DNSSEC: Extensiones de seguridad al sistema DNS

Sergio Ramírez

set 2015

Breve reseña de .UY

- 1990 – Se delega el dominio de internet de primer nivel correspondiente a Uruguay al SeCIU-Udelar. Comienzos de la operación de la Red Académica Uruguaya (RAU).
  - Se define usar dominios estructurados en 5 subdominios: edu.uy, org.uy, gub.uy, net.uy y com.uy
- 1994 – Se delega el subdominio com.uy a Antel para su administración y operación.
- 1999 – Se crea el subdominio mil.uy
- 2012 – Se abre el registro público de nombres de dominios directamente bajo .uy
- 2013 – Se habilita la figura de “Agente Registrador” para los nombres de dominios directamente bajo .uy (descentralización en el registro de dominios)
- 2015 – Se firma la zona .uy y las zonas de segundo nivel de uso público para habilitar DNSSEC en dominios UY.

DNS Introducción

- DNS - **D**omain **N**ame **S**ystem
  - Gestiona información asociada a los nombres de dominios.
- Base de datos distribuída.
  - La base de datos completa del espacio de nombres de dominio no se encuentra en un solo sitio.
- Estructura de nombres jerárquica
  - Similar a la estructura de nombres de archivos unix.
- Arquitectura cliente-servidor.
  - Algunos procesos actúan como clientes y otros como servidores.

DNS Introducción
(base de datos distribuída)

Nombre	TTL	Clase	Tipo	RRDATA
rau.edu.uy.	86400	IN	SOA	seciu.edu.uy. teccom.seciu.edu.uy. 201409160 10800 3600 432000 86400
rau.edu.uy.	86400	IN	NS	tacuabe.rau.edu.uy.
tacuabe.rau.edu.uy	86400	IN	A	164.73.128.70
www.rau.edu.uy.	86400	IN	A	164.73.128.65
www.rau.edu.uy.	86400	IN	AAAA	2001:1328:6::42
rau.edu.uy.	86400	IN	MX	0 distri.rau.edu.uy.

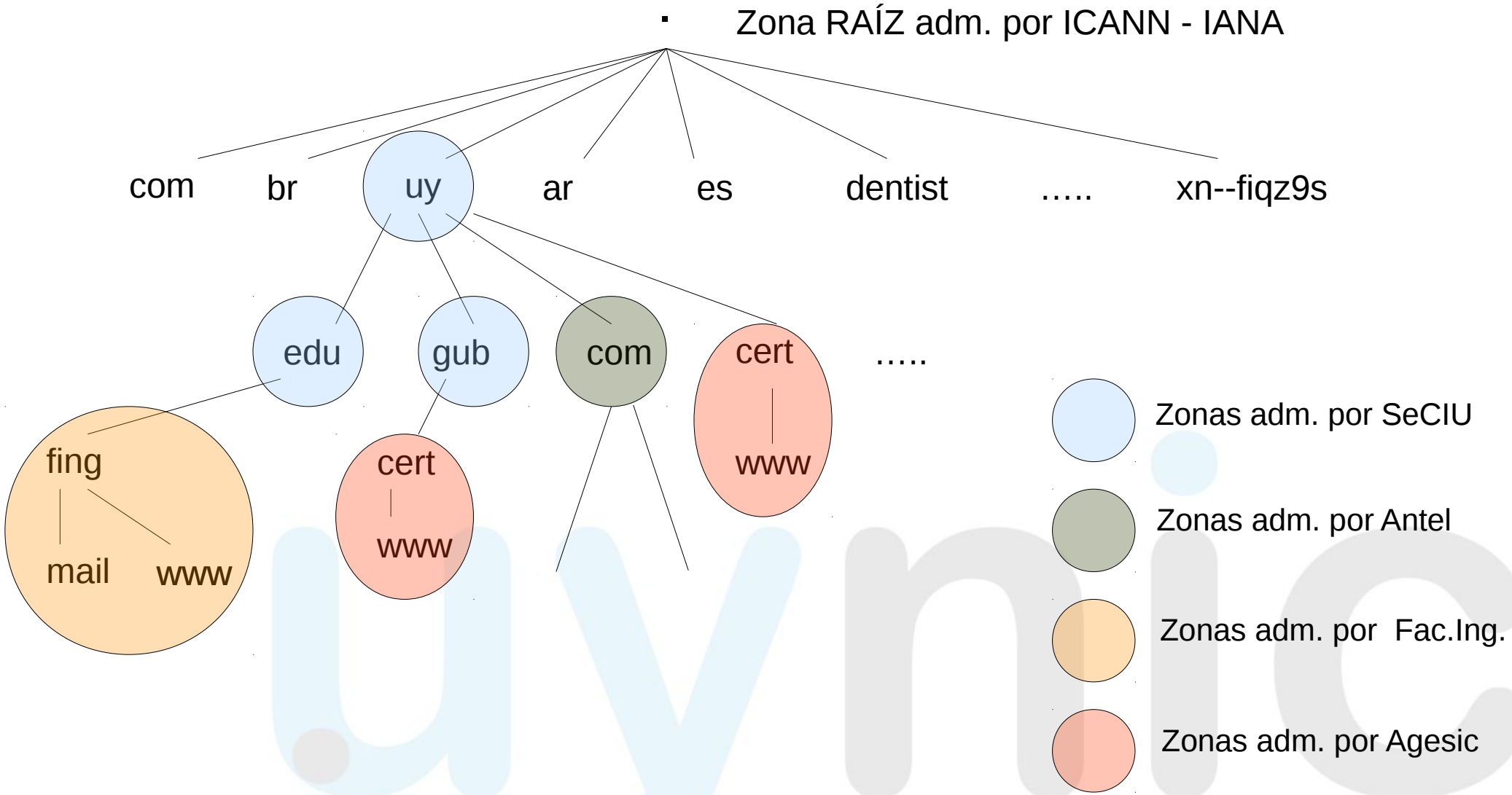
- Los registros son llamados Resource Record (RR).

- En general, las búsquedas se realizan por los campos: Nombre, Clase y Tipo. (el campo Clase casi siempre tiene el valor “IN”).

- Diferentes países, empresas, organizaciones, etc. administran una porción de la base de datos global de nombres de dominios.

- El “.” puede usarse para delimitar las ZONAS de administración de esta base de datos.

DNS Introducción
(estructura de nombres jerárquica)

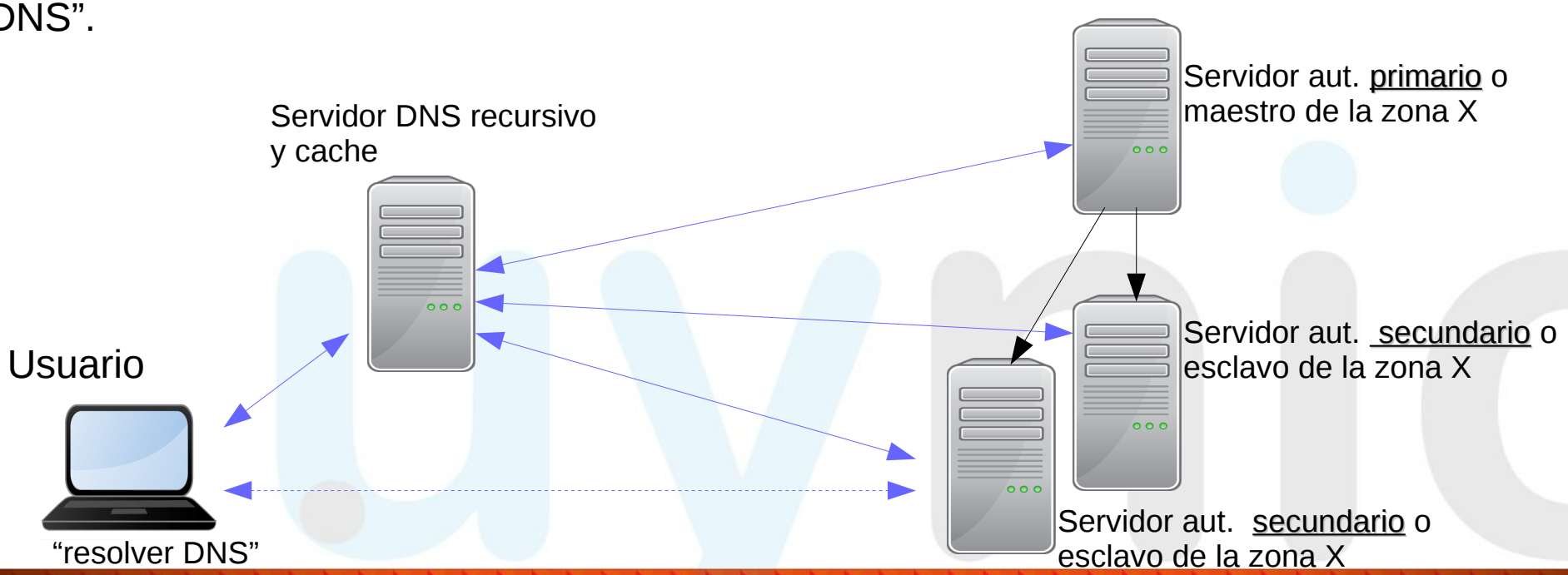


DNS Introducción
(arq. cliente-servidor)

- Servidores “autoritativos” - un servidor “autoritativo” primario y uno o varios servidores “autoritativos” secundarios por cada zona.

- Servidores “recursivos” / “cache” - recibe consultas de los clientes y consulta a los servidores “autoritativos”. Generalmente las respuestas obtenidas son almacenadas temporalmente en un “cache”.

- Los dispositivos y aplicaciones tienen implementado un cliente DNS, también llamado “resolver DNS”.



¿ Cómo funciona el DNS ?

