Tópicos sobre DNS

Daniel Fink daniel.fink@icann.org

IX (PTT) Fórum Regional
Maio 2018

Agenda

O que é a ICANN?

- Missão
- Estrutura
- Modelo Multisetorial
- O grupo dos provedores na ICANN
- IANA / PTI
- Partes contratadas

Aspectos técnicos

- Whois
- Mecanismos de proteção de marcas
- Processo de resolução
- Servidores Raiz
- L-root
- DNSSEC

Anúncios importantes

- DNSSEC
- KSK Rollover
- Universal acceptance
- Referências

O que é a ICANN?

Corporação da Internet para Designação de Nomes e Números

Nomes & Números

ICANN.org

=

192.0.32.7

Missão da ICANN

Especificamente, a ICANN:

- ✓ Coordena a alocação e a atribuição de **nomes na zona raiz do Sistema de Nomes de Domínio** (DNS)
- ✓ Coordena o desenvolvimento e a implementação de **políticas relacionadas a registros de nomes de domínio de segundo nível em Domínios Genéricos de Primeiro Nível** (gTLDs)
- ✓ Promove a coordenação da operação e a **evolução do sistema de servidor de nomes da raiz do DNS**
- ✓ Coordena a alocação e a atribuição no nível mais alto de **números de Protocolo da Internet (IP) e números de Sistemas Autônomos**
- ✓ Colabora com outras entidades, conforme apropriado, para **fornecer os registros necessários para o funcionamento da Internet**, de acordo com as especificações das organizações de desenvolvimento de padrões de protocolo da Internet

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

Para mais informações,

visite:
www.icann.org

Compromissos e valores essenciais

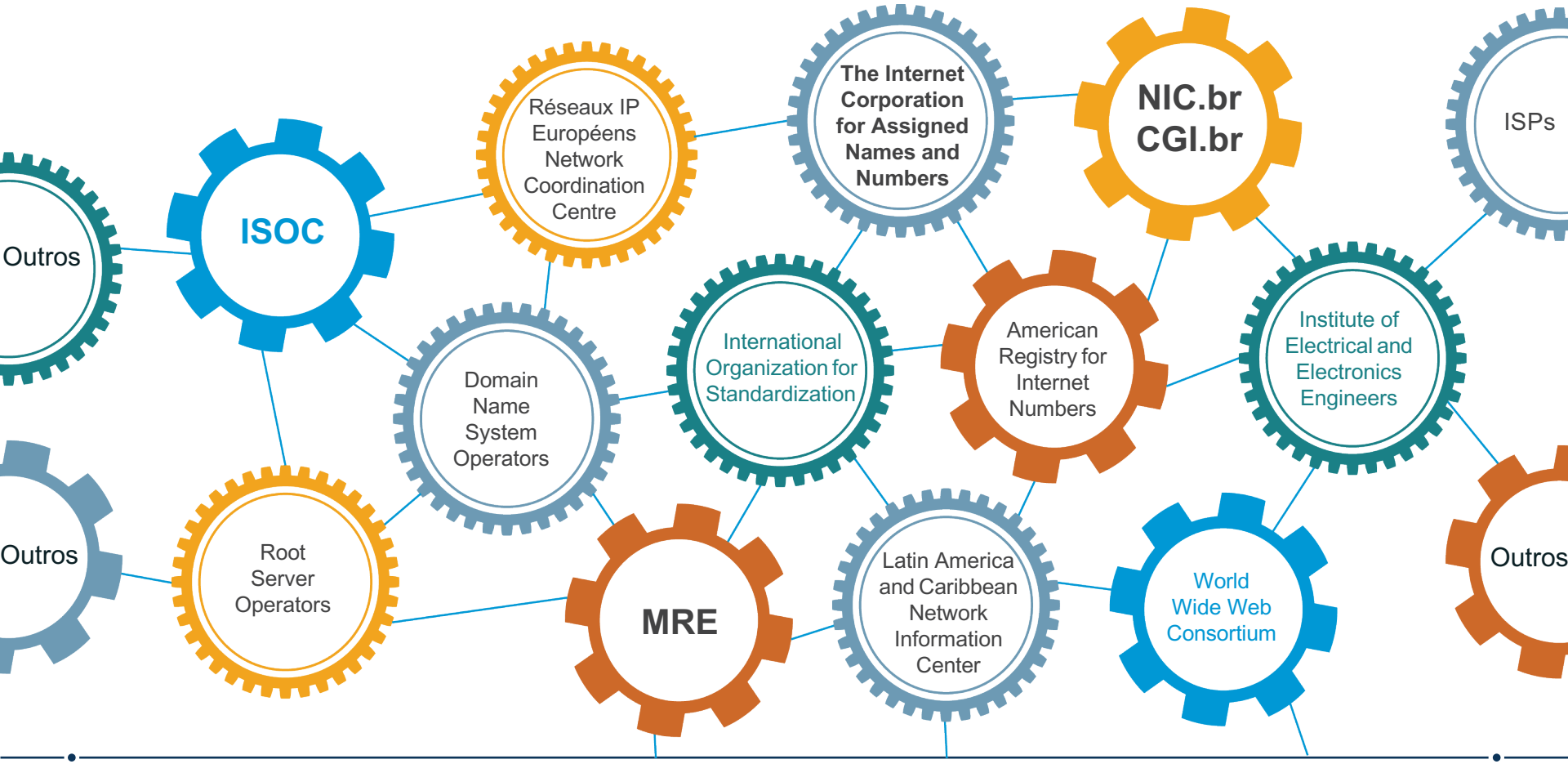
Ao desempenhar sua missão, a ICANN atuará de forma a cumprir e refletir seus compromissos e a respeitar seus valores essenciais

Esses compromissos e valores essenciais incluem:

- ⊙ Preservar e melhorar a **estabilidade**, a **segurança**, a **resiliência** e a **abertura** do DNS e da Internet
- ⊙ Utilizar processos de múltiplas partes interessadas **abertos**, **transparentes** e **ascendentes** para o desenvolvimento de políticas que sejam liderados pelo setor privado
- ⊙ Atuar com **eficiência** e **excelência**, demonstrando integridade tributária e responsabilidade

