

Tópicos sobre DNS e o seu provedor na ICANN.



Daniel Fink daniel.fink@icann.org

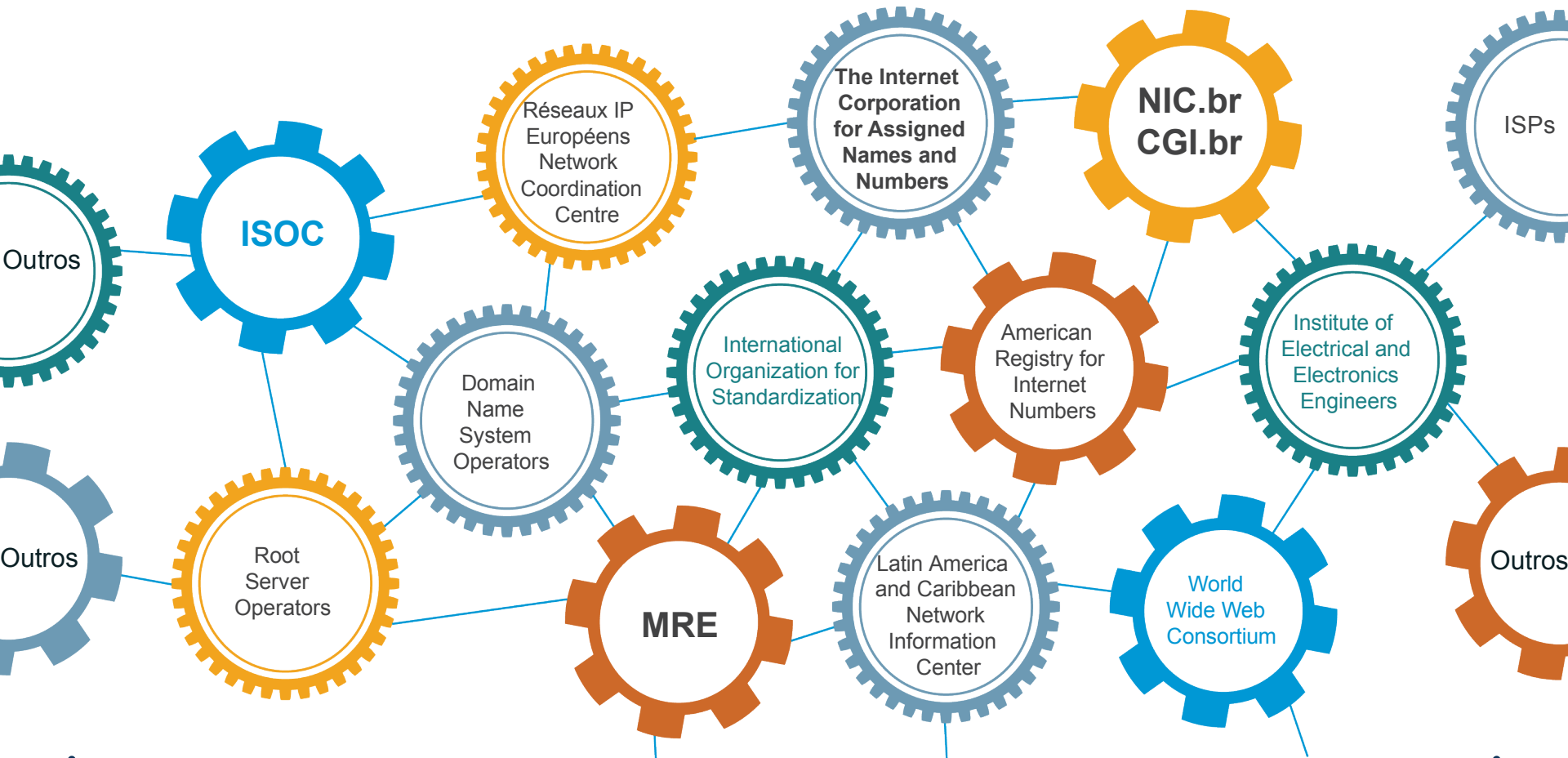
IX Fórum Regional – Belo Horizonte MG
Junho 2019

O que é a ICANN?