Acceder al sitio
http://www.udelar.edu.uy/

Usuario

Servidor DNS recursivo

Servidor DNS aut. RAIZ

a.root-servers.net

Servidor DNS aut. UY

a.nic.uy

Servidor DNS aut. EDU.UY

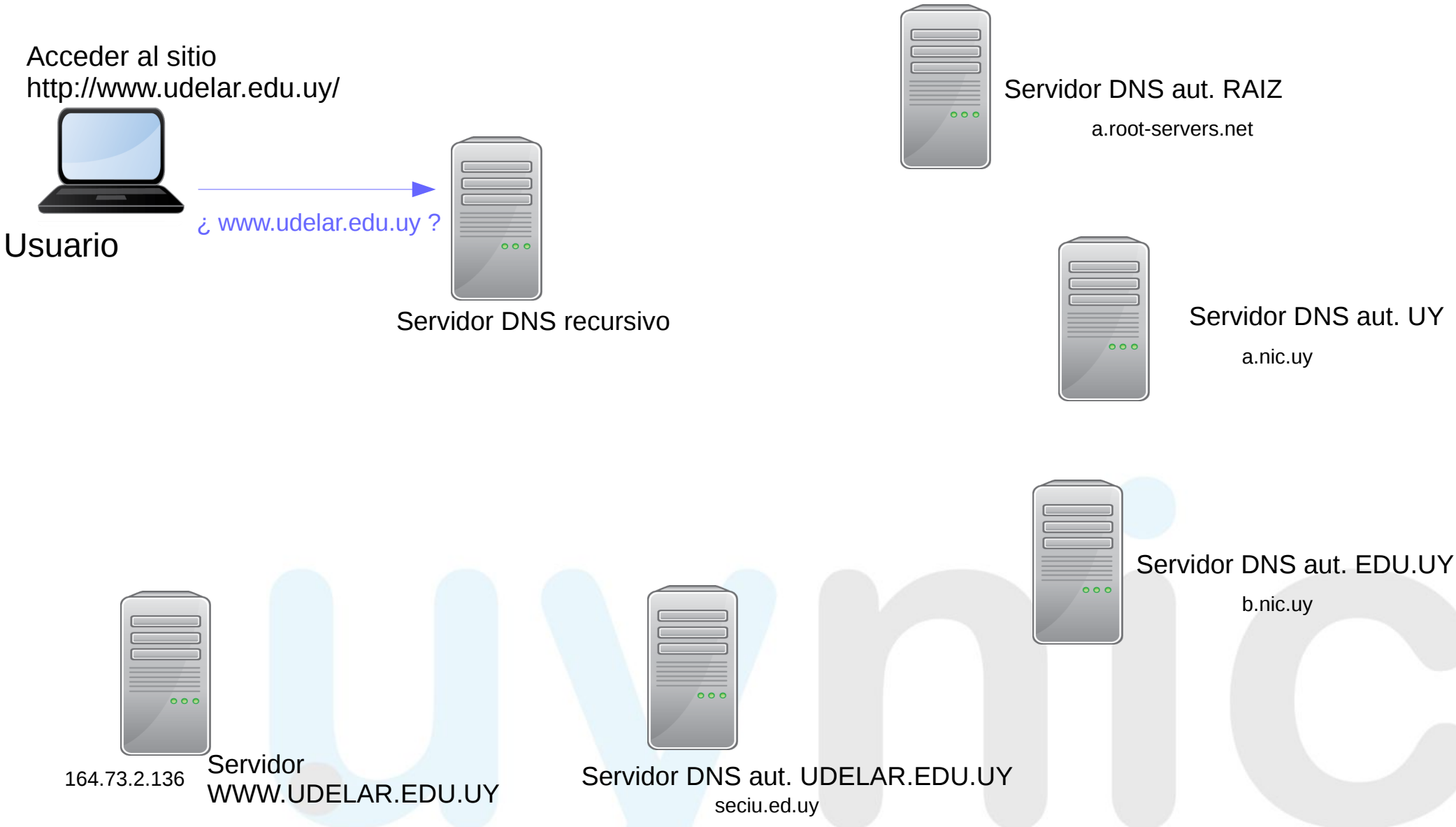
b.nic.uy

164.73.2.136 Servidor
WWW.UDELAR.EDU.UY

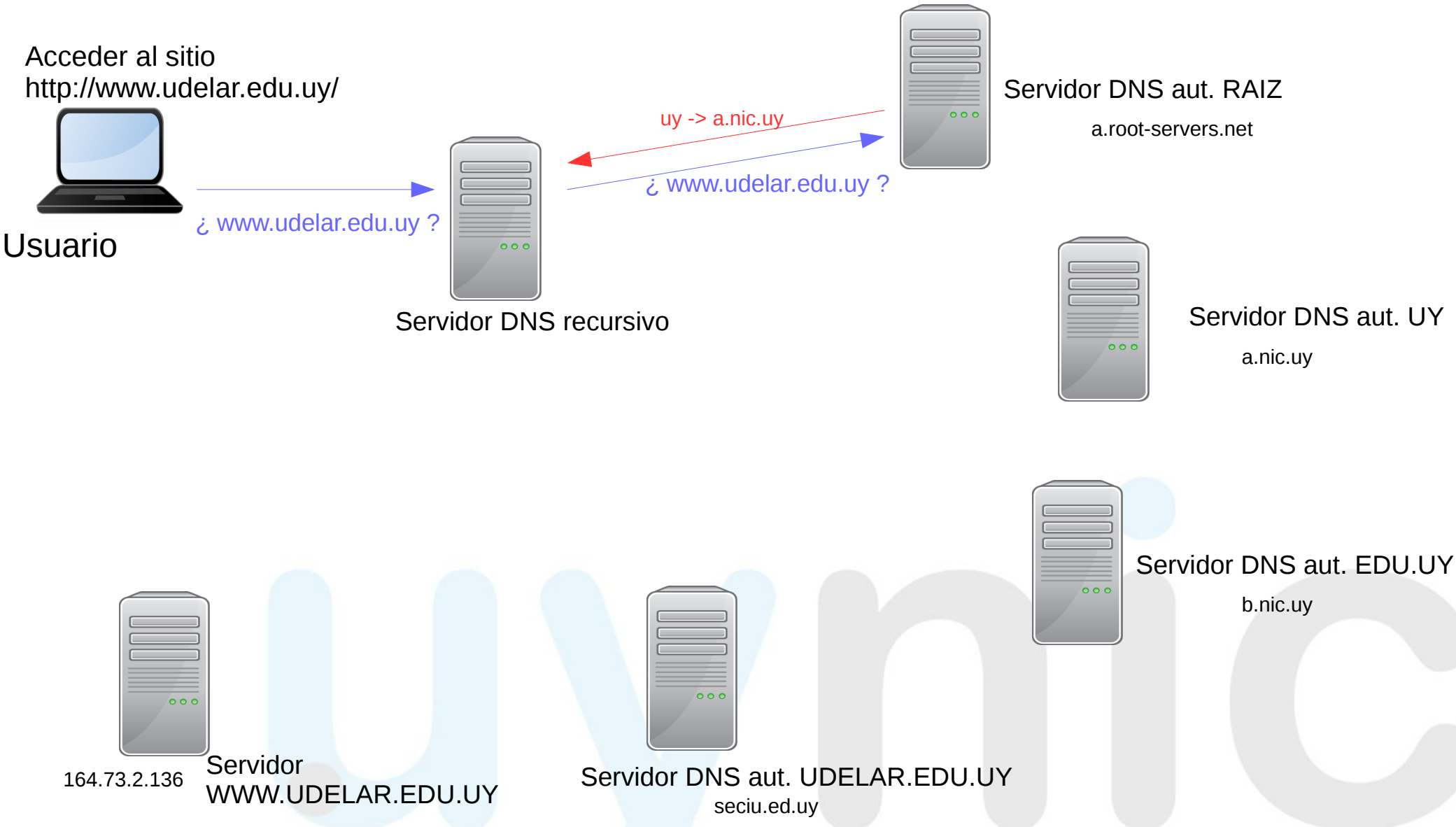
Servidor DNS aut. UDELAR.EDU.UY

seciu.ed.uy

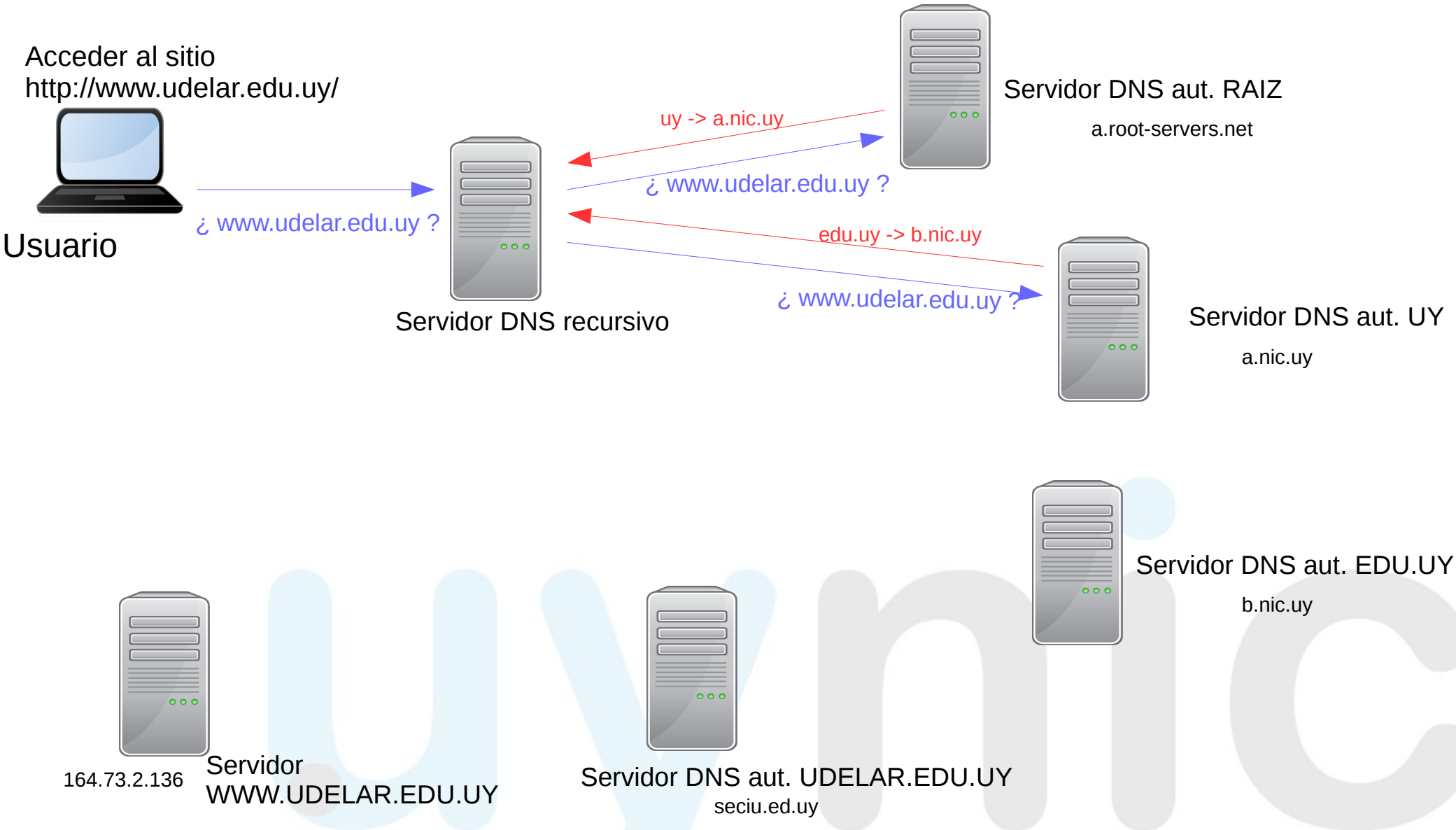
¿ Cómo funciona el DNS ?



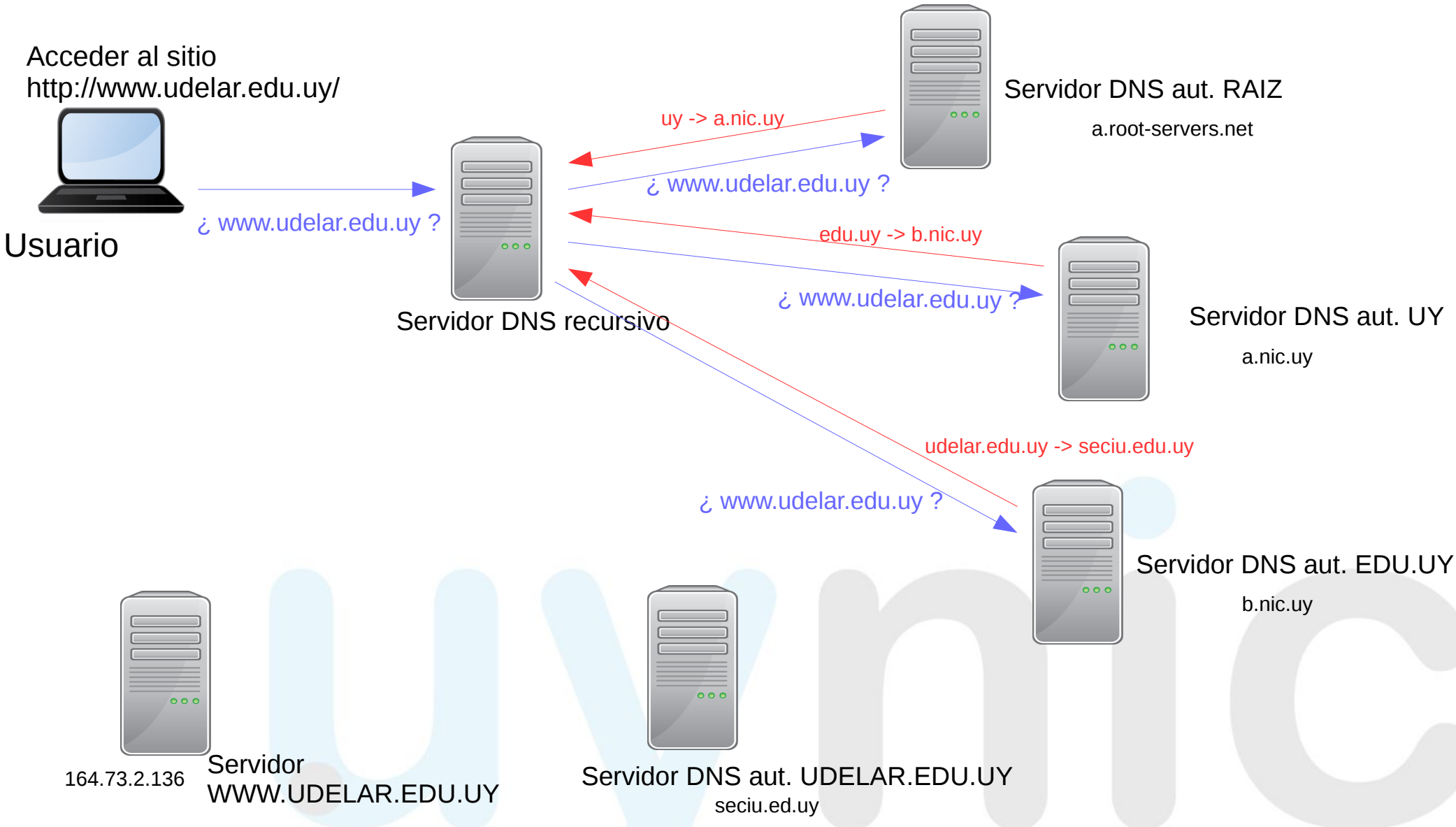
¿ Cómo funciona el DNS ?



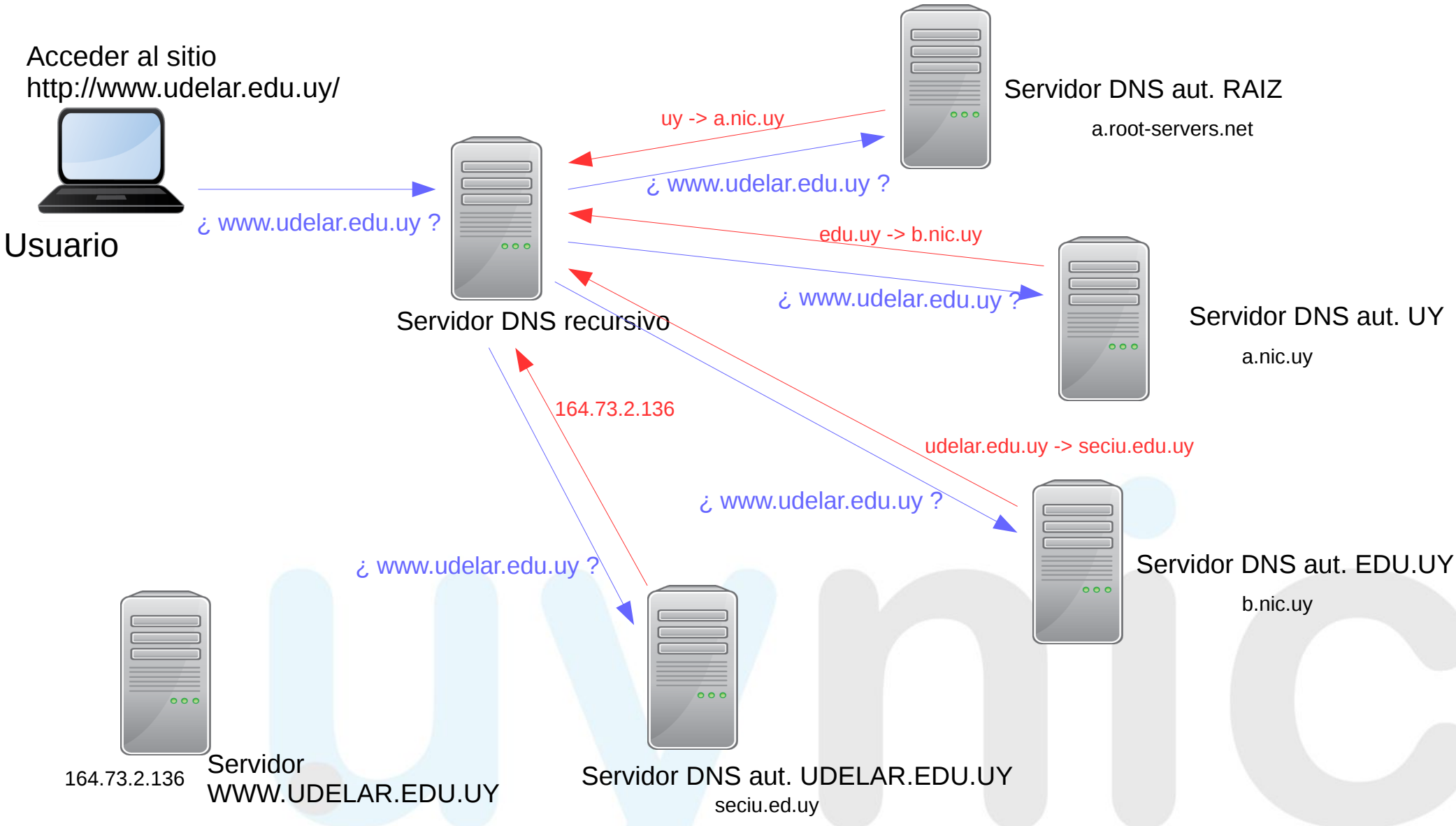
¿ Cómo funciona el DNS ?