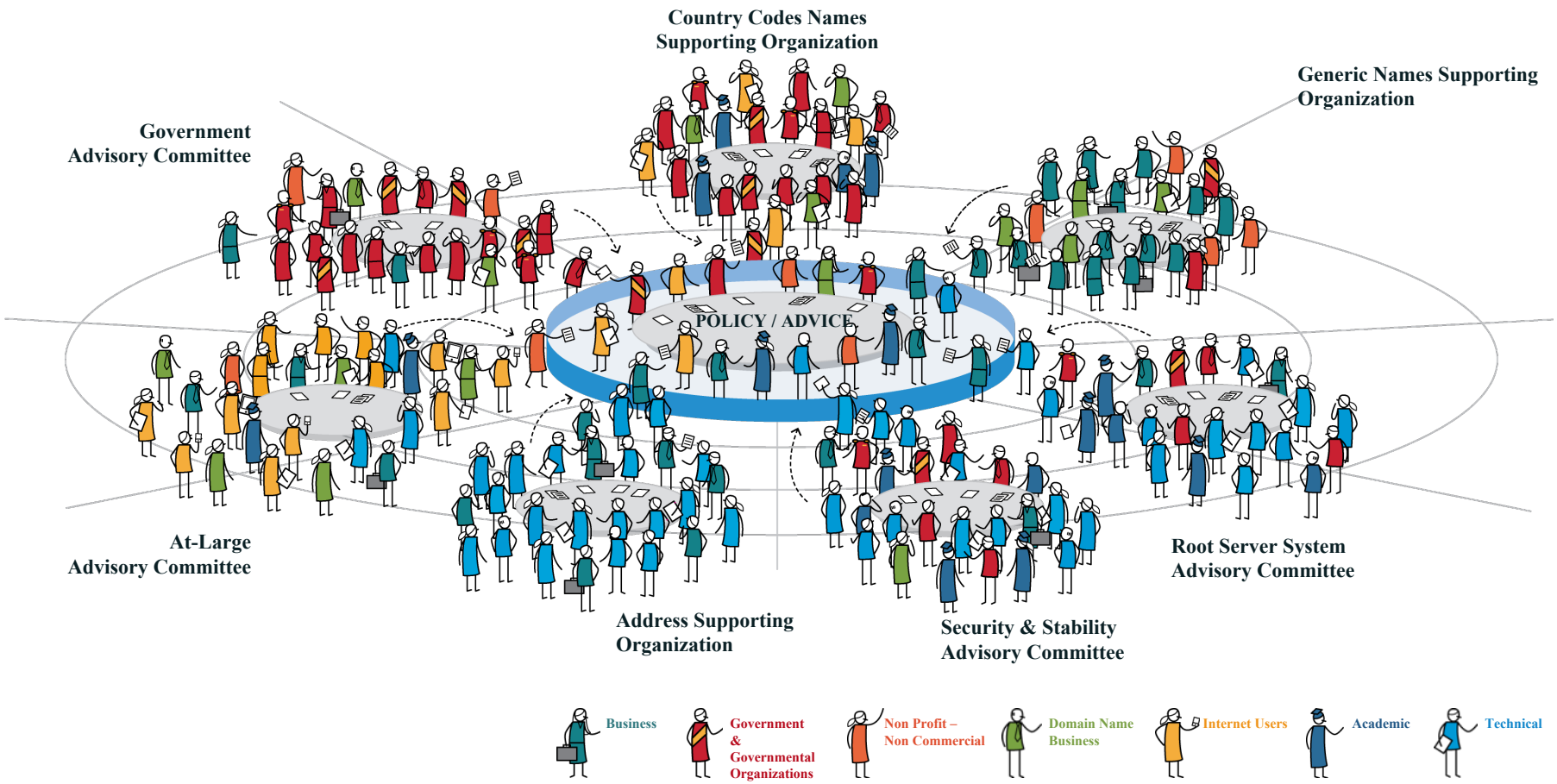
Nossos parceiros

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



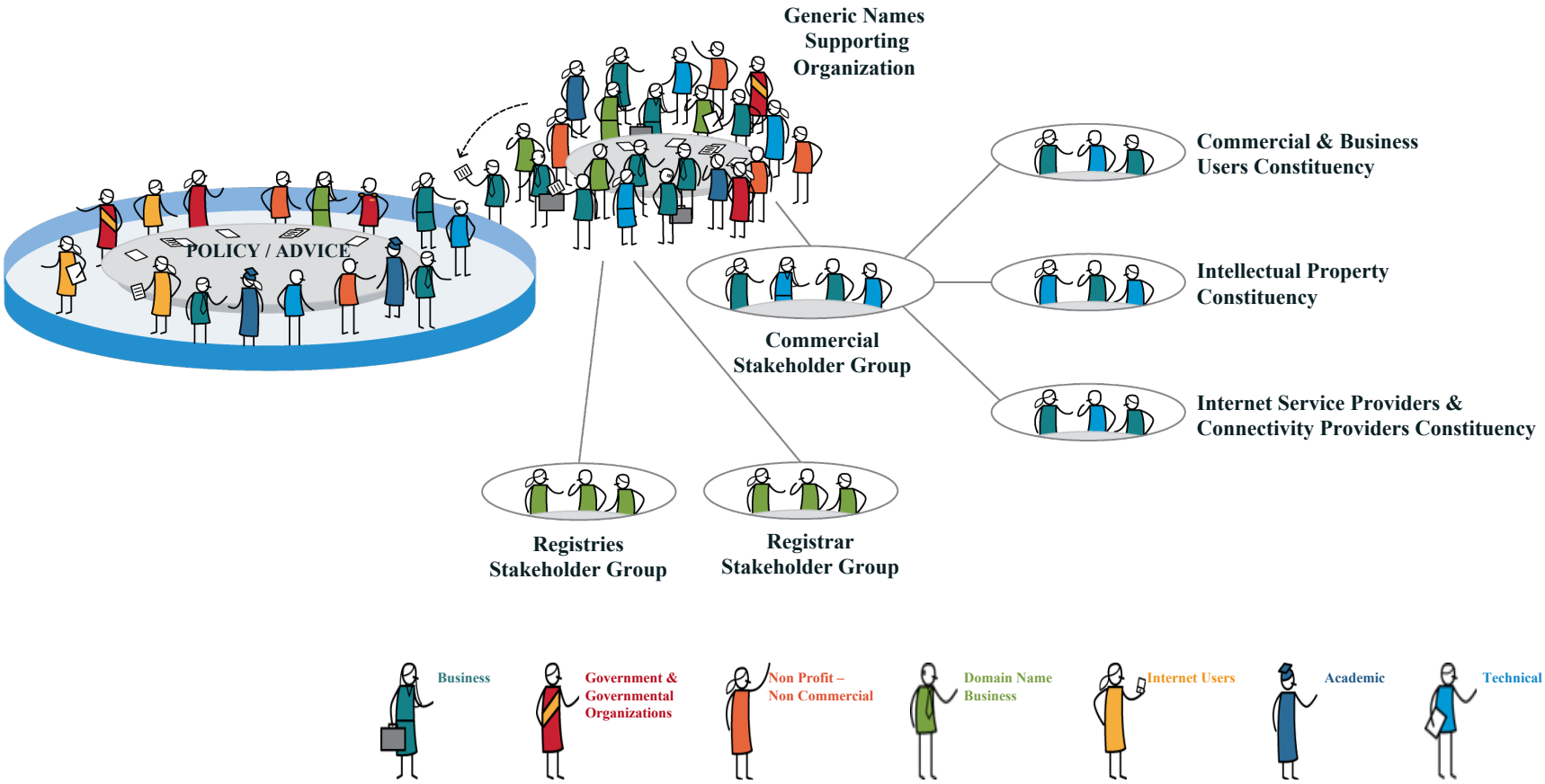
Estrutura da ICANN

Comunidade Multissetorial ICANN

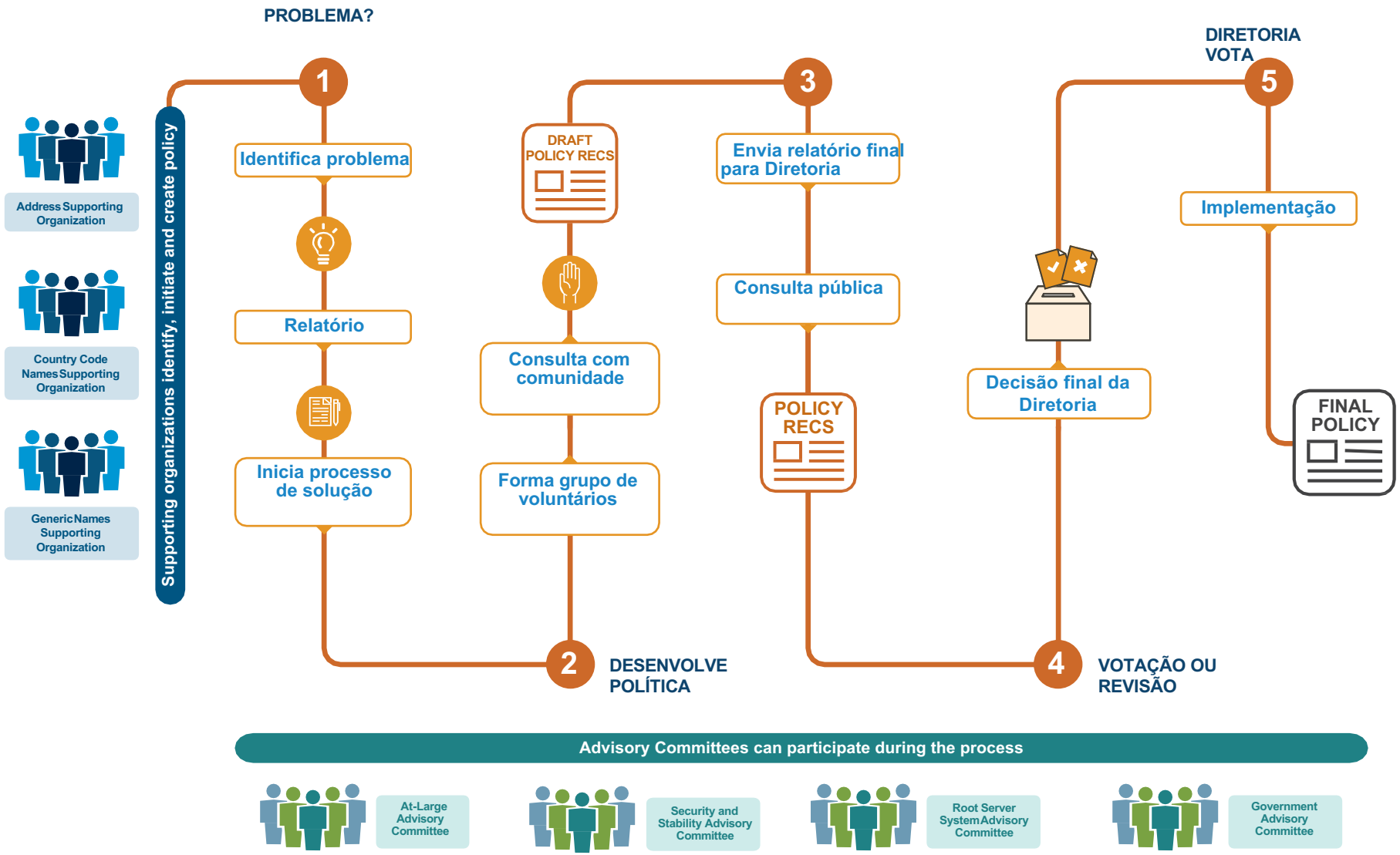


Comunidade Multistakeholder ICANN

Setor Privado



Como a comunidade desenvolve políticas?



O grupo dos provedores na ICANN

ICANN | ISPCP

Internet Service Providers & Connectivity Providers

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

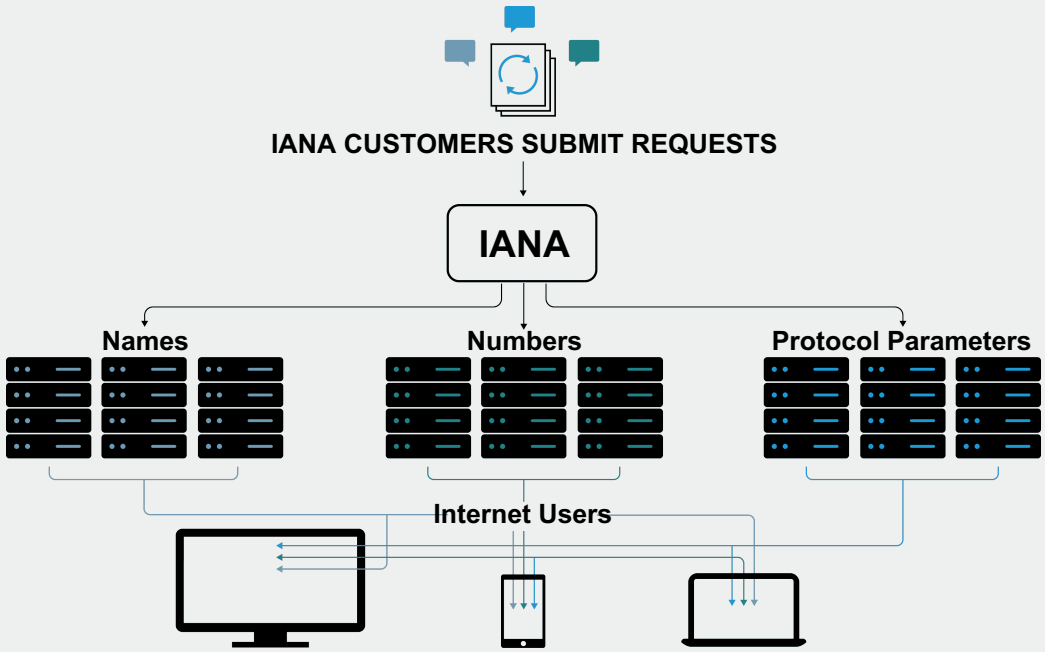
- Impacto do lançamento de novos nomes de domínio genéricos
- Universal Acceptance
- Impactos dos novos gTLD's

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

IANA - Autoridade para Atribuição de Números da Internet

Supervisiona a atribuição global dos números na Internet - entre os quais estão os números das portas, os endereços IP, sistemas autónomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.



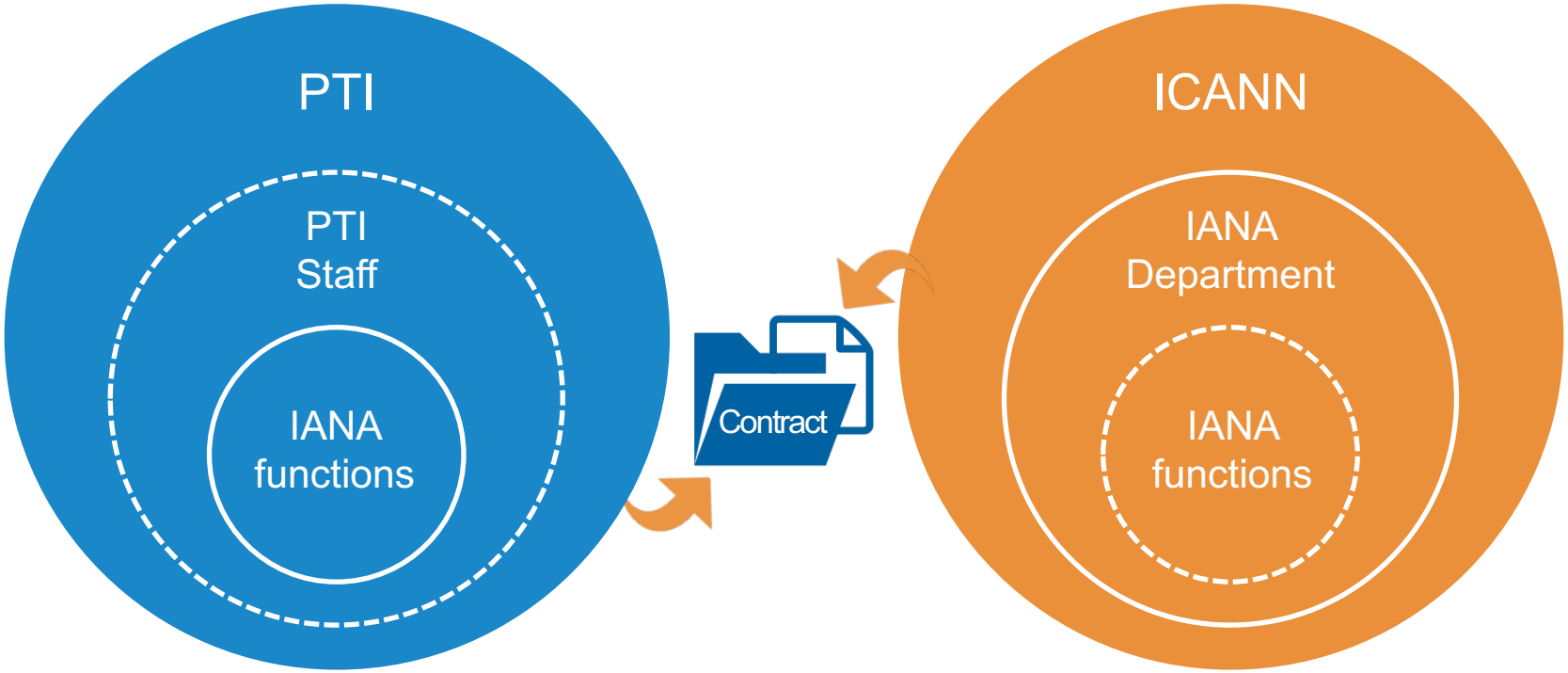
Essas funções incluem:

- A coordenação da atribuição de parâmetros técnicos de protocolo da Internet.
- A administração de certas responsabilidades associadas ao gerenciamento de zona raiz do DNS da Internet.
- A alocação de endereços IP da Internet.

