KINDNS

Una iniciativa de la ICANN para promover las mejores prácticas operativas del DNS

ICANN

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

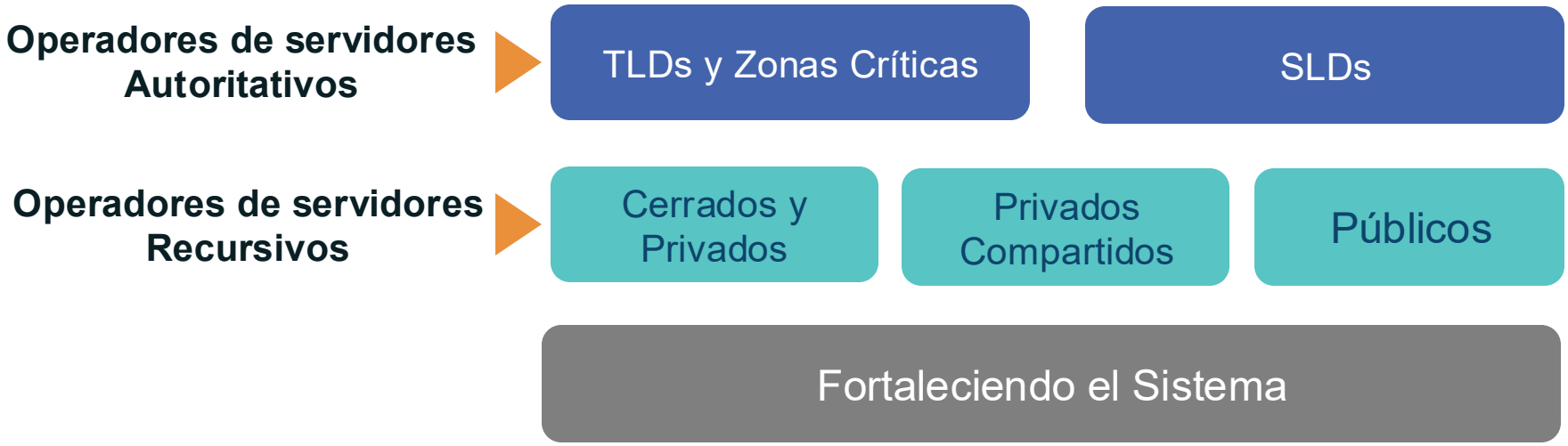
….. is pronounced ”kindness.”

¿De qué se trata?

KINDNS

El intercambio de conocimientos y las normas de creación de instancias para el sistema de nombres de dominio y su seguridad (KINDNS) es una iniciativa lanzada por la Corporación de Internet para la Asignación de Nombres y Números (ICANN) para producir un marco simple y claro de mejores prácticas operativas para los operadores de DNS.

Operadores objetivo



Al unirse a la iniciativa KINDNS, los operadores de DNS se comprometen voluntariamente a adherirse a las prácticas identificadas y actuar como "embajadores de buena voluntad" dentro de la comunidad.

Authoritative DNS Operators of Critical Zones

KINDNS

TLDs & Critical Zones

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive name servers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Authoritative DNS Operators for SLDs

KINDNS

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive name servers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Closed and Private Resolver Operators

Private resolvers are not publicly accessible and cannot be reached over the open Internet. They are typically found in corporate networks or other restricted-access networks

Closed and Private resolvers

1. DNSSEC validation **MUST** be enabled
2. Access control list (ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive name servers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Shared Private Resolver Operators

KINDNS

Shared private resolver operators are typically Internet service providers (ISPs) or similar hosting service providers. They offer DNS resolution services to their customers (mobile, cable/DSL/fiber users, as well as hosted servers and applications).

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. **For pr**ivacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Public Resolver Operators

KINDNS

This category includes both open and closed public resolvers. Closed public resolvers are typically commercial DNS filtering/scrubbing services, such as DNSFilter and OpenDNS.

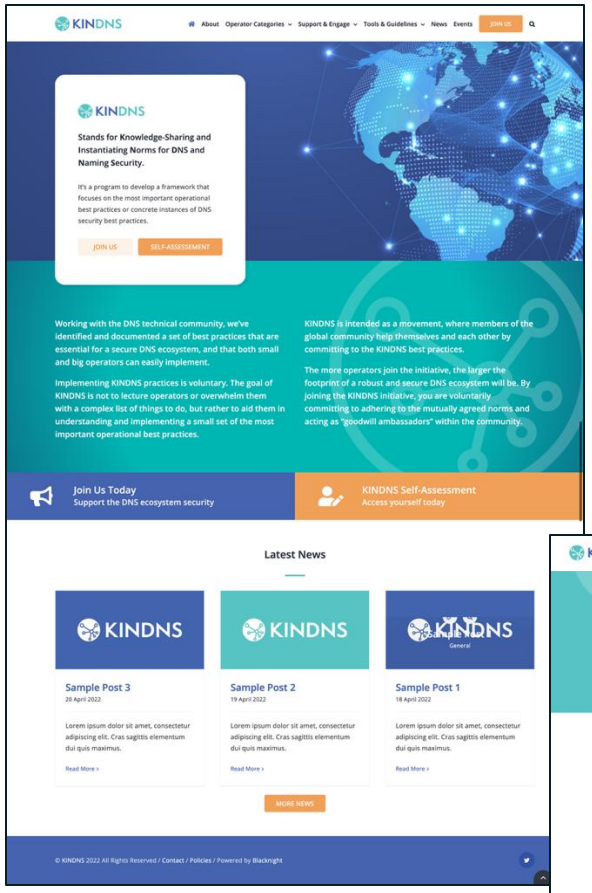
Shared Private resolvers

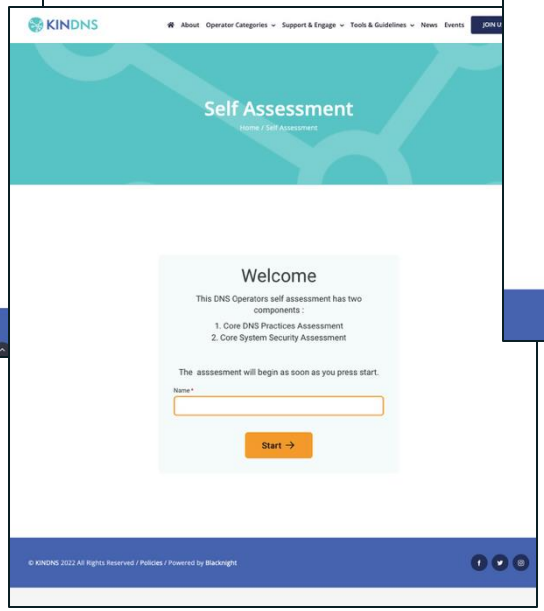
1. DNSSEC validation **MUST** be enabled
2. QNAME minimization **MUST** be enabled
3. **For** privacy considerations: Encryption (DOH or DoT) **SHOULD** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. Data collected through the passive logging of DNS queries **MUST** be limited
6. At least two distinct servers **MUST** be used for providing recursion services
7. Public resolver operators **MUST** ensure operational diversity in their infrastructure.
8. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

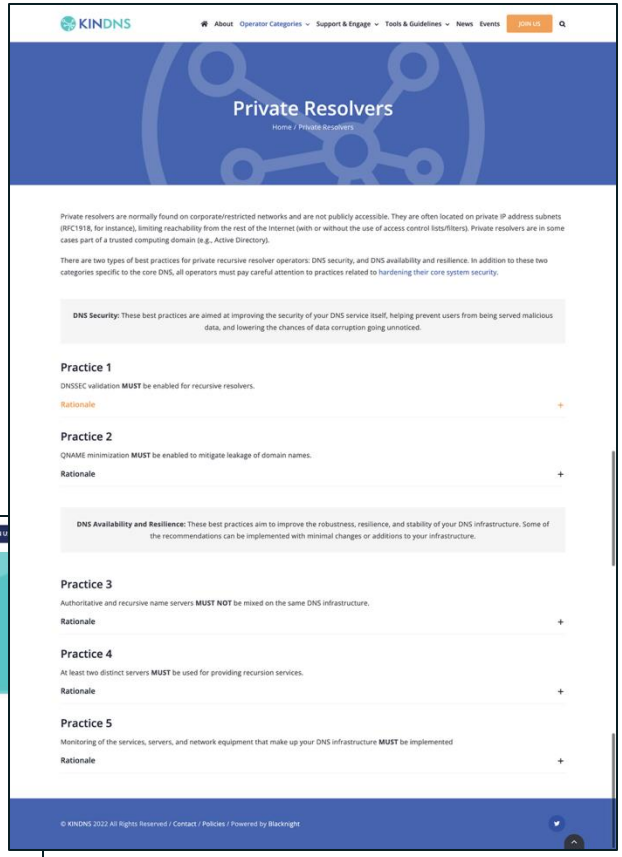
Self-Assessment Reports

KINDNS

Website – kindns.org (kindns.club)







4. Reconhecimentos

KINDNS

KINDNS

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

Engage with ICANN – Thank You and Questions

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