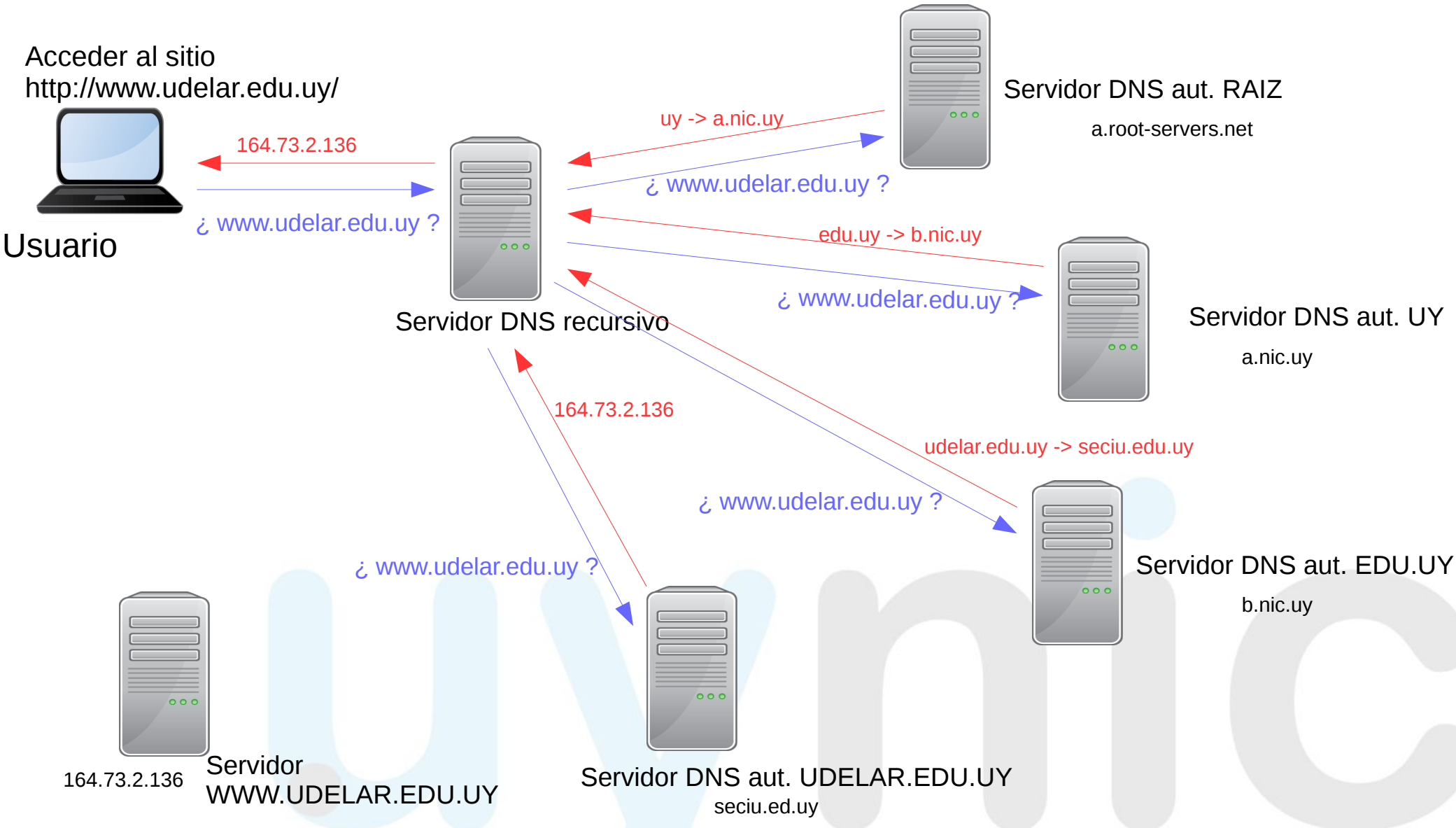
¿ Cómo funciona el DNS ?



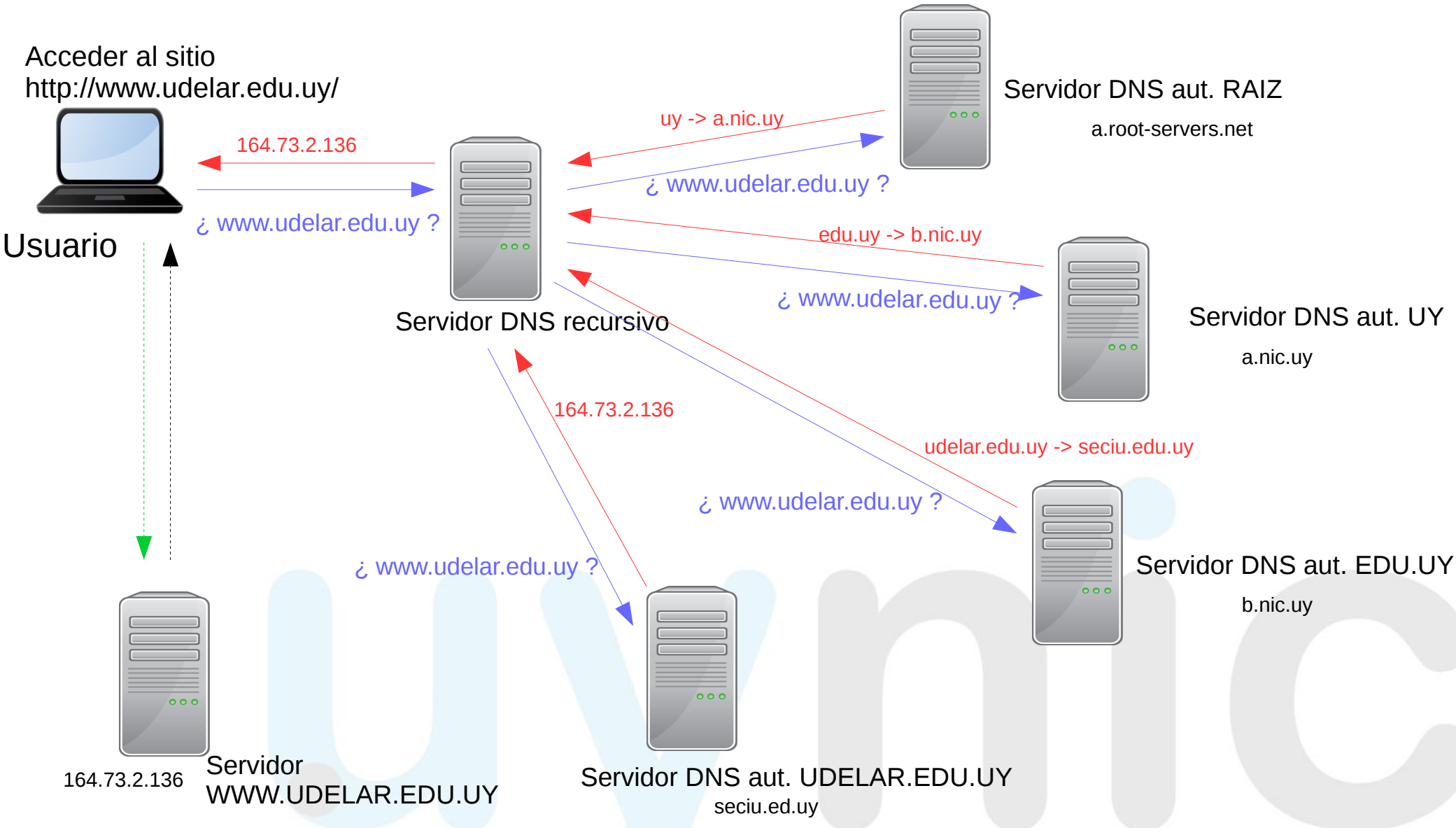
¿ Cómo funciona el DNS ?

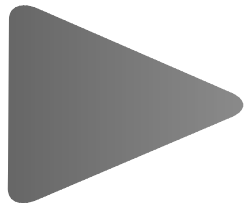


¿ Cómo funciona el DNS ?



¿ Cómo funciona el DNS ?

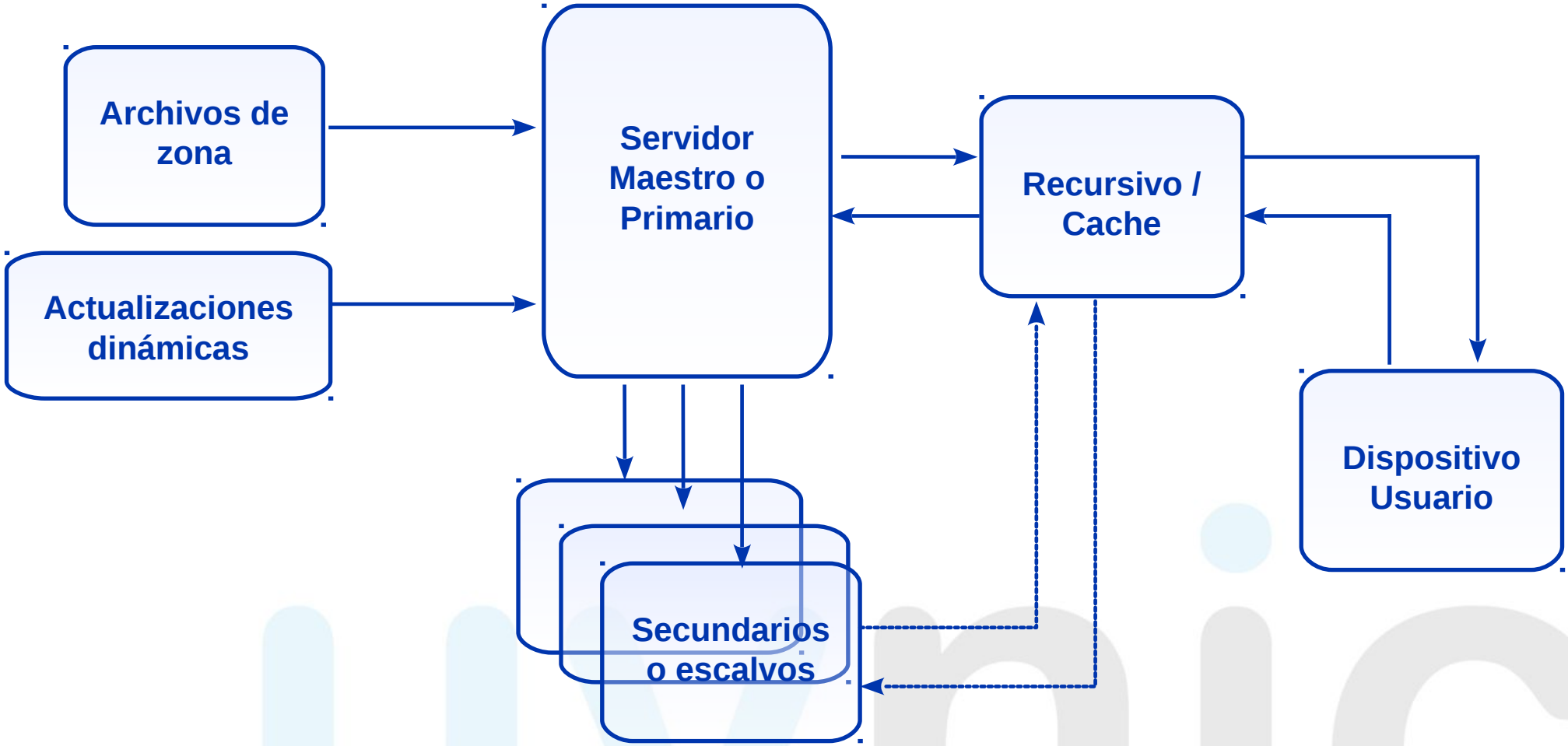




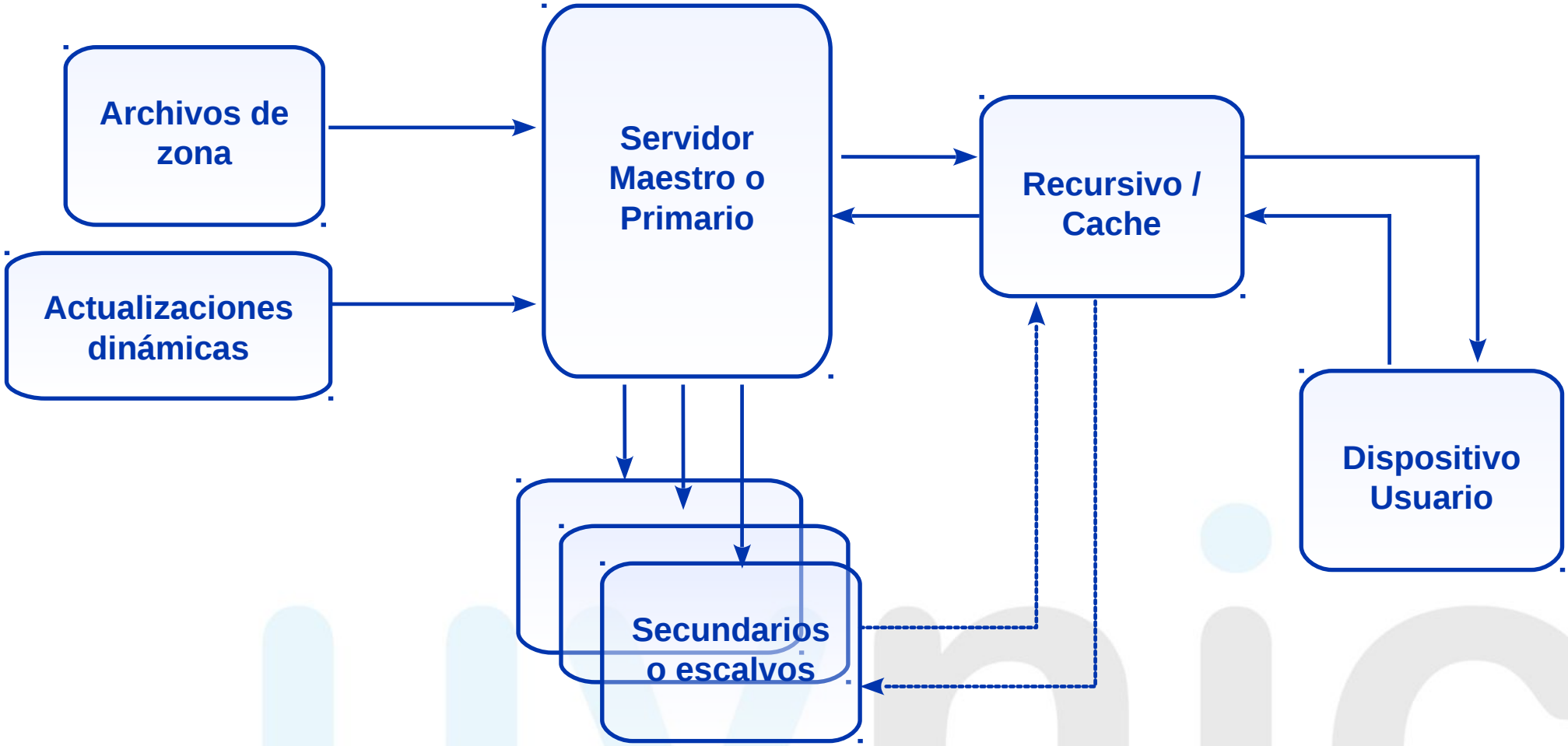
El DNS es parte de la infraestructura crítica de Internet

- Prácticamente todas las aplicaciones de internet necesitan hacer uso del sistema DNS:
  - Envío y recepción de correo
  - Búsquedas de información
  - Acceso a sitios web (varias URLs referenciadas por c/página)
  - Sesiones SIP (llamadas de voz, video)
  - Otros
- Es necesario mejorar la seguridad del sistema original del DNS.