A ICANN foi criada para executar as funções da IANA e fez isso de acordo com um contrato sem custo com o Departamento de Comércio por mais de 15 anos.

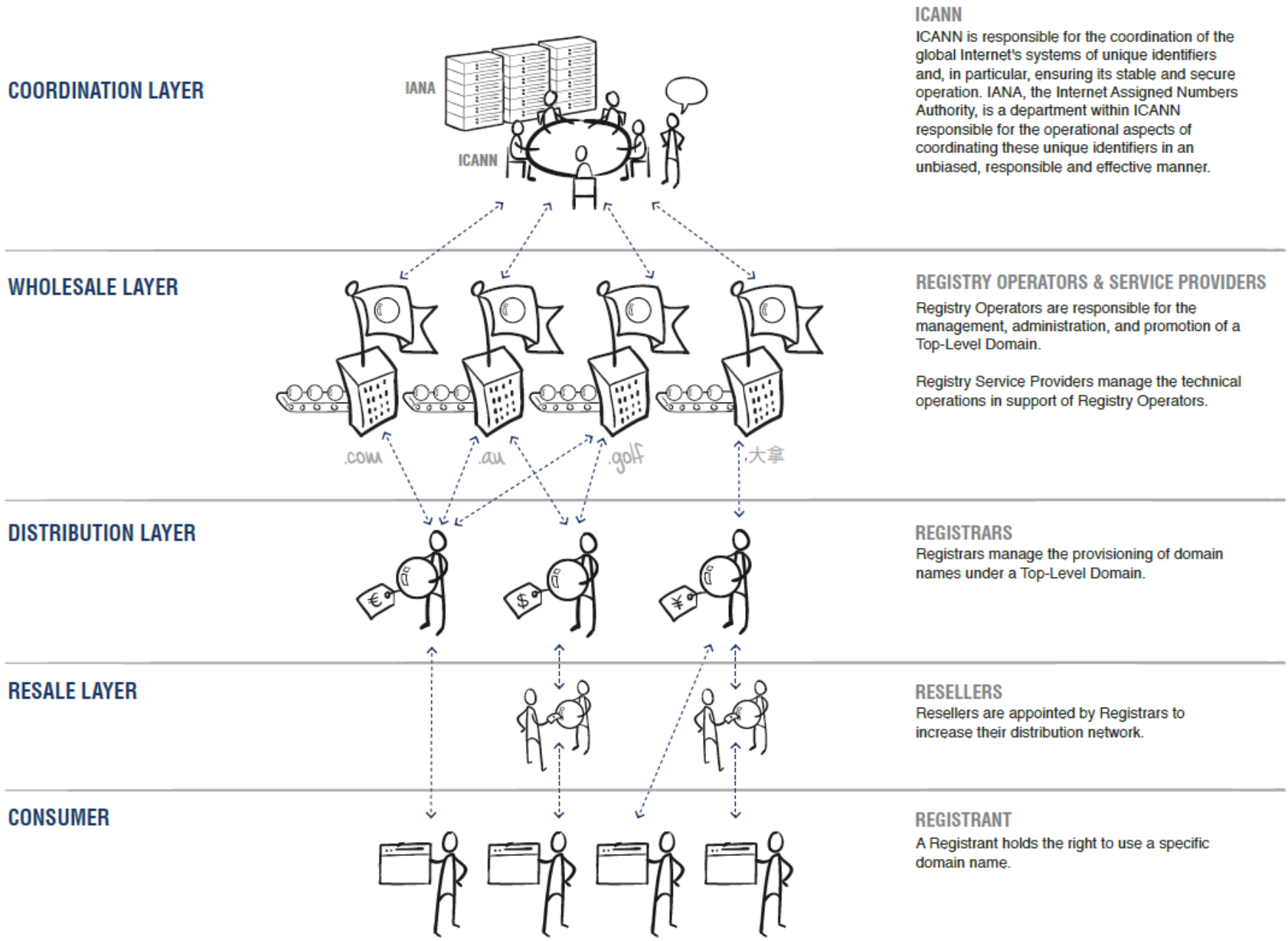
PTI – Public Technical Identifiers

Public Technical Identifiers (PTI) é uma afiliada da ICANN responsável por executar as funções da IANA e fornecer os serviços da IANA em nome da ICANN.



A PTI implementa políticas e princípios acordados desenvolvidos pela comunidade de múltiplas partes interessadas da ICANN.

Partes contratadas



ICANN
ICANN is responsible for the coordination of the global Internet's systems of unique identifiers and, in particular, ensuring its stable and secure operation. IANA, the Internet Assigned Numbers Authority, is a department within ICANN responsible for the operational aspects of coordinating these unique identifiers in an unbiased, responsible and effective manner.

REGISTRY OPERATORS & SERVICE PROVIDERS
Registry Operators are responsible for the management, administration, and promotion of a Top-Level Domain.

Registry Service Providers manage the technical operations in support of Registry Operators.

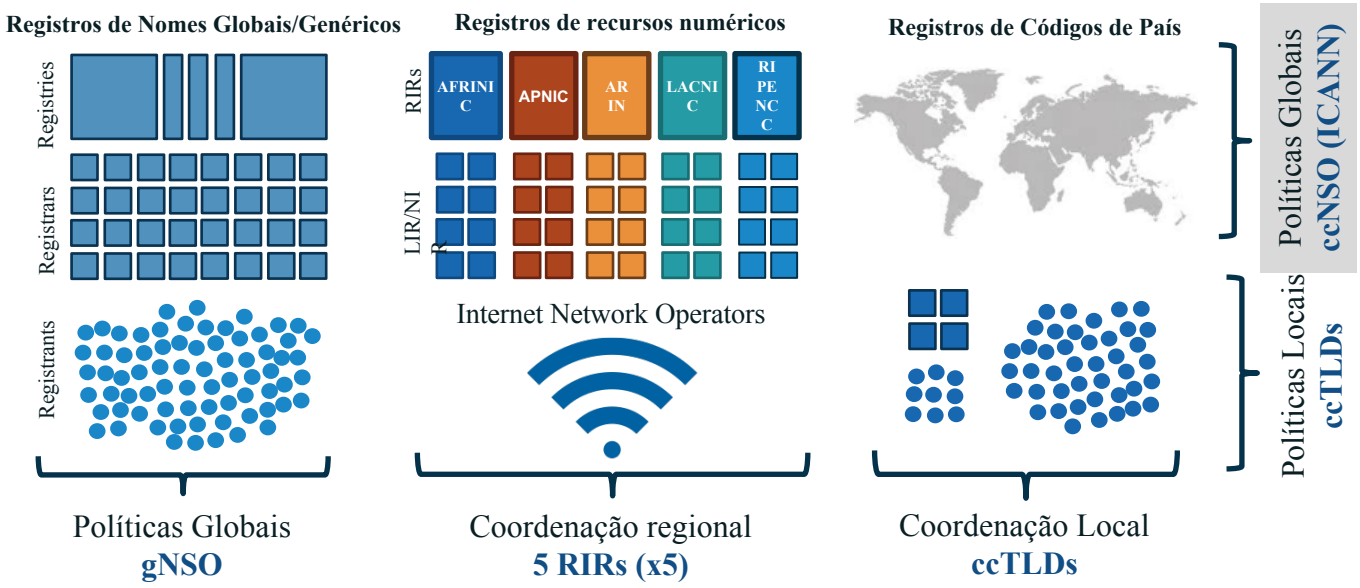
REGISTRARS
Registrars manage the provisioning of domain names under a Top-Level Domain.

RESELLERS
Resellers are appointed by Registrars to increase their distribution network.

REGISTRANT
A Registrant holds the right to use a specific domain name.

Resumindo

Framework de Desenvolvimento de Políticas de Identificadores



- Altamente recomendável acompanhar e participar:

ICANN

lacnic

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

Aspectos técnicos

O Sistema Whois

História do Whois

- Foi criado antes do DNS.
  - Especificado pelo IETF já em 1982.

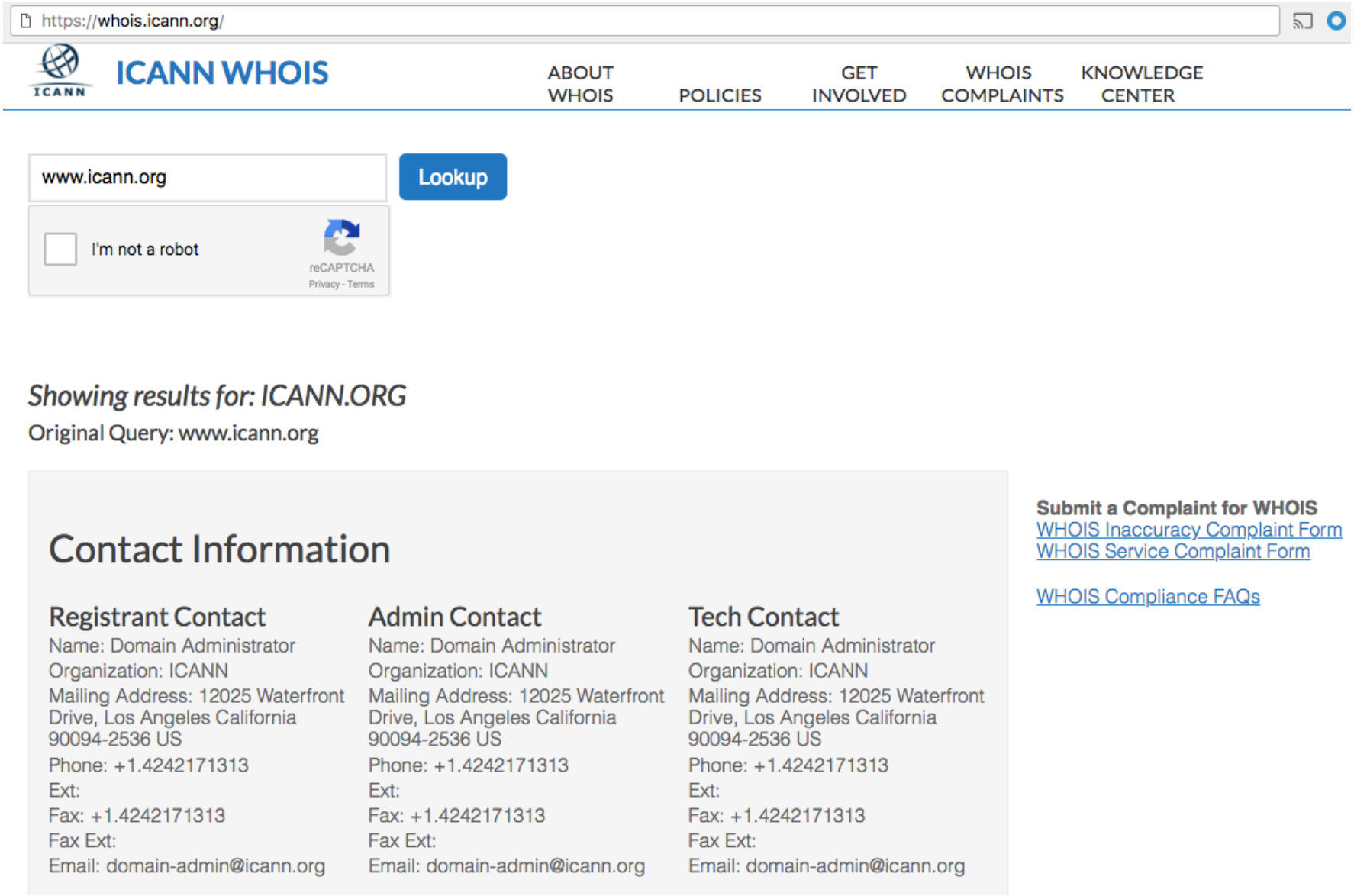
- Função de encontrar quem esta do outro lado do identificador.
  - Simplesmente responde a uma pergunta.

