Monitoreo FORT

Guillermo Cicileo
Guillermo@lacnic.net

online meeting
lacnic34
lacnog 2020

Proyecto **FORT**

FORT es una iniciativa de LACNIC y NIC.MX sobre seguridad de ruteo para una Internet libre y abierta.

CONOCER MÁS

VALIDADOR FORT

Validador RPKI

El Validador FORT es un validador RPKI de código abierto. Esta solución permite a los operadores validar la información de enrutamiento BGP contra el repositorio RPKI para usarla en su configuración y resolución de rutas.

CONOCER MÁS

MONITOREO FORT

Herramienta de monitoreo

Monitoreo FORT es una herramienta de libre acceso para documentar incidentes de ruteo en América Latina y Caribe e identificar tendencias regionales en secuestros de rutas.

CONOCER MÁS

REPORTE FORT

Reporte diagnóstico

El Reporte FORT analiza incidentes de ruteo y secuestros de ruta en LAC en los años 2017, 2018 y parte de 2019. El reporte permite entender el impacto de la seguridad de ruteo en la experiencia de los usuarios finales de Internet en la región.

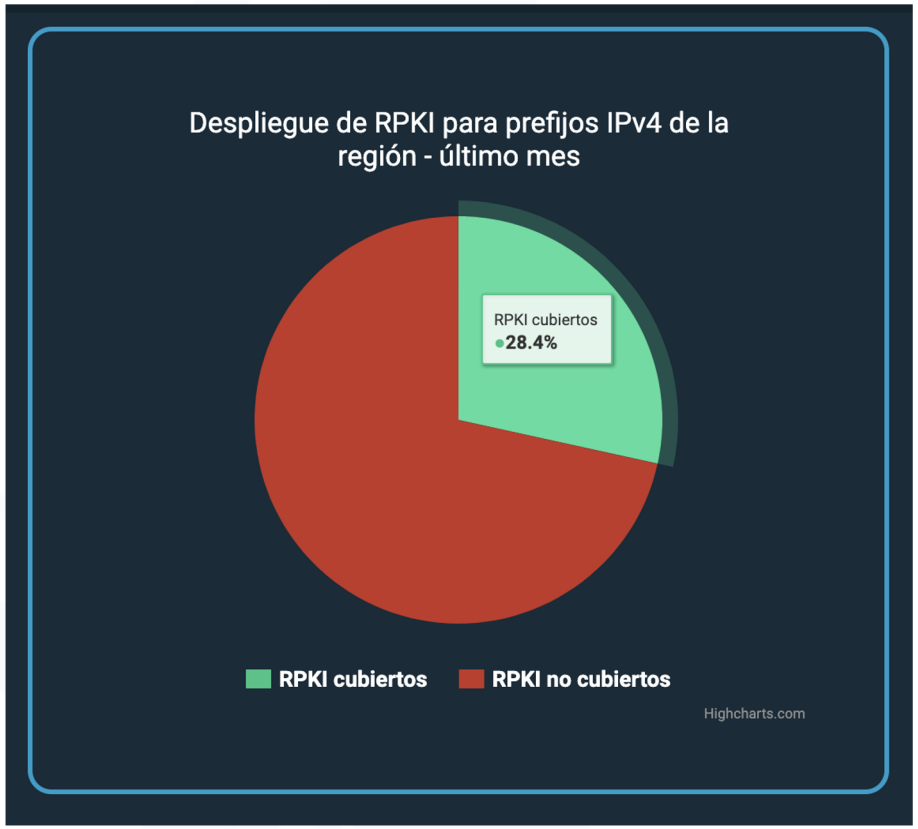
DESCÁRGALO AQUÍ

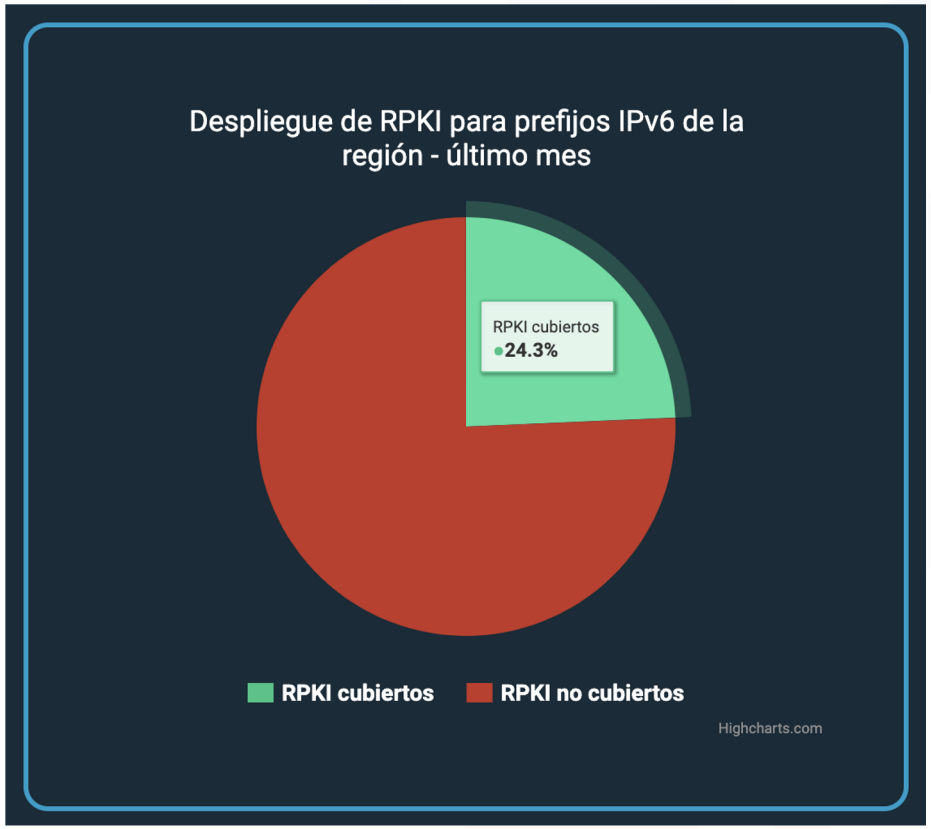
Monitoreo FORT basado en:

- Updates de BGP de **route-views** y **RIPE RIS**
- Información de RPKI: validación utilizando FORT y Routinator
- Información de IRRs (RADB, RIPE)
- Datos de registro de LACNIC y el NRO
- Con esa información se puede determinar:
  - Cobertura por ROAs y validez de los updates BGP
  - Clasificación por país
  - Anomalías en la información de ruteo

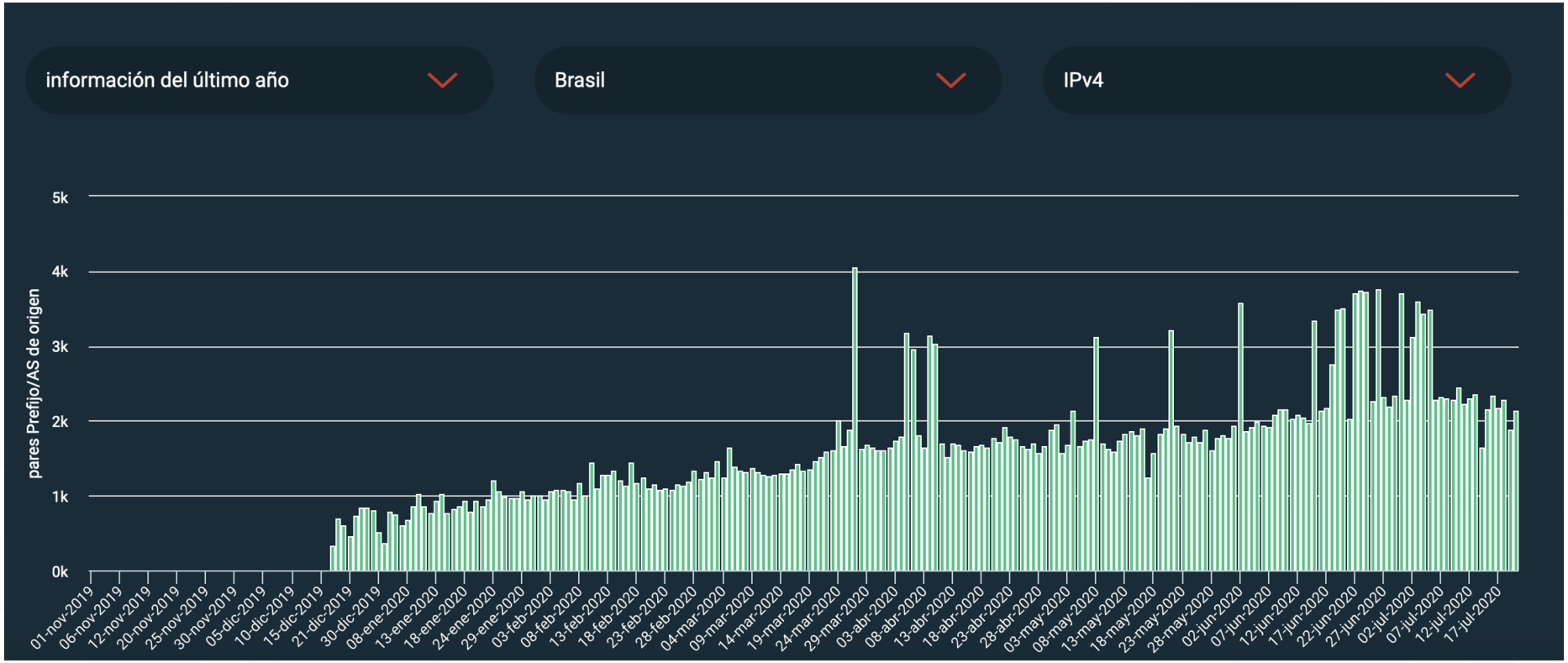
Despliegue RPKI

Despliegue RPKI





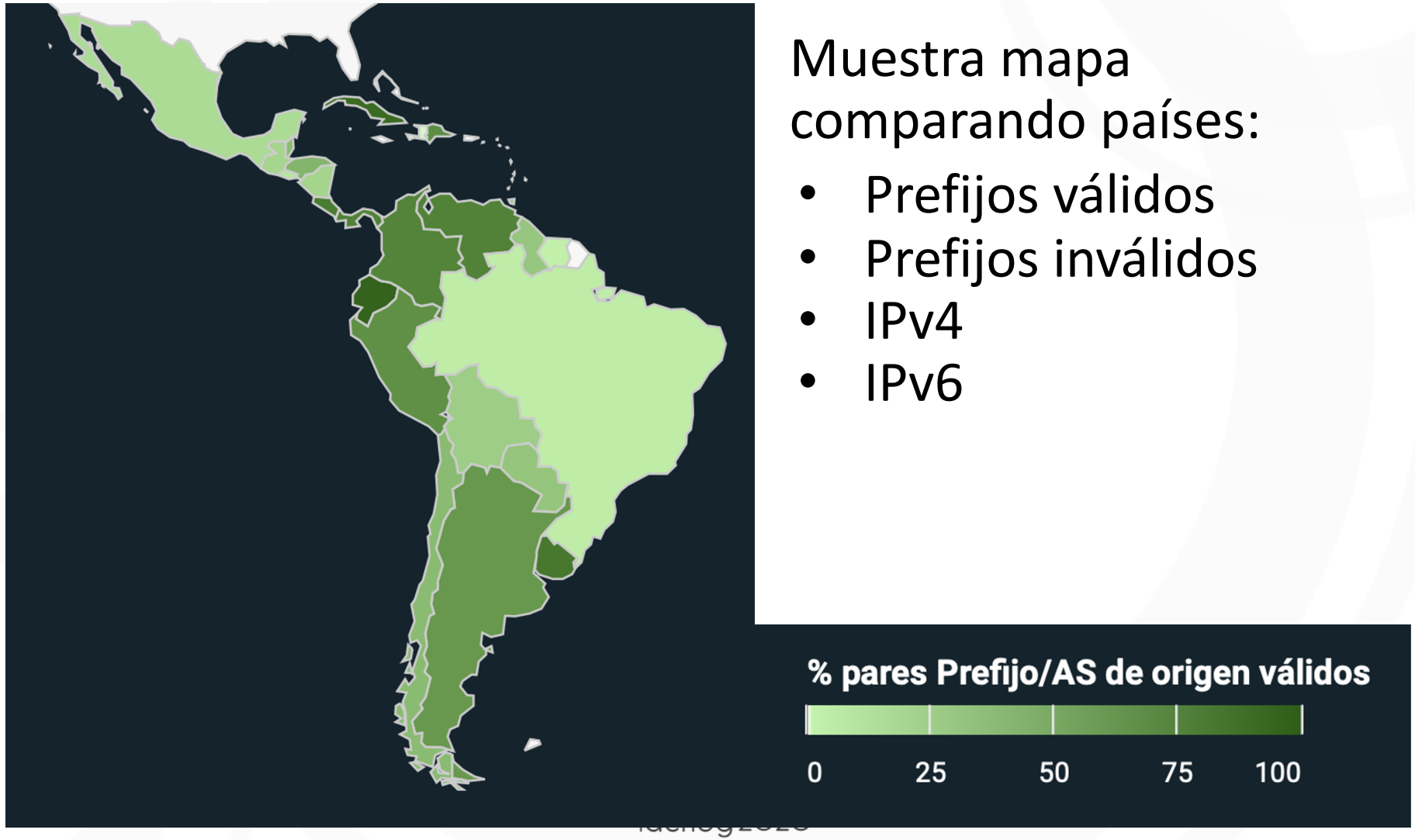
Despliegue RPKI: Evolución IPv4



Ejemplo: Brasil, desplegó RPKI en el último año (Dic 2019)

Validación RPKI

Validación RPKI: Mapa



Muestra mapa comparando países:

- Prefijos válidos
- Prefijos inválidos
- IPv4
- IPv6

Posibles secuestros de Ruta

Posibles secuestros de Ruta

Fuente fidedigna/autorizada

RPKI-valid
RPKI-not found + IRR-valid

Desprotegidos

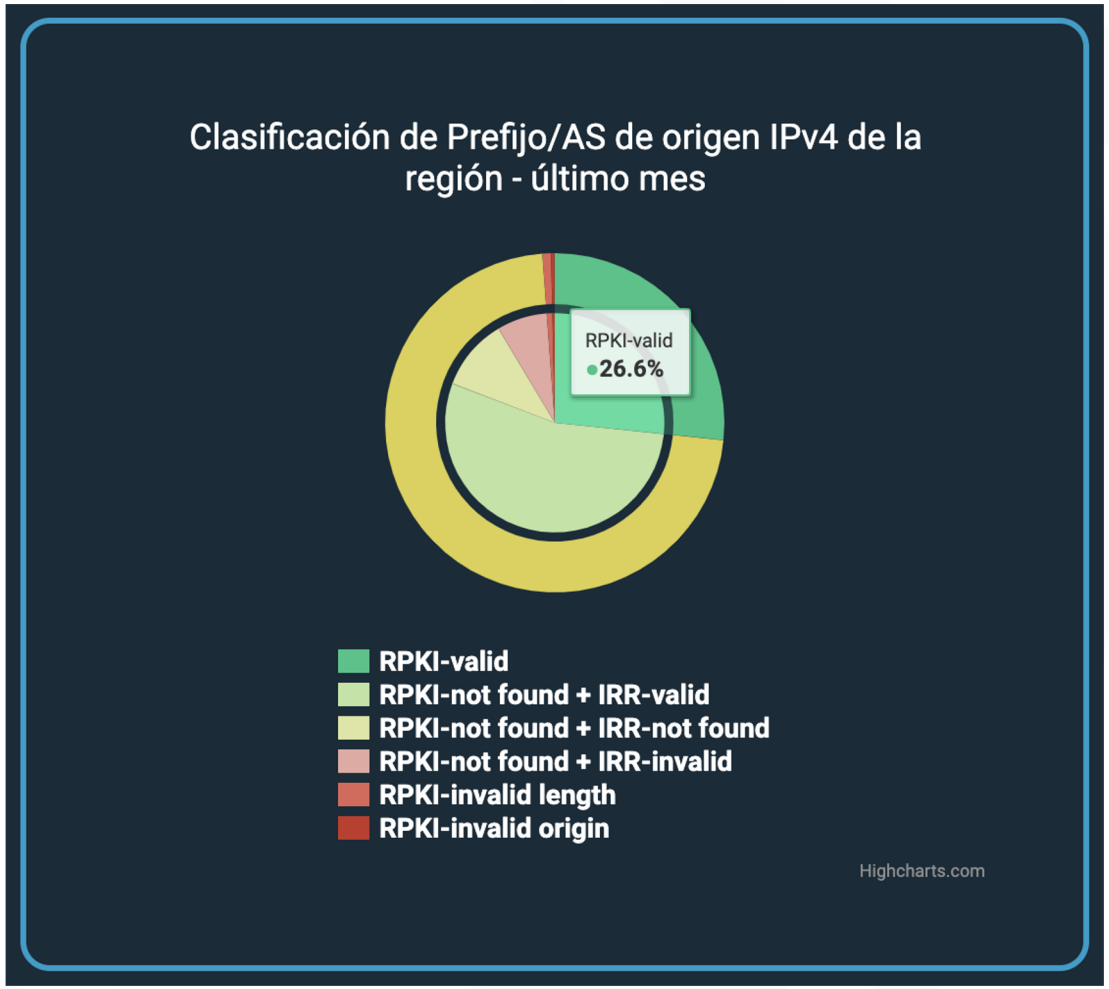
RPKI-not found + IRR-not found

Anomalías/sospechosos

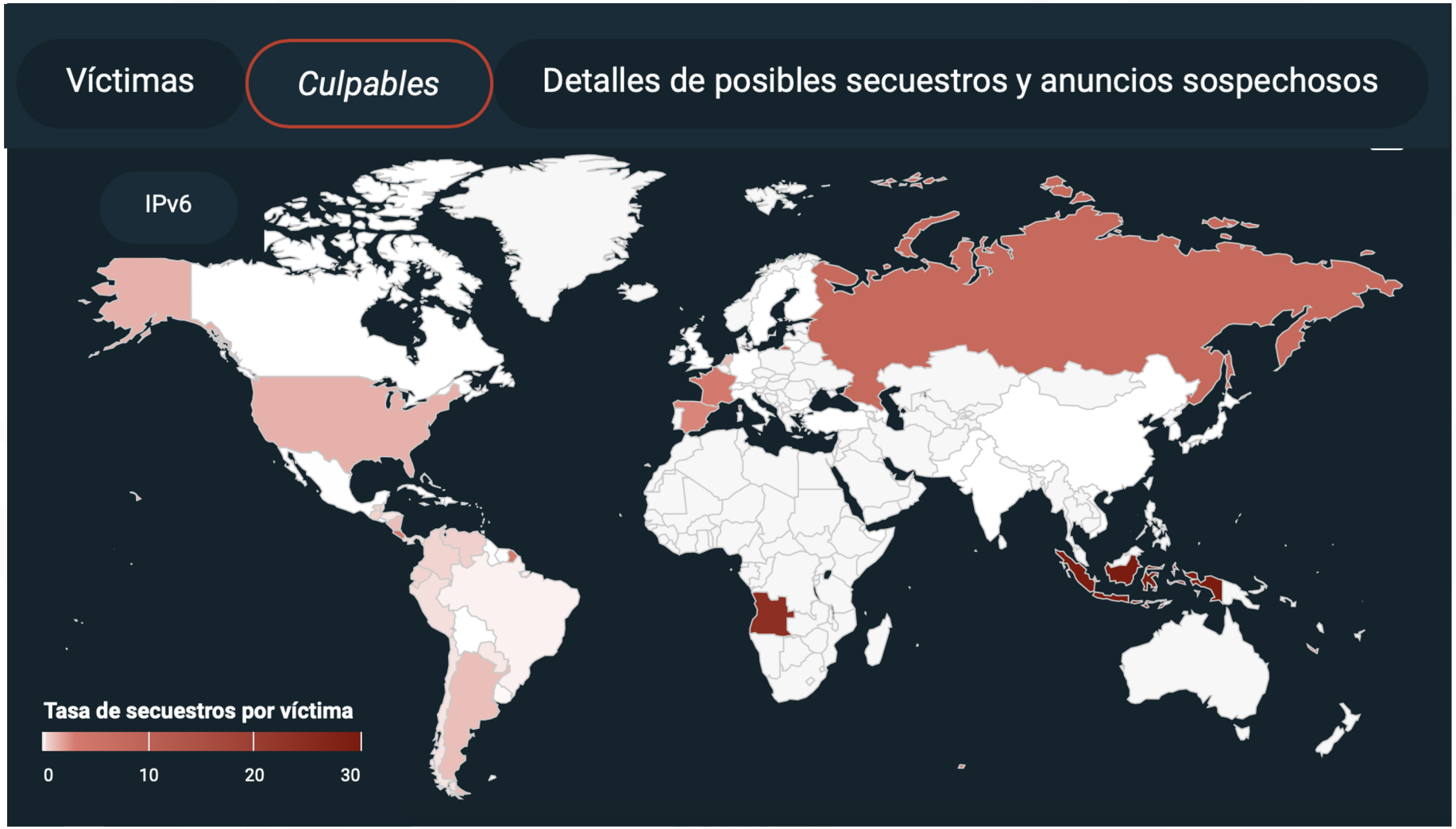
RPKI-not found + IRR-invalid

Posibles secuestros

RPKI-invalid length
RPKI-invalid origin



Posibles secuestros: información ampliada



Detalle de posibles secuestros

yyyy-mm-dd | Prefijo | AS de Origen | Tipo de incidente

Fecha	Prefijo	AS de Origen	Tipo de incidente
16-ago-2020	200.89.208.0/20	ASN 3816 - COLOMBIA TELECOMUNICACIONES S.A. ESP	RPKI-invalid origin
16-ago-2020	170.245.96.0/24	ASN 61748 - Dkirosnet Serviços de Internet	RPKI-invalid length
16-ago-2020	170.245.97.0/24	ASN 61748 - Dkirosnet Serviços de Internet	RPKI-invalid length
16-ago-2020	170.245.98.0/24	ASN 61748 - Dkirosnet Serviços de Internet	RPKI-invalid length
16-ago-2020	170.245.99.0/24	ASN 61748 - Dkirosnet Serviços de Internet	RPKI-invalid length
16-ago-2020	186.169.16.0/21	ASN 3816 - COLOMBIA TELECOMUNICACIONES S.A. ESP	IRR-invalid
16-ago-2020	186.169.24.0/21	ASN 3816 - COLOMBIA TELECOMUNICACIONES S.A. ESP	IRR-invalid
16-ago-2020	186.169.32.0/20	ASN 3816 - COLOMBIA TELECOMUNICACIONES S.A. ESP	IRR-invalid
16-ago-2020	186.169.4.0/22	ASN 3816 - COLOMBIA TELECOMUNICACIONES S.A. ESP	IRR-invalid

Infraestructura crítica

Secuestros sobre Infraestructura Crítica

Protección de Infraestructura Crítica

La Infraestructura Crítica está compuesta por recursos que son esenciales para que Internet pueda funcionar correctamente. En este caso, consideramos Infraestructura Crítica a todos los servidores de nombre que resuelven los dominios de nivel superior de código de país (ccTLDs) tales como el .uy, .br o .mx. Un secuestro a nivel de la infraestructura crítica puede generar un gran impacto. Aquí se presenta la cantidad de secuestros de ruta que impactaron sobre infraestructura crítica de la región en los últimos 3 meses. En “Ampliar información” se presenta información sobre la evolución de la cobertura de infraestructura crítica en la región y detalles de los secuestros ocurridos.

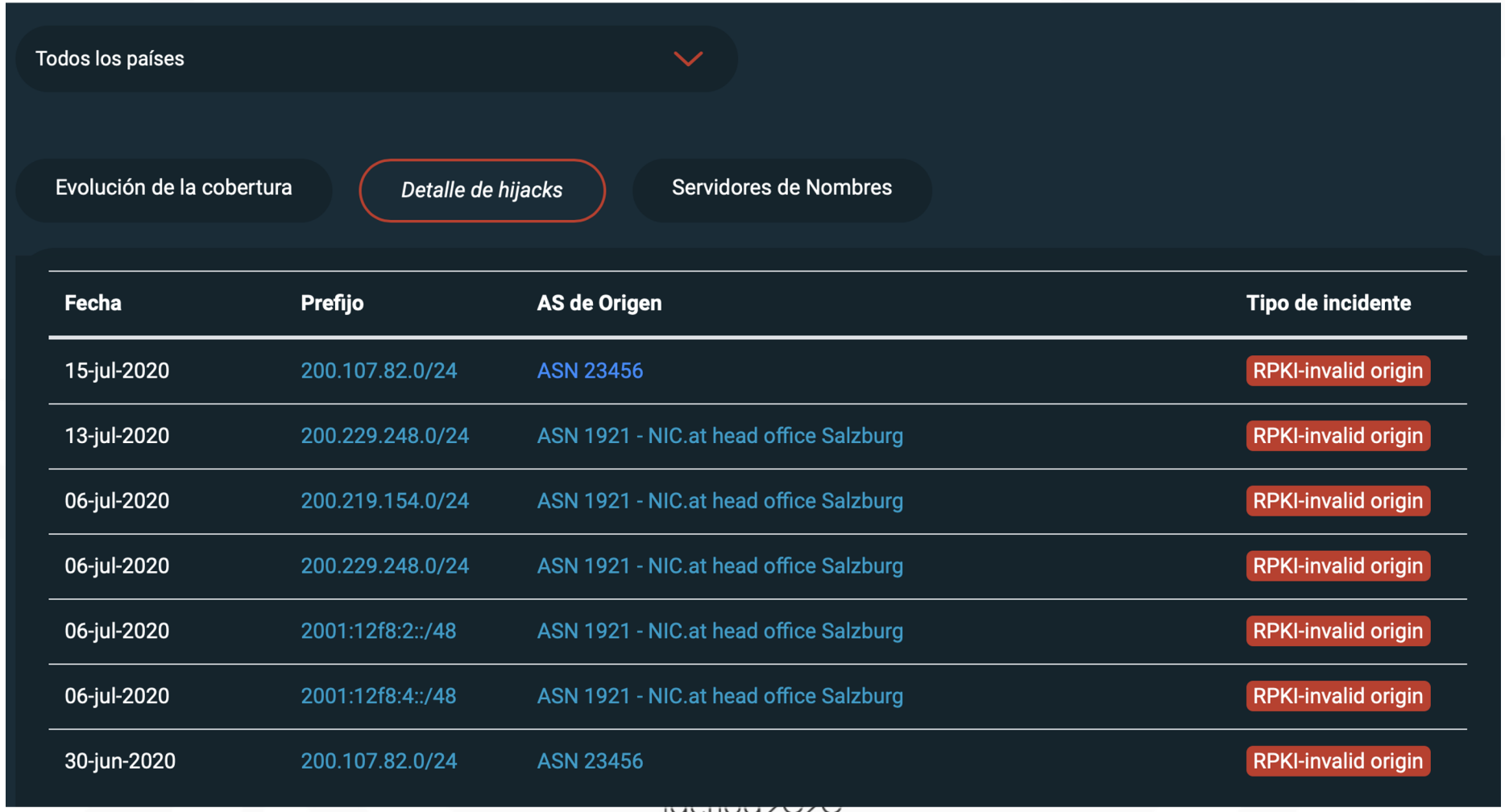
AMPLIAR INFORMACIÓN

En los últimos 3 meses han ocurrido

7

secuestros sobre la infraestructura crítica

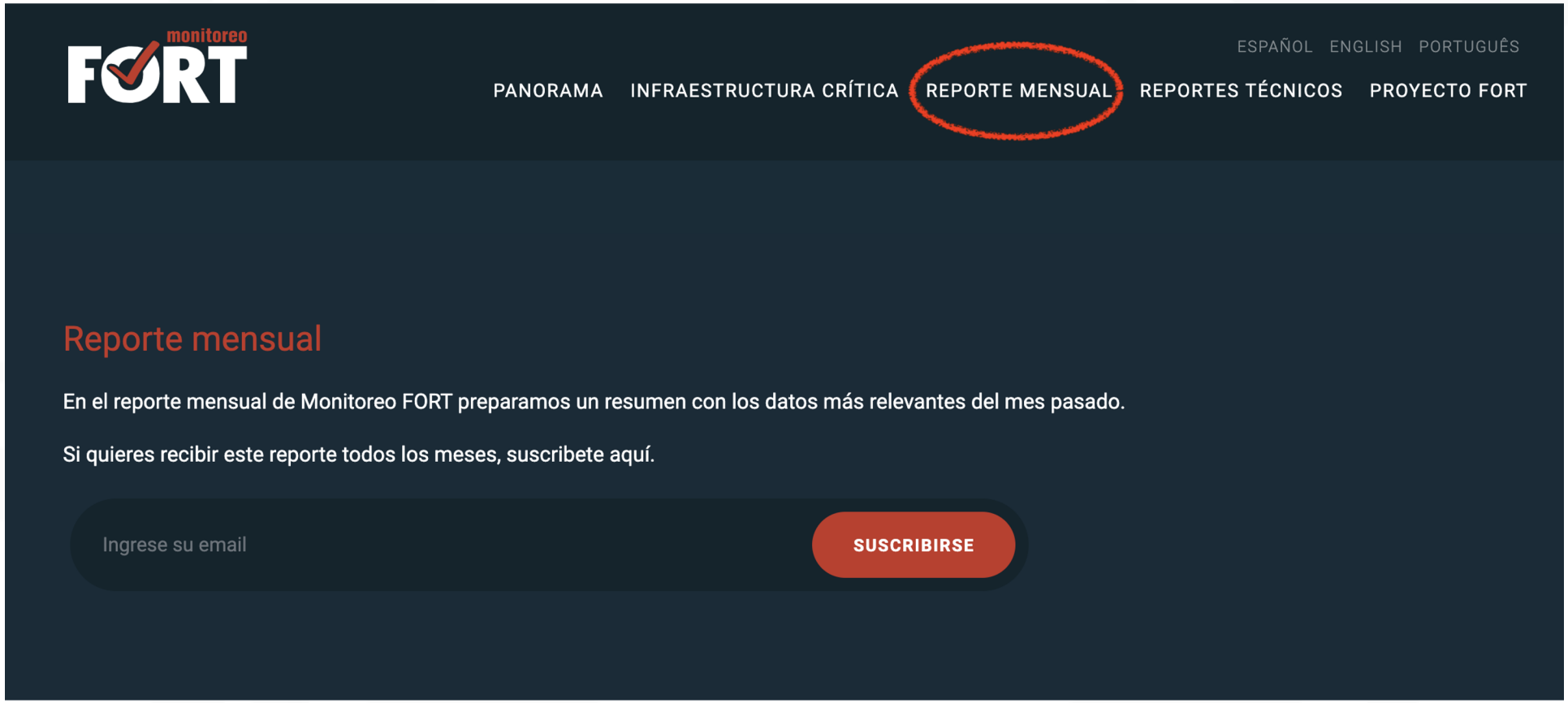
Detalle de posibles secuestros



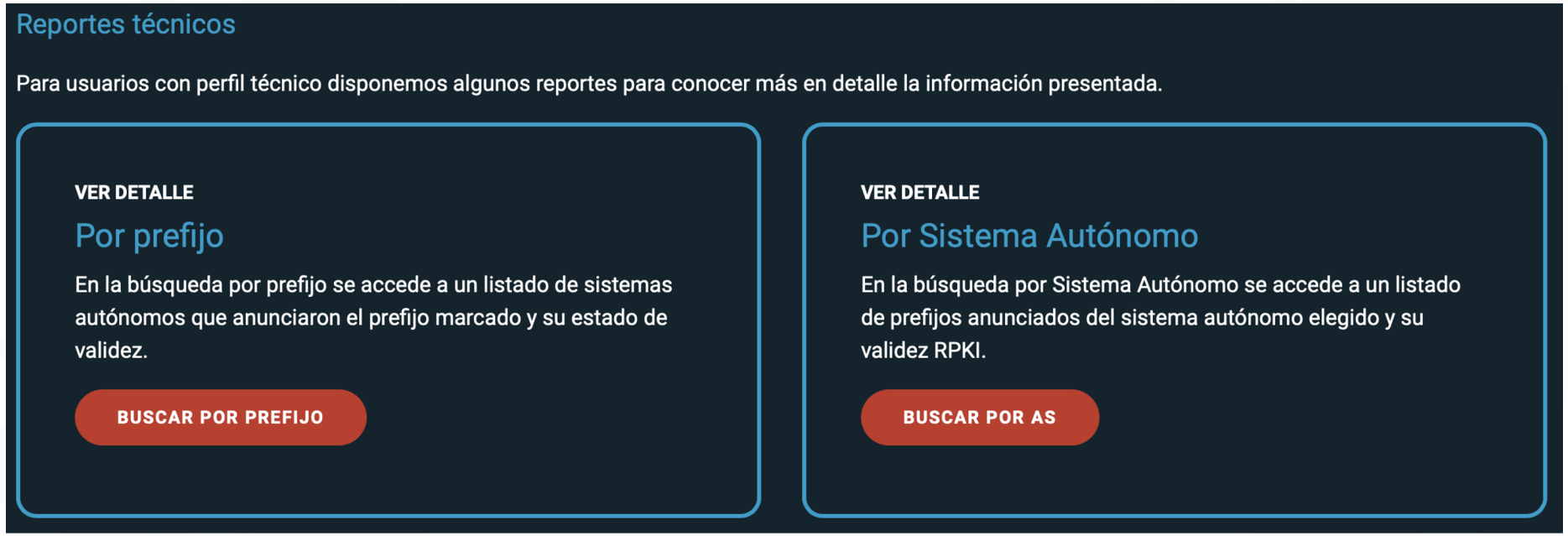
Fecha	Prefijo	AS de Origen	Tipo de incidente
15-jul-2020	200.107.82.0/24	ASN 23456	RPKI-invalid origin
13-jul-2020	200.229.248.0/24	ASN 1921 - NIC.at head office Salzburg	RPKI-invalid origin
06-jul-2020	200.219.154.0/24	ASN 1921 - NIC.at head office Salzburg	RPKI-invalid origin
06-jul-2020	200.229.248.0/24	ASN 1921 - NIC.at head office Salzburg	RPKI-invalid origin
06-jul-2020	2001:12f8:2::/48	ASN 1921 - NIC.at head office Salzburg	RPKI-invalid origin
06-jul-2020	2001:12f8:4::/48	ASN 1921 - NIC.at head office Salzburg	RPKI-invalid origin
30-jun-2020	200.107.82.0/24	ASN 23456	RPKI-invalid origin

Extras

Reporte mensual



Reportes técnicos



Los invitamos a:

Revisar el sitio:

- Reportar errores
- Sugerencias de mejoras
- Nuevas funcionalidades
- Utilizar la información para toma de decisiones

¡Muchas gracias!

Proyecto FORT: https://fortproject.net/

Monitoreo FORT: https://monitor.fortproject.net/

online meeting
lacnic34
lacnog2020