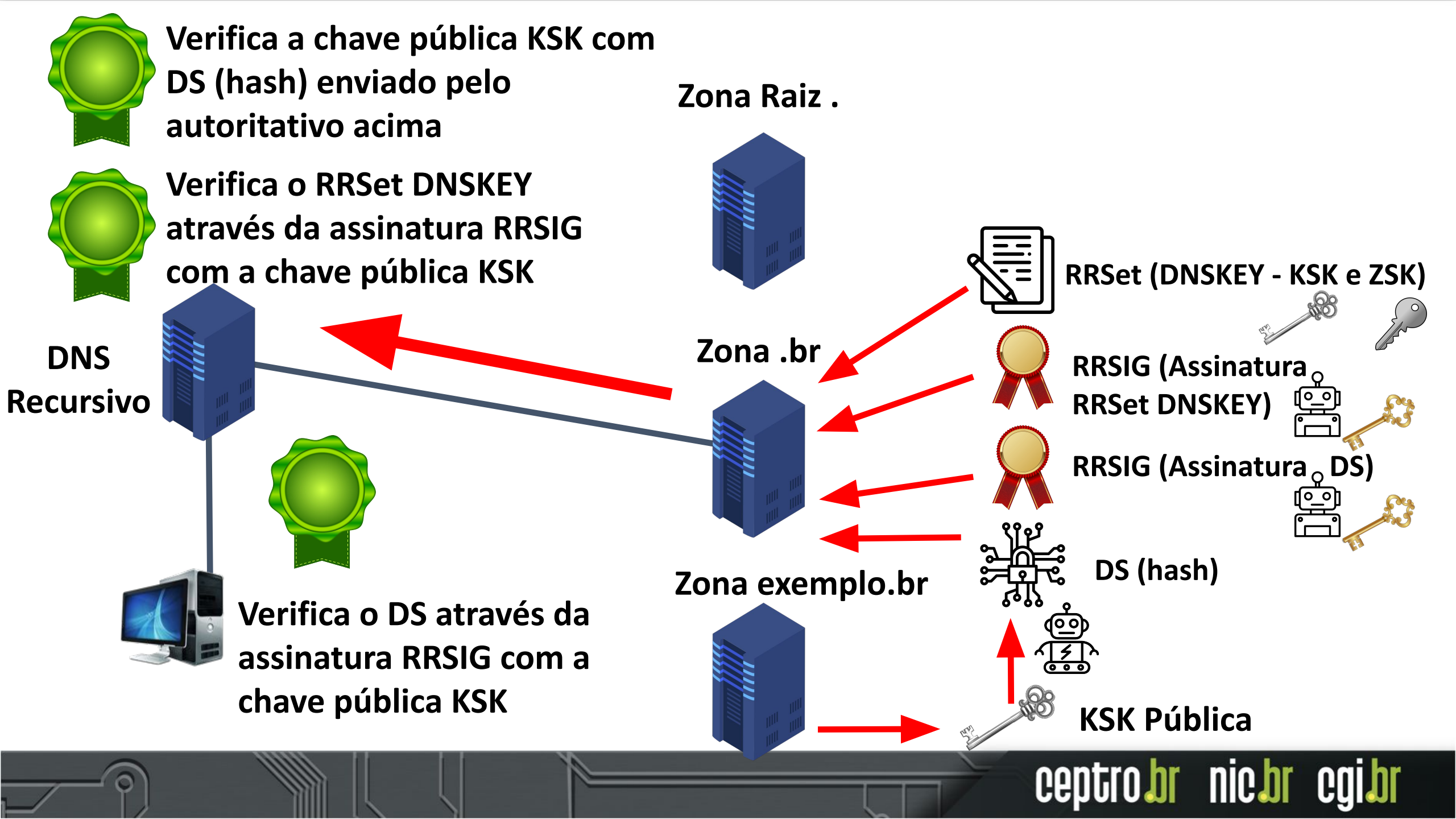
RRSIG (Assinatura RRSet DNSKEY)



DNS Recursivo

Zona .br

Zona exemplo.br


Verifica a chave pública KSK com DS (hash) enviado pelo autoritativo acima
Zona Raiz .
Verifica o RRSet DNSKEY através da assinatura RRSIG com a chave pública KSK
RRSet (DNSKEY - KSK e ZSK)
DNS Recursivo
Zona .br
RRSIG (Assinatura RRSet DNSKEY)
RRSIG (Assinatura DS)
DS (hash)
Zona exemplo.br
Verifica o DS através da assinatura RRSIG com a chave pública KSK
KSK Pública