- Desenvolvido em uma época onde não havia preocupações sobre privacidade, propriedade intelectual, segurança, …

- Com o crescimento da Internet, o WHOIS começou a atender às necessidades de diferentes partes interessadas:
  - Registrantes de nomes de domínio, agentes de aplicação da lei, proprietários de propriedade intelectual e de marca comercial, empresas e usuários individuais.

- O protocolo permaneceu fundamentalmente baseado nos padrões originais da IETF.
  - Este é o protocolo WHOIS que a ICANN herdou quando foi estabelecida em 1998.

Consulta ao Whois (um exemplo)



Formato completo do registro Whois

Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER[1]
Domain Status: clientDeleteProhibited[2]
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Registry Registrant ID: 5372808-ERL[3]
Registrant Name: EXAMPLE REGISTRANT[4]
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP[5]
Registrant Postal Code: A1A1A1[6]
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234[7]
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Registry Admin ID: 5372809-ERL[8]
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: AA
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 1234
Admin Email: EMAIL@EXAMPLE.TLD
Registry Tech ID: 5372811-ERL[9]
Tech Name: EXAMPLE REGISTRANT TECHNICAL
Tech Organization: EXAMPLE REGISTRANT LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: AA
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLE-REGISTRAR.TLD[10]
Name Server: NS02.EXAMPLE-REGISTRAR.TLD
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

Exemplos de uso

Notificação de vítimas	**Quando um site ou servidor de email é atacado: entrar em contato com o responsável.**
Investigações criminais	**Auxiliar a justiça na identificação de criminosos e o escopo dos crimes.**
Infringimento de propriedade intelectual	**Indentificar responsáveis por sites ou emails que infringem termos de marcas. Ex: 'phishing'**
Disponibilidade de nomes	**Anunciar a disponibilidade de um nome para venda.**

Mecanismos de proteção de marcas

Requisitos

(1) a maneira pela qual o nome de domínio é idêntico ou confusamente similar a uma marca;
(2) porque o Respondente (detentor do nome de domínio) deve ser considerado como não tendo direitos
(3) porque o nome de domínio deve ser considerado como tendo sido registrado e usado de má-fé

Trademark Clearinghouse

01

Uniform Rapid Suspension System

02

Uniform Domain Name Dispute Resolution Policy

03

Estrutura do DNS

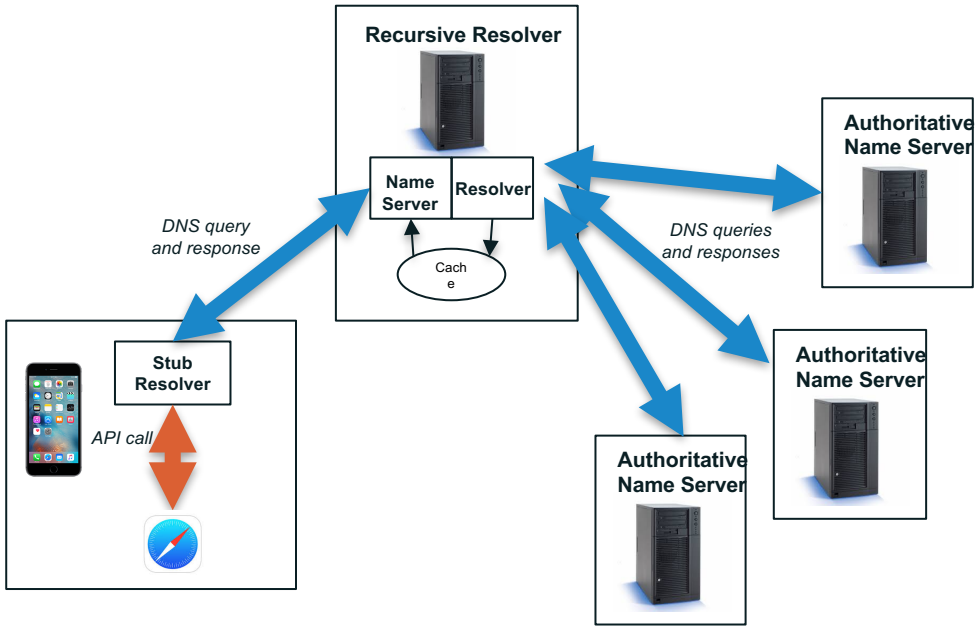
DNS em um slide

- DNS é uma base de dados distribuída
  - Dados são mantidos localmente, mas disponíveis globalmente

- **Resolvedores** enviam consultas
- **Servidores de Nomes** enviam respostas

- Otimizações:
  - Caching para melhorar desempenho
  - Replicação para prover redundância e distribuição de carga

Componentes do DNS



Processo de resolução

O telefone é configurado para enviar consultas para o resolvedor recursivo com IP 4.2.2.2

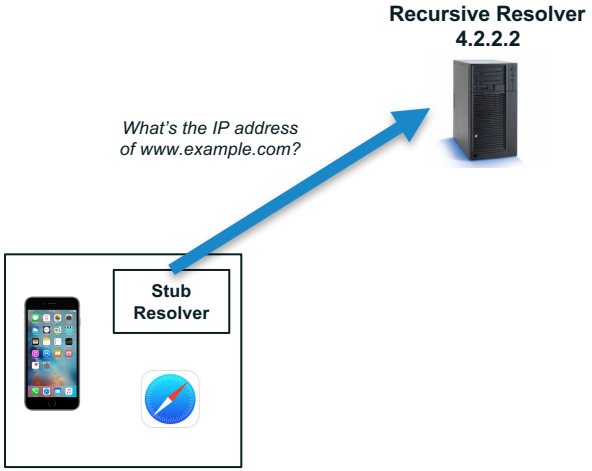
4.2.2.2 is a recursive resolver run by Level 3 Communications

Processo de resolução

O usuário digita www.example.com no Safari do seu telefone. Safari inicia função para resolver nome.

Processo de resolução

O telefone envia a consulta *www.example.com*, IN, A para o 4.2.2.2

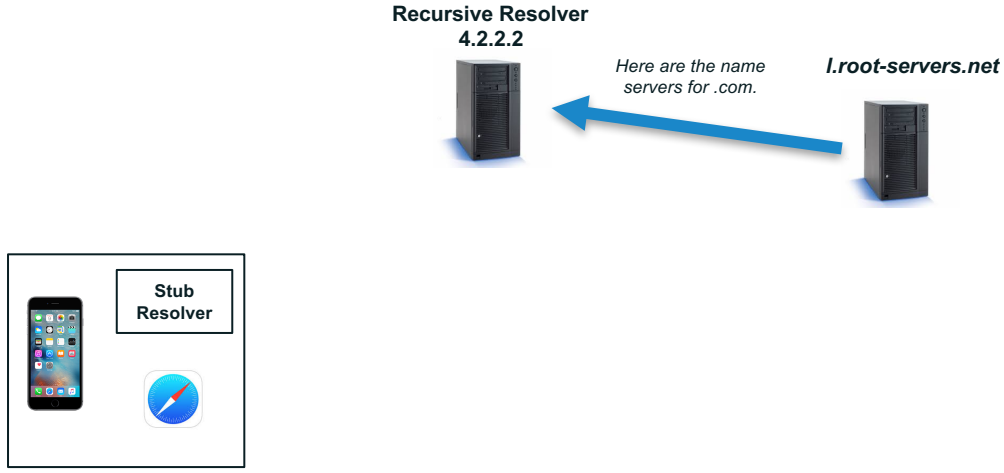


Processo de resolução

Como o cache esta vazio, o servidor recursivo pergunta para o servidor raiz

Processo de resolução

O servidor raiz responde apontando os servidores do .com



Processo de resolução

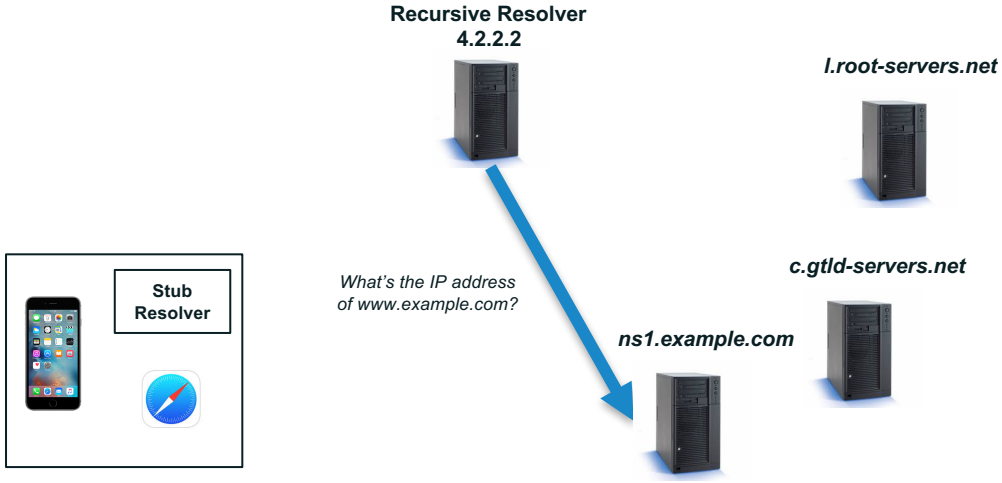
Servidor recursivo pergunta para o servidor .com

Processo de resolução

O servidor .com responde apontando o servidor de nomes para o example.com

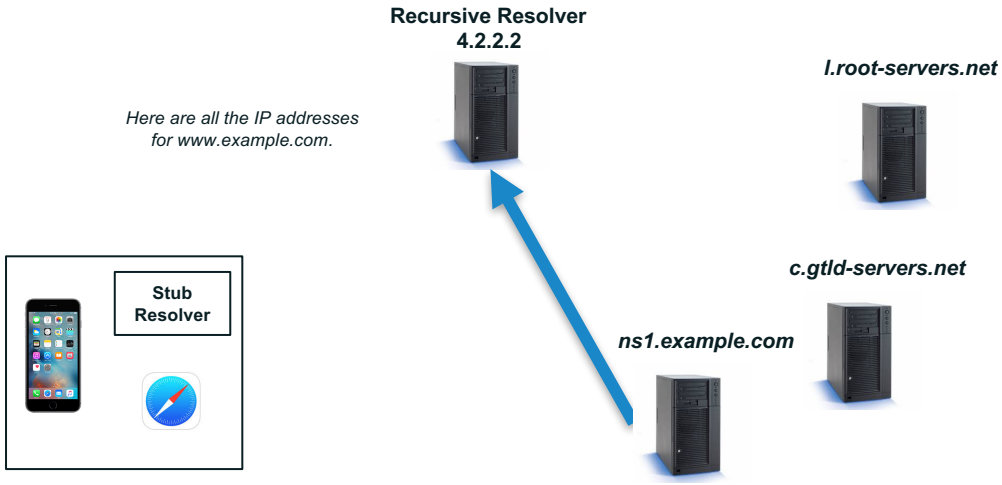
Processo de resolução

Servidor recursivo pergunta para o servidor do example.com



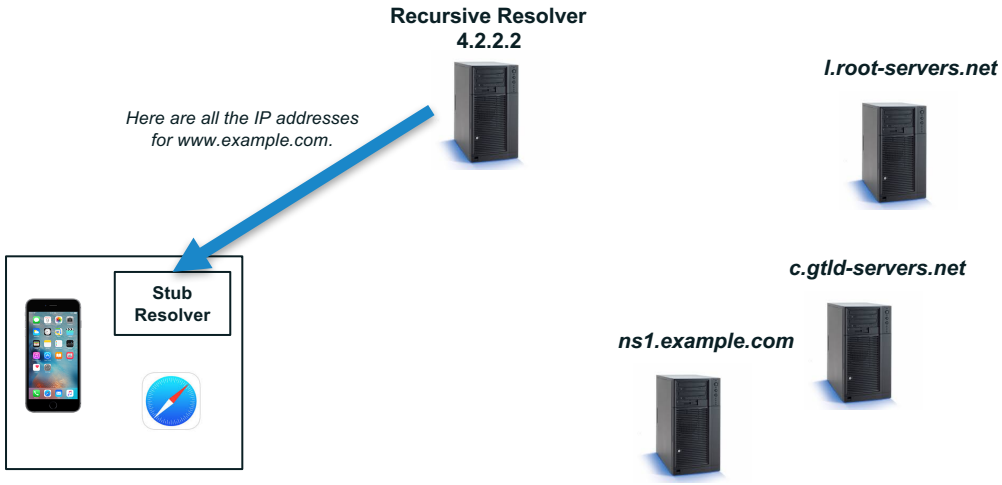
Processo de resolução

Servidor example.com responde a pergunta ao servidor recursivo



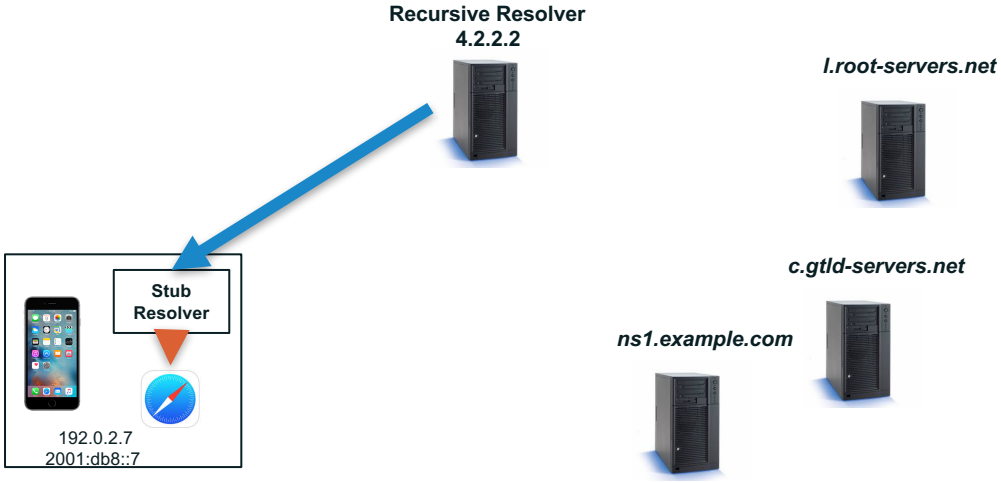
Processo de resolução

Servidor recursivo envia a resposta para o telefone



Processo de resolução

Sabendo o número IP, o Safari pode fazer a conexão com o website www.example.com.



Caching

- Caching acelera o processo de resolução
- Depois da consulta prévia, o servidor recursivo 4.2.2.2 sabe:
  - Nomes e endereços IP dos servidores *.com*
  - Nomes e endereços IP dos servidores *example.com*
  - Endereços IP do servidor *www.example.com*

Abrir o terminal !!

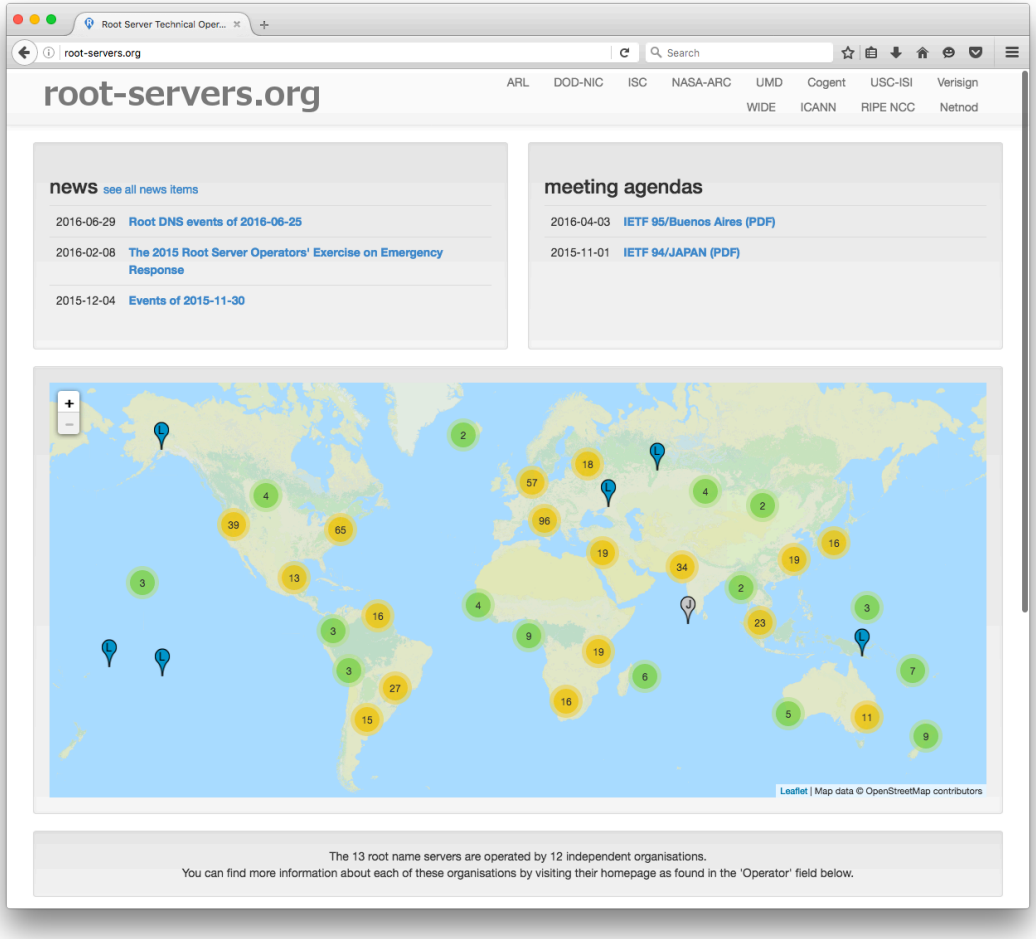
```
$ dig www.example.com

$ dig +trace www.example.com

$ dig + trace www.vogeltelecom.com



$ dig @8.8.8.8 www.example.com
```

Servidores Raiz

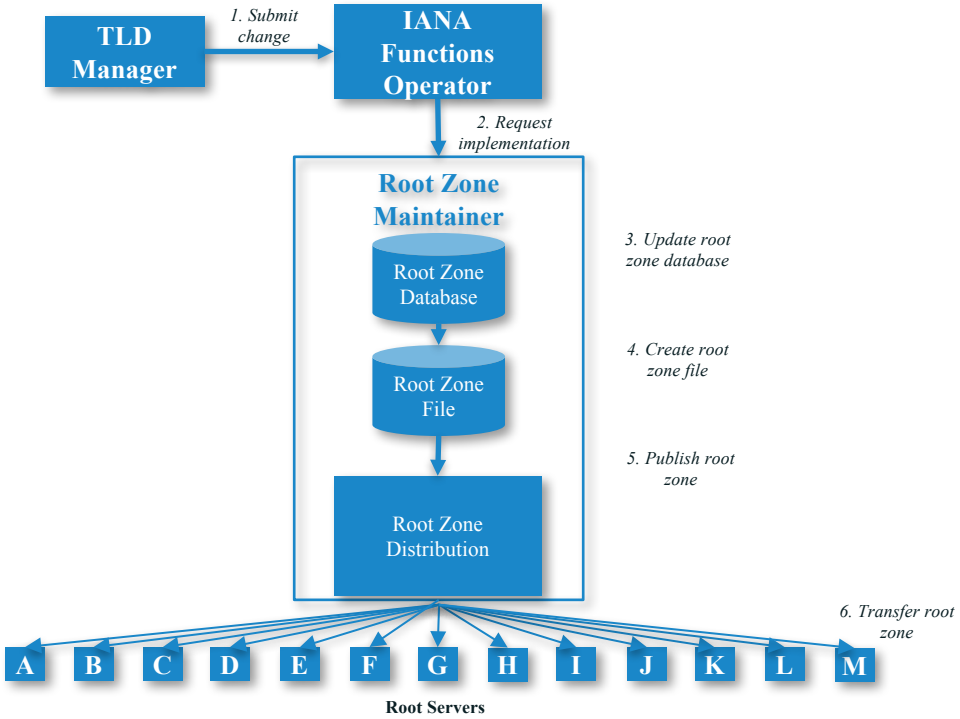
The Root Servers and Operators

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)

The root-servers.org Web Site



Processo de mudanças na Zona Raiz



Vamos baixar uma Zona Raiz?

```
$ dig @b.root-servers.net. AXFR . > ixforum.text
```

Depois vejam
https://www.iana.org/domains/root/db

L-root

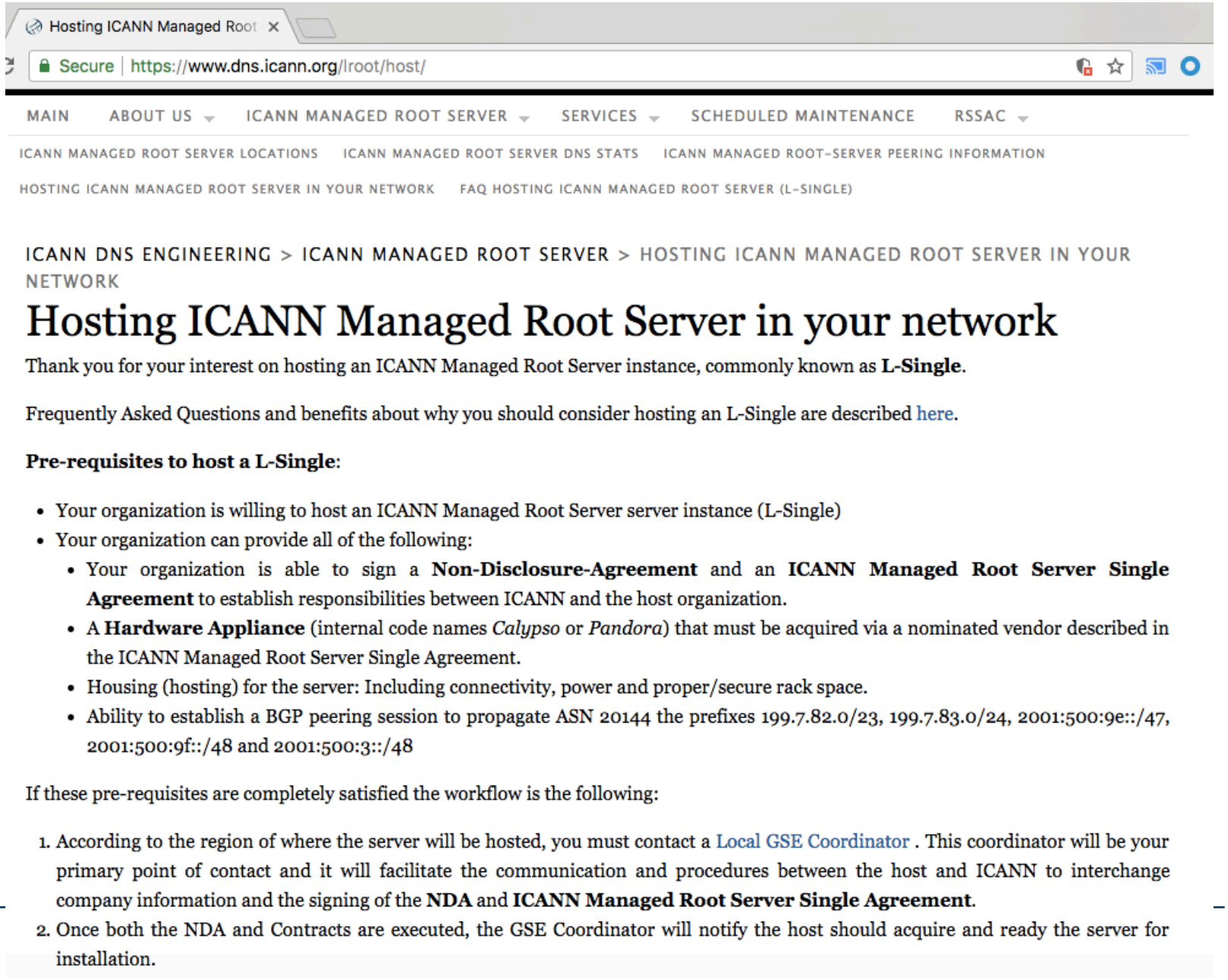
Qual o servidor raiz mais próximo?

```
$ dig @l.root-servers.net id.server ch txt
```

```
DAFI-5572:~ daniel.fink$ dig @l.root-servers.net id.server ch txt

; <<>> DiG 9.8.3-P1 <<>> @l.root-servers.net id.server ch txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28845
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;id.server.                     CH      TXT

;; ANSWER SECTION:
id.server.              0       CH      TXT     "gru01.l.root-servers.org"

;; Query time: 22 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Mon Mar 26 11:45:47 2018
;; MSG SIZE  rcvd: 64
```

```
DAFI-5572:~ daniel.fink$ dig @l.root-servers.net id.server ch txt

; <<>> DiG 9.8.3-P1 <<>> @l.root-servers.net id.server ch txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60716
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;id.server.                     CH      TXT

;; ANSWER SECTION:
id.server.              0       CH      TXT     "iad54.l.root-servers.org"

;; Query time: 140 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Mon Mar 26 11:48:56 2018
;; MSG SIZE  rcvd: 64
```

Quer hospedar um L-root?



Hosting ICANN Managed Root

Secure | https://www.dns.icann.org/lroot/host/

MAIN ABOUT US ICANN MANAGED ROOT SERVER SERVICES SCHEDULED MAINTENANCE RSSAC

ICANN MANAGED ROOT SERVER LOCATIONS ICANN MANAGED ROOT SERVER DNS STATS ICANN MANAGED ROOT-SERVER PEERING INFORMATION

HOSTING ICANN MANAGED ROOT SERVER IN YOUR NETWORK FAQ HOSTING ICANN MANAGED ROOT SERVER (L-SINGLE)

ICANN DNS ENGINEERING > ICANN MANAGED ROOT SERVER > HOSTING ICANN MANAGED ROOT SERVER IN YOUR NETWORK

Hosting ICANN Managed Root Server in your network

Thank you for your interest on hosting an ICANN Managed Root Server instance, commonly known as **L-Single**.

Frequently Asked Questions and benefits about why you should consider hosting an L-Single are described here.

Pre-requisites to host a L-Single:

- Your organization is willing to host an ICANN Managed Root Server server instance (L-Single)
- Your organization can provide all of the following:
  - Your organization is able to sign a **Non-Disclosure-Agreement** and an **ICANN Managed Root Server Single Agreement** to establish responsibilities between ICANN and the host organization.
  - A **Hardware Appliance** (internal code names *Calypso* or *Pandora*) that must be acquired via a nominated vendor described in the ICANN Managed Root Server Single Agreement.
  - Housing (hosting) for the server: Including connectivity, power and proper/secure rack space.
  - Ability to establish a BGP peering session to propagate ASN 20144 the prefixes 199.7.82.0/23, 199.7.83.0/24, 2001:500:9e::/47, 2001:500:9f::/48 and 2001:500:3::/48

If these pre-requisites are completely satisfied the workflow is the following:

1. According to the region of where the server will be hosted, you must contact a Local GSE Coordinator . This coordinator will be your primary point of contact and it will facilitate the communication and procedures between the host and ICANN to interchange company information and the signing of the **NDA** and **ICANN Managed Root Server Single Agreement**.
2. Once both the NDA and Contracts are executed, the GSE Coordinator will notify the host should acquire and ready the server for installation.

Caso da USE Telecom

```
tascom@TSC-SDR01-SMO03:~$ dig @l.root-servers.net id.server ch txt

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> @l.root-servers.net id.server ch txt
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49600
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;id.server.                     CH      TXT

;; ANSWER SECTION:
id.server.              0       CH      TXT     "iad57.l.root-servers.org"

;; Query time: 163 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Thu May 03 17:09:52 BRT 2018
;; MSG SIZE  rcvd: 75
```

Caso da USE Telecom

```
root@TSC-SDR01-SMO01:~# dig @l.root-servers.net id.server ch txt
; <<>> DiG 9.9.5-9+deb8u14-Debian <<>> @l.root-servers.net id.server ch txt
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60682
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;id.server.                     CH      TXT
;; ANSWER SECTION:
id.server.              0       CH      TXT     "ssa02.l.root-servers.org"

;; Query time: 1 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Thu May 10 15:34:33 -03 2018
;; MSG SIZE  rcvd: 75
```

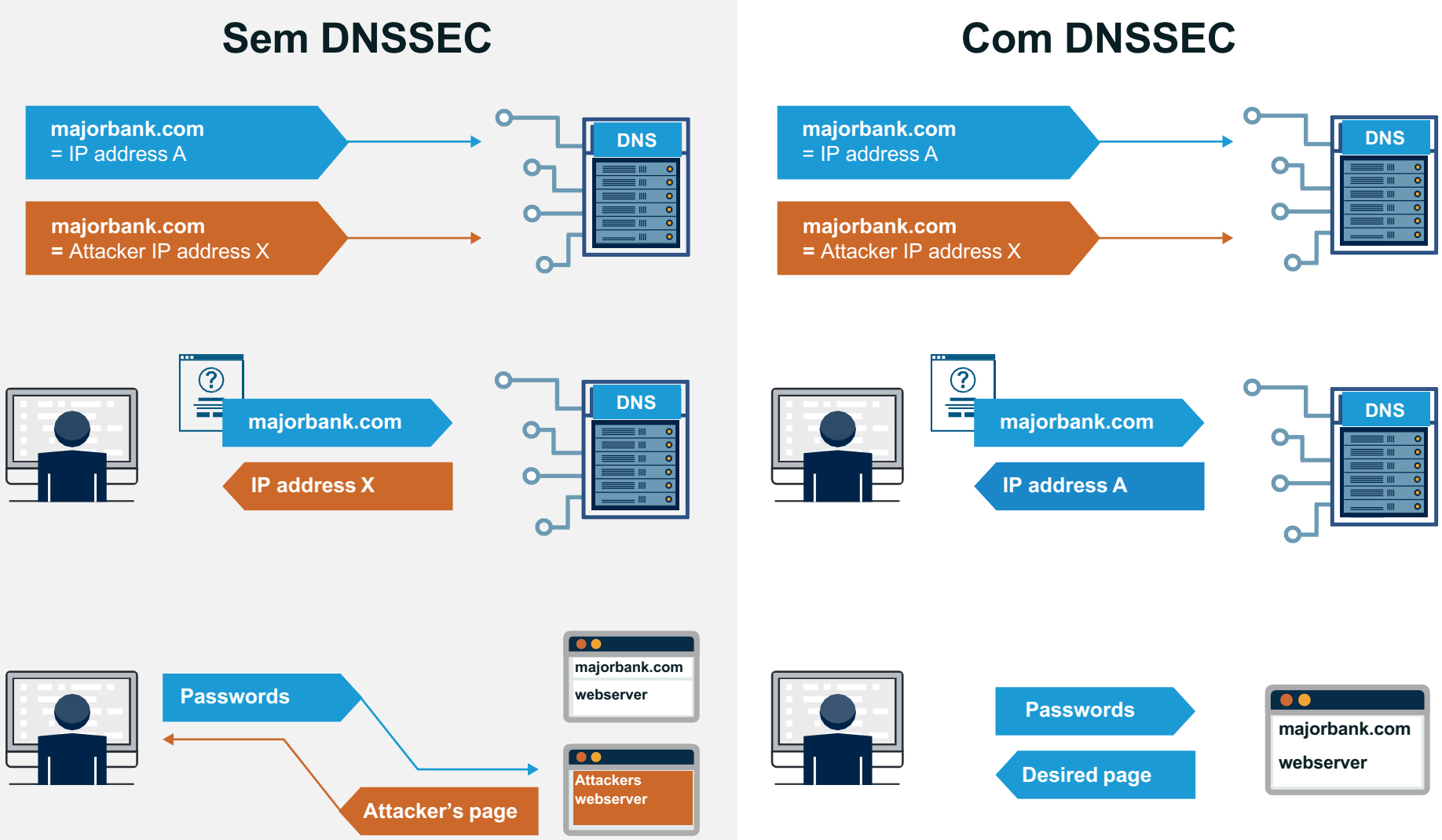
DNSSEC

Implementação da nova Chave de Assinatura de Chaves (KSK)

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

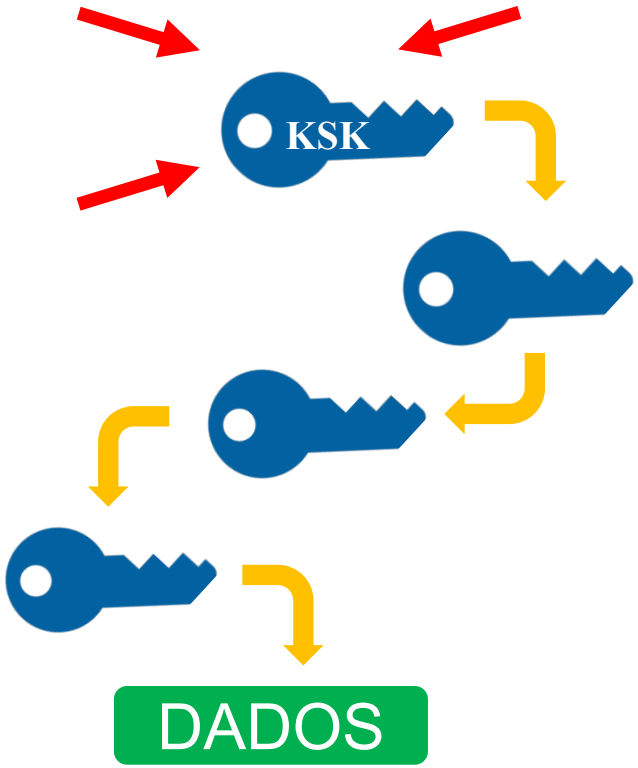
Como DNSSEC funciona?



Implementação da KSK: Uma Visão Geral

A ICANN está prestes a realizar a implementação da Chave de Assinatura de Chaves (KSK) das Extensões de Segurança do DNS (DNSSEC) da zona raiz

- A "**KSK**" (Chave de Assinatura de Chave) de DNSSEC da zona raiz é a principal chave criptográfica na hierarquia do DNSSEC
- A KSK é um par de chaves criptográficas públicas e privadas:
  - Parte pública: ponto inicial confiável para a validação de DNSSEC
  - Parte privada: assina a Chave de Assinatura de Zona (ZSK)
- Constrói uma "cadeia de confiança" de chaves e assinaturas sucessivas para validar a autenticidade de quaisquer dados assinados no DNSSEC



Por que a ICANN está fazendo a implementação da KSK?