Flujo de datos del DNS

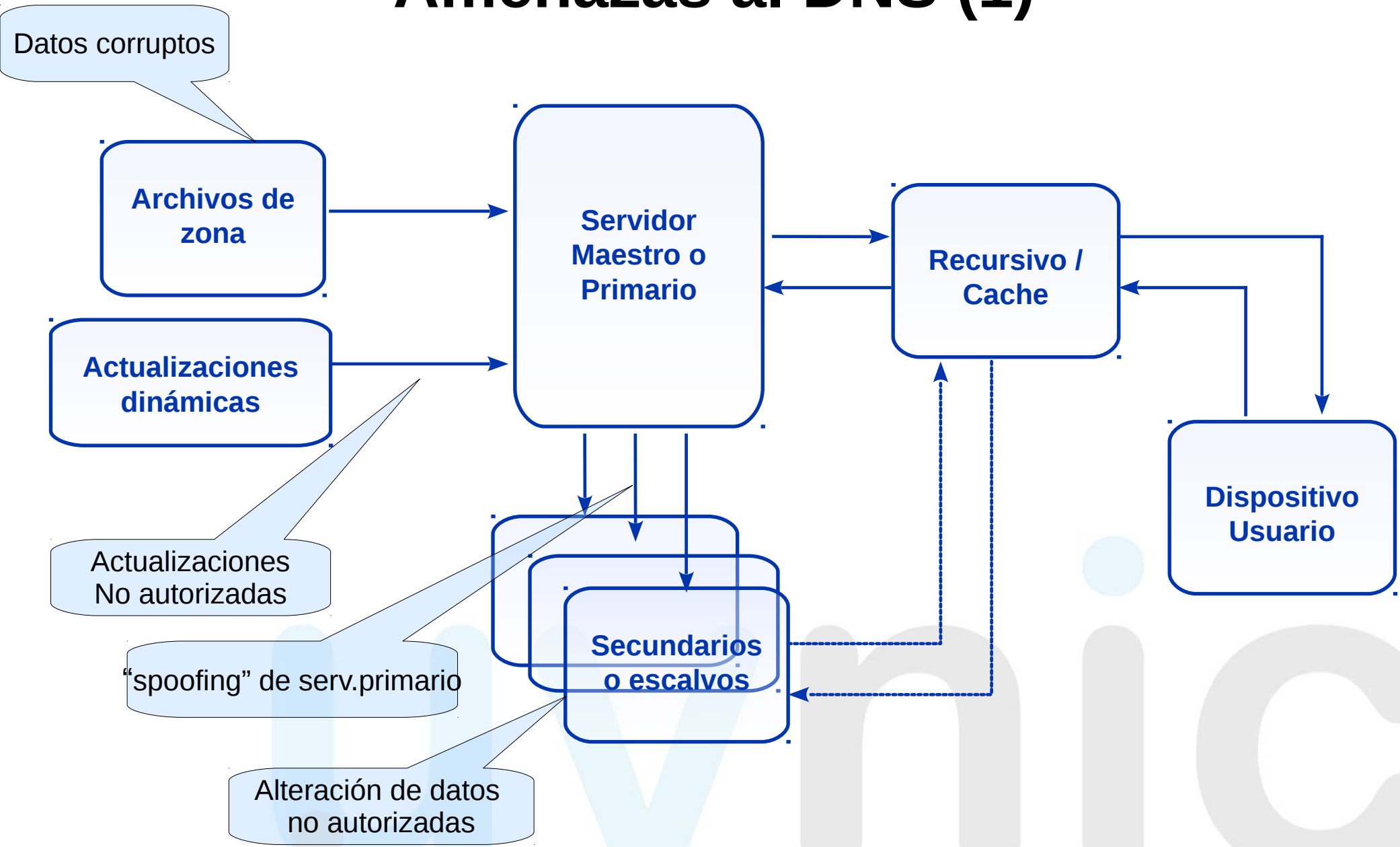


Amenazas al DNS (1)

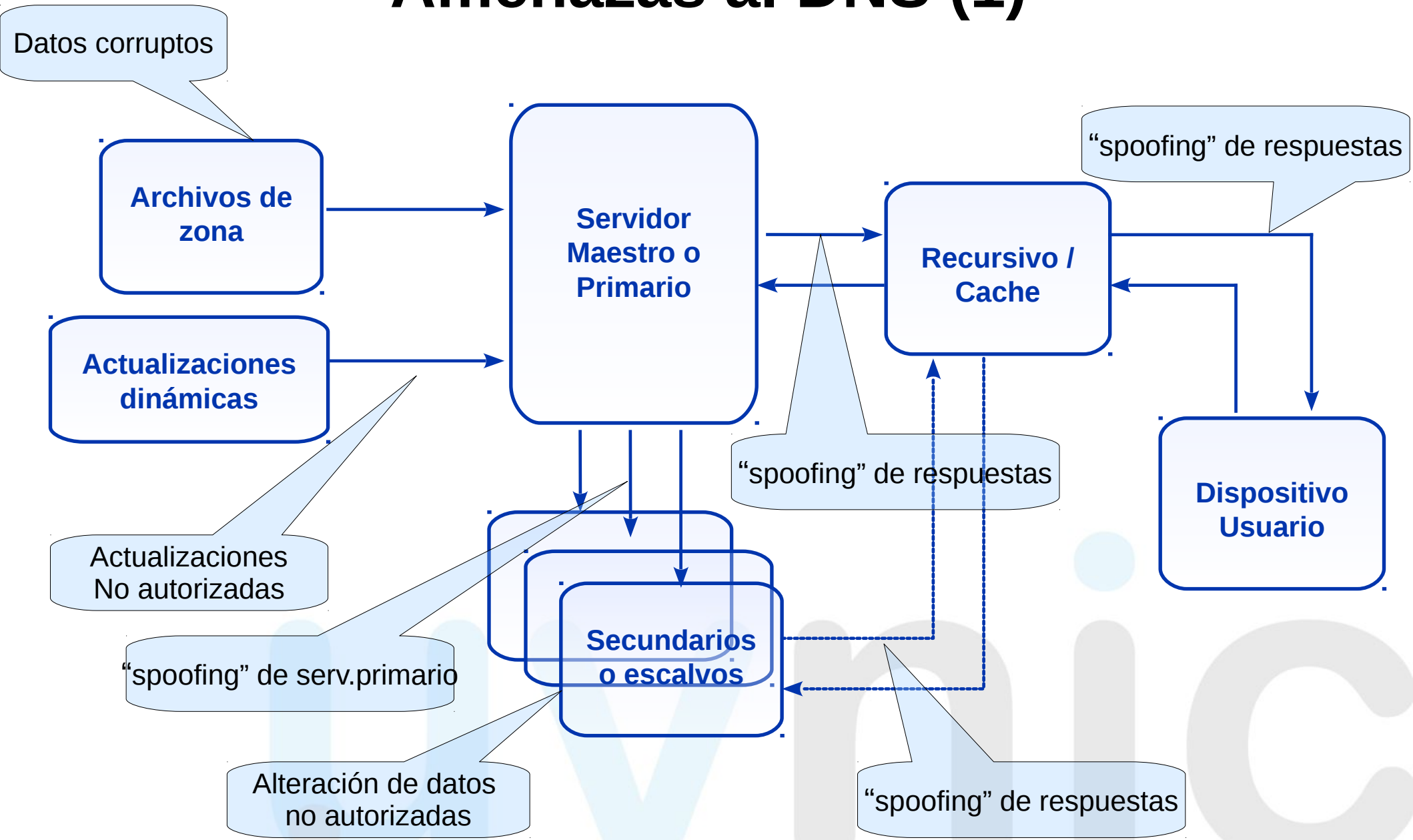


Amenazas al DNS (1)

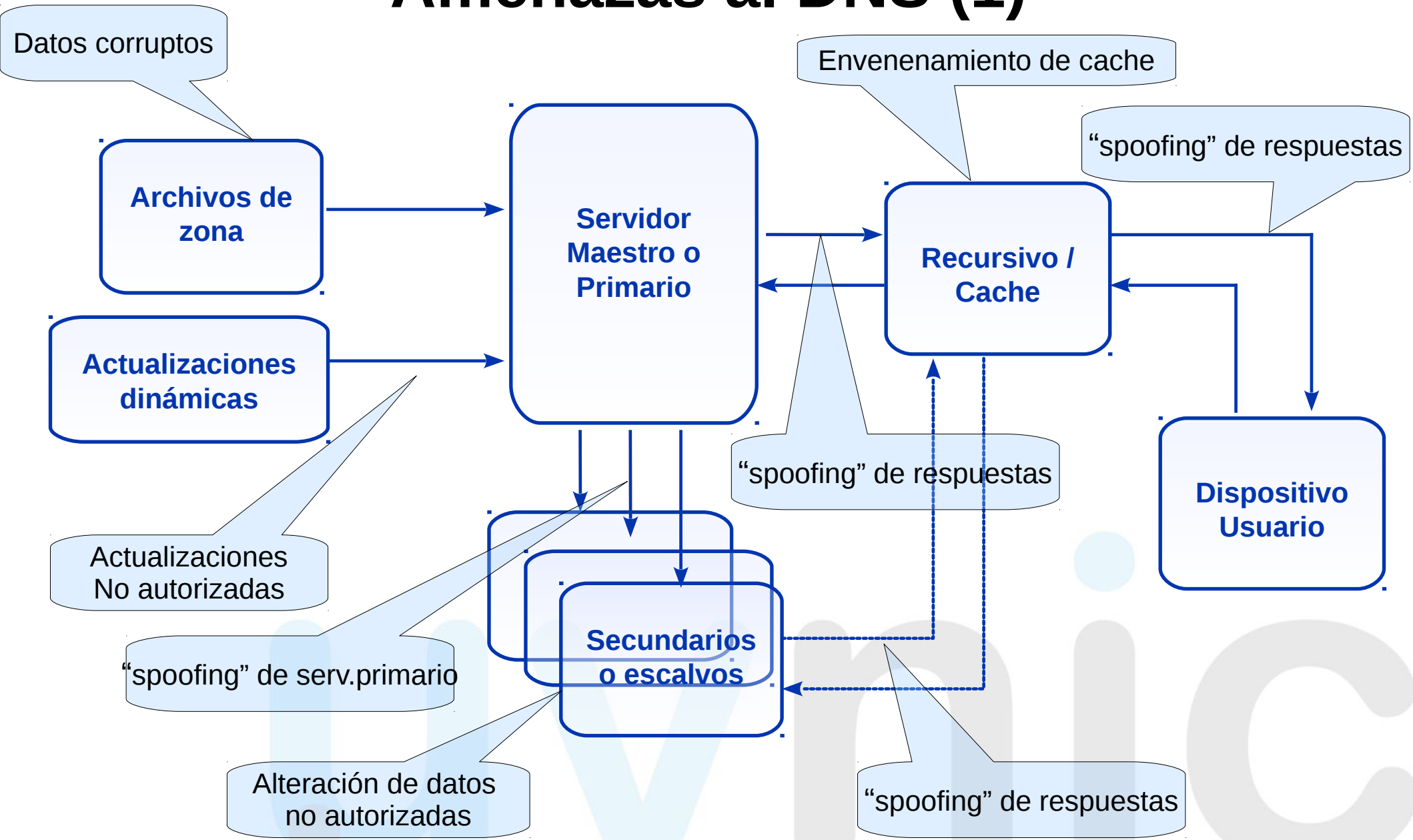
Amenazas al DNS (1)



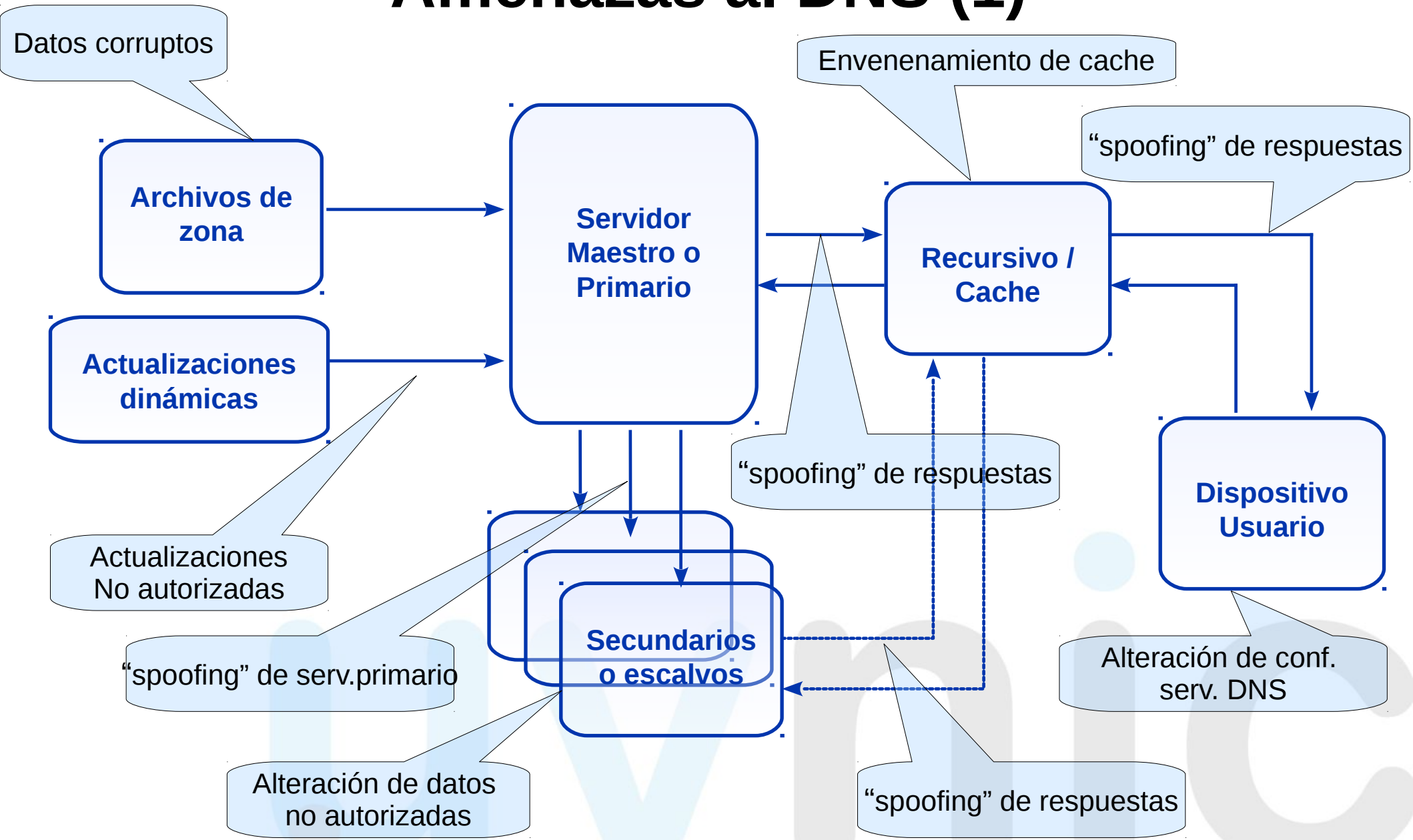
Amenazas al DNS (1)



Amenazas al DNS (1)



Amenazas al DNS (1)



Amenazas al DNS (2)

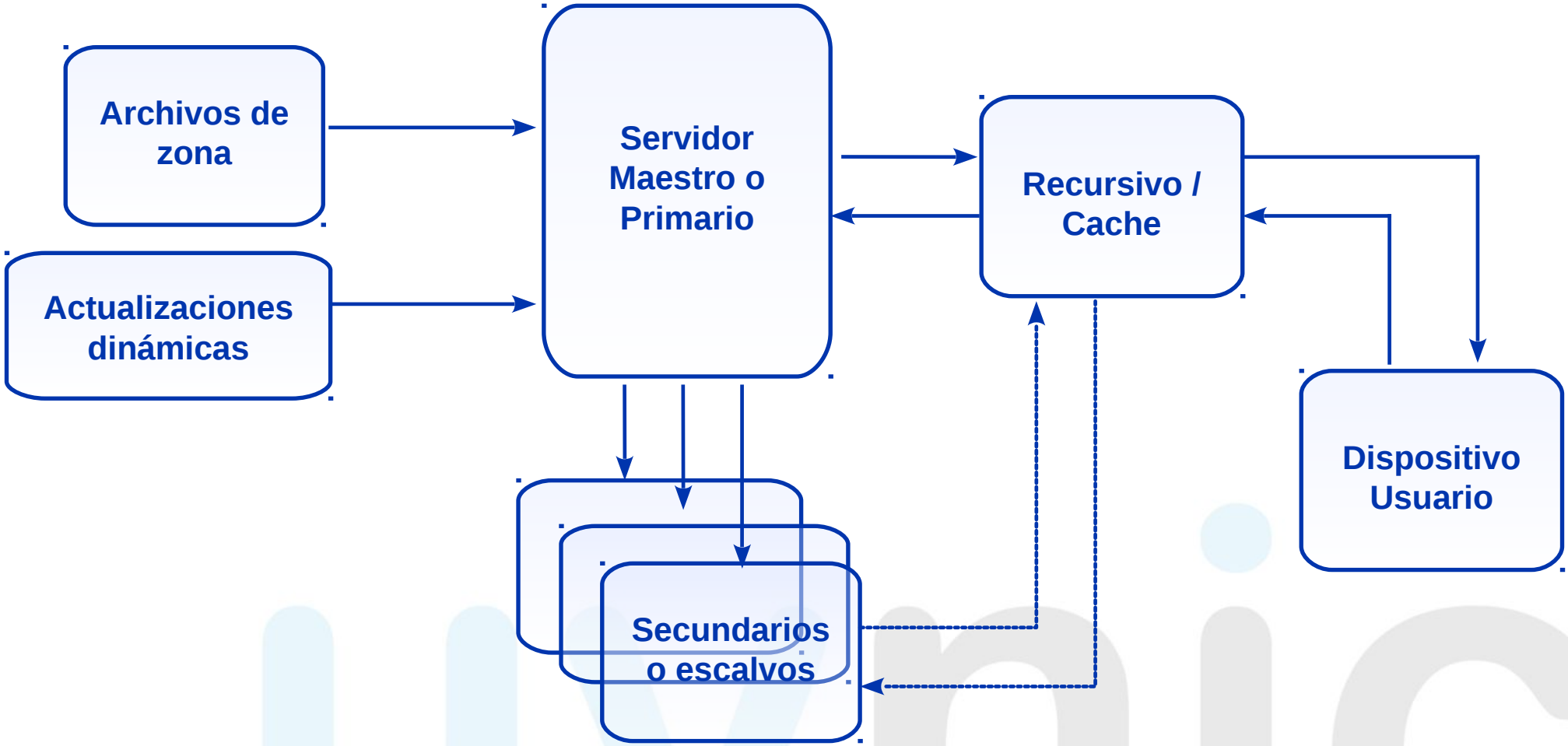
- La información transmitida por los sistemas DNS puede ser interceptada y/o manipulada
  - Entre primario y secundario (al hacer las transferencias de zona)
  - Entre autoritativos y recursivos
  - Entre recursivos y clientes (resolvers)

- El protocolo DNS no permite validar la información contenida en una respuesta
  - Vulnerable a las diferentes técnicas de envenamiento de caché.
  - Datos erróneos causan problemas hasta que se venza el TLL del RR.

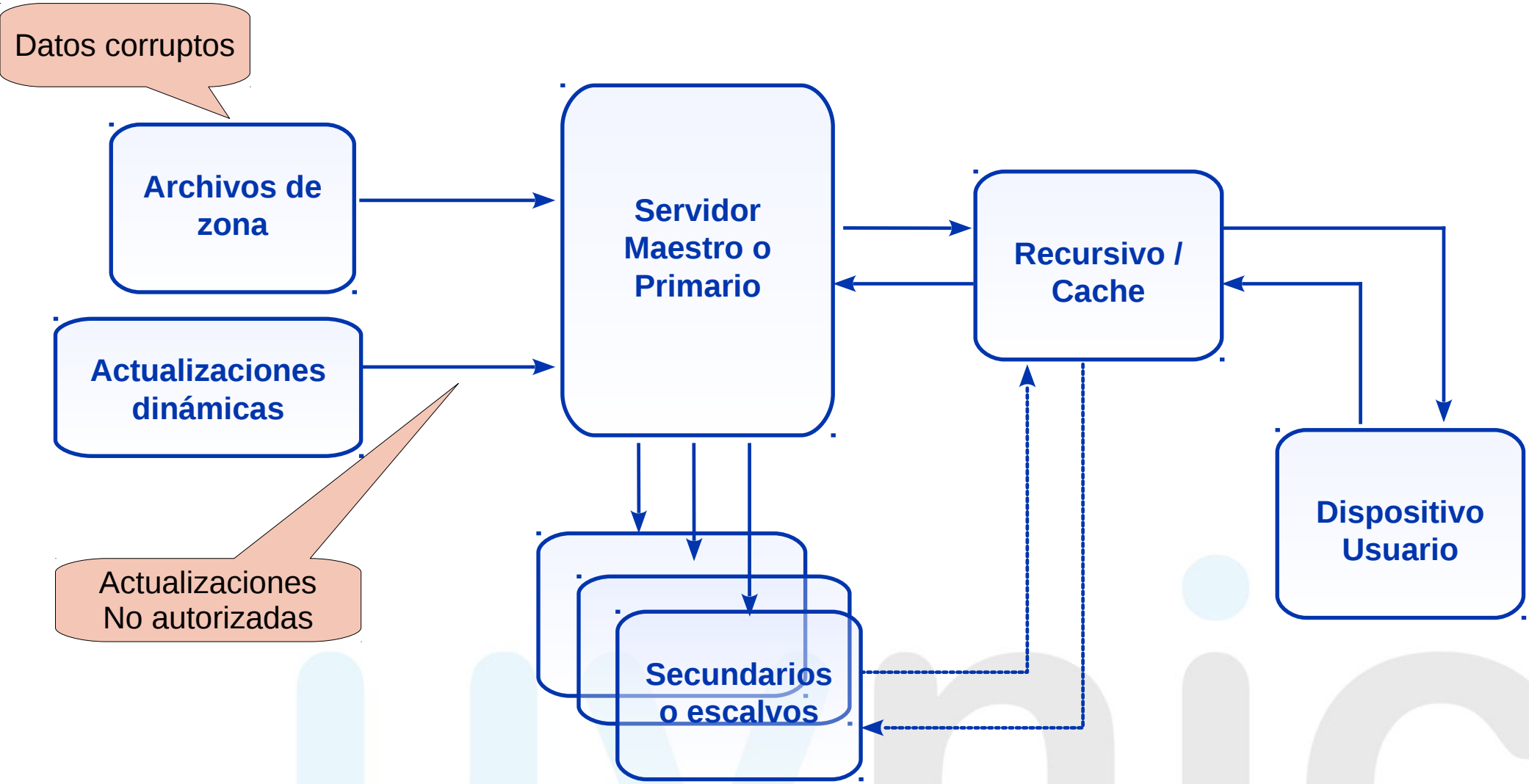
DNSSEC
(Extensiones de Seguridad al protocolo DNS)

- Provee autenticación de origen e integridad de datos
- Provee mecanismos para autenticación de negación de existencia de RR.
- Permite verificar la información de extremo a extremo (de servidor autoritativo a resolver)
- Proporciona mecanismos para delegar la confianza en la delegación de zonas (cadena de confianza)

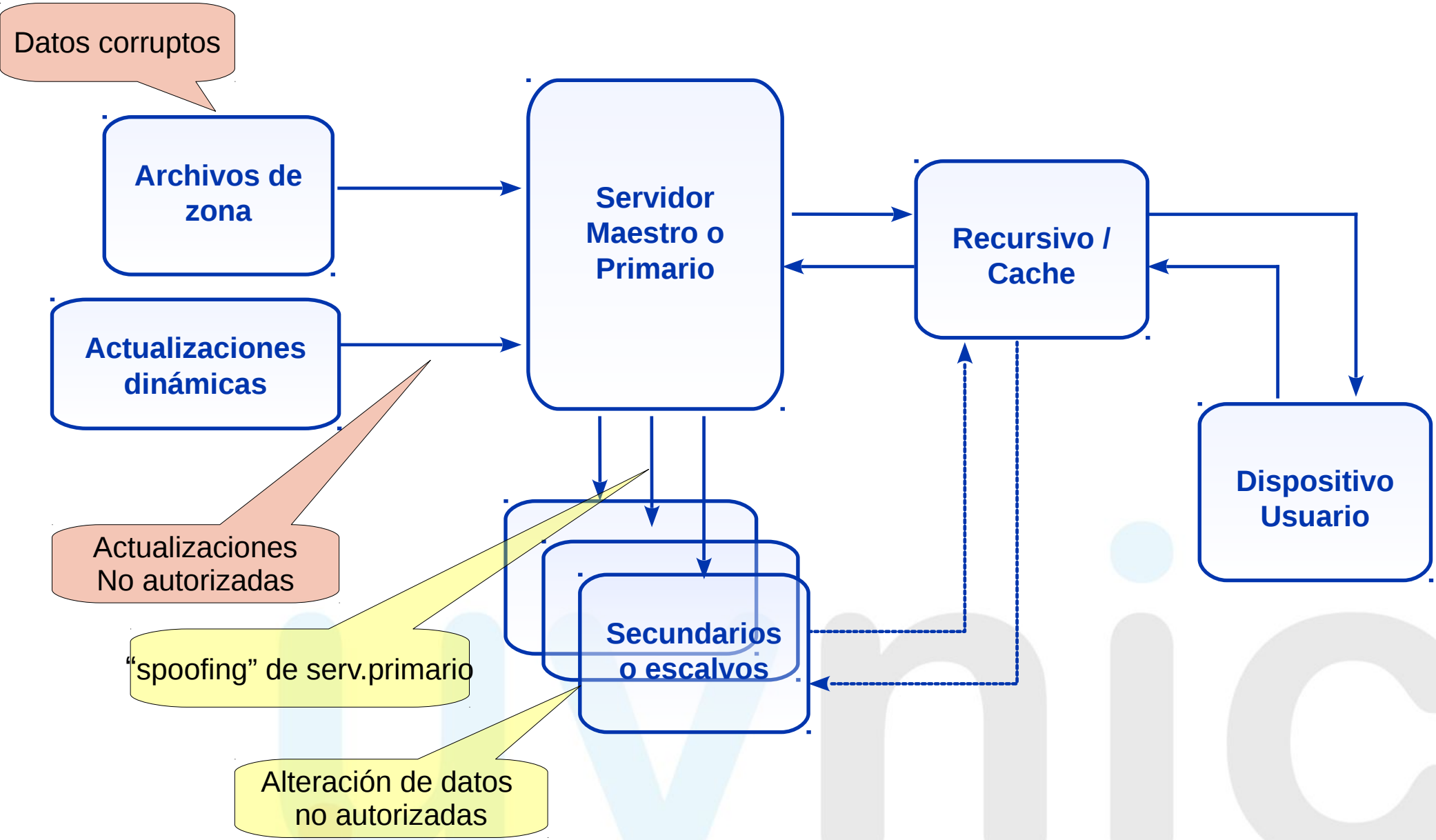
Amenazas al DNS (3) / DNSSEC



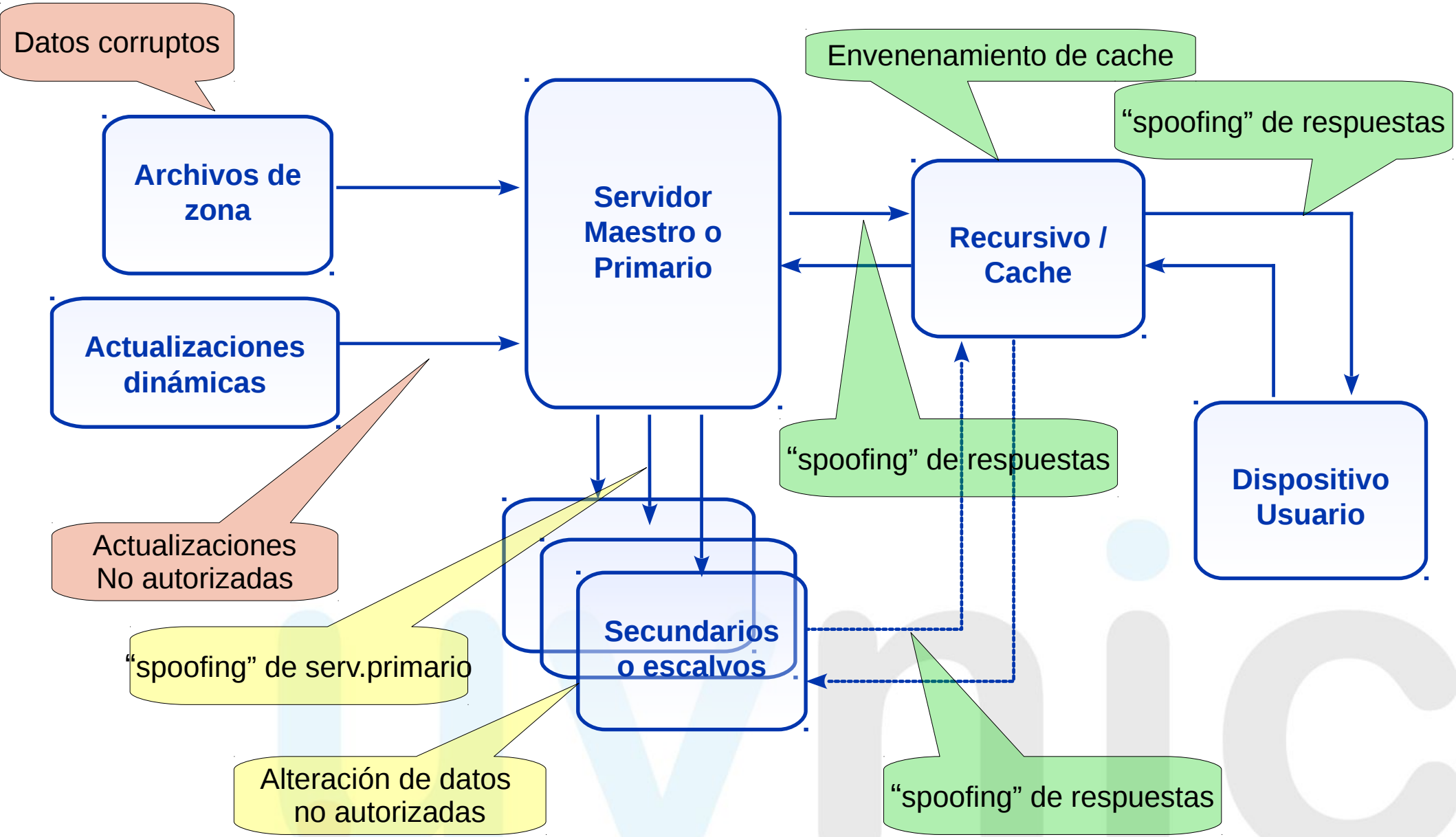
Amenazas al DNS (3) / DNSSEC



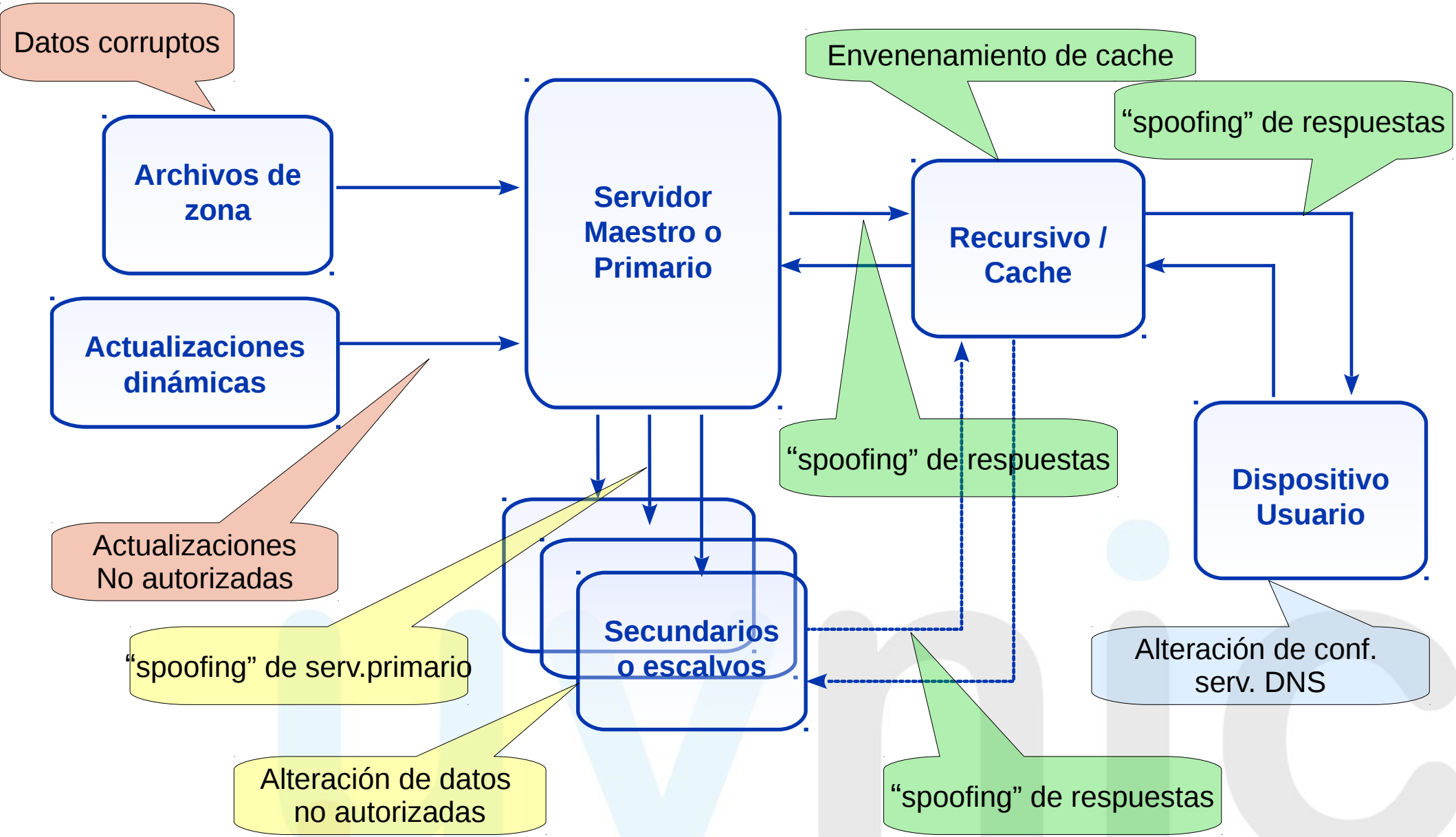
Amenazas al DNS (3) / DNSSEC



Amenazas al DNS (3) / DNSSEC



Amenazas al DNS (3) / DNSSEC

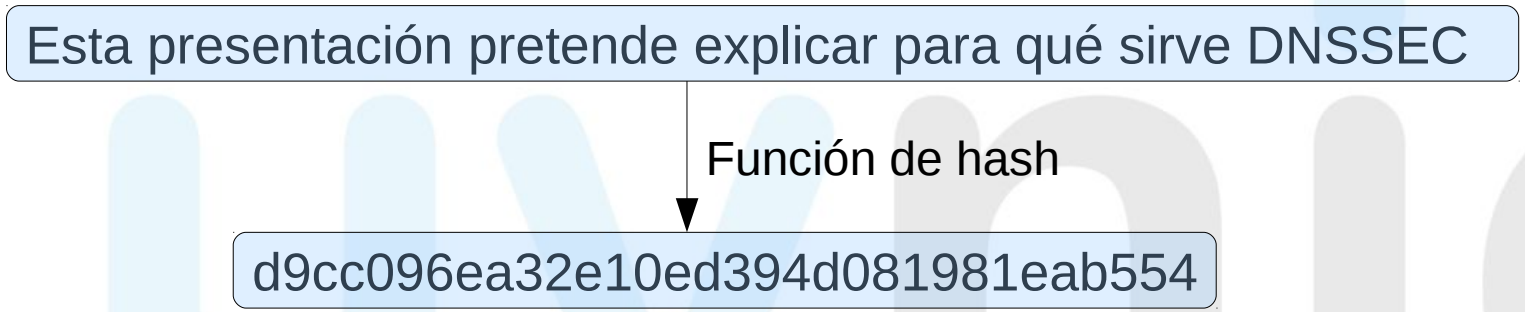


Repaso de Criptografía

- Algoritmos de hashing
- Cifrado de clave pública
- Firma digital
- Cadena de confianza

Repaso de Criptografía

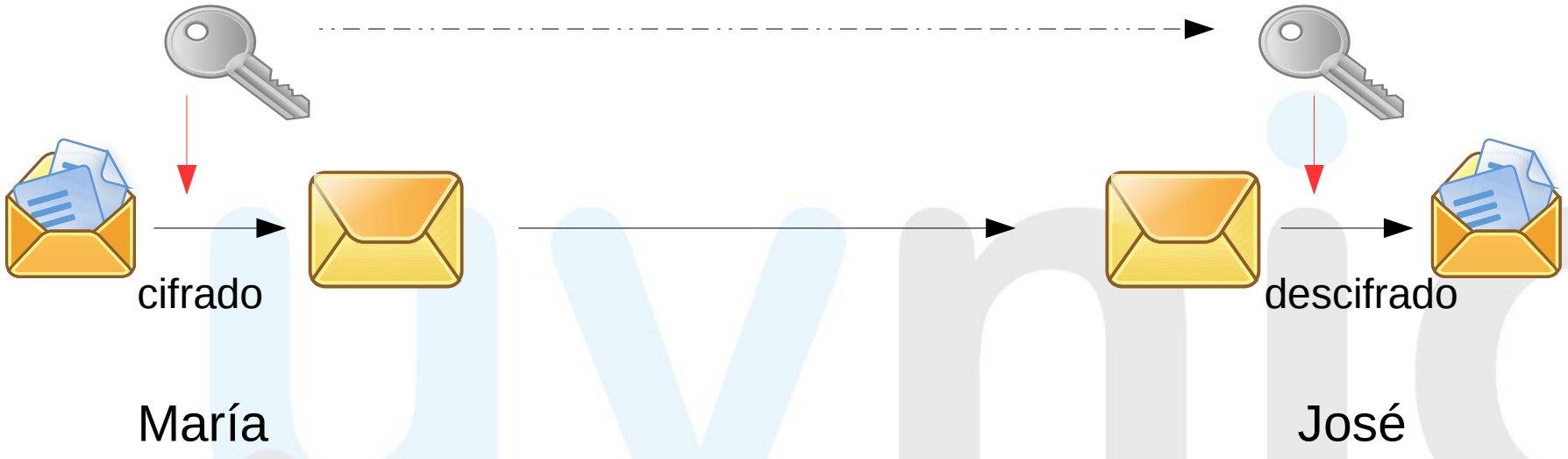
- Función hash:
  - Toma una cadena de largo variable y la convierte en una de largo fijo.
- Función “one-way” hash:
  - Es díficil encontrar la entrada original a partir del hash.
  - Es díficil encontrar 2 entradas diferentes que generen el mismo hash.



Repaso de Criptografía

Llave simétrica

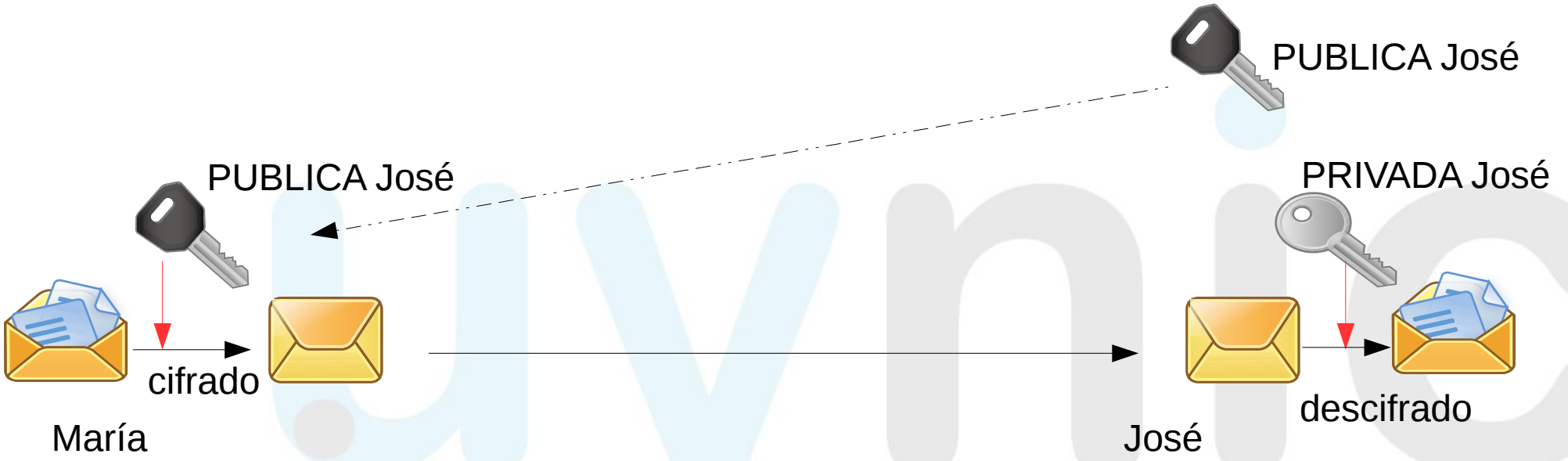
- Se utiliza la misma llave para cifrar y para descifrar la información.
- La llave solo debe ser conocida por el emisor y el receptor



Repaso de Criptografía

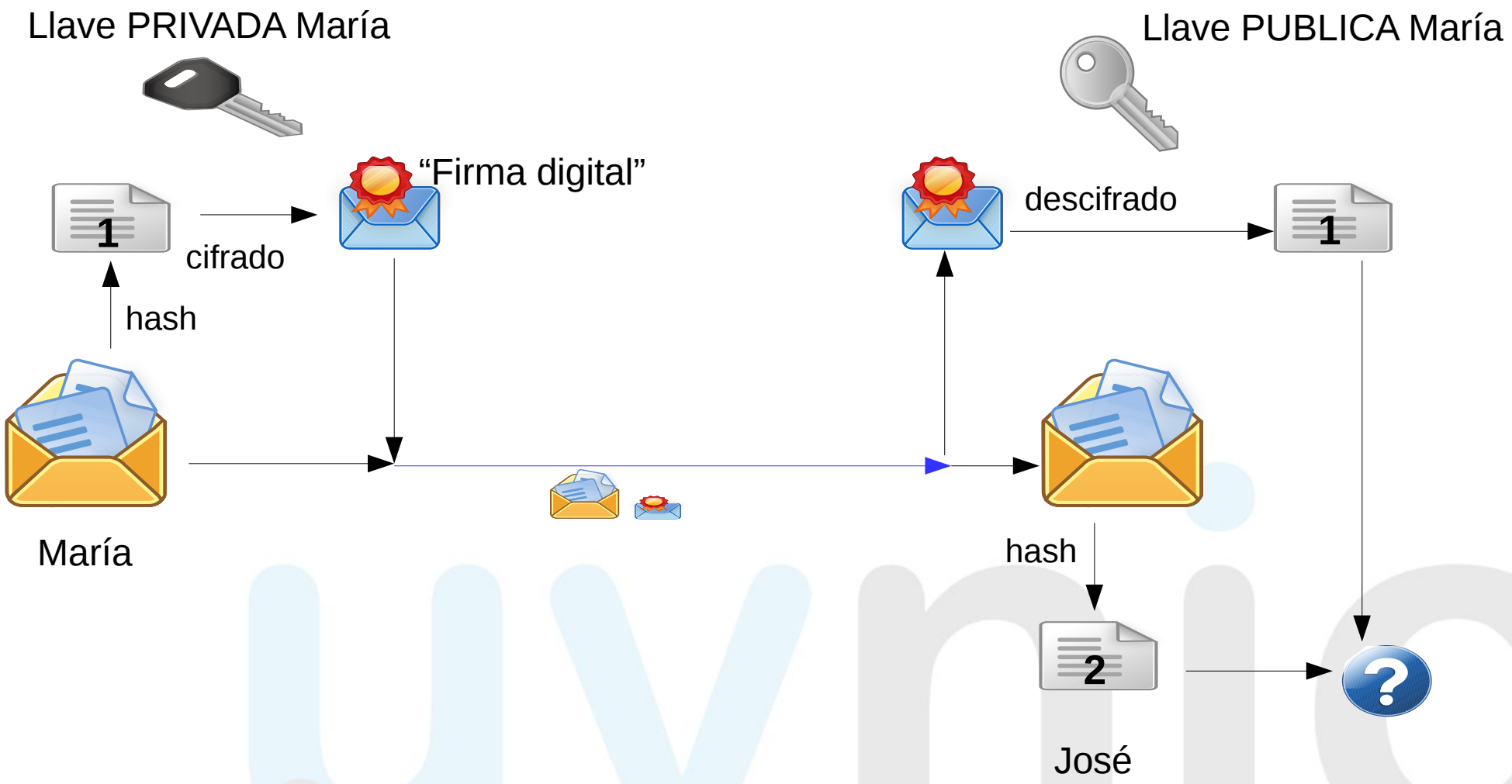
Llave asimétrica

- Se utilizan 2 llaves matemáticamente ligadas entre sí.
  - Una llave privada
  - Una llave pública
- Es muy difícil obtener la privada a partir de la pública
- Usos: para cifrar un mensaje y/o para firmar digitalmente un mensaje.



Repaso de Criptografía

Firmado digital



Repaso de Criptografía

Firmado digital

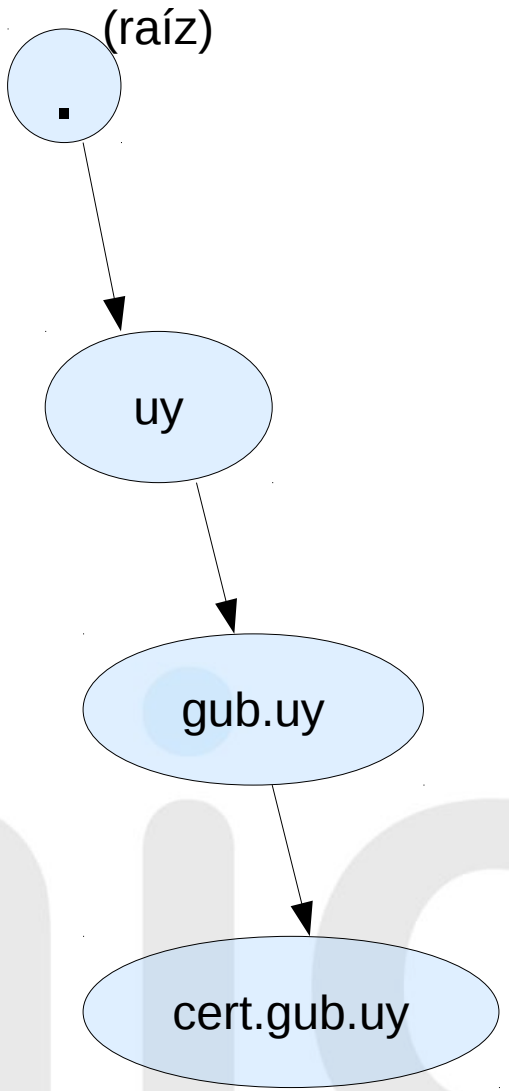
- **Emisor**
  - Genera un “one-way hash” del mensaje
  - Cifra el hash generado con su clave privada
  - Envía el mensaje “en claro”, junto con el hash cifrado (firma)

- **Receptor**
  - Recibe el mensaje “en claro” junto la firma
  - Le aplica la función de hash al mensaje recibido
  - Descifra la firma con la clave pública del emisor
  - Compara el hash del mensaje con la firma descifrada
    - Si son iguales, queda verificado el mensaje

Repaso de Criptografía

Cadena de confianza

- Cada nivel de una jerarquía firma material de la siguiente
- La raíz debe de ser considerada de forma “especial”: firmada por un organismo central, en el cual todos confíen
- Se puede validar en forma ascendente y descendente



DNSSEC

- Mecanismo para validar integridad y autenticidad de los datos contenidos en una zona:
  - Los registros de la zona son firmados digitalmente con la llave privada (ZSK) de administración de la zona.

- Mecanismo para poder establecer la confianza en la delegación de dominios:
  - Las llaves usadas en una zona (KSK) son firmadas en la zona padre que delega el dominio.

DNSSEC

Nombre	TTL	Clase	Tipo	RRDATA
rau.edu.uy.	86400	IN	DNSKEY	256 3 8 AwEAAacIaWlaQGgqcRqu2F.....
rau.edu.uy.	86400	IN	DS	29392 8 2 6261FDE83E...
www.rau.edu.uy	86400	IN	RRSIG	SOA 8 2 86400 20151013143653 20150913143701 9085 rau.edu.uy. SyYGRA.....
6QAPO5.rau.edu.uy.	86400	IN	NSEC3	1 1 10 834AB2 R6P1S.....A RRSIG

- Se agregan 4 nuevos tipos de registros:
  - **DNSKEY:** DNS public Key
  - **DS:** Delegation Signer
  - **RRSIG:** Resource Record Signature
  - **NSEC/NSEC3 :** Next Secure

DNSSEC
Registro RRSIG

- DNSSEC firma “RRsets”, no RR individualmente
- Los RR se agrupan para formar los RRsets según tengan el mismo “nombre,clase y tipo”
- Ejemplo de “RRset”
  - asiap.org. 86400 IN NS ns3.montevideo.com.uy.
  - asiap.org. 86400 IN NS ns2.montevideo.com.uy.
  - asiap.org. 86400 IN NS ns1.montevideo.com.uy.
- Las firmas digitales del RRset son almacenadas en el registro RRSIG

  asiap.org. 86400 IN **RRSIG** NS 8 2 86400 20150925061251 20150904160850 26742 asiap.org. **G11AJOO1tQKVGJ.....**

DNSSEC
Registro RRSIG

- DNSSEC firma “RRsets”, no RR individualmente
- Los RR se agrupan para formar los RRsets según tengan el mismo “nombre,clase y tipo”
- Ejemplo de “RRset”
  - asiap.org. 86400 IN NS ns3.montevideo.com.uy.
  - asiap.org. 86400 IN NS ns2.montevideo.com.uy.
  - asiap.org. 86400 IN NS ns1.montevideo.com.uy.
- Las firmas digitales del RRset son almacenadas en el registro RRSIG

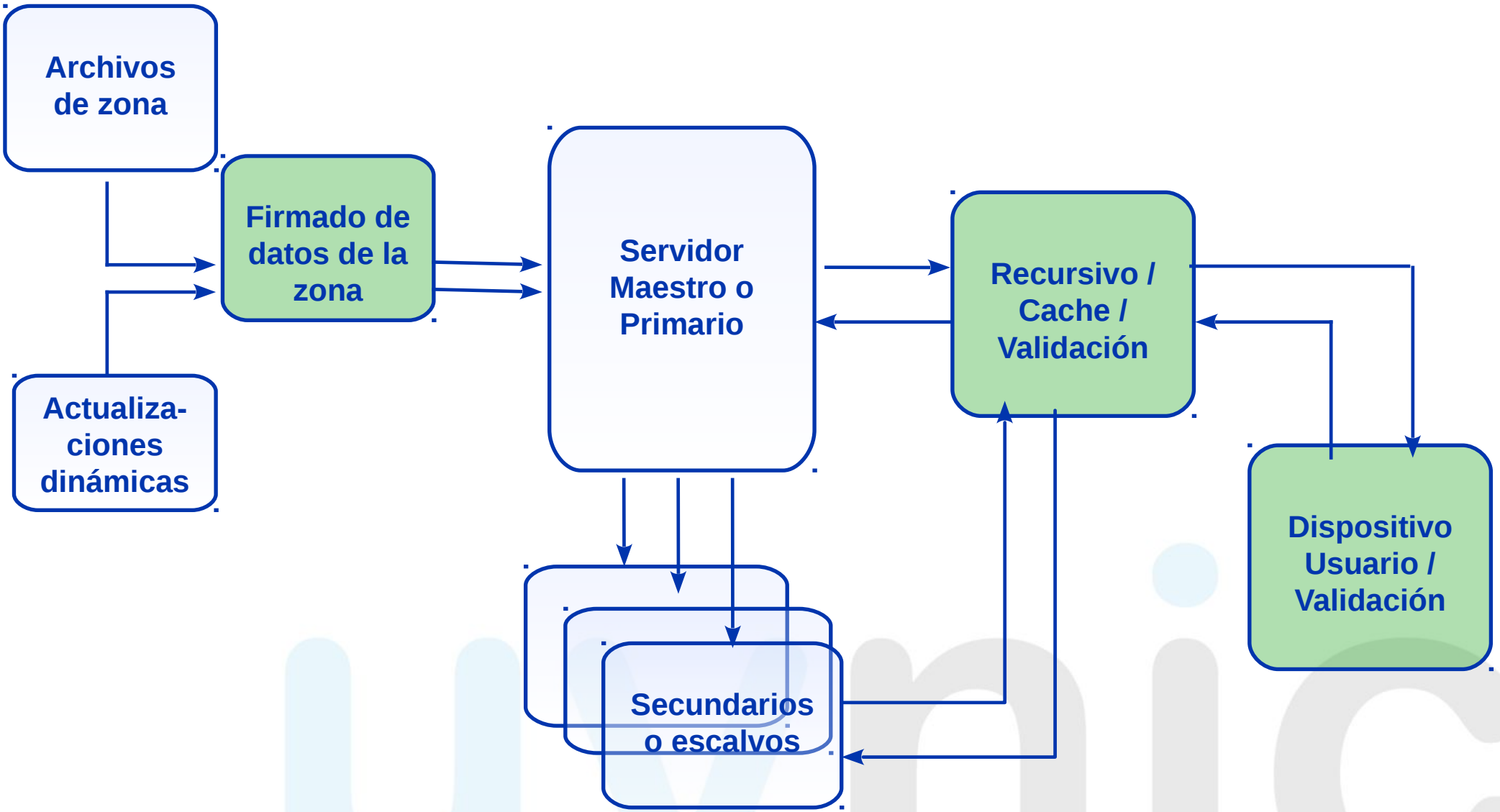
  asiap.org. 86400 IN **RRSIG** NS 8 2 86400 20150925061251 20150904160850 26742 asiap.org. **G11AJOO1tQKVGJ.....**

DNSSEC
Registro RRSIG

- DNSSEC firma “RRsets”, no RR individualmente
- Los RR se agrupan para formar los RRsets según tengan el mismo “nombre,clase y tipo”
- Ejemplo de “RRset”
  - asiap.org. 86400 IN NS ns3.montevideo.com.uy.
  - asiap.org. 86400 IN NS ns2.montevideo.com.uy.
  - asiap.org. 86400 IN NS ns1.montevideo.com.uy.
- Las firmas digitales del RRset son almacenadas en el registro RRSIG

  asiap.org. 86400 IN **RRSIG** NS 8 2 86400 20150925061251 20150904160850 26742 asiap.org. **G11AJOO1tQKVGJ.....**

Flujo de datos del DNS / DNSSEC



DNSSEC

```
; <<>> DiG 9.9.5-3ubuntu0.5-Ubuntu <<>> uy ns
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51865
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 15

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;uy.                    IN    NS

;; ANSWER SECTION:
uy.             300    IN    NS    uy.cctld.authdns.ripe.net.
uy.             300    IN    NS    a.nic.uy.
uy.             300    IN    NS    ns3.nic.mx.
uy.             300    IN    NS    ns.dns.br.
uy.             300    IN    NS    ns2.anteldata.com.uy.
uy.             300    IN    NS    ns1.anteldata.com.uy.
uy.             300    IN    NS    sns-pb.isc.org.
uy.             300    IN    NS    b.nic.uy.
```

DNSSEC

```
; <<>> DiG 9.9.5-3ubuntu0.5-Ubuntu <<>> @8.8.8.8 uy ns +dnssec

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30405
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;uy.                    IN    NS

;; ANSWER SECTION:
uy.             299    IN    NS    b.nic.uy.
uy.             299    IN    NS    ns1.anteldata.com.uy.
uy.             299    IN    NS    ns3.nic.mx.
uy.             299    IN    NS    uy.cctld.authdns.ripe.net.
uy.             299    IN    NS    ns2.anteldata.com.uy.
uy.             299    IN    NS    a.nic.uy.
uy.             299    IN    NS    sns-pb.isc.org.
uy.             299    IN    NS    ns.dns.br.
uy.             299    IN    RRSIG    NS 8 1 300 20151013151456 20150913151502 56685 uy.
PfkKZaM/RCCzrJaPtUS/DYj3RzxeSoamg8o4h4ExX8892iVUpiI7l2kW
9fDm1a9n950SkgKLDG/HSUwDP12l+0MOA+97cxmWfExlz/8Cug0AQYxm
ElsJZj0tW3Fk6wkyijNUnJYeULGb++nHhfwja8yRRqBHfIHdVzkuQYQj
uLuu87wjEFibk6nAwlxS9Pm4fxtErErUTp3ju1gd739tym4ErD+uwR8O
9JdY1T6YzYDEclyifFPYlqox9i8MRVrMNt6/naddZlTJw5rwuJRzfrEN
p1+GE+f0UPdnRmuKyHpCkWqWmbBHYKXEi65wLYYBq3gxsP9b+iPQP8Qm pa5MkQ==
```

DNSSEC

Llaves / Registro DNSKEY

- Para cada zona hay que generar las llaves asimétricas. Estas llaves se asocian a zonas (no a servidores).
- La llave privada se utiliza para firmar la zona (generando los registros RRSIG) y debe ser mantenida en secreto.
- La llave pública se utiliza para autenticar la validez de los registros firmados.
- La forma de hacer disponible las llaves públicas es a través del propio sistema DNS, con el registro DNSKEY.

DNSSEC

Llaves / Registro DNSKEY

```
uy.          86400 IN DNSKEY  256 3 8 (
                 AwEAAcR8BVVqMtX1BI+NkOvwnWog76/0f+UZiYY67FFI
                 llwaqha0IAVaNDgaJ3YqR8OY7uOt2uE08onr4Ecr4Ii0
                 VA2IMQlpOUioe7Wn4GjAW7arRAuAX+QWWesixZly+HTf
                 6PUXnJRrP/1f2lzDSg2Hb+vDsbesRqULT1ZoHxMicP/9
                 Pdnt9WdHpT/Zbf+8BlTMleGyOjbKgyAWIGMyHOr+ukgl
                 FnMmlRH5PpMa9CDRvAUlNfICplCldXCmn9A4UUkRPLdt
                 FG9/YkOtYkUbOMV4G4158Vjlm9ldaBSYlt7DBYyTmJiv
                 3RoWUB8UJHRZv0YmNlgcRmqArvrS0Sp9HY/Y8U0=
                 ) ; ZSK; alg = RSASHA256; key id = 56685
```

DNSSEC

Llaves / Registro DNSKEY

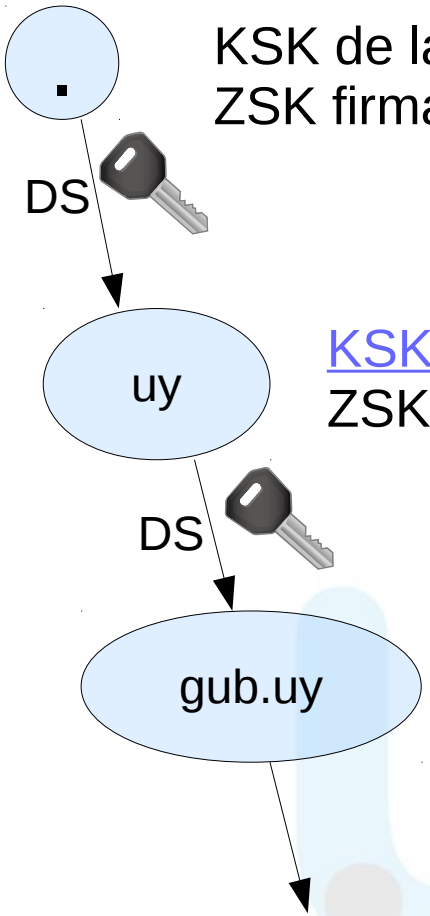
```
uy.        86390 IN DNSKEY 257 3 8 (
                AwEAAdobCN40xS32echTWqQ2ifnSQD1dvf8WIgHRsYYs
                gZ+yC/3pMZ0mrrewlNm/FblMbPMzIDVYNtmeQwxa4bZA
                Zrh8W6mW0itIOuitdeIdYBdj8+IKMdSuev14HOqGGaim
                XCPPUaZ0czaP/E6aqh2N3QfmSbxq78ZNs69AeJJ9LXwl
                oQs9BQ0ogaMnqs/xmqmpFn0eFQHTxa33xkxikd4s3A7Y
                cH35tHSpmGvaQWSetSxJjB2rMMUeC8uM6bE7j90DRT2/
                +XF5mB8Zb8I9Ceyogb0cFS9AsrfeEMpthF5Q3bwFuZf6
                o3W9z1msnTgP74LTRImr05ylKna3Xf2pxT9pzYHPmTvP
                oOxfXwJK61c9+4J1nLyAjjECRvztk4SHAgZY2yaWJpGt
                HRxeaf17tgjtdA7LFC1yGKGlOct3m5BnYiRqw+QYI7WN
                W6KC5YHEO1HnfGzbjyZw8enVsDGoegjCZiFur1wXFBE8
                uClx2sHxrgH2q/pLOIoWG3JCEexE7mjM6fQOSZFsbtOR
                BU2v3IRUaijYFVUCactfdkl89yEYydTUmn1fJFGOYftd
                952yKlACr207JoN+PFTLeV49U+5e7hfY2l3p1zllrxCG
                C7iJlyQeDvDE0EuEMCa+SR5DEEUZONHCdDIek2YYYYuc
                496JWd43hnH85nmoKTQq9ykSrEbv
                ) ; KSK; alg = RSASHA256; key id = 19730
```

DNSSEC
Llaves / Registro DNSKEY

- Operativamente se usan 2 pares de llaves asimétricas:
  - ZSK (Zone Signing Key)
    - Sólo firma los registros (RR) autoritativos de la zona
    - Son cambiadas más seguido que la KSK
  - KSK (Key Signing Key)
    - Sólo firma los registros DNSKEY
    - Es de mayor largo que la ZSK, y se cambia con menos frecuencia que la ZSK
    - Se usa para establecer la cadena de confianza con la zona “padre” a través del registro DS.

DNSSEC
Llaves / Registro DS

- Para establecer y verificar la cadena de confianza desde la raíz (“.”) hasta el dominio consultado, se utiliza el registro DS.



KSK de la raíz firma ZSK de la zona “.”
ZSK firma registro DS que referencia a la KSK de .uy

KSK de .uy firma ZSK de zona .uy
ZSK firma el registro DS que referencia a la KSK de gub.uy

KSK de gub.uy firma ZSK de zona gub.uy
ZSK firma el registro DS que referencia a la KSK de cert.gub.uy

DNSSEC

Llaves / Registro DS

uy. 86400 IN DS 19730 8 2
E85A089D69F869CF923DF395F279F1C92BD136A33B60988748B0186E
12F7B88E

uy. 86400 IN RRSIG DS 8 1 86400 20150923170000
20150913160000 1518
D44f6/7FZSipzFPnIMASZq/QwPo3NOaUcyL4PiBq1Kasd/YQLrXD4fBx
2bknlAsAOY3fI8JmTFUXe2Dl98COv8Kl7zKqbcd4h6SjTFQaEeSsPzRD
NZyQ6zHc8TUsWeAQ0+ytVuH5bDrEoJNFelO+FB4h2isahoS7v/QfqGZp
TjY=

DNSSEC

Registro NSEC / NSEC3

- Los registros NSEC y NSEC3 se usan para autenticar la “no existencia” de nombres de dominio.

1N929EDS2KLPJLQR38L6KTU6L0TLTRR2.uy. 0 IN **NSEC3** 1 1 10 8349A2 25OFVNCPC8M7HKN4A80K8LTV3RKQJ7FV

5A49A1OF0403UQ2QBCFP1OSEM8BIO4UU.uy. 0 IN **NSEC3** 1 1 10 8349A2 5MJK5LMMME730HL1M4RVN79G1ORVLOHC NS SOA RRSIG DNSKEY NSEC3PARAM

DNSSEC
Resumen

- Provee mecanismos para la autenticación e integridad de los datos transmitidos por el DNS.
- Evita manipulación de las datos del DNS entre quién origina los datos y quien los recibe.
- El DNSSEC provee así una infraestructura de intercambio seguro de información en internet, la cual se podría usar para nuevas aplicaciones.
- **Para que funcione, los responsables de dominios deben firmar sus zonas y los responsables de los servidores recursivos deben validar las respuestas a la consultas.**

DNSSEC
Nuevos usos

- DANE - DNS-based Authentication of Named Entities
  - Usa el DNS seguro con DNSSEC para almacenar información de certificados asociados a un nombre de dominio.
  - El propio “dueño” del dominio publica qué certificados son confiables para usar en sus diferentes servicios.
  - DANE/TLSA define un nuevo tipo de registro, TLSA, para almacenar referencias a los certificados X.509 válidos para conectarse con el servicio.
  - Es compatible con el uso actual de los certificados emitidos por las autoridades certificadoras, aumentando la seguridad.
  - Ejemplo:

```
_443._tcp.www.example.com. IN TLSA (
    0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
          7983a1d16e8a410e4561cb106618e971 )
```

DNSSEC

Impactos operacionales

- Administradores / Operadores de zonas

  - Zonas de mayor tamaño
  - Mayor ancho de banda
  - Firmado de zonas periódicamente (validez de firmas)
  - Rotación (“rollovers”) de la llaves ZSK y KSK
  - Gestión de registro DS

- Administradores de Servidores Recursivos / Caché

  - Validación: mayor ancho de banda y mayor capacidad de procesamiento.

- Usuarios

  - Si validan en su propio dispositivo, idem adminstradores de servidores recursivos

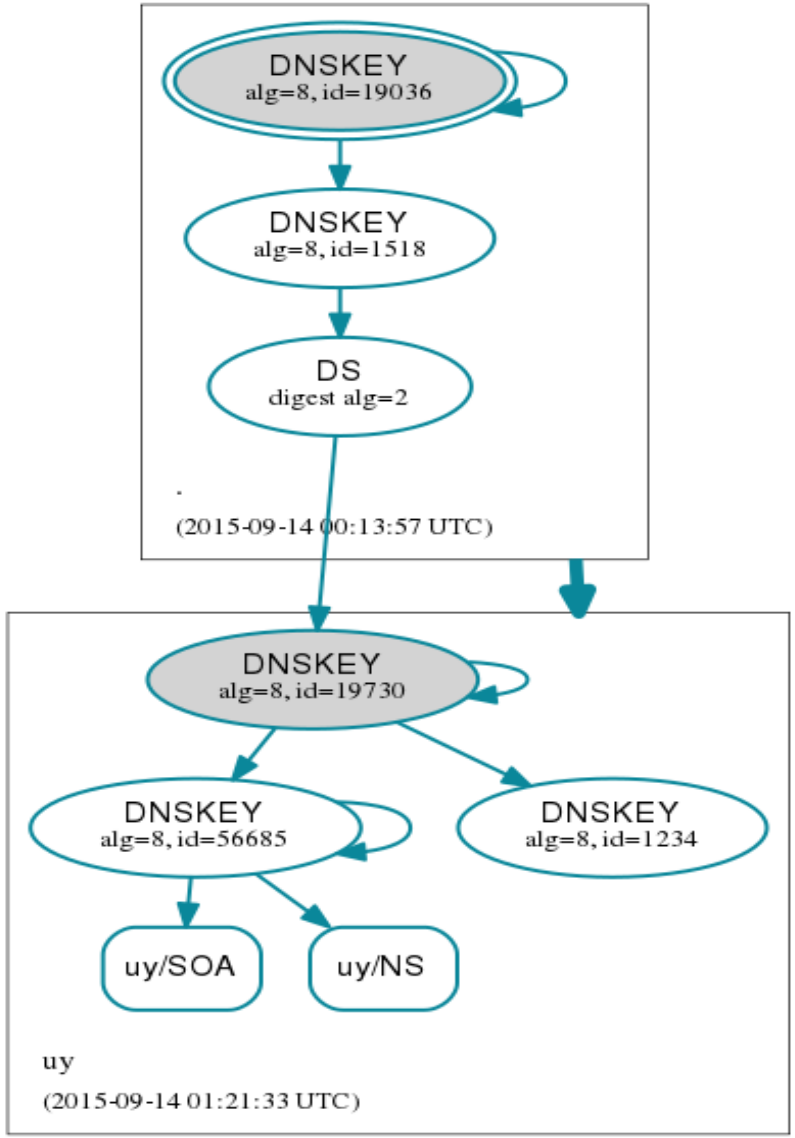
  - Si al validar una respuesta no se verifica la firma, el efecto es similar a que no se haya podido resolver el dominio, por lo que este se vuelve inaccesible.

DNSSEC en .UY

- Principios del mes de agosto/2015:
  - Primer ceremonia de generación de llaves para el firmado de la zona UY y las zonas públicas de segundo nivel.
  - Participaron en el proceso: SeCIU-Udelar, Agesic, Antel y, como observador especial, Lacnic.
  - Llaves privadas de las KSKs se mantienen “off-line”.
  - Se comenzó a firmar dichas zonas
- A fines del mes de agosto/2015:
  - Se “sube” el registros DS a la raíz y queda activa la cadena de confianza.
  - La zona UY y las de segundo nivel se pueden validar desde internet.

DNSSEC en .UY

http://dnsviz.net/d/uy/dnssec/



DNSSEC en .UY

- Octubre/noviembre 2015 – se comenzará a aceptar registros DS de zonas firmadas a un número limitado de usuarios.
- En 2016 se activará la gestión del registro DS, en forma automática, mediante el sistema de registro de dominios de SeCIU-Udelar.
- Los agentes registradores deberán adecuar sus sistemas de registro para gestionar los registros DS.
- Los proveedores de “DNS Hosting” deberán adecuar sus servicios para firmar las zonas de sus usuarios.
- Los operadores de redes de acceso a Internet (ISPs) deberán activar la validación en los servidores DNS recursivos.
- anuncios-dnssec@seciu.edu.uy - Lista de correo para recibir información y novedades de la implantación de dnssec en UY. Para suscribirse: http://listas.rau.edu.uy/mailman/listinfo/anuncios-dnssec

DNSSEC en .UY

- Algunos sitios para seguir interiorizándose con DNSSEC

http://registro.br/tecnologia/dnssec.html?secao=dnssec
http://www.internetsociety.org/deploy360/dnssec/
http://www.internetsociety.org/deploy360/resources/dane/
https://centr.org/dns-explained/dnssec
https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-es
http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html

- Software (open source)

Servidores DNS autoritativos con soporte DNSSEC:
- BIND - KNOT DNS - NSD

Para firmar zonas en forma automatizada:
- BIND - KNOT - OpenDNSSEC

Servidores DNS recursivos que validan DNSSEC
- BIND - Unbound

Plugin validador de DNSSEC para navegador web:
- https://www.dnssec-validator.cz/

Jiap

¡¡GRACIAS!!

DNSSEC:
Extensiones de seguridad al sistema DNS

uynic