Lab 4: DNSSEC

ceptro.br nic.br cgi.br

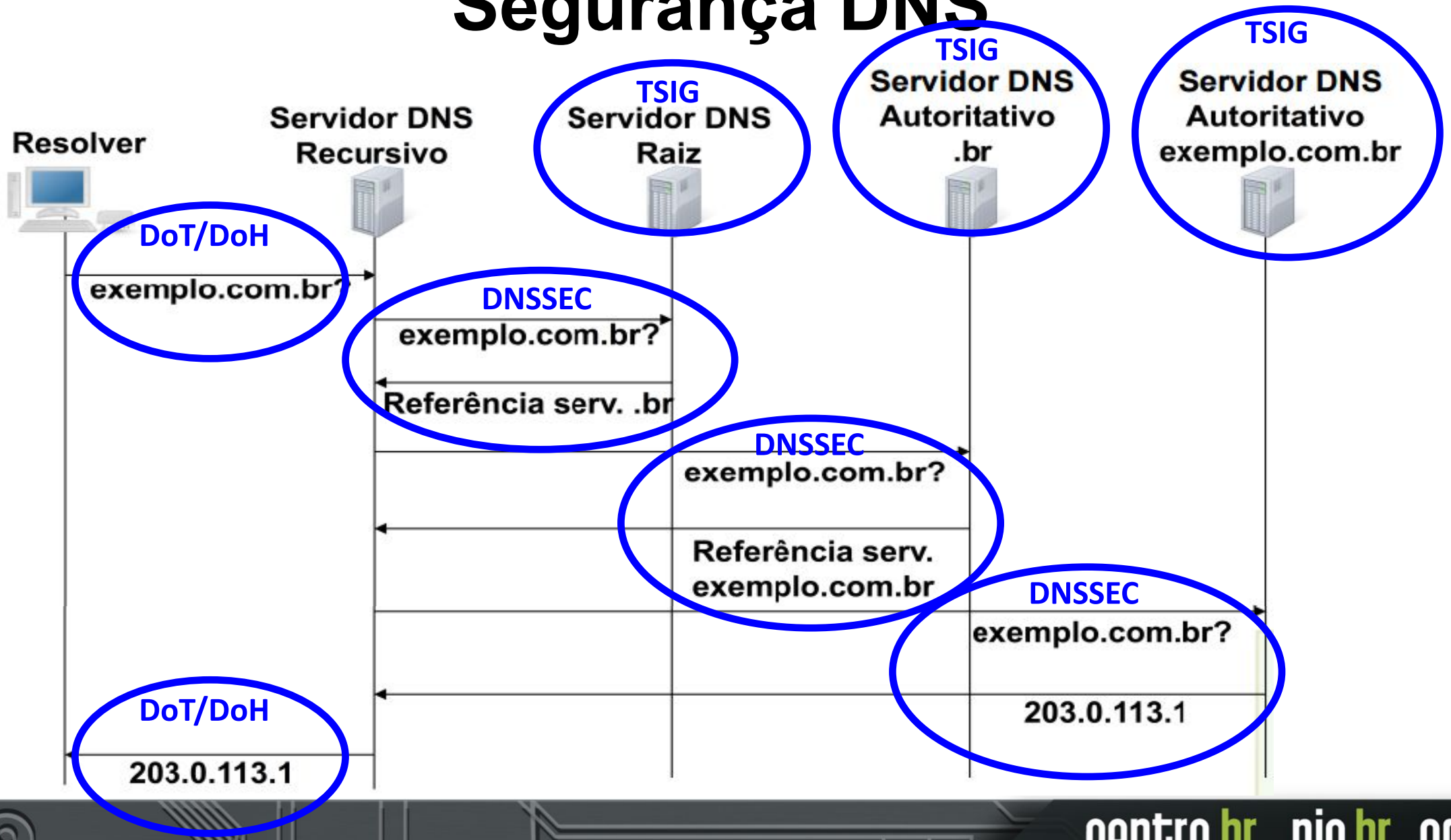
Lab 5: Integração com o Registros.br

ceptro.br nic.br cgi.br

DoT e DoH

ceptro.br nic.br cgi.br

Segurança DNS



DoT e DoH

- DoT - DNS over TLS (RFC 7858)
- DoH - DNS over HTTPS (RFC 8484)
- São técnicas equivalentes de criptografia da conexão das consultas DNS

DoT e DoH

- A principal diferença entre eles é a porta de conexão
  - DoT - Porta 853
  - DoH - Porta 443

DoT e DoH

- DoT
  - Melhor para administradores de rede
  - Como o tráfego DNS ocorre em porta separada é mais fácil de identificar atividade maliciosa

DoT e DoH

- DoH
  - Melhor para os usuários
  - Como utiliza a porta padrão do HTTPS, as consultas e tráfego DNS ficam mascarados

KINDNS

Knowledge-Sharing and **I**nstantiating **N**orms for **D**NS and **N**aming **S**ecurity

ceptro.br nic.br cgi.br

KINDNS

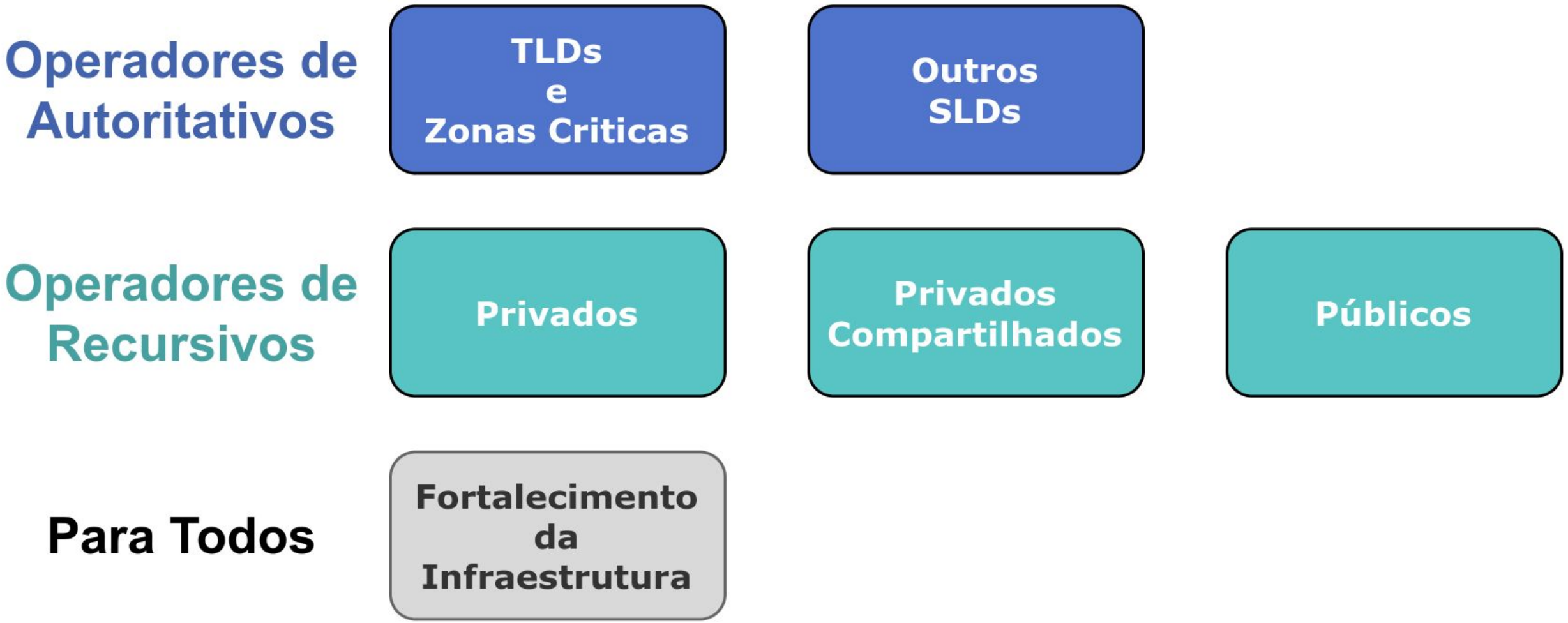
- Iniciativa da **ICANN**
- Promover boas práticas de segurança de DNS
  - Ajuda operadores de DNS a se proteger
  - Medidas simples que se realizadas evitam vulnerabilidades
  - Guias de Configuração

An ICANN Initiative

KINDNS

- **K**nowledge-Sharing and **I**nstantiating **N**orms for **D**NS and **N**aming **S**ecurity
- **Traduzindo:** Normas de Compartilhamento de Conhecimento e Instanciamento para DNS e Segurança de Nomes de Domínio

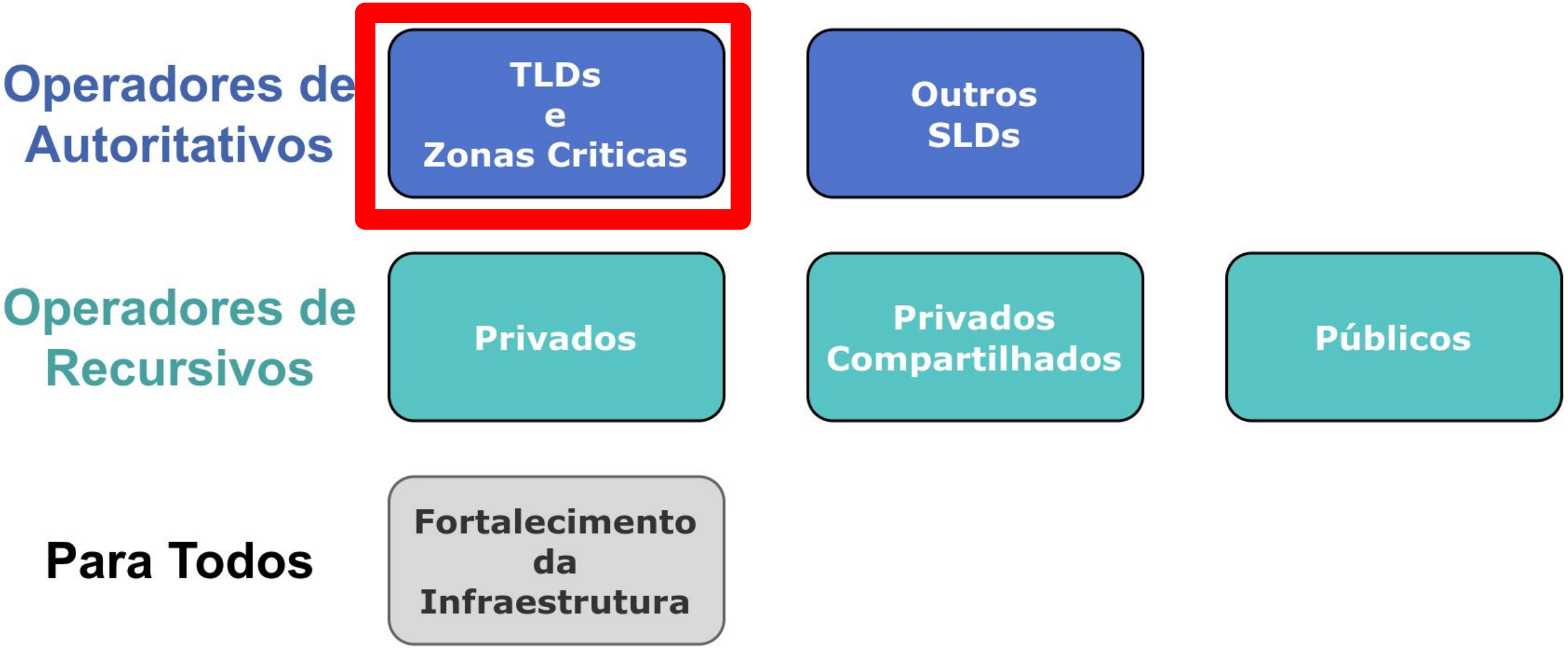
KINDNS - Categorias



KINDNS - Práticas

- **DNS Security (Segurança de DNS):**
  - Melhorar segurança
  - Prevenir usuários de receber informações de DNS maliciosas
  - Diminuir as chances de corrupção de dados
- **DNS Availability and Resilience (Disponibilidade e Resiliência do DNS):**
  - Robustez,
  - Resiliência
  - Estabilidade

KINDNS - Categorias



Autoritativo - TLDs e Zonas Críticas

- Zonas gerenciadas por operadores d TLDs (Top-level Domain)
- TLDs e seus sub-domínios
- Zonas necessárias para o funcionamento de ccTLDs
- SLDs (Second Level Domain) de serviços críticos
  - serviços públicos, serviços médicos, sister governamentais e etc.
- Sistemas Bancários e Financeiros

Autoritativo - TLDs e Zonas Críticas

DNS Security (Segurança do DNS)

1. As zonas autorizadas **DEVEM** ser assinadas pelo DNSSEC e as melhores práticas para gerenciamento de chaves **DEVEM** ser seguidas.

2. O acesso à transferência de zona entre servidores autoritativos **DEVE** ser limitado. Configure ACLs e TSIG no pacote de software de DNS Autoritativo para restringir transferências de zona somente para servidores secundários.

3. A integridade do arquivo de zona **DEVE** ser controlada para evitar modificações inesperadas (maliciosa ou acidental).

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.

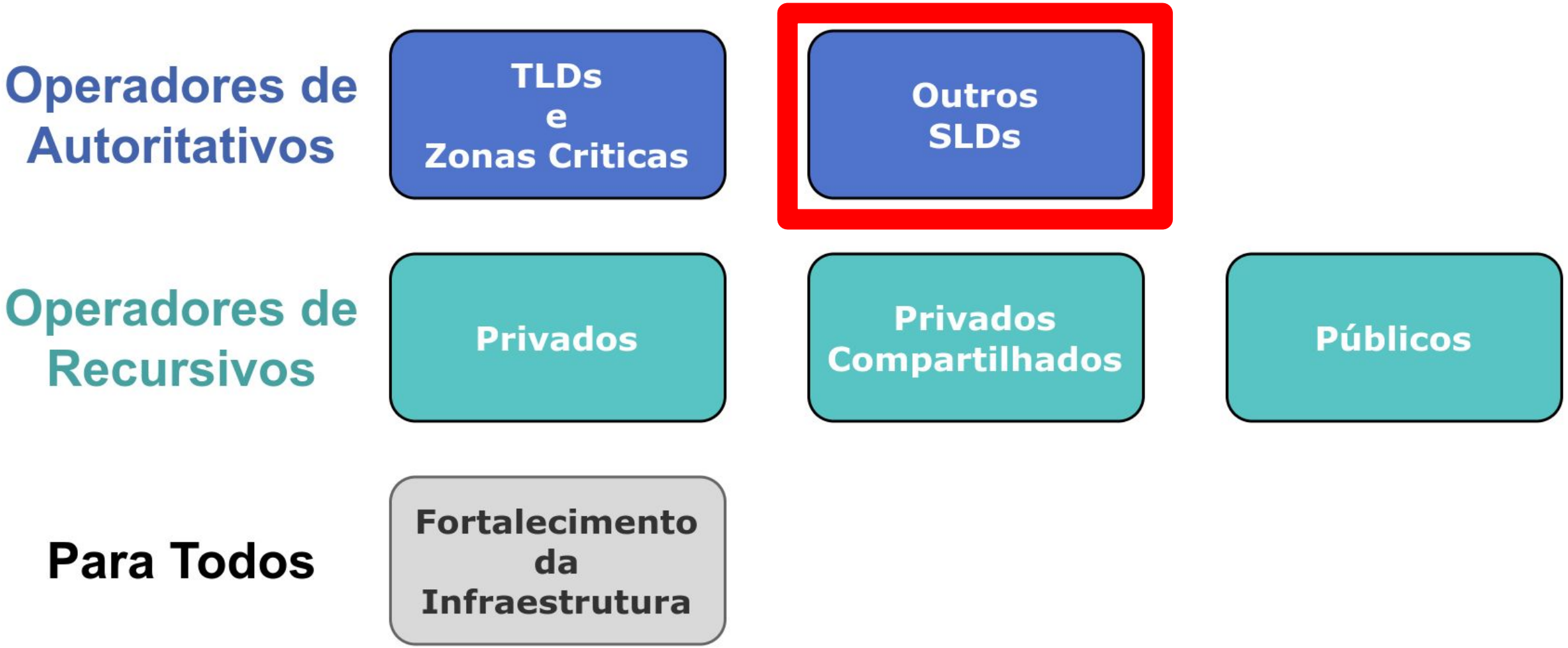
5. Pelo menos dois servidores de nomes distintos **DEVEM** ser usados para qualquer zona.

6. DEVE haver diversidade nas operações autoritativas para promover resiliência. Isto **DEVE** abranger uma ou mais das práticas seguintes: Programas, Redes e Geográfica

7. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

Fonte: https://kindns.org/other-sld-zones/

KINDNS - Categorias



Autoritativo - SLDs

- Isto inclui todas as zonas SLDs, exceto aquelas especificamente designadas como **Zonas Críticas.**

exemplo.com.br

domain.uk

minhaloja.net.br

canaldetv.br

Autoritativo - Outros SLDs

DNS Security (Segurança do DNS)

1. As zonas autorizadas **DEVEM** ser assinadas pelo DNSSEC e as melhores práticas para gerenciamento de chaves **DEVEM** ser seguidas.

2. O acesso à transferência de zona entre servidores autoritativos **DEVE** ser limitado. Configure ACLs e TSIG no pacote de software de DNS Autoritativo para restringir transferências de zona somente para servidores secundários.

3. A integridade do arquivo de zona **DEVE** ser controlada para evitar modificações inesperadas (maliciosa ou acidental).

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

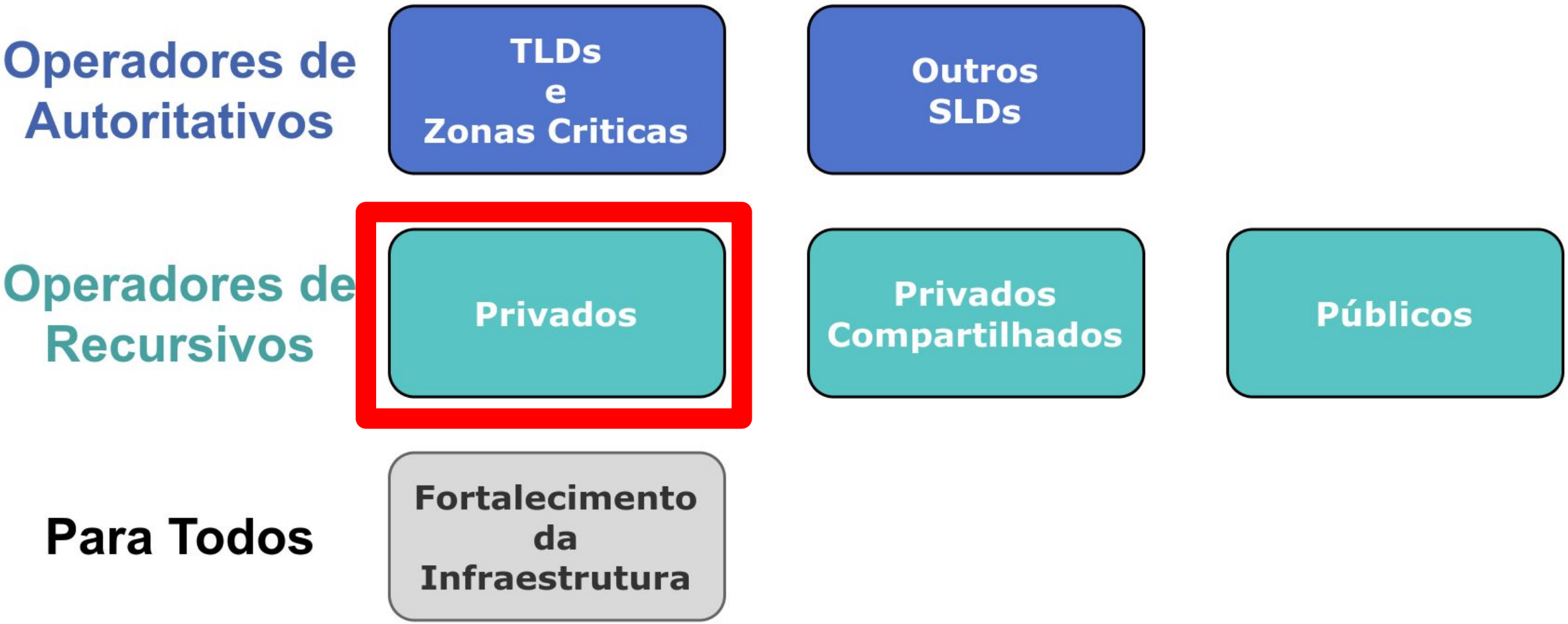
4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.

5. Pelo menos dois servidores de nomes distintos **DEVEM** ser usados para qualquer zona, tendo em mente a diversidade nas práticas operacionais e geográficas.
   1. Todos os servidores autoritativos para uma determinada zona **NÃO DEVEM** ser colocados na mesma sub-rede.
   2. Todos os servidores autoritativos para uma determinada zona **DEVEM** estar em locais físicos diferentes (não no mesmo rack, sala, cidade ou país).

6. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

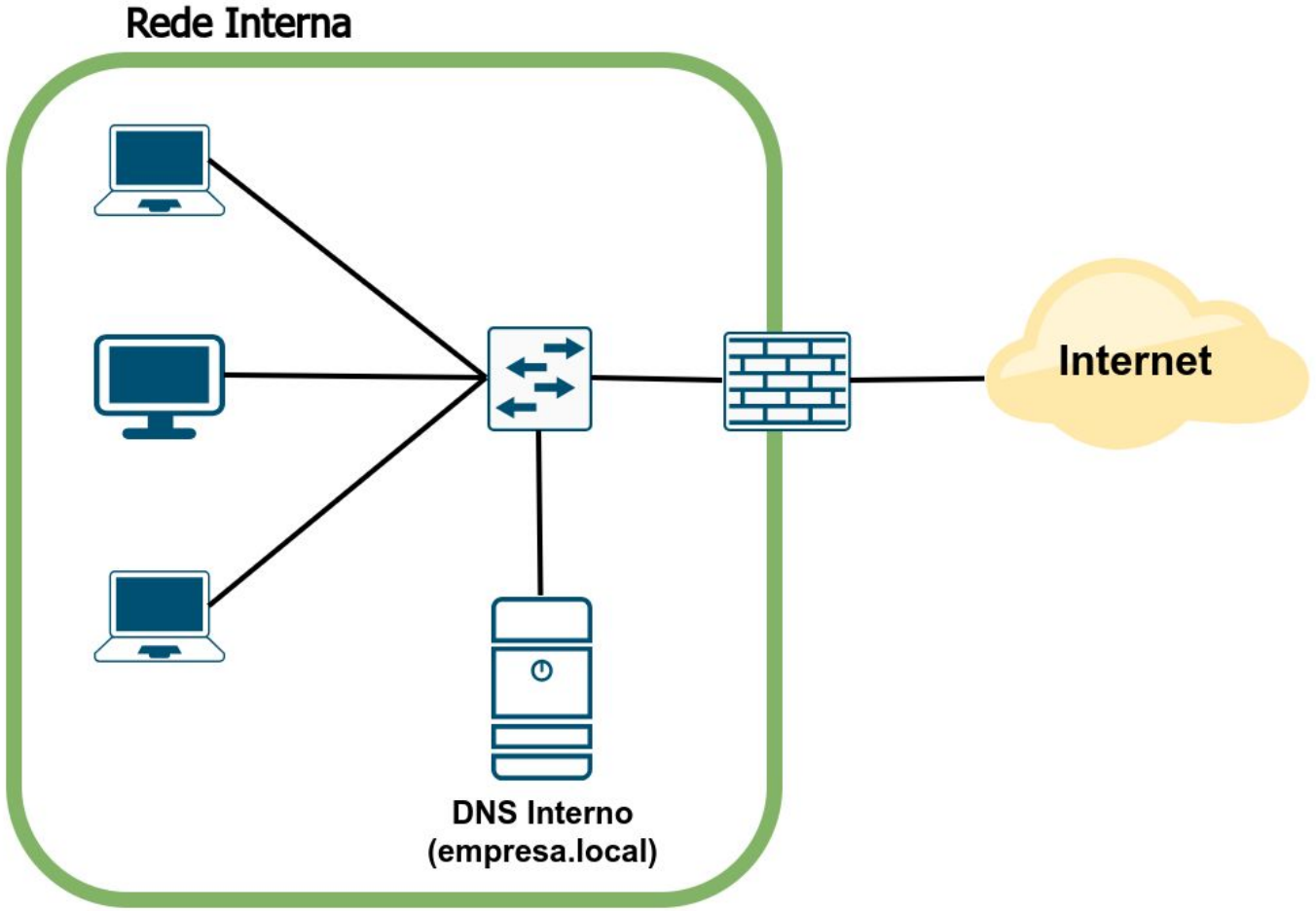
Fonte: https://kindns.org/other-sld-zones/

KINDNS - Categorias



Recursivo - Privados

- Servidores não acessíveis pela Internet aberta
- Encontrado em redes corporativas
- Podem fazer parte de um domínio interno
  - Active Directory e etc.



Recursivo - Privados

DNS Security and Privacy (Segurança e Privacidade do DNS)

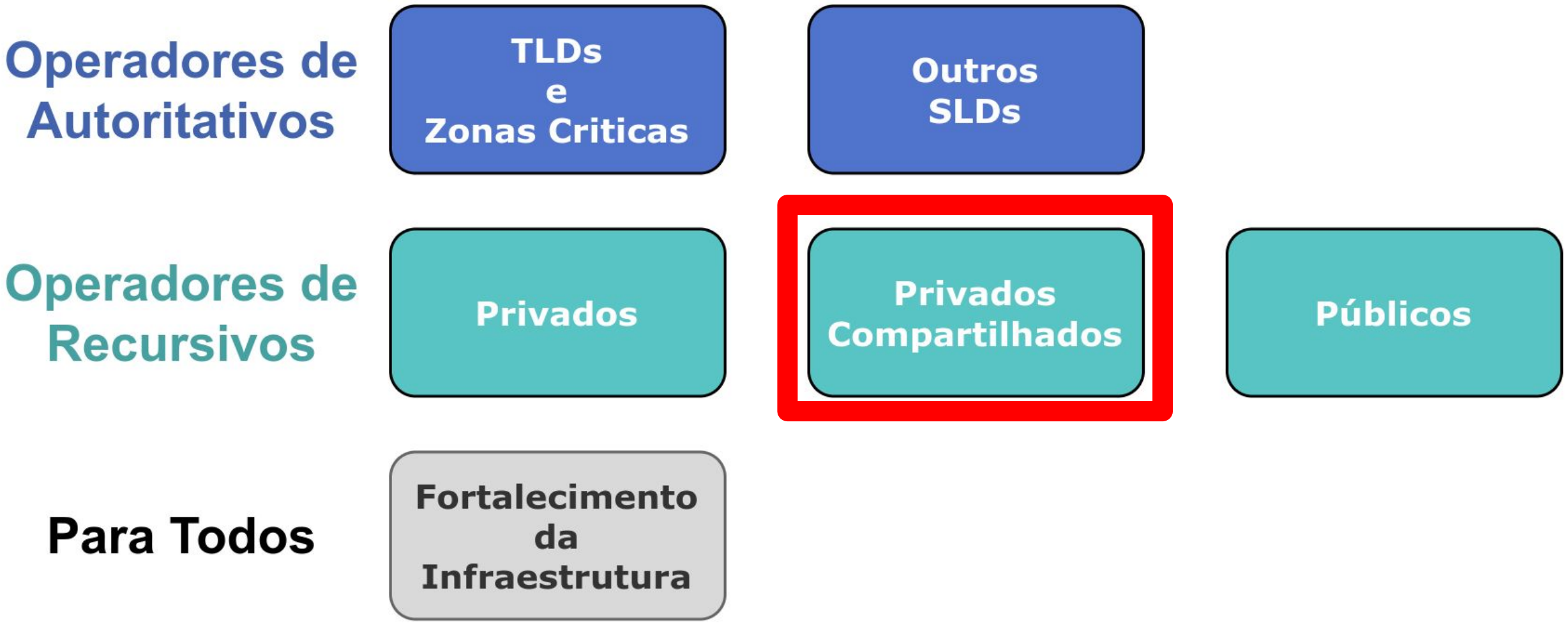
1. A validação DNSSEC **DEVE** ser habilitada para servidores recursivos.
2. ACLs **DEVEM** ser usadas para restringir quem pode enviar consultas recursivas aos seus servidores/validadores DNS.
3. A minimização de QNAME **DEVE** ser habilitada para mitigar o vazamento de nomes de domínio.

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.
5. Pelo menos dois servidores distintos DEVEM ser usados para fornecer serviços de recursão.
6. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

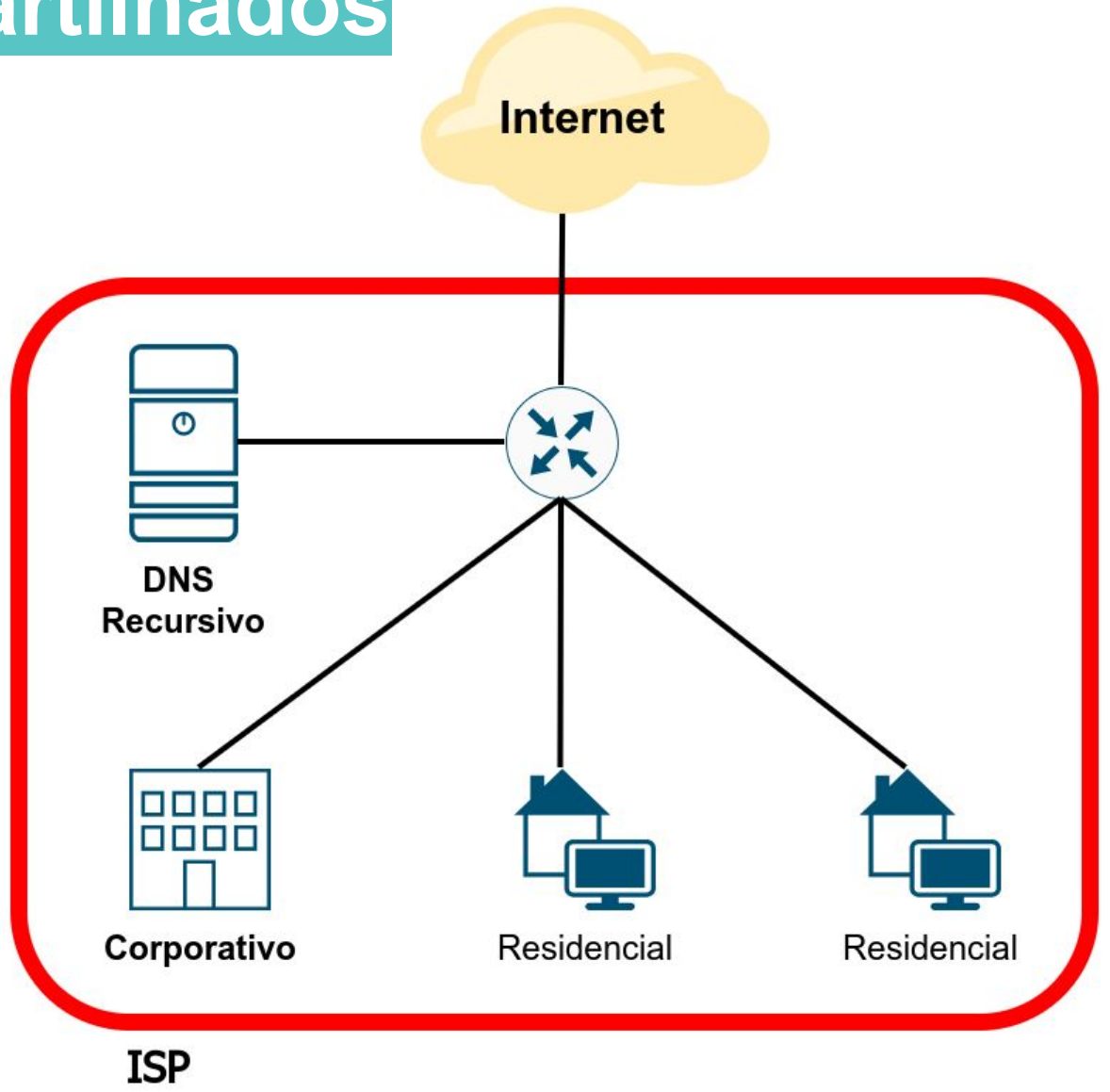
Fonte: https://kindns.org/private-resolvers/

KINDNS - Categorias



Recursivo - Privados Compartilhados

- Normalmente encontrados em ISPs
- Fornecem serviço para seus clientes
  - Residenciais
  - Empresariais
  - Corporativos
  - Móveis



Recursivo - Privados Compartilhados

DNS Security (Segurança do DNS)

1. A validação DNSSEC **DEVE** ser habilitada para servidores recursivos.

2. ACLs **DEVEM** ser usadas para restringir quem pode enviar consultas recursivas aos seus servidores/validadores DNS.

3. A minimização de QNAME **DEVE** ser habilitada para mitigar o vazamento de nomes de domínio. **(Privacidade)**

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.

5. Seus serviços de recursivo **DEVEM** ter resiliência, usando pelo menos dois servidores distintos que levem em consideração a diversidade (Programas, Redes e Geográfica).

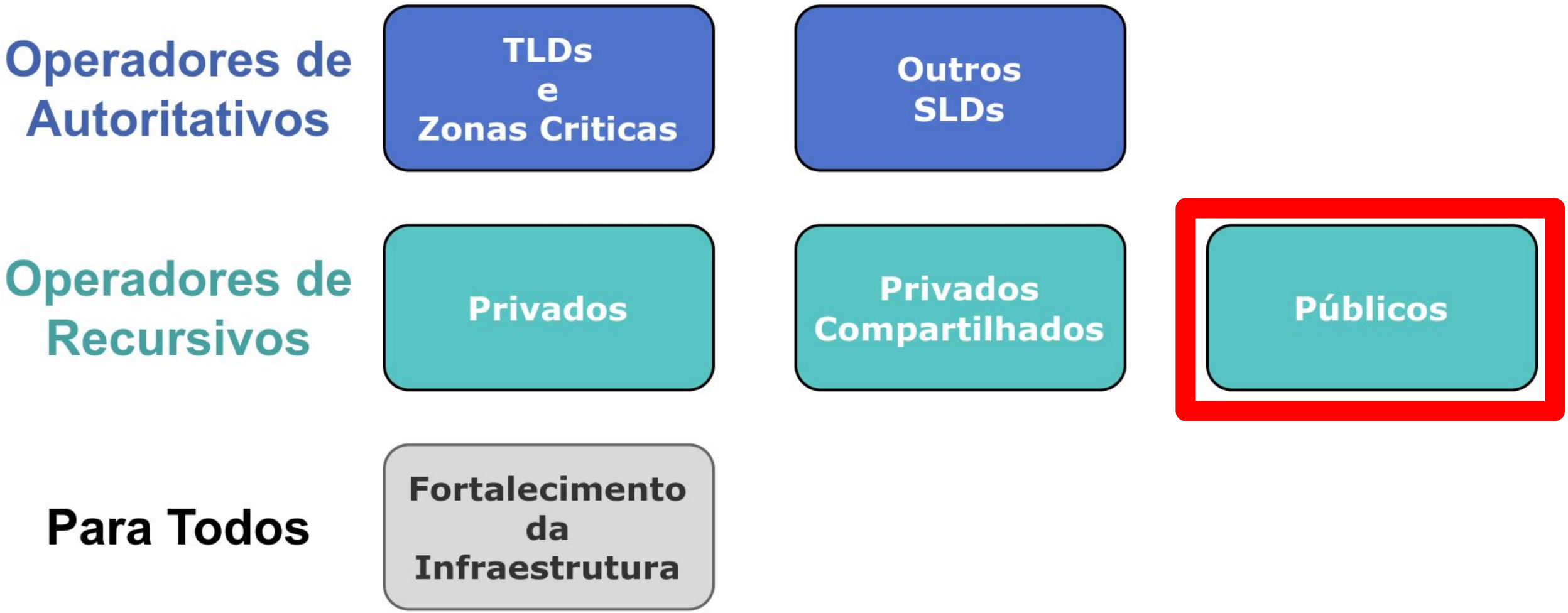
6. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

Bônus (prática adicional recomendada acima e além dos requisitos mínimos do KINDNS).

7. DoT (DNS sobre TLS) ou DoH (DNS sobre HTTPS) **DEVEM** estar habilitados.

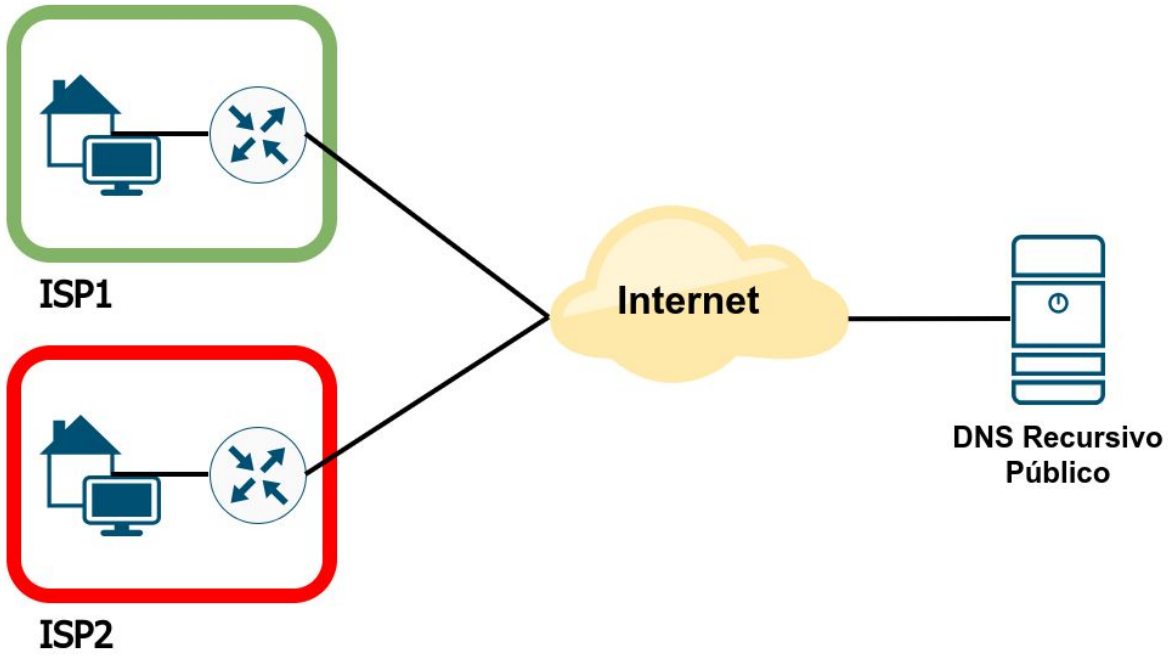
Fonte: https://kindns.org/shared-private-resolvers/

KINDNS - Categorias



Recursivo - Públicos

- Incluem dois tipos:
  - **Públicos Abertos:** acessíveis para todos conectados à Internet
  - **Públicos Fechados:** acessíveis apenas mediante a contratação do serviço (ex: filtragem de DNS)



Recursivo - Públicos

DNS Security (Segurança do DNS)

1. A validação DNSSEC **DEVE** ser habilitada para servidores recursivos.

2. A minimização de QNAME **DEVE** ser habilitada para mitigar o vazamento de nomes de domínio. **(Privacidade)**

3. DoT (DNS sobre TLS) ou DoH (DNS sobre HTTPS) **DEVEM** ser habilitados e oferecidos aos clientes junto com o DNS Tradicional e não criptografado. **(Privacidade)**

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.

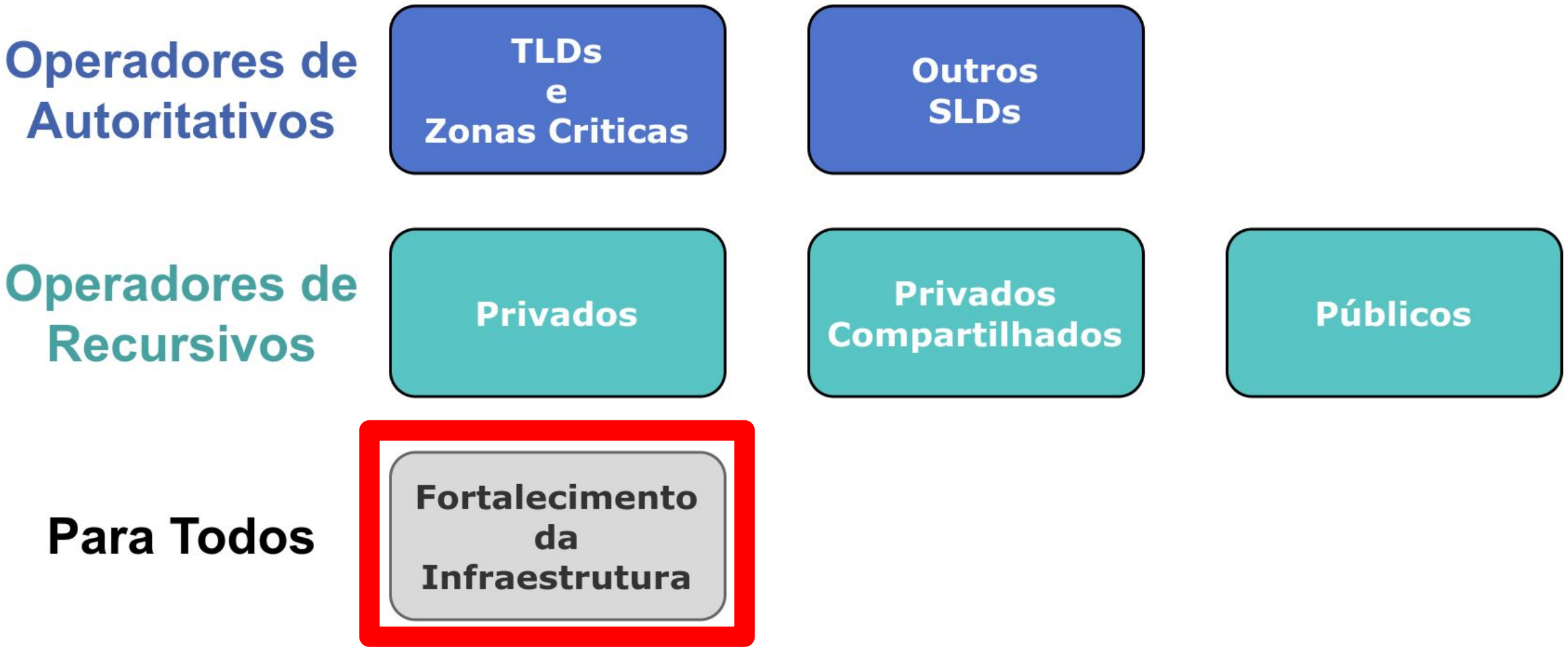
5. Os dados coletados por meio do registro passivo de consultas DNS **DEVEM** ser retidos apenas pelo tempo necessário para o bom funcionamento do serviço oferecido, incluindo solução de problemas, pesquisa e atendimento aos requisitos legais locais sobre retenção de dados.

6. Seus serviços de recursivo **DEVEM** ter resiliência, usando pelo menos dois servidores distintos que levem em consideração a diversidade (Programas, Redes e Geográfica).

7. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

Fonte: https://kindns.org/public-resolvers/

KINDNS - Categorias



Para Todos - Fortalecimento da Infraestrutura

- ***Network Security*:**
  - **Segurança de Rede**
  - Prevenir acesso não autorizado aos servidores de DNS
  - Garantir que o tráfico interno não vaze para outras redes
- ***Host and Service Security*:**
  - **Segurança de Hospedeiros e Serviços**
  - Melhorar a segurança do equipamento hospedando o serviço de DNS
  - Reduzir o possibilidade de:
    - Comprometimento da segurança do equipamento
    - Ataques de DoS (*Denial of Service)*
    - Outros ataques direcionados ao serviço DNS
- **Customer-Facing Portal and Service Security:**
  - **Portal do Cliente e Segurança de Serviço**
  - Dar suporte às necessidades de segurança dos clientes

Para Todos - Fortalecimento da Infraestrutura

Network Security (Segurança de Rede)

1. As ACLs **DEVEM** ser implementadas para restringir o tráfego de rede aos seus servidores DNS.

1.1 Para operadores autoritativos, as ACLs **DEVEM** permitir apenas tráfego DNS e códigos de resposta ICMP associados aos seus servidores DNS autoritativos; o acesso a todos os outros serviços e portas da sua rede para servidores DNS **DEVE** ser negado.

1.2 Para todos os tipos de operadores DNS (autoritativos e recursivos), o tráfego de entrada de todas redes Bogons **DEVE** ser bloqueado, incluindo endereços privados (RFC 1918) e possivelmente, RFC 6598 (espaço de endereço IPv4 compartilhado) para IPv4. É claro que os operadores de DNS recursivos **NÃO** devem bloquear o espaço de endereços IP privados/compartilhados implantado na organização. Consulte: https://ipgeolocation.io/resources/bogon.html

2. A filtragem de saída **DEVE** ser implementada para que nenhum tráfego de rede possa sair da sua rede com um endereço IP de origem que não esteja atribuído a você ou a seus clientes (conforme BCP38/MANRS).

Fonte: https://kindns.org/platform-hardening/

Para Todos - Fortalecimento da Infraestrutura

Host and Service Security (Segurança de Hospedeiros e Serviços)

3. A configuração de cada servidor DNS DEVE ser bloqueada. Isso inclui o seguinte:

3.1 Todos os serviços e pacotes de software que não são necessários para oferecer o serviço DNS no sistema **DEVEM** ser desinstalados ou desativados.

3.2 Os equipamentos hospedam os serviços DNS **DEVEM** executar apenas software DNS. Em outras palavras, os servidores DNS **NÃO DEVEM** executar outros serviços, como servidores web ou de e-mail.

3.3 Todos os *logs* relevantes para o subsistema DNS **DEVEM** estar habilitados. Os registros **DEVEM** ser enviados para um local central para arquivamento, inspeção e auditoria, e **DEVEM** ser retidos por um período razoável, de acordo com as políticas de retenção.

4. As permissões do usuário e o acesso de aplicações aos recursos do sistema **DEVEM** ser limitados. As permissões de arquivo e as restrições de propriedade **DEVEM** ser definidas para que os usuários e serviços não diretamente associados ao gerenciamento do subsistema DNS não tenham acesso de leitura ou gravação à configuração do serviço DNS, aos arquivos de dados e aos subsistemas de banco de dados.

Fonte: https://kindns.org/platform-hardening/

Para Todos - Fortalecimento da Infraestrutura

5. Os arquivos de configuração do sistema e do serviço **DEVEM** ter controle de versão. Para operadores autorizados, os arquivos/dados de zona também **DEVEM** ser versionados.

6. O acesso aos serviços de gerenciamento (por exemplo, SSH, ferramentas de configuração baseadas na web) **DEVE** ser restrito. Todos os serviços não necessários para DNS ou gerenciamento **DEVEM** ser desabilitados ou desinstalados se possível, caso contrário, o acesso à rede aos serviços desnecessários **DEVE** ser bloqueado.

7. O acesso ao console do sistema **DEVE** ser protegido por meio de chaves criptográficas, protegidas por uma senha (por exemplo, chaves SSH) ou por meio de autenticação de dois fatores adequada (gerador de OTP ou baseada em token).

Customer-Facing Portal and Service Security (Portal do Cliente e Segurança de Service)

8. As credenciais para acesso do cliente (registrantes e outros contatos do domínio) **DEVEM** seguir práticas sólidas de gerenciamento de credenciais, incluindo a oferta de autenticação de dois fatores como opção.

Fonte: https://kindns.org/platform-hardening/

KINDNS - Como fazer parte?

- **Auto Avaliação**
  - Anônimas
  - Perguntas sobre a sua infraestrutura e as práticas que você utiliza.
  - Relatório para verificar os pontos de melhoria
- **Formulário de Inscrição**
- **Uma vez a organização aceita:**
  - Nota de Boas Vindas
  - Badge de Conformidade KINDNS
  - Adicionado à lista de participantes

KINDNS - Site

KINDNS

An ICANN Initiative

https://kindns.org

Dúvidas

Obrigado

ipv6.br

wanderson@nic.br

20 de agosto de 2025

nic.br cgi.br

www.nic.br | www.cgi.br