- Porque não é bom que uma chave criptográfica continue sempre a mesma. As chaves criptográficas usadas nos dados DNS de assinatura de DNSSEC devem ser alteradas periodicamente
  - Garante que a infraestrutura tenha suporte para a alteração de chaves no caso de emergência
- Esse tipo de alteração nunca foi realizada antes no nível da raiz
  - Há uma única KSK de DNSSEC da zona raiz funcional e operacional desde 2010
- Porque é melhor fazer mudanças proativas durante a operação normal, quando as coisas estão funcionando bem, em vez de responder a emergências. A implementação da KSK precisa de uma coordenação ampla e cuidadosa para garantir que ela não interfira nas operações normais

Quando será feita a implementação?

- A mudança ou "rolagem" da chave KSK estava programada para ocorrer em 11 de outubro de 2017, mas foi adiada porque alguns dados obtidos em setembro de 2017 mostraram que um número significativo de resolvedores usados por provedores de serviços de Internet (ISPs) e operadores de rede ainda não está pronto para a mudança de chave.

- Pode haver vários motivos pelos quais os operadores não têm o novo KSK instalado em seus sistemas: alguns podem não ter seu software de resolução configurado adequadamente.

- Depois de uma consulta preliminar com a comunidade, a ICANN publicou um plano para iniciar o processo de rolagem novamente. Esse plano foi aberto para comentários da comunidade em https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en .

- O plano pede que a ICANN implante o KSK raiz em **11 de outubro de 2018**, incentivando os ISPs e os operadores de rede a usar esse período adicional para garantir que seus sistemas estejam prontos para a substituição de chaves.

Quem será afetado?

Desenvolvedores e distribuidores de software do DNS

Integradores de sistemas

Operadores de rede

Operadores do servidor raiz

Operadores do servidor raiz

Usuários finais
(se nenhuma ação for realizada pelos operadores resolvedores)

Por que você precisa se preparar

Se você ativou a validação de DNSSEC, é necessário atualizar seus sistemas com a nova KSK para garantir que os usuários tenham acesso à Internet sem problemas

- Atualmente, 25% dos usuários da Internet no mundo todo, ou **750 milhões de pessoas**, usam resolvedores de validação de DNSSEC que poderão ser afetados pela implementação da KSK
- Se esses resolvedores de validação não tiverem a nova chave quando a KSK for implementada, os usuários finais que dependem deles encontrarão erros e **não poderão acessar a Internet**

O que os operadores precisam fazer?

Verificar se o DNSSEC está ativado nos seus servidores

Verificar como a confiança é avaliada nas suas operações

Testar/verificar suas configurações

Inspecionar os arquivos de configuração para ver se eles (também) estão atualizados

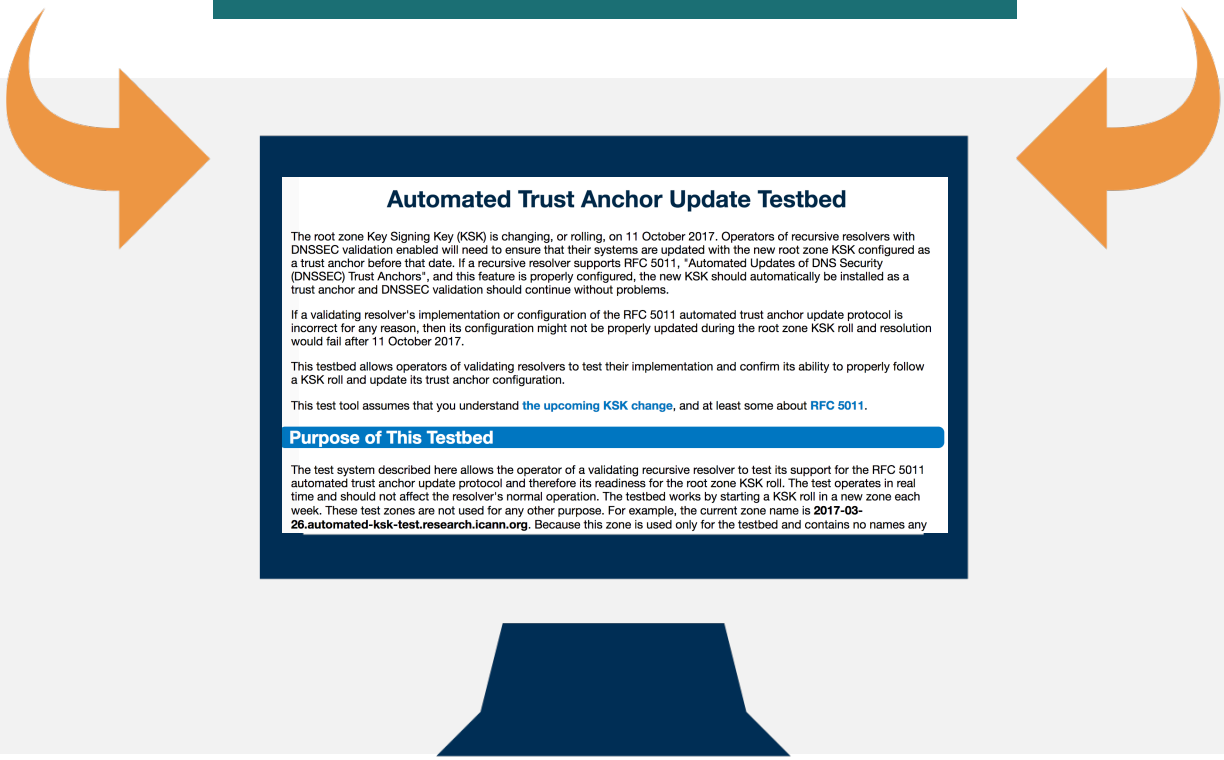
Se a validação de DNSSEC está ativada ou planejada no seu sistema

- Tenha um plano para participar na implementação da KSK
- Conheça as datas, os sintomas e as soluções

Verifique se os seus sistemas estão prontos

A ICANN está oferecendo um **ambiente de teste** para os operadores ou qualquer parte interessada confirmarem se os seus sistemas dão conta do processo automático de atualização corretamente.

Verifique se os seus sistemas estão prontos acessando:
go.icann.org/KSKtest



Como atualizar seu sistema

Se o seu software for compatível com atualizações automáticas das âncoras de confiança de DNSSEC (RFC 5011):

- A KSK será atualizada automaticamente no momento apropriado
- Você não precisará realizar nenhuma ação adicional
  - Os dispositivos off-line durante a implementação precisarão ser atualizados manualmente quando estiverem on-line após o término da implementação

Se o seu software não for compatível com atualizações automáticas das âncoras de confiança de DNSSEC (RFC 5011) ou não estiver configurado para usar esse recurso:

- O arquivo da âncora de confiança do software precisará ser atualizado manualmente
- A nova KSK de zona raiz está disponível aqui após março de 2017:

http://data.iana.org/root-anchors/

Reconhecimento da KSK-2017

- **A tag chave da KSK-2017 é**

  20326

- **O registro de recurso do Signatário de Delegação (DS) da KSK-2017 é**

```
IN  DS    20326 8 2
          E06D44B80B8F1D39A95C0B0D7C65D084
          58E880409BBC683457104237C7F8EC8D
```

Observação: a formatação foi alterada para esta apresentação

A KSK-2017 em um registro de recurso de DNSKEY

- **O registro de recurso de DNSKEY será:**

```
. IN DNSKEY  257 3 8
 AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
    +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
    ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
    0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
    oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
    RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
    R1AkUTV74bU=
```

"Raiz"

To distinguish between the old root root key-signing key and the new one, the old root zone key-signing key will appear as:

```
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0Ezr
AcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf
5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMj
JPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmR
LKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=
```

The new (current) root zone key-signing key will appear as:

```
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOL
AJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3Eg
VLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWe
L3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfhHdY6+cn8HFRm+2hM8AnXGXws9555Kr
UB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
```

Aceitação Universal

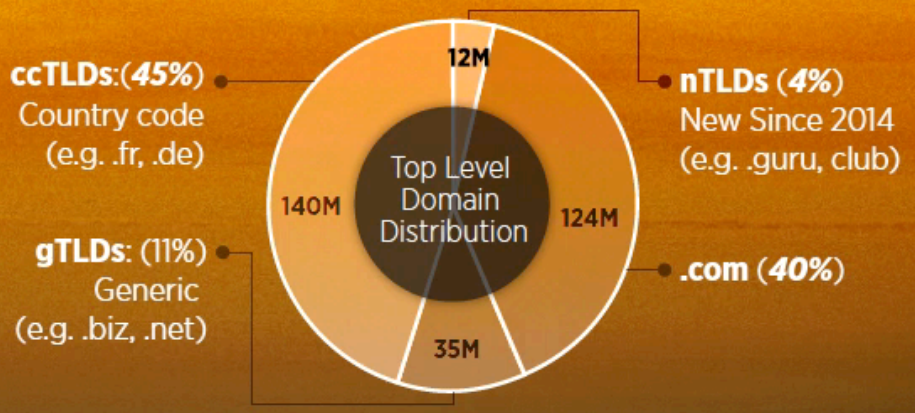
EUROPEAN DOMAIN CENTRE

READY FOR A NEW ERA?

THE LIST OF ALL 882 DOMAIN EXTENSIONS (2016)

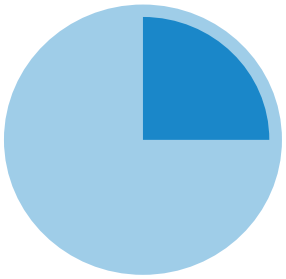
+300M DOMAIN NAMES

Source: CENTR, Jan. 2016



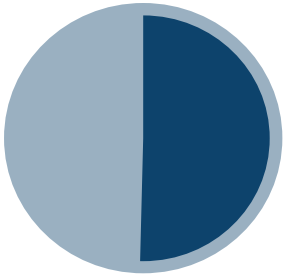
Exercício

Qual destes gráficos mostra a fração de de sites que usam inglês como idioma primário?



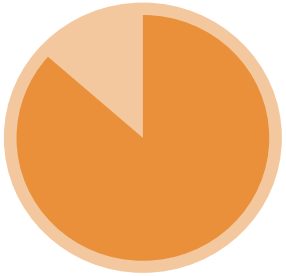
25%
Inglês

25% Inglês
75% Outros



50%
Inglês

50% Inglês
50% Outros



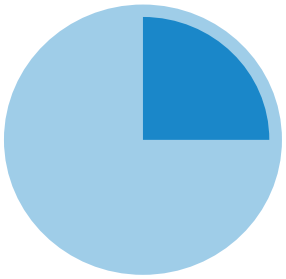
75%
Inglês

75% Inglês
25% Outros

https://w3techs.com/technologies/history_overview/content_language/ms/y

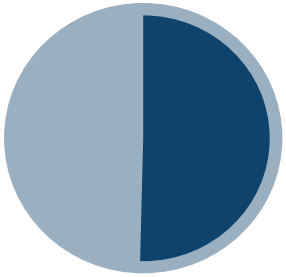
Exercício

Qual destes gráficos mostra a fração de de sites que usam inglês como idioma primário?



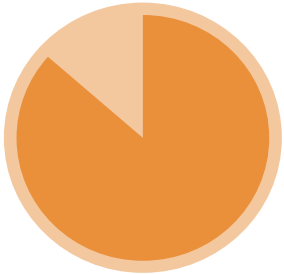
25%
Inglês

25% Inglês
75% Outros



50%
Inglês

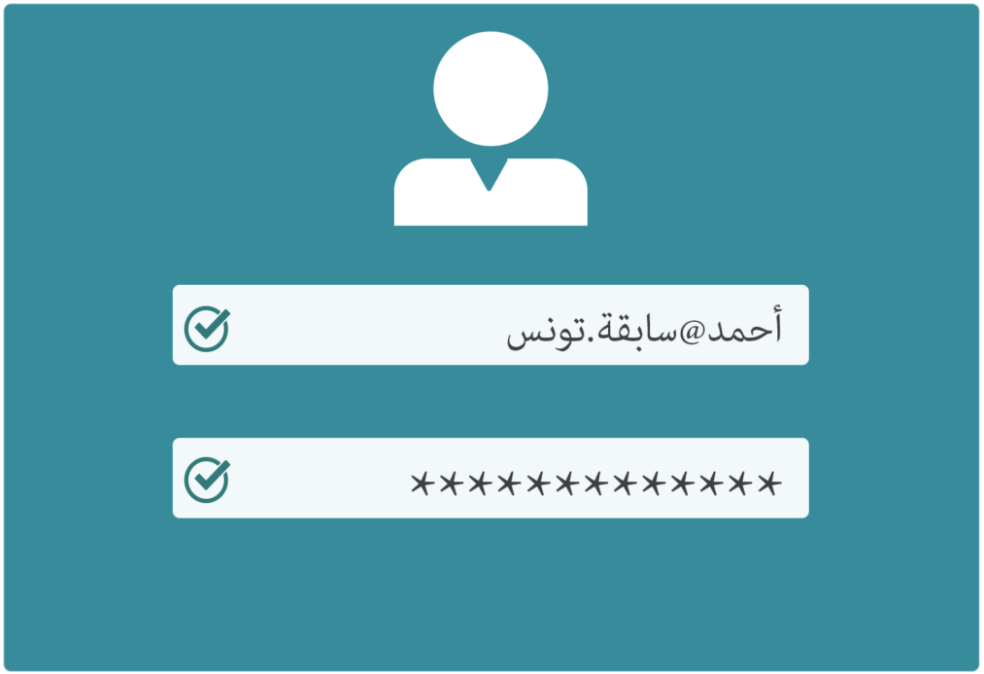
50% Inglês
50% Outros



75%
Inglês

75% Inglês
25% Outros

https://w3techs.com/technologies/history_overview/content_language/ms/y


أحمد@سابقة.تونس
****


impressos
.store
www.impressos.store
636
impressos
.store

O que significa “Aceitação Universal”?

UA (Universal Acceptance, Aceitação Universal) é o estado em que todos os nomes de domínio e endereços de e-mail válidos são aceitos, validados, armazenados, processados e exibidos de maneira correta.

ACEITAR

Aceitar é o processo pelo qual um endereço de e-mail ou um nome de domínio é recebido como uma cadeia de caracteres de uma interface de usuário, arquivo ou API (Application Program Interface, Interface entre Programa e Aplicativo) usado por um aplicativo de software ou serviço on-line.

Recomendações do UASG

- Qualquer elemento da interface do usuário que exigir que o usuário digite um nome de domínio ou endereço de e-mail precisa ser compatível com Unicode e cadeias de caracteres com até 256 caracteres.
- Os usuários devem ter permissão, mas não obrigação, de inserir texto compatível com codificação ASCII (também conhecido como "Punycode") no lugar do seu Unicode equivalente. No entanto, o Unicode deve ser exibido por padrão, sendo que o texto com Punycode é exibido para o usuário apenas quando for vantajoso para ele.

VALIDAR

O processo pelo qual um endereço de e-mail ou nome de domínio, recebido ou emitido, é verificado para garantir que a sintaxe está correta. Muitos programadores foram treinados para validar seguindo a heurística que exige verificar se um domínio de primeiro nível tem o número "correto" de letras ou se as letras são do mesmo conjunto de caracteres ASCII. Essas heurísticas são se aplicam mais devido à introdução de nomes de domínio com mais de três caracteres e caracteres Unicode (diferente de ASCII).

Recomendações do UASG

- As validações não devem ocorrer a menos que sejam exigidas para a operação do aplicativo ou do serviço. Essa é a maneira mais fácil de garantir que todos os nomes de domínio válidos sejam aceitos nos sistemas.
- Se a validação for obrigatória, considere o seguinte:
  - Verifique a porção TLD de um nome de domínio em comparação a uma tabela oficial:
    http://www.internic.net/domain/root.zone
    http://www.dns.icann.org/services/authoritative-dns/index.html
    http://data.iana.org/TLD/tlds-alpha-by-domain.txt
    Consulte também o SAC070: https://tinyurl.com/sac070.
  - Consulte o nome de domínio com relação ao DNS (Domain Name System, Sistema de Nomes de Domínio).
  - Exija que o endereço de e-mail seja informado mais de uma vez para descartar os erros de digitação.
  - Valide os caracteres nos rótulos para determinar se o rótulo U não contém pontos de código "NÃO PERMITIDO" ou pontos de código que não estão atribuídos na sua versão em Unicode. Visite: https://tools.ietf.org/html/rfc5892.
  - Limite a validação de rótulos para uma quantidade pequena de regras de rótulos inteiros definidas nas RFCs (Request for Comments, Solicitações de Comentários). Visite: https://tools.ietf.org/html/rfc5894.
  - Se uma cadeia de caracteres semelhante a um nome de domínio contiver o caractere de ponto final ideográfico '。', ele deve ser convertido para um '.' antes de realizar a validação.

ARMAZENAR

Armazenar refere-se ao armazenamento a longo prazo e/ou transiente de nomes de domínio e endereços de e-mail. Independentemente do tempo de vida dos dados, eles devem ser armazenados nos formatos definidos nas RFCs (preferencialmente) ou em outros formatos que podem ser transformados em formatos definidos na RFCs.

Recomendações do UASG

- Os aplicativos e serviços devem ser compatíveis com os padrões adequados de Unicode.
- As informações devem ser armazenadas em UTF-8 (Unicode Transformation Format, Formato de Transformação Unicode) sempre que possível. Alguns sistemas também podem exigir compatibilidade com o UTF-16, mas geralmente há uma preferência pelo UTF-8. UTF-7 e UTF-32 devem ser evitados.
- Consider all end-to-end scenarios before converting A-Labels to U-Labels and Considere todos os cenários completos antes de converter rótulos A em rótulos U, e vice-versa, ao armazenar. Pode ser interessante manter apenas rótulos U em um arquivo ou banco de dados, porque isso simplifica as pesquisas e classificações. No entanto, a conversão pode ter implicações na interoperabilidade com aplicativos e serviços mais antigos que não usam Unicode. Considere armazenas nos dois formatos.
- Marque claramente os endereços de e-mail e nomes de domínio durante o armazenamento para facilitar o acesso. Instâncias em que os endereços de e-mail e nomes de domínio foram arquivados no campo "author" (autor) de um documento ou "contact info" (informações de contato) em um arquivo de registro resultaram na perda da origem enquanto um endereço.

PROCESSAR

O processamento ocorre sempre que um endereço de e-mail ou nome de domínio é usado por um aplicativo ou serviço para executar uma atividade (por exemplo, para pesquisar ou classificar uma lista) ou é transformado em um formato alternativo (por exemplo, para armazenar ACSII como Unicode). É possível que seja realizada validação adicional durante o processamento.

Os nomes de domínio e endereços de e-mail podem ser processados de maneiras ilimitadas*, o que reforça a necessidade de haver convenções que garantam que os dados estão sendo compreendidos e classificados de modo consistente.

Recomendações do UASG

- Uma vez que o padrão Unicode é expandido continuamente, os pontos de código não definidos quando o aplicativo ou serviço foi criado devem ser verificados para garantir que eles não "interromperão" a experiência do usuário. Fontes ausentes no sistema operacional subjacente podem fazer com que alguns caracteres não sejam exibidos (muitas vezes o caractere "☒" é usado para representá-los), mas essa situação não deve resultar em uma falha fatal.
- Use APIs compatíveis com Unicode.
- Use os documentos mais recentes do protocolo [http://tools.ietf.org/html/rfc5891] e tabelas [http://tools.ietf.org/html/rfc5892] de IDNA (Internationalized Domain Names in Applications, Nomes de Domínio Internacionalizados em Aplicativos) para IDNs (Internationalized Domain Names, Nomes de Domínio Internacionalizados).
- Processe no formato UTF-8 sempre que possível.
- Certifique-se de que o produto ou recurso lide com os números da maneira esperada. Por exemplo, numerais ASCII e representações de números ideográficas asiáticas devem ser tratados como números. [RFC5892, link acima]
- Faça o upgrade de aplicativos e servidores/serviços juntos. Se o servidor for Unicode e o cliente não for Unicode, ou vice-versa, será necessário converter os dados para cada página de código sempre que os dados forem transferidos entre o servidor e o cliente.
- Faça análises da codificação para enviar ataques de buffer overflow. Ao fazer a transformação de caracteres, as cadeias de texto podem aumentar ou diminuir significativamente.

Ejemplos: Identificar personas en Nueva Zelanda al buscar dentro del ccTLD .nz; identificar farmacéuticos al buscar direcciones de correo electrónico usuario@.farmacéutico.

EXIBIR

A ação exibir ocorre sempre que um endereço de e-mail ou um nome de domínio é renderizado em uma interface de usuário. Exibir nomes de domínio e endereços de e-mail é geralmente algo bastante simples quando as escritas usadas são compatíveis com o SO subjacente e as cadeias de caracteres são armazenadas em Unicode. No entanto, algumas transformações específicas de aplicativos podem exigir algo a mais.

Recomendações do UASG

- Exiba todos os códigos de pontos Unicode compatíveis com o sistema operacional subjacente. Se um aplicativo tiver seus próprios conjuntos de fontes, é necessário oferecer um suporte abrangente a Unicode para a coleta de fontes disponíveis no sistema operacional.
- Ao desenvolver um aplicativo ou um serviço ou ao operar um registro, considere os idiomas compatíveis e certifique-se de que o SO e os aplicativos aceitem esses idiomas.
- Converta dados diferentes de Unicode para Unicode antes de exibir. Por exemplo, o usuário final deve ver "todos.みんな", em vez de "todos.xn--q9jyb4c". (Essa conversão é um exemplo de processamento compatível com a UA).
- Exibir Unicode por padrão. Usar texto com Punycode para o usuário apenas quando isso for vantajoso para ele. Aumente a exibição de Unicode com texto em Punycode exibido ao passar o mouse sobre ele como uma forma de mitigação.
- Considere que endereços com misturas de escritas serão mais comuns. Alguns caracteres Unicode podem parecer iguais ao olho humano, mas diferente para os computadores. Não presuma que as cadeias de caracteres com mistura de escritas são destinadas a fins maliciosos, como phishing, e se a interface do usuário chamar a atenção do usuário para as cadeias de caracteres, certifique-se de que isso seja feito de maneira que não prejudique os usuários de escritas não latinas. Saiba mais sobre considerações de segurança com Unicode em: http://unicode.org/reports/tr36/.
- Use o processamento de compatibilidade de IDNA para Unicode a fim atender às expectativas dos usuários. Para saber mais, acesse: http://unicode.org/reports/tr46/.
- Esteja atento a caracteres não atribuídos ou não permitidos. Saiba mais na RFC 5892: https://tools.ietf.org/rfc/rfc5892.txt.

Referências

- O papel da ICANN na gestão dos identificadores únicos da Internet | Material: Funções IANA [icann.org]; Guia de Participação [icann.org]

- Implementação da KSK no DNSSEC
  Material: https://www.icann.org/resources/pages/ksk-rollover-2016-07-27-pt [icann.org]

- Aceitação Universal | Material: Artigo em Português [itforum365.com.br]; Guia rápido [uasg.tech]; Introdução a Aceitação Universal [uasg.tech]

- Grupo dos Provedores na ICANN | Material: http://www.ispcp.info/

Muito obrigado !

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann