Observatorio DNS LAC

Mediciones y cumplimiento de recomendaciones

Maite González NICLabs .CL

Vulnerabilidades del DNS

Vulnerabilidades de DNS

Bajo nivel de Dispersión.

Respuestas sin Autoridad.

Envenenamiento de Caché y Fallo Kaminsky.

Isla de seguridad.

Etc.

¿Qué Medir?

¿Qué Medir por cada nombre de dominio?

Dispersión de Servidores de nombre autoritativos.

Nivel de implementación de IPv4 e IPv6 de los servidores de nombre autoritativos.

Nivel de implementación de DNSSEC.

¿Qué Medir por cada Servidor Autoritativo?

Permiso de recursión

DNSSEC/EDNS activado

Permiso de uso de TCP

Transferencia de zona

Respuestas a consultas raras (ej: LOC)

¿Cómo Medirlo?

Datos de Entrada

Lista de Nombres de Dominio a analizar.

Actualmente:

Zona .CL y .SV + dominios LAC del ranking de Alexa Top 1 Million.

(Proximamente .GT)

Mediciones para cada Dominio

Consulta DNS solicitando todos los nombres de los autoritativos de cada dominio.

Consulta solicitando el uso de DNSSEC

Mediciones para cada Servidor Autoritativo(1)

Obtención de todas las direcciones IP asociadas (IPv4 e IPv6).

Obtención de sistema autónomo asociado a cada IP.

Obtención del país asociado a cada IP (Maxmind Geo IP database).

Mediciones para cada Servidor Autoritativo(2)

Consulta solicitando Recursividad

Solicitud de recurso utilizando DNSSEC.

Consulta solicitando uso de TCP.

Solicitud de Transferencia de Zona.

Solicitud de recurso de tipo LOC.

Resultados

Dispersión de Servidores de Nombres

Dispersión de Servidores de Nombre

Cantidad de Servidores de Nombre

Recomendación mínima: **2** (RFC 1912) -> **3** (RFC 2182)

Cantidad de Sistemas Autónomos

Recomendación mínima: 3

Cantidad de Países en los que se distribuyen

Recomendación mínima: 3

Dispersión de Servidores de Nombre

Cantidad de Servidores de Nombre

nsnum >= 2 (%)	98.03%	98.09%	98.19%	98.27%	98.34%	98.45%	98.50%	98.52%	98.62%
nsnum >= 3 (%)	36.05%	36.21%	36.86%	36.91%	37.42%	37.66%	37.62%	37.96%	38.74%

(06/2017 - 06/2019 trimestral)

Dispersión de Servidores de Nombre

Cantidad de Sistemas Autónomos en los que se distribuyen

asn >= 2 (%)	33.64%	33.84%	33.19%	32.81%	32.99%	32.19%	32.50%	32.11%	31.99%
asn >= 3 (%)	12.42%	13.82%	14.29%	14.19%	14.74%	15.26%	16.26%	16.33%	16.66%

(06/2017 - 06/2019 trimestral)

Dispersión de Servidores de Nombre

Cantidad de Países en los que se distribuyen

country >= 2 (%)	23.61%	24.23%	22.99%	23.21%	23.57%	22.24%	23.97%	23.86%	23.26%
country >= 3 (%)	1.84%	1.89%	1.96%	1.95%	2.06%	1.93%	10.52%	10.56%	10.89%

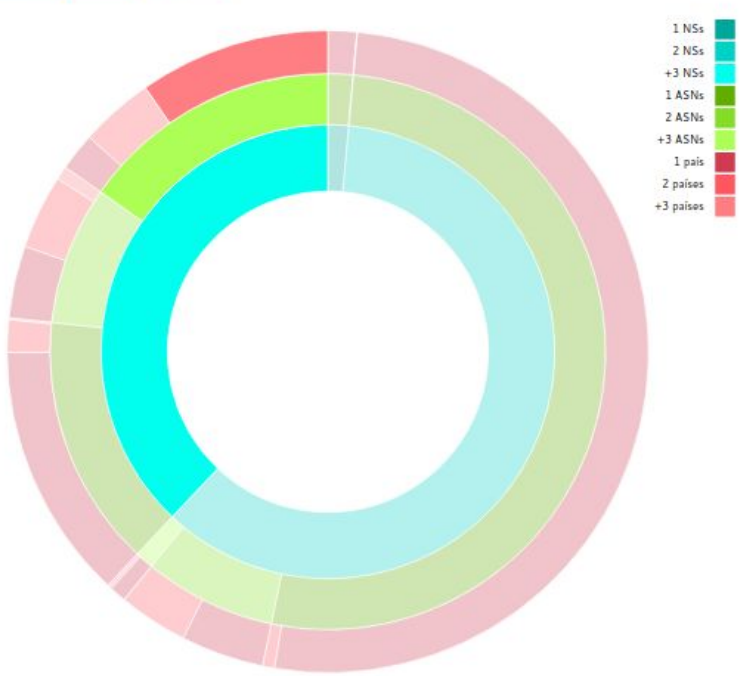
(06/2017 - 06/2019 trimestral)

Dispersión de Servidores de Nombre

Cumplen con las 3 recomendaciones

all>=2 (%)	22.96%	23.46%	22.08%	22.24%	22.63%	21.43%	22.12%	21.53%	20.82%
all>=3 (%)	0.97%	1.05%	1.09%	1.11%	1.23%	1.20%	9.60%	9.63%	10.07%

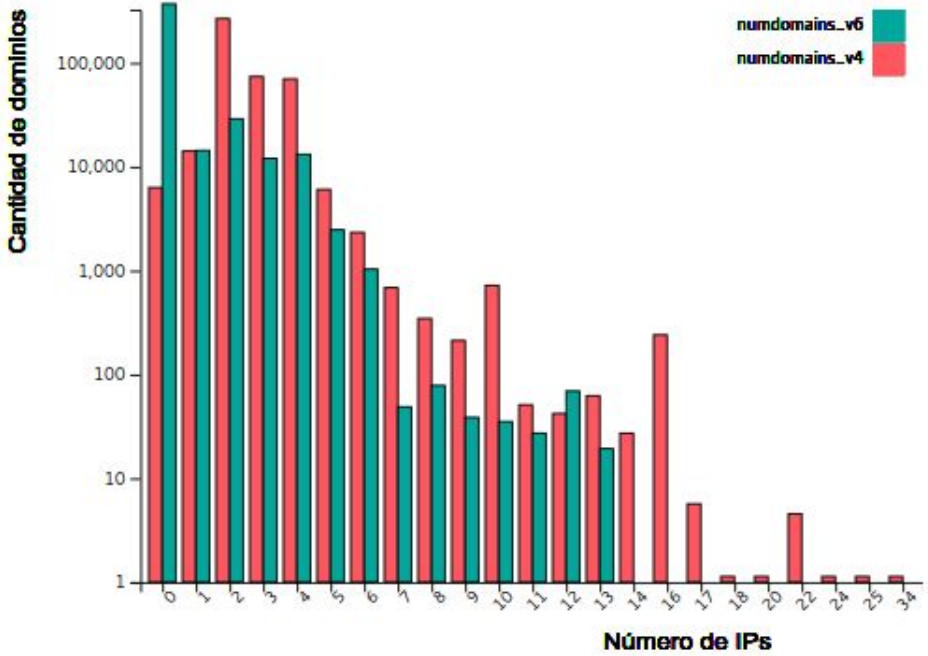
(06/2017 - 06/2019 trimestral)



Cumplen con las 3 recomendaciones

(9.63% de los dominios. 03/2019)

Dominios con Servidores de nombre con IPv4 vs IPv6



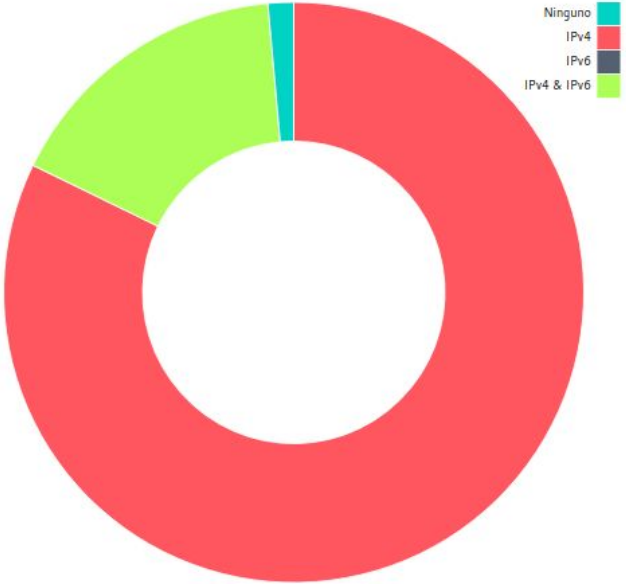
Cantidad de servidores de cada dominio por versión de IP

(Datos 03/2017)

Dominios con Servidores de nombre con IPv4 vs IPv6

No ip	1.43%	1.87%	1.37%	1.46%	1.36%	1.30%	1.32%	1.36%	1.31%
IPv4 & IPv6	16.36%	16.86%	17.27%	18.13%	18.83%	19.41%	18.77%	19.57%	20.80%
Only IPv4	82.22%	81.27%	81.36%	80.40%	79.81%	79.29%	79.91%	79.07%	77.89%
Only IPv6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

(06/2017 - 06/2019 trimestral)



Versión de IP que implementan los servidores de nombre de los dominios

(Datos 03/2017)

DNSSEC

Nivel de implementción de DNSSEC

No dnssec (%)	99.55%	99.52%	99.51%	99.32%	99.26%	99.30%	99.57%	99.44%	99.22%
dnssec fail (%)	0.11%	0.12%	0.14%	0.15%	0.18%	0.20%	0.19%	0.23%	0.28%
dnssec ok (%)	0.34%	0.35%	0.35%	0.53%	0.55%	0.50%	0.23%	0.33%	0.50%

(06/2017 - 06/2019 trimestral)

Errores típicos encontrados

Negación de Existencia (%)	62.53%	64.04%	64.39%	66.57%	66.06%	65.62%	61.18%	68.44%	61.58%
Validación de llaves (%)	14.46%	12.81%	12.44%	8.57%	7.40%	6.73%	4.71%	5.23%	6.15%
Validación de DS (%)	70.26%	70.88%	74.49%	75.00%	76.31%	78.86%	85.86%	81.29%	80.32%

(06/2017 - 06/2019 trimestral)

Nivel de cumplimiento de recomendaciones de servidores de nombre

Cumplimiento de recomendaciones de NS

Permite Recursividad fail (%)	2.19%	2.48%	2.66%	2.49%	1.51%	1.23%	1.08%	0.70%	0.54%
Permite Recursividad comply (%)	97.81%	97.52%	97.34%	97.51%	98.49%	98.77%	98.92%	99.30%	99.46%
EDNS activado fail (%)	4.06%	3.66%	3.91%	4.24%	3.29%	2.58%	1.92%	1.95%	2.08%
EDNS activado comply (%)	95.94%	96.34%	96.09%	95.76%	96.71%	97.42%	98.08%	98.05%	97.92%
comunicacion TCP fail (%)	5.04%	4.98%	5.10%	7.97%	4.17%	4.02%	3.42%	2.53%	2.28%
comunicacion TCP comply (%)	94.96%	95.02%	94.90%	92.03%	95.83%	95.98%	96.58%	97.47%	97.72%
Transferencia de zona TCP fail (%)	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Transferencia de zona TCP comply (%)	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Respuesta a consultas LOC fail (%)	0.01%	0.01%	0.01%	0.01%	0.01%	0.01%	0.01%	0.01%	0.01%
Respuesta a consultas LOC comply (%)	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%

(06/2017 - 06/2019 trimestral)

Conclusiones

Conclusiones (1)

Actualmente más del 98% de los dominios cumple con la regulación -obsoleta- de tener al menos 2 servidores de nombre.

Y tan solo un 38.74% cumple la recomendación de tener al menos 3.

Sin embargo se ve que desde el 2017 estos números han ido en aumento.

Conclusiones (2)

Sobre las recomendaciones de tener al menos 2 servidores, en 2 ASN’s distintos y distribuidos en al menos 2 países, no se ve una clara tendencia, pero se mantienen en valores de cumplimiento del 20% aproximadamente.

Para la misma métrica, pero con 3 servidores, se observa un último valor de un 9.63%.

Conclusiones (3)

La implementación de IPv6 en los servidores de nombre se ve en crecimiento del 16% al 20% en tan sólo 2 años.

Aún existen dominios (+1%) con servidores de nombre mal configurados (sin una IP por ejemplo, no funcionan!)

Es demasiado baja la tasa de implementación de DNSSEC!

Lo peor es que muchos de los que sí lo implementan tienen serios fallos en su funcionamiento.

Conclusiones (4)

La recolección constante de datos permite mantener un histórico y ver cuál es el estado actual, donde se está fallando y cómo se pueden solucionar ciertos problemas.

Datos de los países distintos a .cl y .sv podrían estar sesgados, ya que se utilizan sitios muy populares(Ranking Alexa) que podrían cumplir mejor con las métricas que los menos populares.

(Únanse al proyecto, para obtener valores más representativos de la zona LAC y poder mejorar juntos)

Gracias por su atención!

Maite González (maite@niclabs.cl) Hugo Salgado (hsalgado@nic.cl)

Observatorio DNS LAC

Mediciones y cumplimiento de recomendaciones

Maite González NICLabs .CL