Corporação
da Internet
para Designação
de Nomes
e Números

Nossos parceiros






Em coordenação com nossos parceiros, ajudamos a fazer a Internet funcionar.



Missão da ICANN

A missão da Corporação da Internet para Designação de Nomes e Números (ICANN) é **garantir a operação estável e segura dos sistemas de identificadores exclusivos da Internet.**

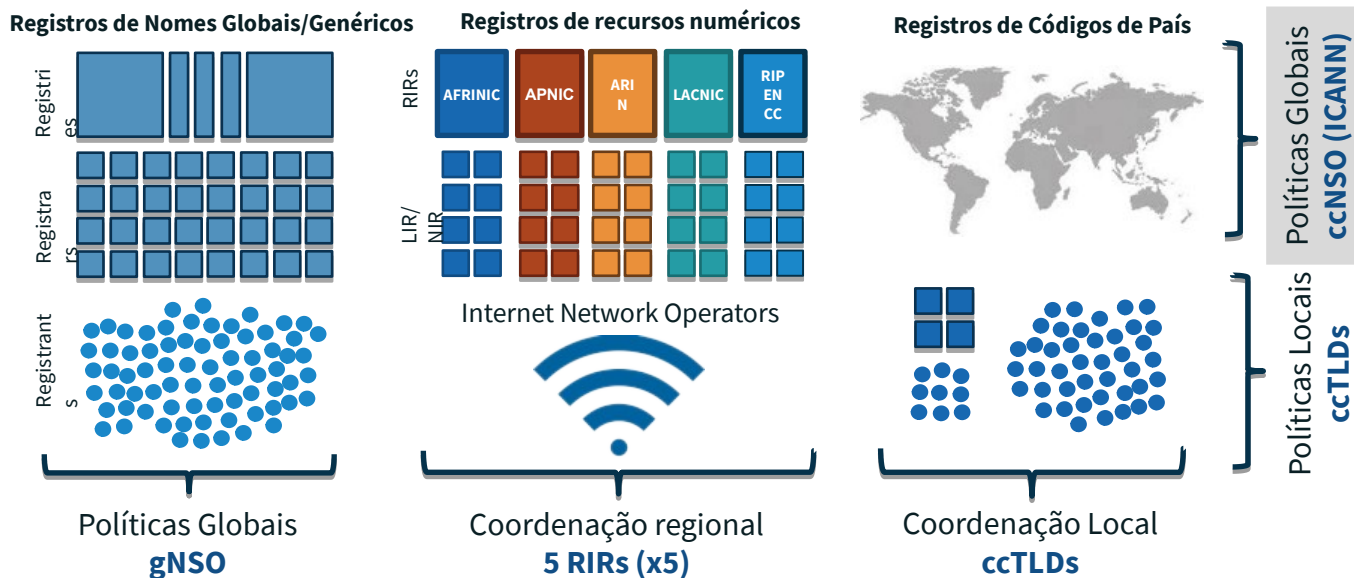
Especificamente, a ICANN:

-  **1** Coordena atribuições na **zona-raiz** do DNS
-  **2** Coordena políticas para nomes de domínio de **segundo nível** em gTLDs
-  **3** Facilita a coordenação da operação e evolução dos servidores raiz do DNS
-  **4** Coordena a distribuição de blocos IP e números de AS
-  **5** Colabora com outras entidades para prover registros necessários para o funcionamento da Internet de acordo com especificações.

Estrutura da ICANN



Framework de Desenvolvimento de Políticas de Identificadores



- Altamente recomendável acompanhar e participar:



ICANN | ISPCP

Internet Service Providers & Connectivity Providers

Representa o setor de conectividade, contribui nas diversas discussões técnicas e macropolíticas:

- ⦿ Impacto do lançamento de novos nomes de domínio genéricos
- ⦿ Universal Acceptance
- ⦿ SSR de DNS

Se você é um provedor de Internet, participe da ISPCP na ICANN. Não há custos, simplesmente cadastre-se e receberá todas as novidades e oportunidades para participar nas atividades do grupo. Ademais, você poderá antecipar-se às oportunidades de negócios quando surgirem.

Visite: <http://www.ispcp.info>

ICANN | ISPCP

Internet Service Providers & Connectivity Providers

Member Logout 

Search our Articles... 

Home

About

ISPCP Bulletin

Membership

Policy Resources

Policy Statements

Meetings

Contact the ISPCP

Membership Application

Membership

Choose a member type below to join as a new member.

Member Type*

Internet Service Provider

Membership Options

1 period - \$0.00 (through Apr 25, 2020)

Automatically Renew

Organization Name*

Quick Links

[Informational Brochure - 2019](#)

[Informational Videos - learn about the ISPCP](#)

[ISPs in the GNSO at ICANN](#)

[ISPCP Membership Application](#)

Upcoming Events

Mon May 6, 2019

[ISPCP Monthly Membership Meeting \(date and time to be confirmed on the ISPCP email list\)](#)

Category: Events

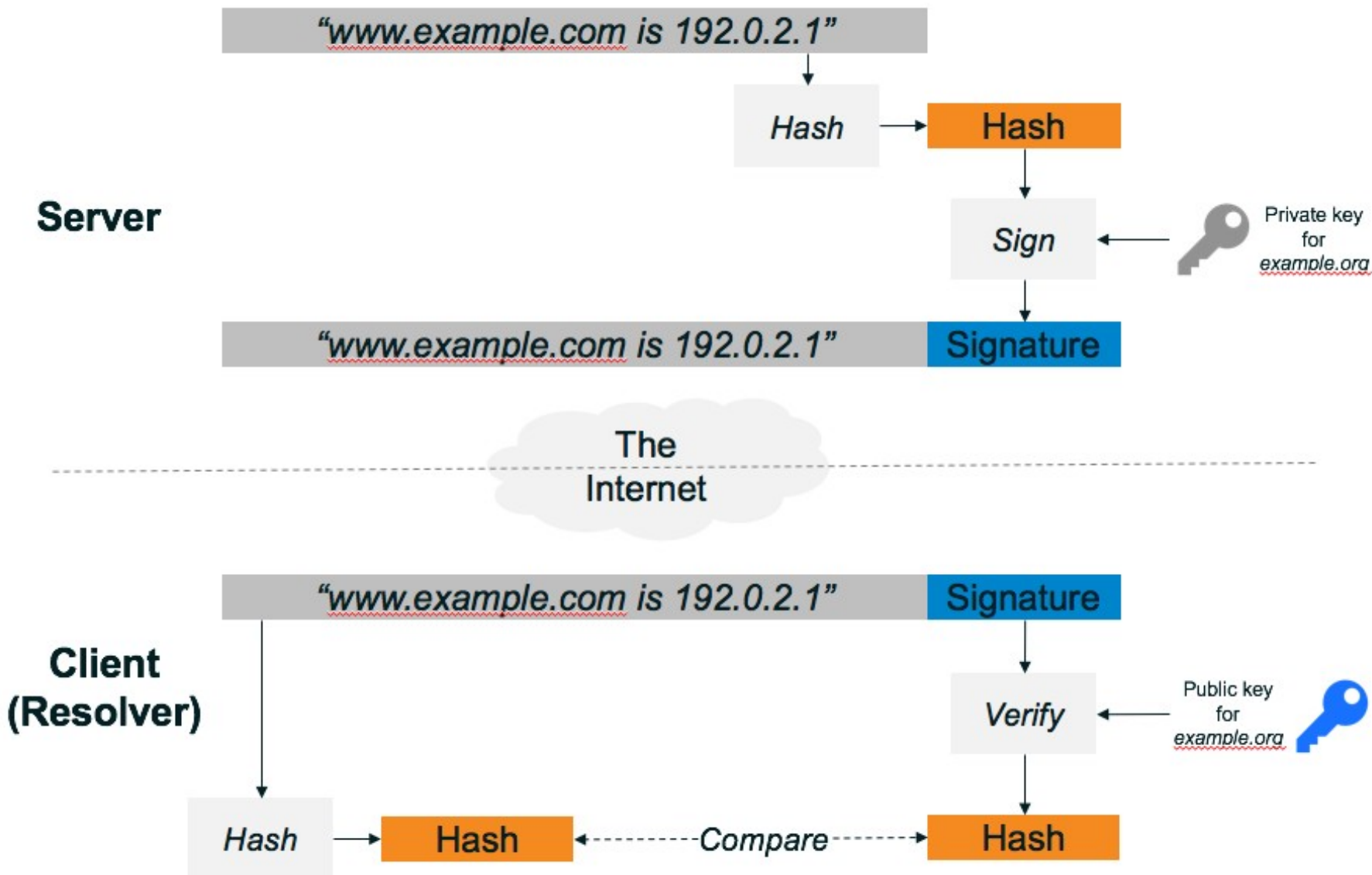
Mon Jun 24, 2019

O que é DNSSEC?



- ⊙ DNSSEC = “**DNS Security Extensions**”
- ⊙ É um protocolo que está sendo implantado atualmente para proteger o Sistema de Nomes de Domínio (DNS).
- ⊙ O DNSSEC adiciona segurança ao DNS ao incorporar criptografia de chave pública na hierarquia do DNS, resultando em uma PKI (Public Key Infrastructure, infraestrutura de chave pública) única e aberta para nomes de domínio.
- ⊙ Resultado de mais de uma década de desenvolvimento de padrões abertos

Criptografia de Chave Pública e DNSSEC



Hyperlocal Alternativa ao IMRS

Servidores Raiz e Operadores

- A** Verisign
- B** University of Southern California Information Sciences Institute
- C** Cogent Communications, Inc.
- D** University of Maryland
- E** United States National Aeronautics and Space Administration (NASA) Ames Research Center
- F** Information Systems Consortium (ISC)
- G** United States Department of Defense (US DoD)
Defense Information Systems Agency (DISA)
- H** United States Army (Aberdeen Proving Ground)
- I** Netnod Internet Exchange i Sverige
- J** Verisign
- K** Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- L** Internet Corporation For Assigned Names and Numbers (ICANN)
- M** WIDE Project (Widely Integrated Distributed Environment)

Instâncias Anycast (aprox. 1000 cópias)

The screenshot shows the website root-servers.org. The page features a navigation menu with links to various operators: ARL, DOD-NIC, ISC, NASA-ARC, UMD, Cogent, USC-ISI, Verisign, WIDE, ICANN, RIPE NCC, and Netnod. The main content area is divided into two columns: 'news' and 'meeting agendas'. The 'news' section lists three items: 'Root DNS events of 2016-06-25', 'The 2015 Root Server Operators' Exercise on Emergency Response', and 'Events of 2015-11-30'. The 'meeting agendas' section lists two items: 'IETF 95/Buenos Aires (PDF)' and 'IETF 94/JAPAN (PDF)'. Below these sections is a world map showing the locations of root name servers. The map is populated with colored circles and pins, each labeled with a number representing the number of servers at that location. The numbers range from 2 to 96. The map also includes a search bar and zoom controls. At the bottom of the map, it says 'Leaflet | Map data © OpenStreetMap contributors'. Below the map, there is a text box that reads: 'The 13 root name servers are operated by 12 independent organisations. You can find more information about each of these organisations by visiting their homepage as found in the 'Operator' field below.'

RFC 1546 1993

→ No Brasil: 14 instaladas pelo NIC.br

E se mesmo assim algo der errado?



Ameaça de DDoS

Capacidade de ataque > mecanismos de defesa



Alternativa

Diminuir dependência dos servidores recursivos aos servidores raiz.



Como?

Manter e usar uma cópia local da zona raiz

→ **Hyperlocal**

RFC 7706



1

Cópia da Zona Raiz junto ao recursivo.

2

Consultas mais rápidas e discretas.

3

DNSSEC cada vez mais importante.

4

Como baixar a zona raiz de forma segura.

5

'Framework' será apresentado 2019

6

Arquivos de zona não são confidenciais





RFC 7706

1. BIND 9.9
 - Recursivo e Autoritativo
2. Unbound 1.4 and NSD 4
 - Softwares diferentes
3. Microsoft Windows Server 2012
 - Recursivo e Autoritativo

<https://tools.ietf.org/html/draft-ietf-dnsop-root-loopback-05>

Teste do Hyperlocal na RLINE Telecom, Planalto-PR



Rosauero Baretta



Fabio Ortlieb

Maquina virtualizada VMware

4 x Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz

8G Memoria

Disco 16G SSD

Não ocupada nada de recursos, foi instalado em uma maquina com CentOS7,
Bind na versão 9.

Teste do Hyperlocal na RLINE Telecom, Planalto-PR

1 - recursivo da google (8.8.8.8) para dominio uol.com.br

```
[root@master ~]# dig @8.8.8.8 uol.com.br
; <<> DiG 9.9.4-RedHat-9.9.4-72.el7 <<> @8.8.8.8 uol.com.br
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22386
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; QUESTION SECTION:
; uol.com.br.                IN      A
;
;; ANSWER SECTION:
uol.com.br.                47     IN      A      200.147.35.149
;
;; Query time: 27 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Qui Jun 06 12:53:12 -03 2019
;; MSG SIZE rcvd: 55
```

1 - recursivo da google (8.8.8.8) para um dominio invalido

```
[root@master ~]# dig @8.8.8.8 domaininvalid.rrrrrrrrrrrrrrrrrrrrrrrrrrrrrr
; <<>> DiG 9.9.4-RedHat-9.9.4-72.e17 <<>> @8.8.8.8 domaininvalid.rrrrrrrrrrrrrrrrrrrrrrrrrrrrrr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 17346
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;domaininvalid.rrrrrrrrrrrrrrrrrrrrrrrrrrrrrr. IN      A
;; AUTHORITY SECTION:
.           86398     IN      SOA     a.root-servers.net. nstld.verisign-grs.com.
;; Query time: 70 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Qui Jun 06 12:53:34 -03 2019
;; MSG SIZE rcvd: 139
```

2 - recursivo local para o dominio uol.com.br

```
[root@master ~]# dig @ [REDACTED].4 uol.com.br
; <<> DiG 9.9.4-RedHat-9.9.4-72.el7 <<> @ [REDACTED].4 uol.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65160
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uol.com.br.                IN      A
;; ANSWER SECTION:
uol.com.br.                27     IN      A      200.147.3.157
;; Query time: 0 msec
;; SERVER: [REDACTED].4#53([REDACTED].4)
;; WHEN: Qui Jun 06 12:55:40 -03 2019
;; MSG SIZE rcvd: 55
```

2 - recursivo local para um dominio invalido

```
[root@master ~]# dig @[REDACTED].4 domaininvalid2.rrrrrrrrrrrrrrrrrrrrrrrrrrr
; <<> Dig 9.9.4-RedHat-9.9.4-72.e17 <<> @[REDACTED].4 domaininvalid2.rrrrrrrrrrrrrrrrrrrrrrrrrrr
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 20333
; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
; domaininvalid2.rrrrrrrrrrrrrrrrrrrrrrrrrr. IN A
; AUTHORITY SECTION:
; . 637 IN SOA a.root-servers.net. nstld.verisign-grs.com.
; Query time: 2 msec
; SERVER: [REDACTED].4#53([REDACTED].4)
; WHEN: Qui Jun 06 12:59:35 -03 2019
; MSG SIZE rcvd: 140
```



One World, One Internet

Visit us at icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann