

Participe do programa KINDNS e contribua no combate a abusos de DNS



Daniel Fink
daniel.fink@icann.org

IX Fórum Rio de Janeiro
24 de outubro de 2025

O que é a ICANN?

Corporação
da Internet
para Designação
de Nomes

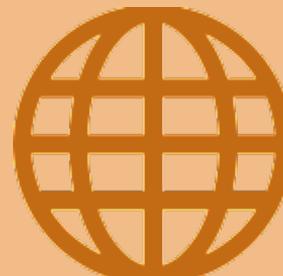
Missão da ICANN

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

Participe do KINDNS



Knowledge-sharing and Instantiating Norms for DNS (Domain Name System) and Naming Security

*Normas de Compartilhamento de
Conhecimento e Instanciamento
para DNS e Segurança de Nomes
de Domínio*

Para quem?



KINDNS

Operadores de Autoritativos



TLDs e Zonas Críticas

SLDs

Operadores de Recursivos



Fechados e privados

Privados compartilhados

Públicos

Fortalecimento da infraestrutura

Operadores de Recursivos Privados e Compartilhados



KINDNS

Os operadores de recursivos privados compartilhados geralmente são provedores de serviços de Internet (ISPs).

Recursivos Privados Compartilhados

1. A validação DNSSEC **DEVE** estar ativada
2. As instruções ACL **DEVEM** ser usadas para restringir quem pode enviar consultas recursivas
3. A minimização de QNAME **DEVE** estar ativada
4. Servidores de nomes autoritativos e recursivos **DEVEM** ser executados em infraestruturas separadas.
5. Pelo menos dois servidores distintos **DEVEM** ser usados para fornecer serviços de recursão.
6. A infraestrutura **DEVE** ser monitorada
7. Para consideração de privacidade: Criptografia (DOH ou DoT) **DEVE** ser ativada
8. Operadores de resolvedores privados **DEVEM** ter diversidade de software

Como participar do KINDNS ?

<https://kindns.org>

1. Autoavaliação



1. Os operadores de cada categoria podem realizar uma autoavaliação de suas práticas operacionais em relação ao KINDNS e usar o relatório para corrigir/ajustar suas práticas.
 - As autoavaliações serão anônimas e os relatórios serão baixados diretamente do site.

KINDNS

Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.

It's a program supported by ICANN to develop and promote a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.

JOIN US

SELF-ASSESSMENT

An ICANN Initiative

ICANN

2. Inscrição



Os operadores podem se inscrever para participar de uma ou várias categorias cobertas pelo KINDNS.

- A participação na iniciativa KINDNS significa comprometer-se voluntariamente a implementar/aderir às práticas acordadas.



Get in touch

Name *

Organization

Email *

Phone

How can we help?

I want to join KINDNS

Message

3. Envio das informações



De: KINDNS-INFO <kindns-info@icann.org>

Para: Provedor

Dear Provedor,

Thank you for your interest in KINDNS and apologies for the delay following up on your request. We will be delighted to welcome "Provedor" as participant and supporter of KINNDS.

In order to proceed we will need some additional technical informations on how you are implementing the relevant practices in your infrastructure. Please answer the following questions:

- Under which category of operator you would like to join?
[See: <https://kindns.org/operator-categories>]
- How are you implementing the DNS operation practices associated with your selected category/categories? [Please provide for each of the practices your implementation status and the technical details of how you are implementing them - or plan to do so]
- If you are applying for any of the authoritative server operator's categories, please provide the domain name(s) you are managing or running authoritative server(s) for.
- If you are applying for any of the resolver operator's categories, please provide the IP addresses (and/or names) of your resolver(s).
- Do you agree to be listed on the kindns.org website as participant once the process is successfully completed?

Kind regards.

4. Reconhecimentos



[About](#) [Operator Categories](#) [Support & Engage](#)

Organization Name	Practice-1	Practice-2	Practice-3	Practice-4
i8 Digital Brazil	✓	✓	✓	✓
RNP Brazil – EduDNS	✓	✓	✓	✓
Brazil TecPar	✓	✓	✓	✓
PowerNet Solutions	✓	✓	✓	✓
Intercol Brazil	✓	✓	✓	✓
Tempus Group, Paraguay	✓	✓	✓	✓
NETServ	✓	✓	✓	✓
REDESIM	✓	✓	✓	✓
MTN Ghana	✓	✓	✓	✓
LCI Telecom	✓	✓	✓	✓
RR64 Brazil	✓	✓	✓	✓
RUPI Telecom	✓	✓	✓	✓

Qual é o site?



KINDNS

An ICANN
Initiative



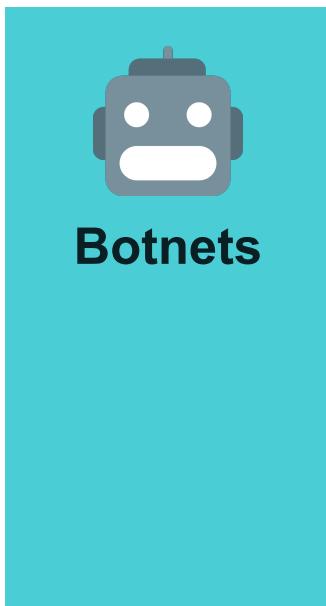
<https://kindns.org>

Abusos de DNS

Como ajudar neste combate

Definição básica de abuso do DNS para a ICANN

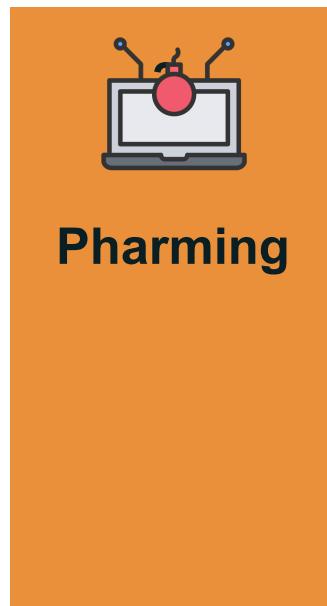
Para a ICANN, o uso indevido do DNS se refere às cinco categorias gerais seguintes de atividades nocivas:



Botnets



Malware



Pharming



Phishing



Spam

Quando usado como vetor para um ou mais dos outros quatro tipos de abusos do DNS.

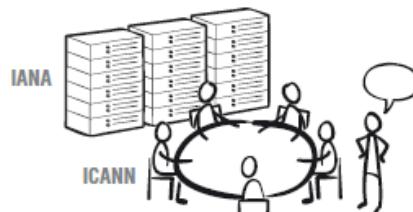
A ICANN não regula conteúdo on-line nem tem os recursos para remover conteúdo. No entanto, essas limitações não impedem que a ICANN estude ou ajude na mitigação de abusos do DNS.

Alta ocorrência em TLDs genéricos

Rank	Registrar	TLD	#Domains
1.	NameSilo	top	1,807
2.	NameSilo	com	852
3.	GoDaddy	com	832
4.	Hostinger	online	764
5.	NameSilo	info	513
6.	Hostinger	com	479
7.	Namecheap	com	479
8.	Alibaba Cloud	com	327
9.	NameSilo	xyz	233
10.	Hostinger	cloud	225
11.	NameSilo	buzz	222
12.	Sav	com	211
13.	Alibaba Cloud	shop	197
14.	NameSilo	us	191
15.	Hostinger	site	179
16.	NameSilo	life	178
17.	NameSilo	sbs	171
18.	Hostinger	shop	156
19.	NameSilo	cc	149
20.	Alibaba Cloud	top	148

Distribuição de domínios genéricos

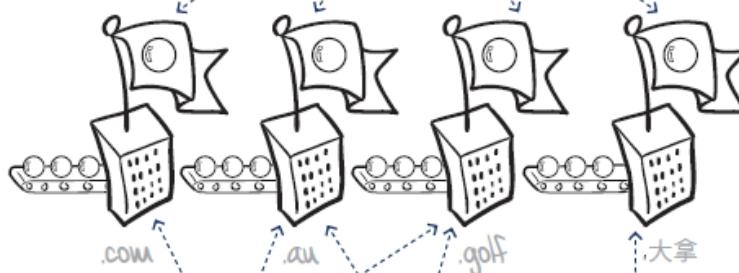
COORDINATION LAYER



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.

WHOLESALE LAYER



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.

DISTRIBUTION LAYER



REGISTRARS

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

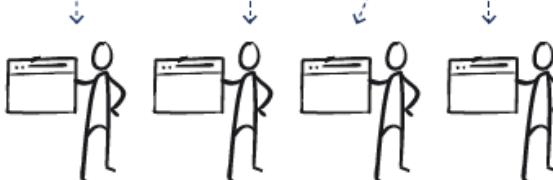
RESALE LAYER



RESELLERS

Resellers are appointed by Registrars to increase their distribution network.

CONSUMER



REGISTRANT

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

Casos: cristalprimebr.store



A screenshot of the cristalprimebr.store website. At the top left is the company logo. To its right is a search bar with the placeholder "Pesquisar..." and a green "Buscar" button. Further right are links for "Entrar / Criar conta" and "Minha conta". Below the header are four navigation links: "INÍCIO", "ENTRAR EM CONTATO", "PARA A SUA OBRA", and "TODOS OS PRODUTOS".

A screenshot of a Reclame Aqui page for the company "cristal prime". The page has a header with the Reclame Aqui logo, a search bar, and a "Instale a extensão" button. Below the header are dropdown menus for "Para você", "Melhores empresas", "Detector de Site Confiável", and "Compare". The main content area shows a large circular rating icon with a "C" in the center, labeled "Referente aos últimos 12 meses". It also displays "0 de visualização", a "Não Recomendada" badge, and a "Não verificada" badge. Navigation links include "Home", "Sobre", "Reclamações" (which is underlined in green), and "Principais problemas". A "Publicidade" link is at the bottom. A sidebar on the left asks "Qual a reputação de cristal prime?", showing a purple circle with a sad face icon and the text "Reputação Não recomendada". Another sidebar on the right lists "Todas as reclamações para cristal prime" with the note "Exibindo 10 de 19 reclamações (todas as reclamações ativas da empresa cristal prime)".

Casos: Rastreamento Correios

The screenshot shows a web browser window with a URL starting with "pay.rastrementodeencomendaa.online". The page features the official Correios logo at the top left. A prominent yellow warning banner at the top center reads: "⚠ ATENÇÃO: Caso não finalize agora, sua encomenda será cancelada e poderá acarretar em pendências no seu CPF!" Below the banner, there are two more Correios logos. To the right, there are logos for ICMS (Imposto de Circulação Móvel do Serviço), Receita Federal, and Ministério da Economia. The main form area contains fields for "Identificação" (Email and Phone) and a "Seu carrinho" (Shopping Cart) section.

Identificação

E-mail
email@email.com

Telefone
(99) 99999-9999

Não tenho e-mail

Seu carrinho 1

GUIA DE LIBERAÇÃO
Produto taxado 1 un.

Subtotal R\$ 86,67

Como ajudar?

Como fazer uma denúncia de Abuso de DNS

ETAPA 1 – Identificação do abuso

Antes de tudo, verifique se há indícios claros de abuso. Os sinais incluem:

- Sites falsos pedindo dados sensíveis (phishing)
 - Download forçado de arquivos ou comportamentos estranhos (malware)
 - Redirecionamentos não solicitados para domínios suspeitos
-  Dica: Tire prints e registre os links suspeitos.

Como fazer uma denúncia de Abuso de DNS

◆ ETAPA 2 – Coleta de informações

Reúna dados essenciais para embasar sua denúncia:

- URL completa do site/domínio suspeito
- Tipo de abuso (phishing, malware, spam, etc.)
- Data e hora da ocorrência
- Descrição objetiva do problema
- Evidências (capturas de tela, e-mails recebidos, links internos)

Como fazer uma denúncia de Abuso de DNS

◆ ETAPA 3 – Consulta ao WHOIS

Antes de denunciar, é necessário identificar o **registraror** do domínio:

1. Acesse uma ferramenta WHOIS (ex: <https://lookup.icann.org>)
2. Insira o domínio suspeito
3. Anote os dados de contato que aparecem no campo "Registrar Information":

- Nome do registrar
- Abuse contact email
- Abuse contact phone

 Dica: Você também pode acessar os canais de abuso dos registradores nas suas páginas oficiais listadas em: <https://www.icann.org/en/contracted-parties/accredited-registrars/list-of-accredited-registrars>

Consulta no Whois: [lookup.icann.org](https://lookup.icann.org/en)

The screenshot shows the ICANN Registration data lookup tool interface. At the top, there is a navigation bar with icons for back, forward, search, and other browser functions. The URL 'lookup.icann.org/en' is displayed. Below the URL, there are language links: العربية, 简体中文, English, Français, Русский, and Español. The main header reads 'ICANN | LOOKUP'. The main section title is 'Registration data lookup tool'. Below it, there is a text input field with placeholder text 'Enter a value' and a blue 'Lookup' button. To the right of the input field, there is a link to 'Frequently Asked Questions (FAQ)'. Below the input field, there is a terms of service agreement text. At the bottom, there is a section titled 'About ICANN's registration data lookup tool' with a descriptive paragraph.

lookup.icann.org/en

العربية 简体中文 English Français Русский Español

ICANN | LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource
(IP Network or ASN)

Frequently Asked Questions (FAQ)

Enter a value

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

For additional information on ICANN Accredited Registrars including website and contact information, please visit <https://www.icann.org/en/accredited-registrars>.

About ICANN's registration data lookup tool

The ICANN registration data lookup tool gives you the ability to look up the current registration data for domain names and Internet number resources. The tool uses the Registration Data Access Protocol (RDAP) which was created as a replacement of the WHOIS (port 43) protocol. RDAP was developed by the technical community in the [Internet Engineering Task Force \(IETF\)](#).

lookup.icann.org/en

العربية 简体中文 English Français Русский Español

ICANN | LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource
(IP Network or ASN)

[Frequently Asked Questions \(FAQ\)](#)

[Lookup](#)

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the registration data lookup tool [Terms of Use](#).

For additional information on ICANN Ac contact information, please visit <https://www.icann.org>

About ICANN's registrar

The ICANN registration data lookup tool can be used to look up registration information for domain names and Internet number resources. The tool uses the replacement of the WHOIS (port 43) protocol by the IETF's [Engineering Task Force \(IETF\)](#).

Registrar Information

Name: GoDaddy.com, LLC

IANA ID: 146

Abuse contact email: abuse@godaddy.com

Abuse contact phone: tel:480-624-2505



One World, One Internet

Visit us at icann.org

e_Mail: kindns-info@icann.org



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg