Introducción a DNSSEC

Nicolás Antoniello
Daniel Fink

ANUIES, Mexico
26 August 2020

Vulnerabilidades de DNS

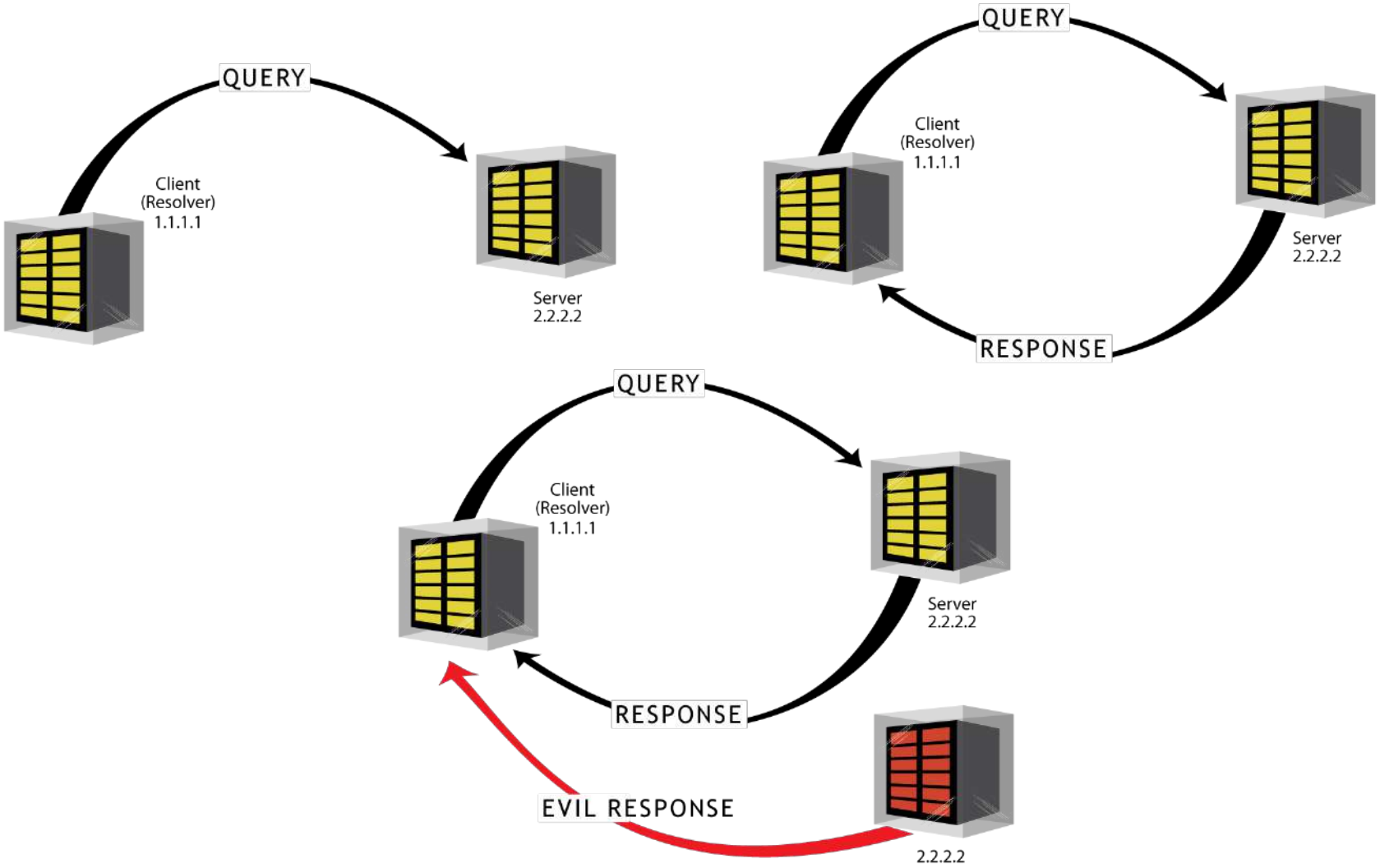
- ***La estructura básica del DNS (década de 1970) no tenía en cuenta los problemas de seguridad.***
  - ***Enfoque: rendimiento.***
  - ***Principio: confianza.***

3 areas de vulnerabilidades

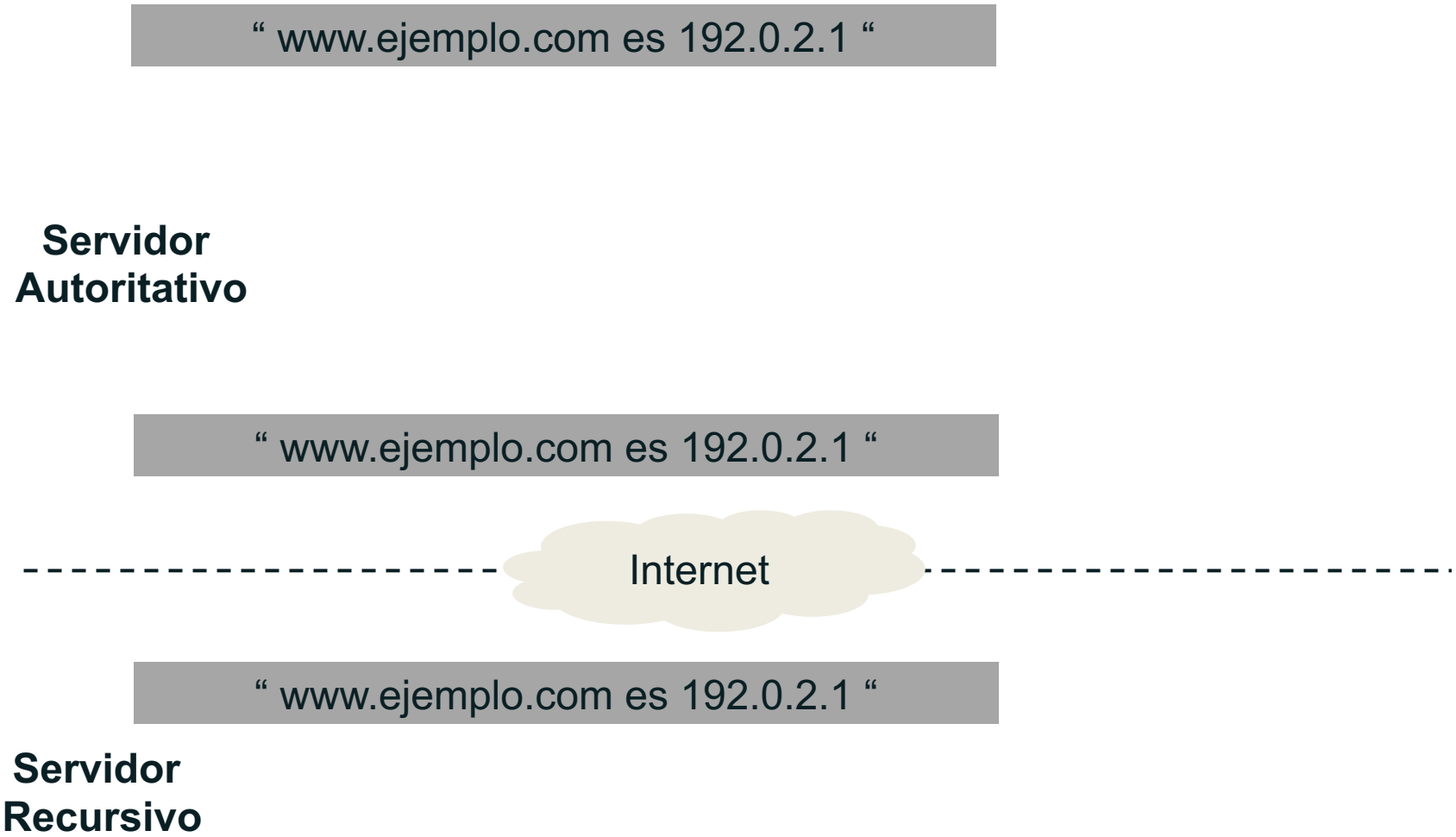
- ***Confidencialidad***
  - ***Acceso no deseado de información a terceros***
- ***Disponibilidad***
  - ***Pérdida de capacidad de acceso***
- ***Integridad***
  - ***Modificación o destrucción no deseada***

← DNSSEC actúa aquí

Vulnerabilidades de DNS



Visión General (sin DNSSEC)



Qué es DNSSEC? …

… lo que hace

- DNSSEC utiliza criptografía de clave pública y firmas digitales para proporcionar:
  - Autenticación de origen de los datos
  - Integridad de los datos
- DNSSEC ofrece protección contra la falsificación de datos de DNS

… lo que NO hace

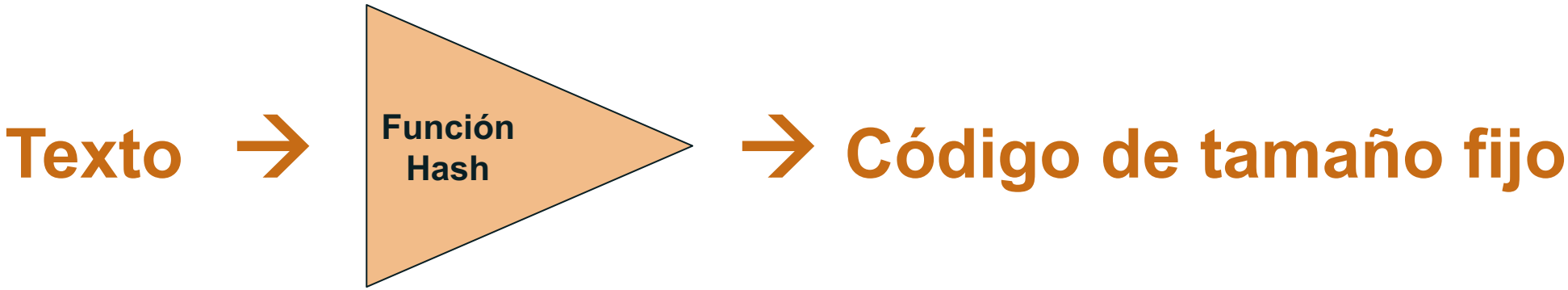
- Proveer confidencialidad en el intercambio de datos de DNS
- Evitar algunos ataques dirigidos al software de DNS o los sistemas
  - DDoS

Como funciona?

- Función “Hash”
- Par de Calves (o llaves) (Pública e Privada)
- Firma Digital

Función “Hash”

- Convierte información en una serie de caracteres de longitud fija.




```
Este equipo no tiene copa del mundo  →  5d242b5294d72df332ca2c492d2c0b9b

Este equipo tiene copa del mundo  →  e3d688adde84cf3e3fa493466dadba89
```

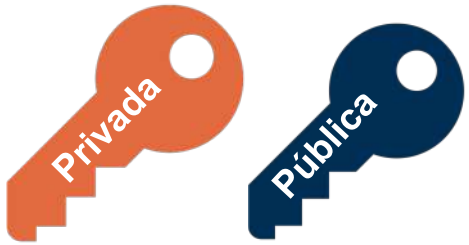
Criptografía de llaves Públicas

- Encriptación simétrica
  - 1 llave para encriptar y desencriptar

- Encriptación asimétrica **(DNSSEC utiliza esta)**
  - 1 llave para encriptar + 1 llave para desencriptar
    - 1 llave privada
    - 1 llave pública

Llaves de encriptación

- **Par de llaves**
  - **Llave privada**
  - **Llave pública**



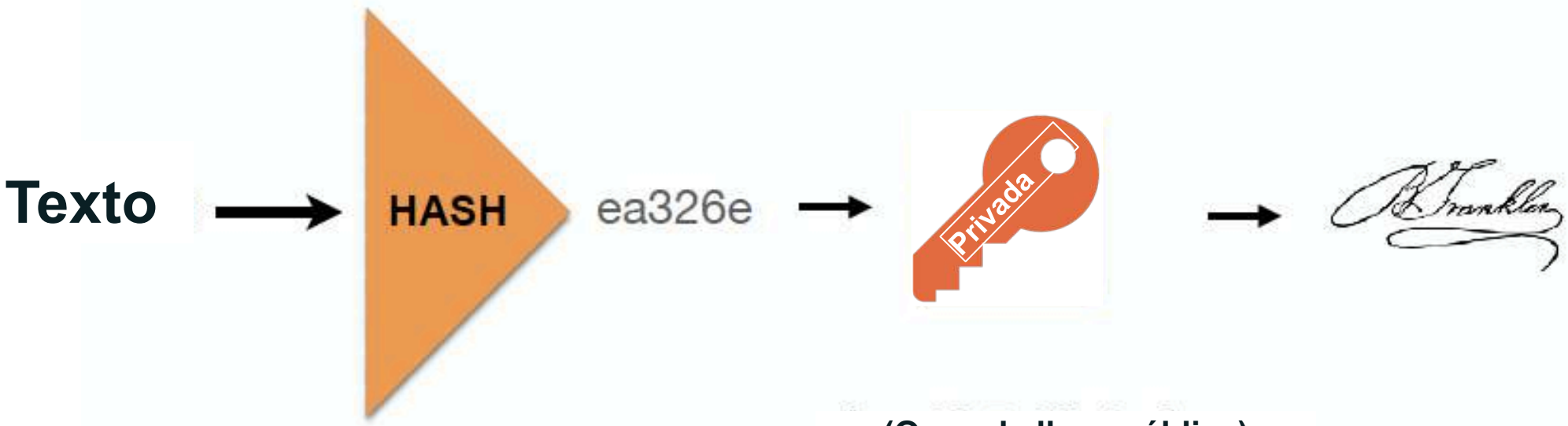
- **El contenido cifrado con una clave solo se puede descifrar con la otra.**
  - La clave pública puede "abrir" el contenido cifrado con la clave privada y viceversa.

Llaves de encriptación

Firmas digitales

- Si combinamos hashes con cifrado de clave pública, tenemos una firma digital
- Generamos un hash y luego lo encriptamos con una clave

Hashing + Encriptación = Firma Digital

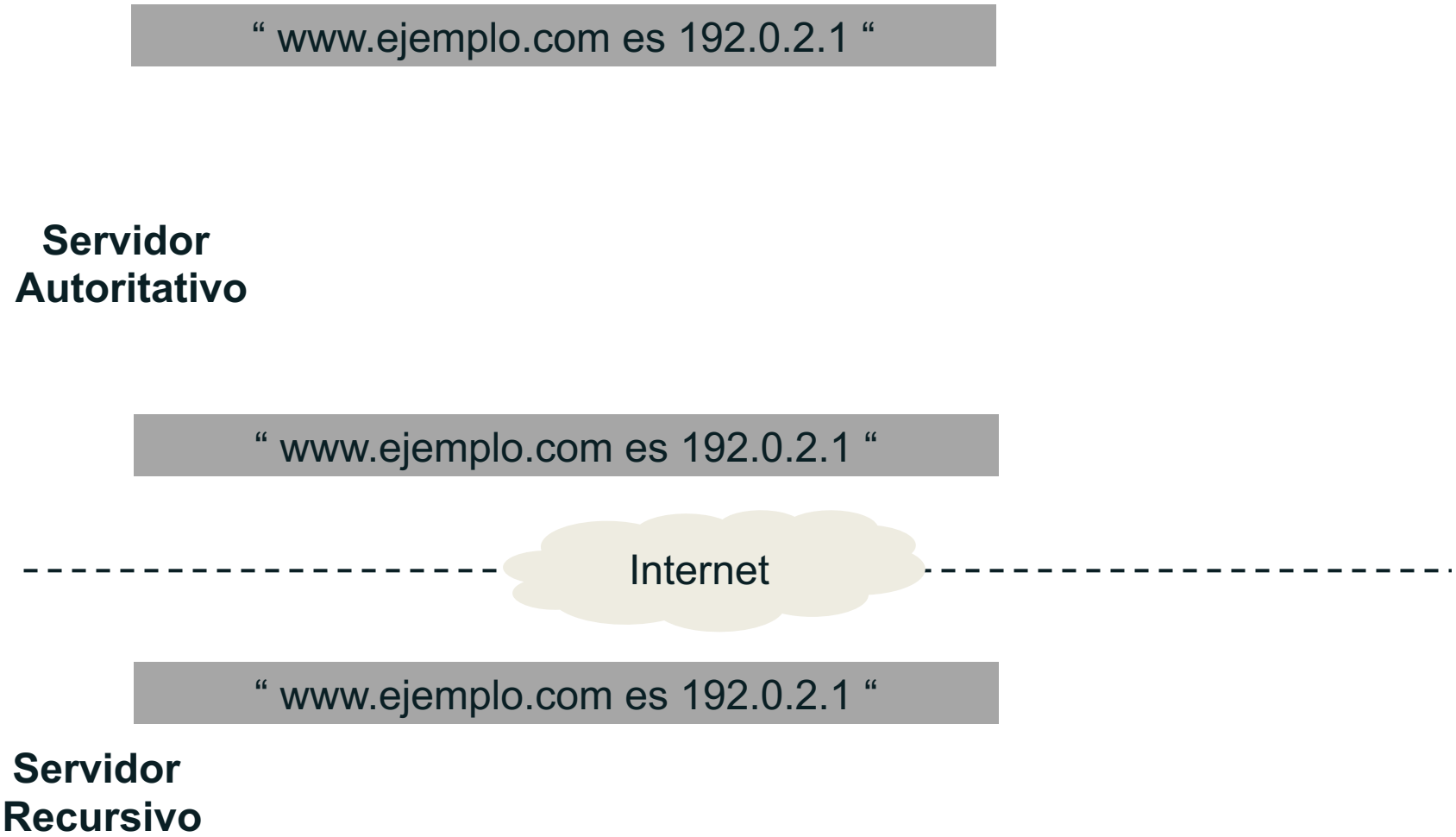


(O con la llave pública)

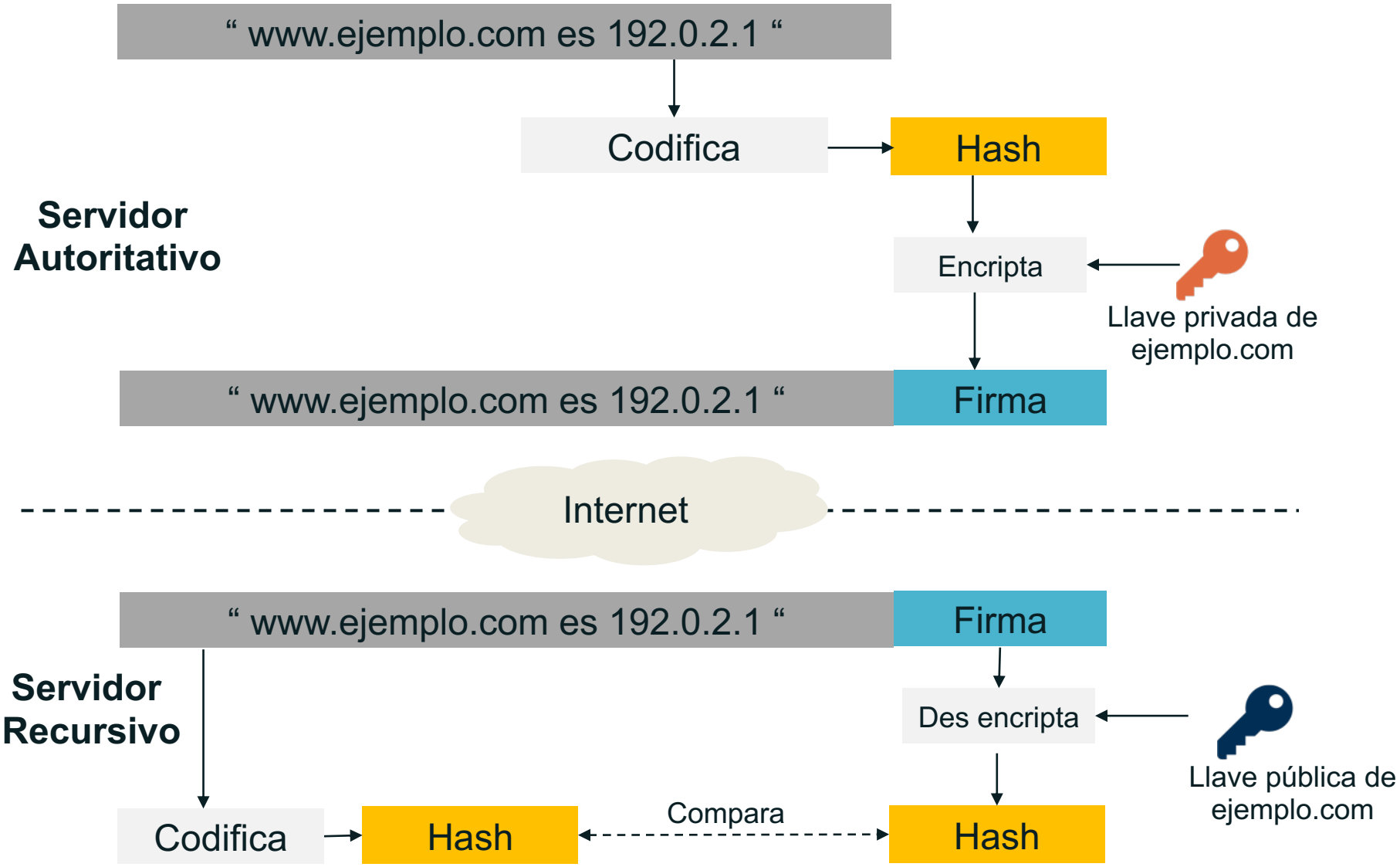
Verificando la autenticidad de las firmas

- Des encriptamos el mensaje
  - Obtenemos el hash.
- Convertir el mensaje original en un hash
- Comparar con el hash recibido
- Si los 2 hashes coinciden, el mensaje no se ha modificado.

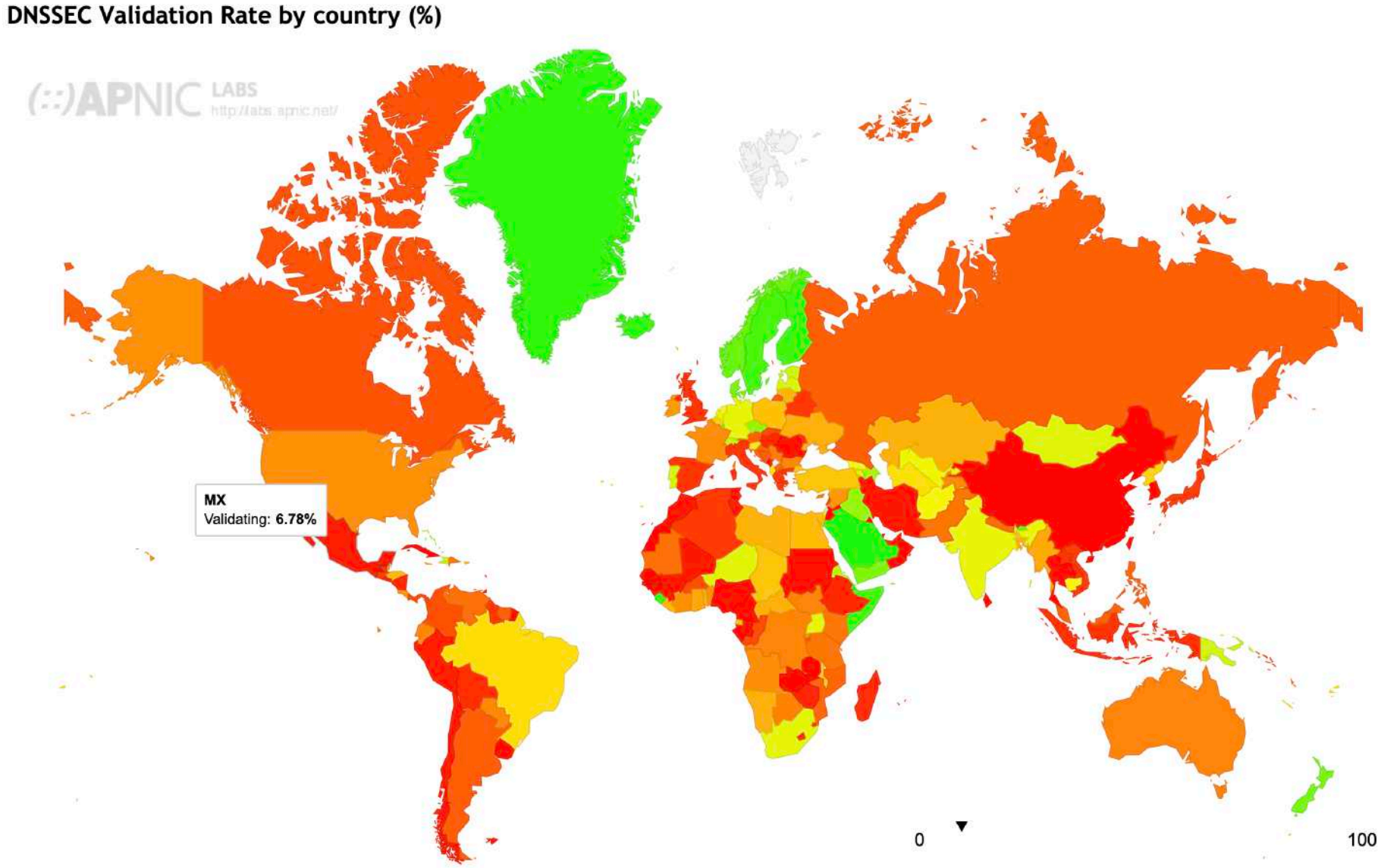
Visión General (sin DNSSEC) - recordando -



Visión General (con DNSSEC)

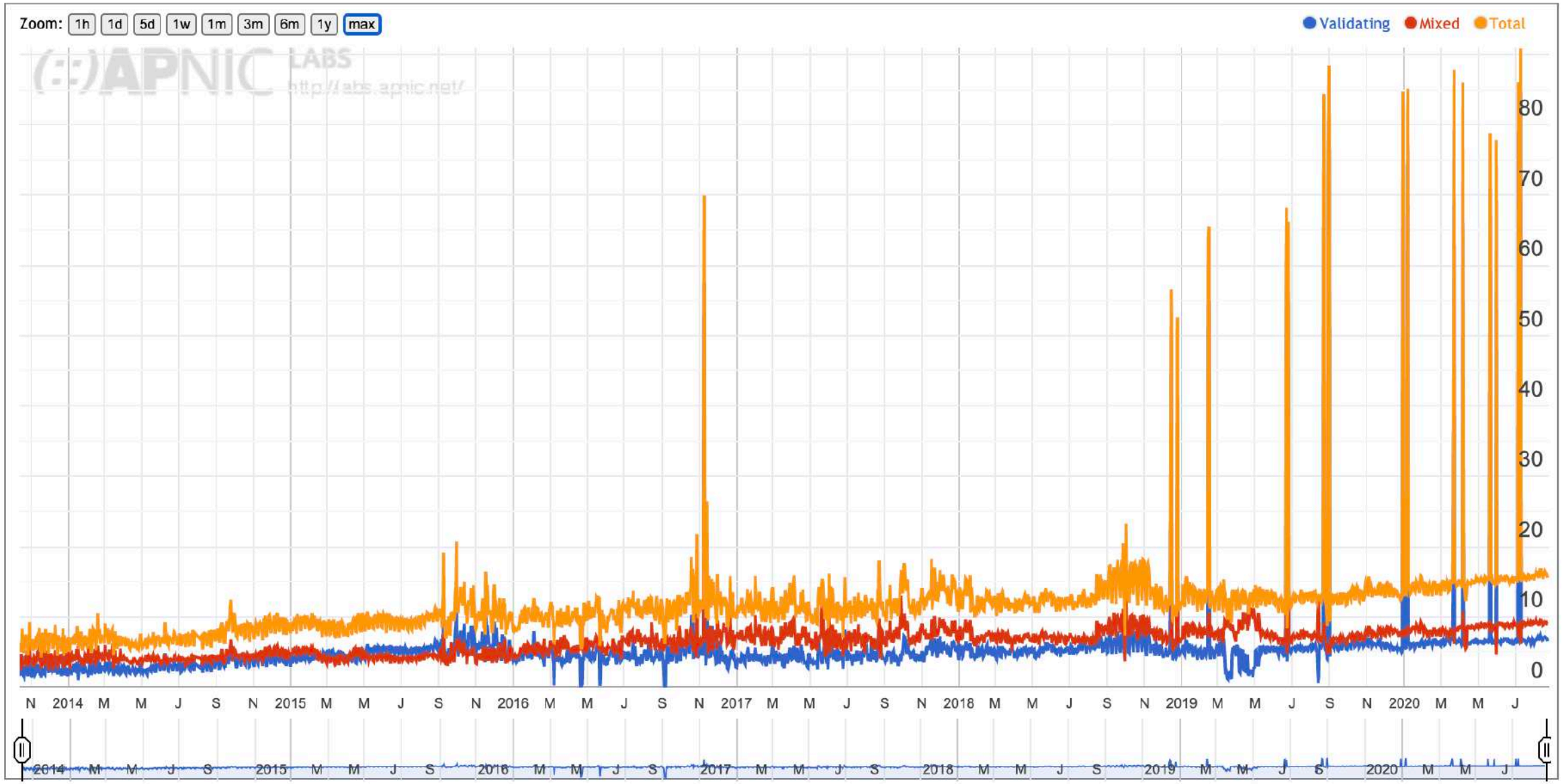


Validación DNSSEC en servidores recursivos, por país



https://stats.labs.apnic.net/dnssec

Validación DNSSEC en servidores recursivos en México (2014-2020)



https://stats.labs.apnic.net/dnssec/MX

Lista de AS's que envian muestras

ASN	AS Name	DNSSEC Validates	Partial Validation	Samples
AS265570	INALAMBRICO DEDICADO S.A. DE C.V.	98.67%	1.33%	75
AS28411	Aire Cable S.A. de C.V.	98.11%	1.89%	53
AS28419	Senal Interactiva, S.A De C.V	96.92%	2.31%	130
AS265530	FIBRATV SA DE CV	96.49%	0.88%	114
AS265605	VELOCOM SA DE CV	94.87%	5.13%	78
AS28409	ENI NETWORKS	93.71%	0.70%	143
AS32098	TRANSTELCO-INC	92.67%	2.00%	150
AS265566	TELESISTEMAS PENINSULARES SA DE CV	88.24%	11.76%	102
AS174	COGENT-174	87.50%	11.54%	104
AS28378	TV Rey de Occidente, S.A. de C.V.	87.10%	12.90%	62
AS265525	TV CABLE DEL GUADIANA S.A DE C.V.	84.80%	7.60%	171
AS28432	Telecable del Mineral, S. A. de C.V.	84.18%	4.43%	158
AS262916	Mega Cable, S.A. de C.V.	84.13%	9.52%	63
AS18734	Operbes, S.A. de C.V.	74.19%	14.84%	310
AS28458	IENTC S DE RL DE CV	71.08%	21.69%	83
AS11172	Alestra, S. de R.L. de C.V.	64.11%	14.29%	287
AS28438	ATC HOLDING FIBRA MEXICO, S. DE R.L. DE C.V.	52.00%	42.40%	125
AS265561	LANTOINTERNET SA DE CV	50.63%	15.19%	79
AS22566	Maxcom Telecomunicaciones, S.A.B. de C.V.	30.08%	6.78%	236
AS28418	NUEVA RED INTERNET DE MEXICO S DE RL DE CV	23.08%	44.23%	52
AS17072	TOTAL PLAY TELECOMUNICACIONES SA DE CV	17.31%	78.72%	8,667
AS265591	HNS DE MEXICO, S.A. DE C.V.	16.67%	11.11%	90
AS13591	Mexico Red de Telecomunicaciones, S. de R.L. de C.V.	14.46%	9.64%	83
AS22884	TOTAL PLAY TELECOMUNICACIONES SA DE CV	14.24%	83.22%	12,477
AS28376	Gigacable de Aguascalientes, S.A. de C.V.	13.73%	7.84%	102
AS6503	Axtel, S.A.B. de C.V.	13.59%	2.11%	1,656
AS28523	Cablevision Red, S.A de C.V.	9.82%	0.00%	224
AS28541	Mega Cable, S.A. de C.V.	7.11%	0.00%	408
AS8151	Uninet S.A. de C.V.	6.43%	1.03%	88,140
AS28545	Cablemas Telecomunicaciones SA de CV	4.48%	0.36%	1,943
AS27672	SERVICIO Y EQUIPO EN TELEFONIA INTERNET Y TV S.A. DE C.V.	4.28%	0.67%	747
AS28556	Cablemas Telecomunicaciones SA de CV	4.21%	0.00%	214
AS16960	Cablevision Red, S.A de C.V.	3.96%	4.40%	3,134
AS28531	Mexico Red de Telecomunicaciones, S. de R.L. de C.V.	3.50%	0.58%	515
AS13999	Mega Cable, S.A. de C.V.	3.28%	0.43%	26,023
AS265540	ALTAN REDES, S.A.P.I. de C. V.	3.20%	3.39%	2,658
AS28534	Mexico Red de Telecomunicaciones, S. de R.L. de C.V.	2.79%	0.70%	574
AS28512	Cablemas Telecomunicaciones SA de CV	2.07%	0.97%	822
AS28532	Mexico Red de Telecomunicaciones, S. de R.L. de C.V.	1.95%	0.16%	616
AS28509	Cablemas Telecomunicaciones SA de CV	1.94%	0.37%	5,887
AS7438	Pegaso PCS, S.A. de C.V.	1.41%	0.41%	3,396
AS28543	Mexico Red de Telecomunicaciones, S. de R.L. de C.V.	1.32%	0.00%	152

https://stats.labs.apnic.net/dnssec/MX

Test simple de DNSSEC

- http://dnssec.vs.uni-due.de/

- http://www.dnssec-or-not.com/

Muchas gracias !

One World, One Internet

Visit us at **icann.org** Email:

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann