

# Actualidad de DNS

**48º GGTT RedIRIS**

Valladolid, 28 de noviembre de 2019

Juan Carlos Rodríguez

[Jcarlos.rodriguez@rediris.es](mailto:Jcarlos.rodriguez@rediris.es)

RedIRIS

# Servicios DNS

---

- Delegacion DNS
  - Delegar resoluciones inversas del direccionamiento IP que provee RedIRIS
  - Aceptamos registros DS (DNSSEC)
- Secundario DNS
  - Publicar zonas como secundarios
  - Dos nubes Anycast DNS
- Hosting DNS
  - Gestionar y publicar zonas de instituciones
  - Gestión desde aplicación IRISDNS
  - Firmado DNSSEC
  - Publicación en las nubes Anycast

# Servicios DNS

---

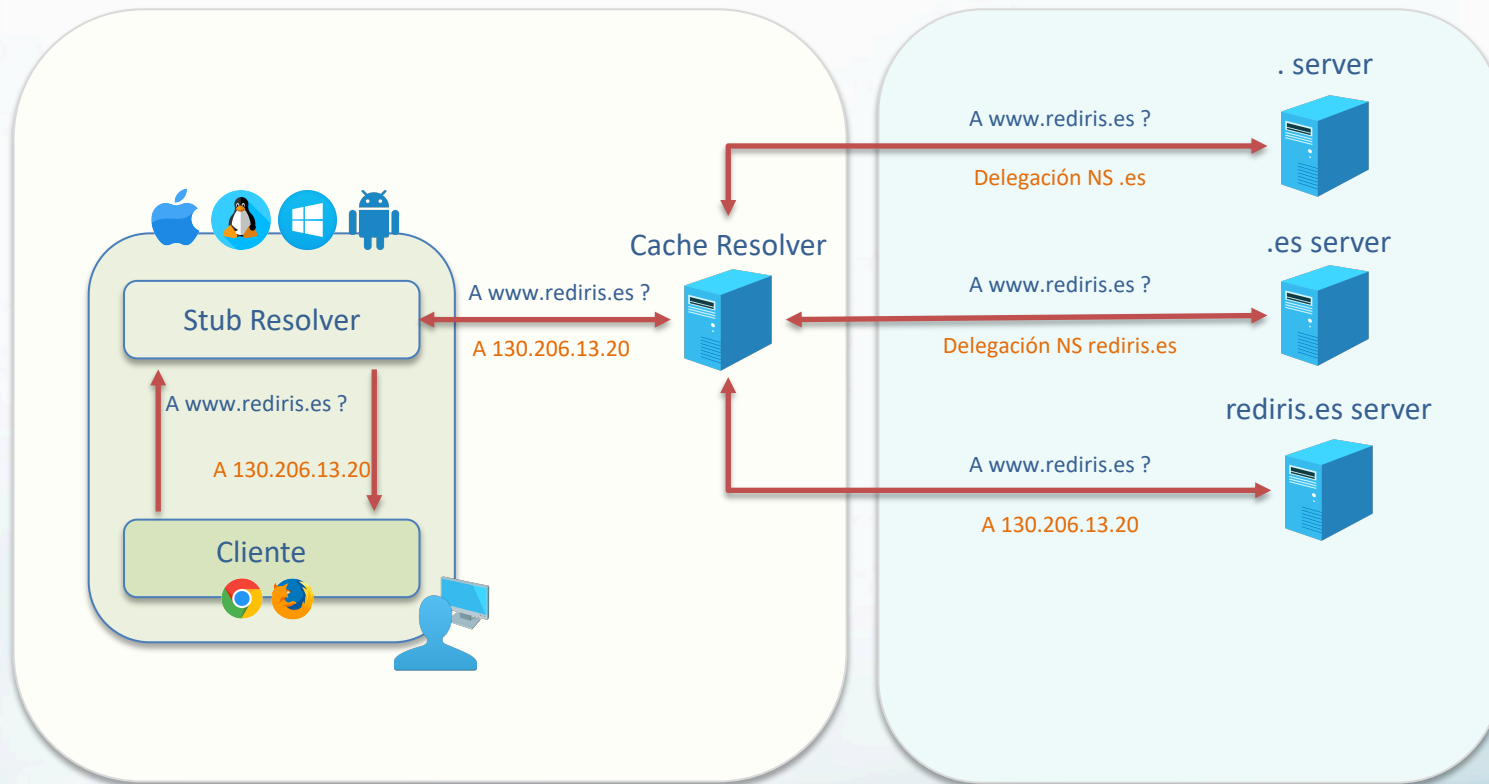
- Lista IRIS-DNS
  - Coordinación de servicio, novedades, incidencias, etc.
  - Cada administrador de DNS de la institución debería estar suscrito
    - Enviadnos los contactos para el servicio DNS ([iris-nic@rediris.es](mailto:iris-nic@rediris.es))
- Herramienta IRISDNS <https://irisdns.rediris.es>
  - Gestión de los servicios Delegacion DNS, Secundario DNS y Hosting DNS
  - Monitorización de la configuración
- Formación
  - Cursos de formación DNS
- <http://www.rediris.es/servicios/conectividad/dns/>

# DNSSEC ¿qué es?

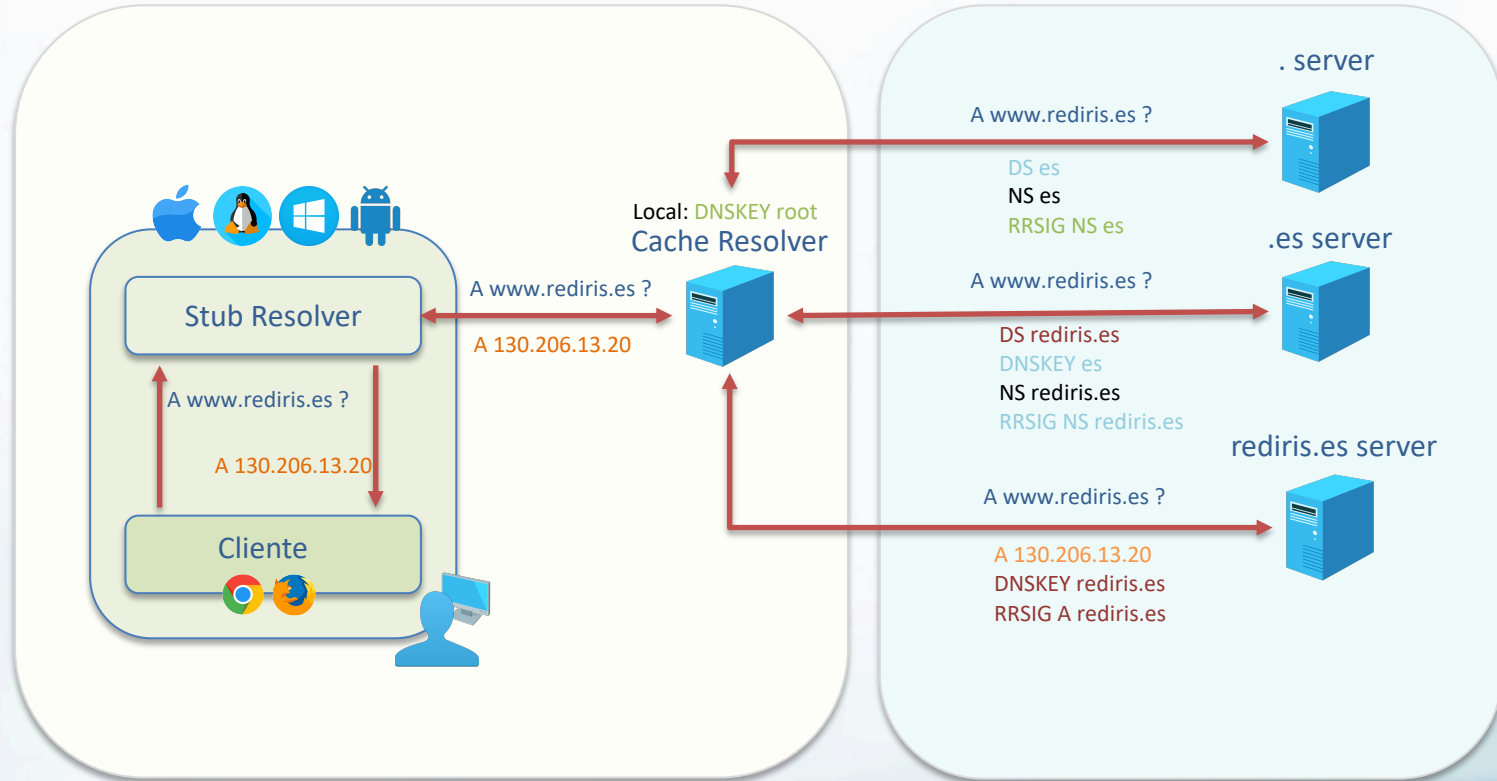
---

- DNSSEC verifica la autenticidad e integridad de la respuesta
  - Firmado criptográfico mediante clave pública/privada
  - Se garantiza la cadena de confianza mediante delegaciones firmadas por el dominio superior
  - Protege contra ataques man-in-the-middle y de envenenamiento de caché
    - Redirecciones a servidores comprometidos
  - Nuevas funcionalidades: DANE
- DNSSEC no cifra el mensaje
  - No añade privacidad ni confidencialidad
- DNSSEC todavía en etapa de adopción

# Funcionamiento DNS



# Funcionamiento DNSSEC



# DANE: DNS-based Authentication of Named Entities

- Permite asociar certificados de tipo X.509 a dominios
  - Permite validar certificados creados por una CA o autofirmados
- Es un paso extra de seguridad y requiere DNSSEC
- Define un nuevo registro tipo TLSA:
  - *\_25.\_tcp.mx09.puc.rediris.es. IN TLSA 3 1 2*  
*6f4d03121ce3a83ab3c7b8dab9df0024ee53fc791e09d146169e0ff01ab7a1e15ac*  
*b0144353840fa176a35aec73956f51ba0bda16e1b27a3a5a99d4c8fd54d1d*
  - *\_443.\_tcp.redirisnova.es. IN TLSA 3 1 1*  
*d011d8cfea96ba7afcf914e2f9d60aaac172f93bd6a3dd109aae2c58633f6c81*
- Correo electrónico como caso de uso (RFC 7929)
  - Permite el SMTP cifrado y verificado
  - La existencia de un registro TLSA exige el uso de TLS

# DNSSEC actividades 2019

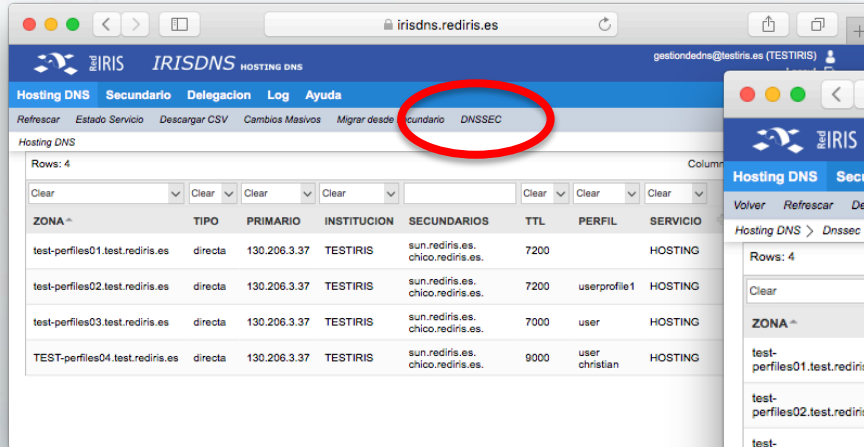
---

- Firmados todos los dominios de RedIRIS desde Junio
- Disponible firmado de zonas en servicio "Hosting DNS"
- Disponible despliegue de delegaciones inversas firmadas (registros DS)



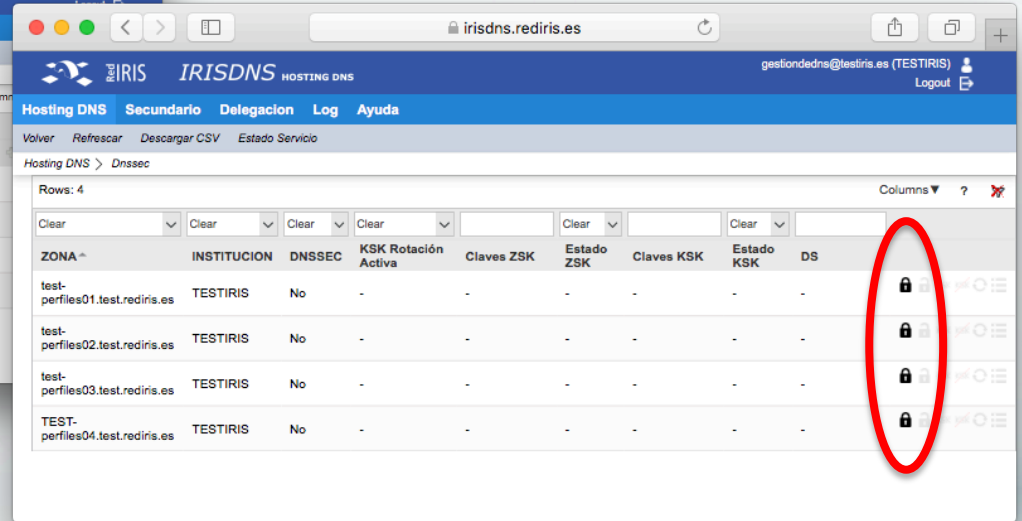
# DNSSEC actividades 2019

Disponible firmado de zonas en servicio "Hosting DNS"



The screenshot shows the IRISDNS web interface. The navigation menu includes 'Hosting DNS', 'Secundario', 'Delegacion', 'Log', and 'Ayuda'. Below this, there are links for 'Refrescar', 'Estado Servicio', 'Descargar CSV', 'Cambios Masivos', 'Migrar desde', 'Secundario', and 'DNSSEC'. The 'DNSSEC' link is circled in red. Below the navigation, there is a table with 4 rows and 7 columns: ZONA, TIPO, PRIMARIO, INSTITUCION, SECUNDARIOS, TTL, and PERFIL. The table contains data for four different zones.

ZONA	TIPO	PRIMARIO	INSTITUCION	SECUNDARIOS	TTL	PERFIL
test-perfiles01.test.rediris.es	directa	130.206.3.37	TESTIRIS	sun.rediris.es, chico.rediris.es	7200	HOSTING
test-perfiles02.test.rediris.es	directa	130.206.3.37	TESTIRIS	sun.rediris.es, chico.rediris.es	7200	userprofile1
test-perfiles03.test.rediris.es	directa	130.206.3.37	TESTIRIS	sun.rediris.es, chico.rediris.es	7000	user
TEST-perfiles04.test.rediris.es	directa	130.206.3.37	TESTIRIS	sun.rediris.es, chico.rediris.es	9000	user christian



The screenshot shows the IRISDNS web interface with the 'DNSSEC' sub-menu selected. The table has 4 rows and 10 columns: ZONA, INSTITUCION, DNSSEC, KSK Rotación Activa, Claves ZSK, Estado ZSK, Claves KSK, Estado KSK, and DS. The 'DS' column contains lock icons, which are circled in red.

ZONA	INSTITUCION	DNSSEC	KSK Rotación Activa	Claves ZSK	Estado ZSK	Claves KSK	Estado KSK	DS
test-perfiles01.test.rediris.es	TESTIRIS	No	-	-	-	-	-	🔒
test-perfiles02.test.rediris.es	TESTIRIS	No	-	-	-	-	-	🔒
test-perfiles03.test.rediris.es	TESTIRIS	No	-	-	-	-	-	🔒
TEST-perfiles04.test.rediris.es	TESTIRIS	No	-	-	-	-	-	🔒

## Disponible despliegue de delegaciones inversas firmadas (registros DS)

https://irisdns.rediris.es

IRIS IRISDNS HOSTING DNS

Hosting DNS Secundario Delegacion Hosting DNS(Admin) Secundario(Admin) Delegacion(Admin) Indicadores

Estado Usuarios Log Ayud **Editar delegacion**

Recarga lista de delegaciones Estado Ser

Delegacion

Modificación de los datos de una delegación

**Bloque a delegar:**  
130.206.13.0/24

**Nombre completo de la zona:**  
13.206.130.in-addr.arpa

**Acronimo Institucion:**  
REDIRIS

**Servidor donde delegar:**  
sun.rediris.es

**Registros DS:**  
26890 8 1 FE97CDD67FB0756D8D119A377E1F325  
26890 8 2 FF4B1CFE21E1AE585FE4384AA6487D7E

Confirmar Cancelar

RedIRIS	Si	ofelia.rediris.es. polonio.rediris.es.
RedIRIS	Si	balsev.lav.puc.rediris.es. balmad.lav.puc.rediris.es.
RedIRIS		tais.rediris.es. sun.rediris.es. chico.rediris.es.
RedIRIS	Si	nahum.rediris.es. sun.rediris.es. chico.rediris.es.

# ANYCAST ¿qué es?

---

- Servicio Unicast: una localización
  - Problemas si hay una caída o un ataque DDoS
- Servicio Anycast: múltiples localizaciones compartiendo dirección IP
  - El cliente es redirigido mediante routing al nodo más cercano
  - Si un nodo cae, el routing redirige el cliente al siguiente nodo más próximo
  - Si hay un ataque DDoS
    - Cada elemento del ataque sólo ataca al nodo más cercano
      - Contra más nodos, más difícil es saturar cualquiera de ellos
    - Aunque un nodo se saturase, sólo afectaría parcialmente a los clientes

# ANYCAST actividades 2019

---

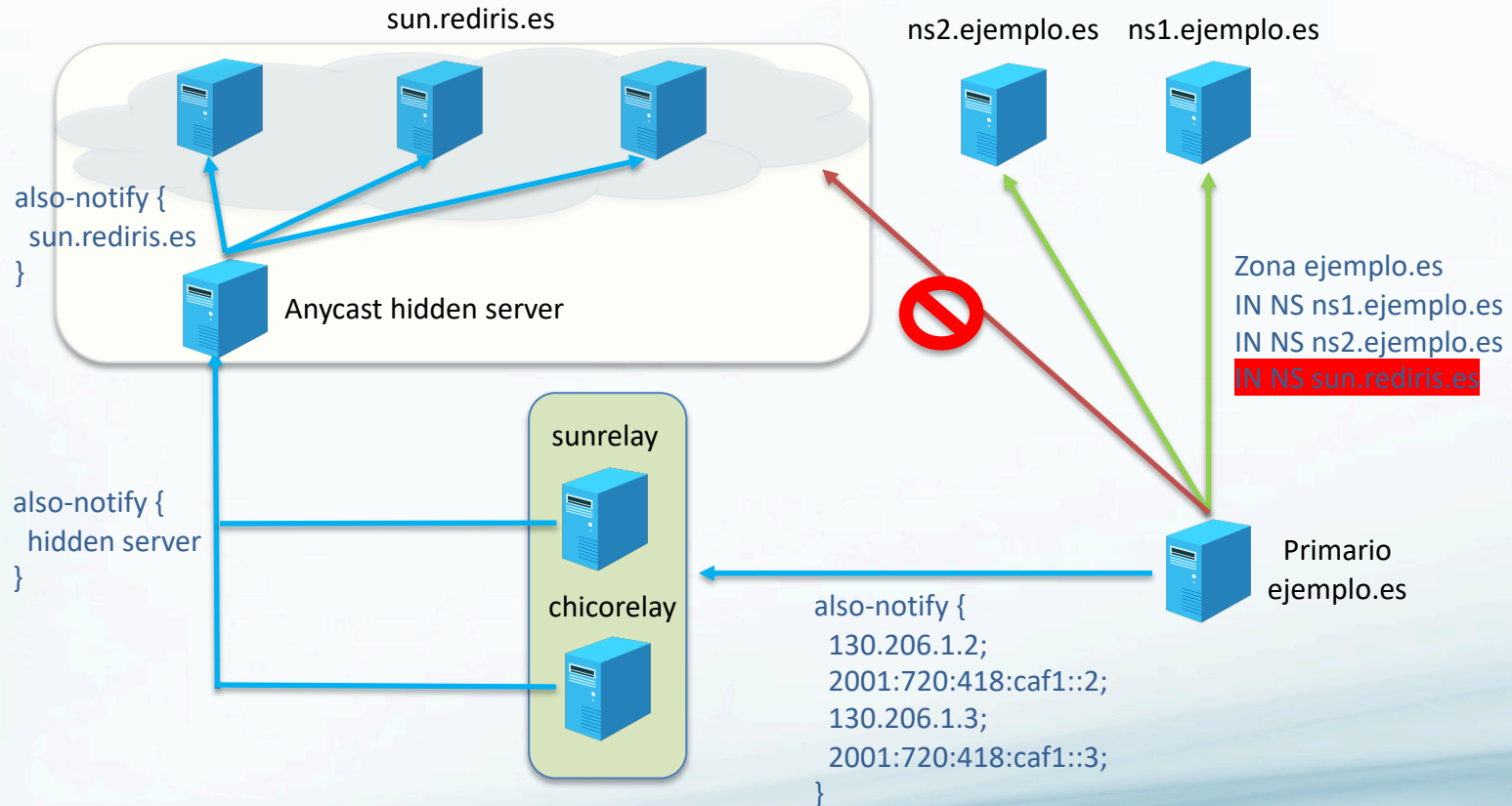
- Sustitución de los servidores unicast de RedIRIS por nubes Anycast
  - sun.rediris.es
    - 130.206.1.2 -> 199.184.182.1
    - 2001:720:418:CAF1::2 -> 2620:171:808::1
- Los antiguos unicast quedan como intermediarios para las transferencias de zona
  - sun.rediris.es -> sunrelay.rediris.es (130.206.1.2 // 2001:720:418:CAF1::2)
- Licitación y despliegue de dos nubes Anycast de diferentes proveedores comerciales
  - PCH (Packet Clearing House): licitado, desplegado y migrado
  - CIRA (Canadian Internet Registry Authority): adjudicado

# ANYCAST cambios de configuración

¡Se requiere configuración adicional!

```
zone "rediris.es" {  
    type master;  
    file "rediris.es.db";  
    also-notify {  
        130.206.1.2;  
        130.206.1.3;  
        2001:720:418:caf1::2;  
        2001:720:418:caf1::3;  
    };  
    allow-transfer {  
        130.206.1.2;  
        130.206.1.3;  
        2001:720:418:caf1::2;  
        2001:720:418:caf1::3;  
    };  
};
```

# ANYCAST transferencias de zona



# ANYCAST comprobación de configuración

A través de IRISDNS podéis ver el estado de vuestra configuración

The screenshot shows the IRISDNS web interface. The navigation bar includes links for 'Hosting DNS', 'Secundario', 'Delegación', 'Hosting DNS(Admin)', 'Secundario(Admin)', 'Delegación(Admin)', 'Indicadores', 'Estado', 'Usuarios', 'Log', and 'Ayuda'. The 'Estado Servicio' link is circled in red. The main content area displays a table with 173 rows, showing the status of various DNS zones. A detailed view of the table is shown in an inset window, highlighting the 'ESTADO\_SERIAL' column with a green background, indicating that the configuration is correct.

ZONA	REDIRIS	SECUNDARIOS	RELAY	MASTERS
0.0.0.0.0.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
0.0.A.C.8.1.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
0.1.A.C.8.1.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
0.206.130.in-addr.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
1.0.A.C.8.1.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
1.1.A.C.8.1.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64
1.F.A.C.8.1.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	chico.rediris.es sun.rediris.es	chico.rediris.es sunrelay.rediris.es	130.206.3.64

ZONA	REDIRIS	SERIAL	ESTADO_SERIAL	NAMESERVERS	ESTADO_NAMESERVERS	DIAGNOSTICO	FECHA
0.0.0.0.0.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	130.206.3.64 serial (from chico.rediris.es): 2019102025 130.206.3.64 serial (from sunrelay.rediris.es): 2019102025 chico.rediris.es serial: 2019102025 sun.rediris.es serial: 2019102025 sunrelay.rediris.es serial: 2019102025	OK	chico.rediris.es. sun.rediris.es.	OK	OK	27/11/2019 14:03:42
0.0.a.c.8.1.4.0.0.2.7.0.1.0.0.2.ip6.arpa	REDIRIS	130.206.3.64 serial (from chico.rediris.es): 2019101174 130.206.3.64 serial (from sunrelay.rediris.es): 2019101174	OK	chico.rediris.es. sunrelay.rediris.es.	OK	OK	27/11/2019 14:03:42

# ANYCAST tamaños de las zonas

---

- Algunas zonas del servicio Secundario DNS son MUY grandes (decenas y centenares de miles de registros)
  - Contienen registros en desuso...
  - Contienen direccionamiento privado...
  - No están debidamente jerarquizadas...
- Es conveniente sanear las zonas
  - Son más difíciles de gestionar
  - Aumentan los costes
  - Publican vistas privadas de la infraestructura



# Resumen de mejoras en el servicio durante 2019 (inicio 2020)

---

- Hosting DNS
  - Nueva funcionalidad de firmado DNSSEC
  - Despliegado servidores de publicación Anycast
- Secundario DNS
  - Servidores Anycast
- Delegación
  - Aceptamos registros DS
  - Zonas de RedIRIS firmadas
    - cadena de validación DNSSEC completa
- Organizado curso presencial de DNS

# Evolución y próximas mejoras

---

- Terminar despliegue Anycast migrando chico.rediris.es (principios 2020)
- TSIG disponible en IRISDNS para servicio Secundario DNS (principios 2020)
- Estudio de interés/viabilidad de nuevo servicio DNS firewall (2020)
- Formación (2020)
  - Cursos
  - VideoseSIONes

# ¡Muchas gracias!



*Más de 25 años al servicio de la investigación*