MANRS

Normas Mutuamente Acordadas para el Enrutamiento Seguro en Internet:

Operadores de Red de Universidades

MANRS

Contenido

- Introducción
- MANRS para Operadores de Red de Universidades
- Experiencia: Retos, Aciertos y Áreas de Oportunidad
- Preguntas y Respuestas

MANRS

Introducción

MANRS en Universidades: Actores

La Corporación Universitaria para el Desarrollo de Internet (CUDI), es una asociación civil sin fines de lucro que gestiona la Red Nacional de Educación e Investigación (RNEI) para promover el desarrollo de nuestro país y aumentar la sinergia entre sus integrantes; cuenta con 266 miembros.

La ANUIES es una asociación civil y principal promotor de la educación superior en México, cuenta actualmente con 191 Instituciones de Educación Superior afiliadas que son las más importantes a nivel nacional, dentro del que hacer de la ANUIES se ha creado el Comité de Tecnologías de la Información y Comunicaciones (**ANUIES-TIC**) que asesora y promueve sobre las mejores prácticas para el uso y aprovechamiento de las tecnologías de la información y comunicaciones (TIC) en las IES.

Cooperación Latino Americana de Redes Avanzadas, es una Organización de Derecho Internacional sin fines de lucro. Desarrolla y opera la única red de Internet Avanzada de América Latina interconectando a RNIEs de 12 países y conectarlas a las redes académicas avanzadas del resto del mundo para beneficiar el desarrollo de la ciencia y la academia, generando capacidades para investigaciones intraregionales y transcontinentales en todas las áreas del saber, potenciando el desarrollo de aplicaciones que eliminan fronteras.

MANRS

Clave: Acciones Coordinadas de la Comunidad LAC

lacnic

Internet Society

lacnog

NIC MÉXICO

Red CLARA

ANUIES

ANUIES - TIC

cudi

MANRS

Antecedentes

Todos los que operan una red son corresponsables de la estabilidad del ruteo global, es una responsabilidad compartida.

Los Operadores de Red de las Universidades no quedamos excentos de esa responsabilidad.

Una mala configuración de una red no solo afecta el servicio para sus usuarios, sino que puede afectar a otros operadores en cualquier parte del mundo.

Desafíos en el Ecosistema

Si bien las cualidades del sistema de enrutamiento han permitido su éxito en general, estos mismos atributos pueden contribuir también a algunos de sus desafíos.

En 2017 hubo cerca de 14,000 incidentes de enrutamiento registrados en total. Los incidentes afectaron a más del 10% de los sistemas autónomos (AS) en Internet.

Hay tres tipos principales de incidentes de enrutamiento:

- **Apropiación de ruta/prefijo**
- **Fugas de ruta**
- **Falsificación de IP**

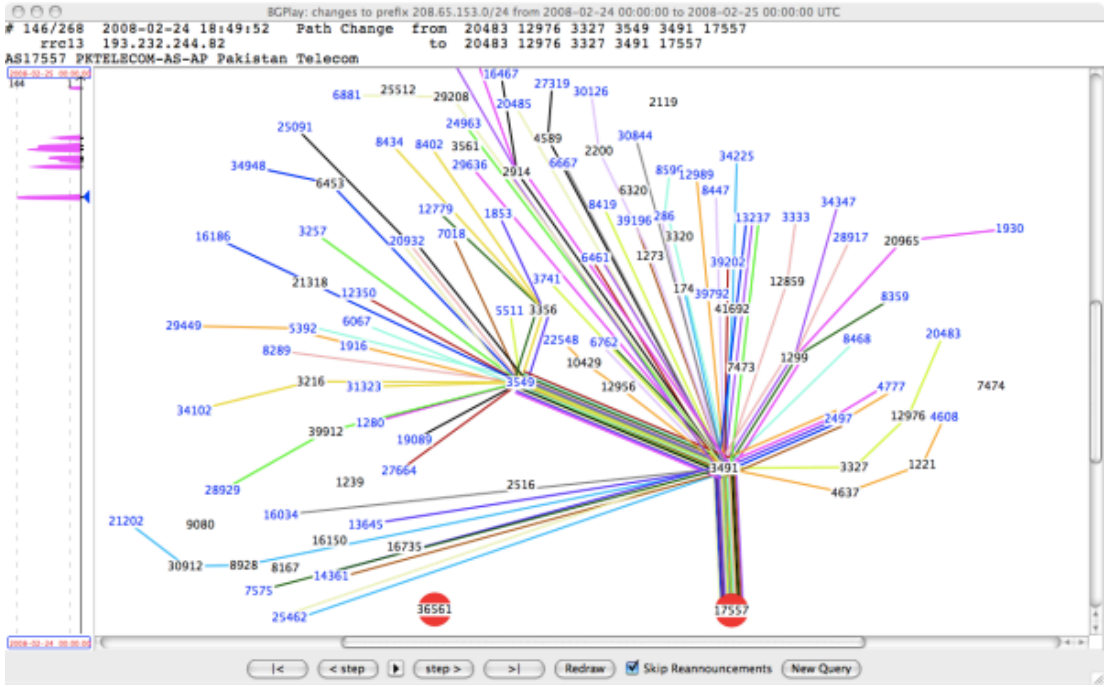
Desafíos en el Ecosistema

- Esos incidentes pueden ejercer mucha presión sobre la infraestructura y provocar caída de tráfico, proveer los medios para la inspección de tráfico o incluso usarse para realizar ataques de amplificación de servidores de nombres de dominio (DNS) o cualquier otro ataque de amplificación reflectiva (RA).
- Las prácticas recomendadas en la seguridad del enrutamiento ya están disponibles y se consideran muy efectivas en contra de estas formas de incidentes de enrutamiento.

Apropiación de ruta/prefijo

Fugas de ruta

Falsificación de IP

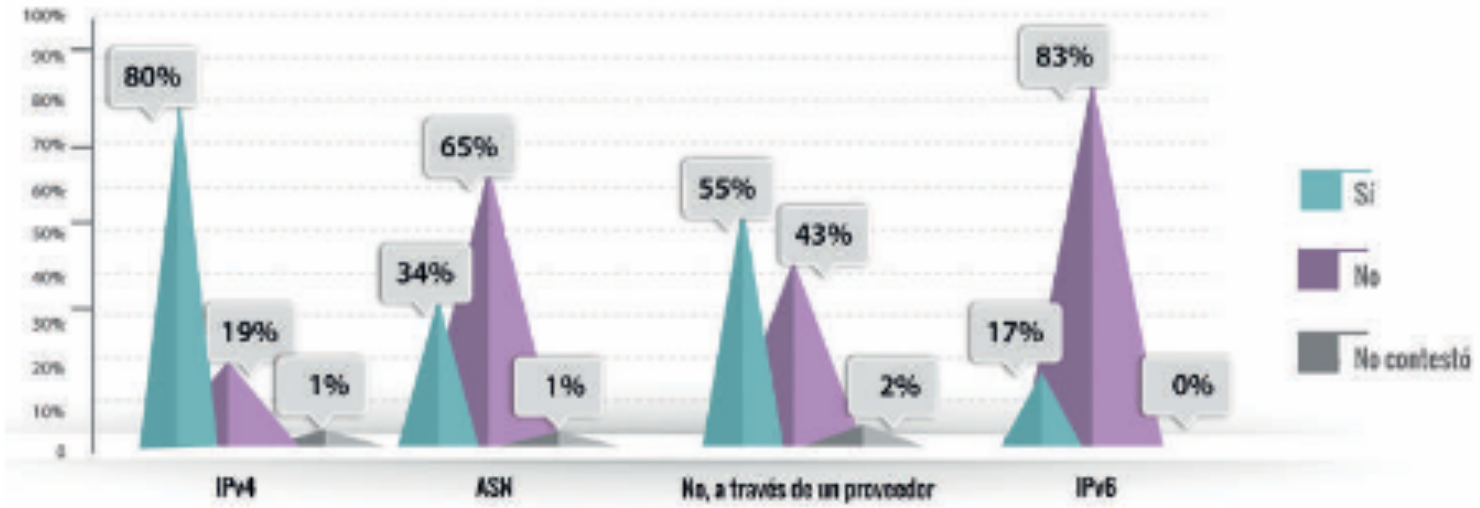


MANRS

Estado actual de las Tecnologías de la Información y Comunicaciones en las Instituciones de Educación Superior en México Estudio 2018.

IES que cuentan con servicios propios o públicos de Internet

Figura 2.9.12 IES que cuentan con servicios propios/públicos de Internet



"4 de cada 5 IES entrevistadas cuentan con redes IPv4 públicas".

Recursos de Internet en Universidad de México:

34% cuentan con ASN

http://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2018.pdf

Análisis de Indicadores: Encuesta ANUIES-TIC 2018

¿Qué mecanismos utiliza para proteger la infraestructura y los sistemas de información?

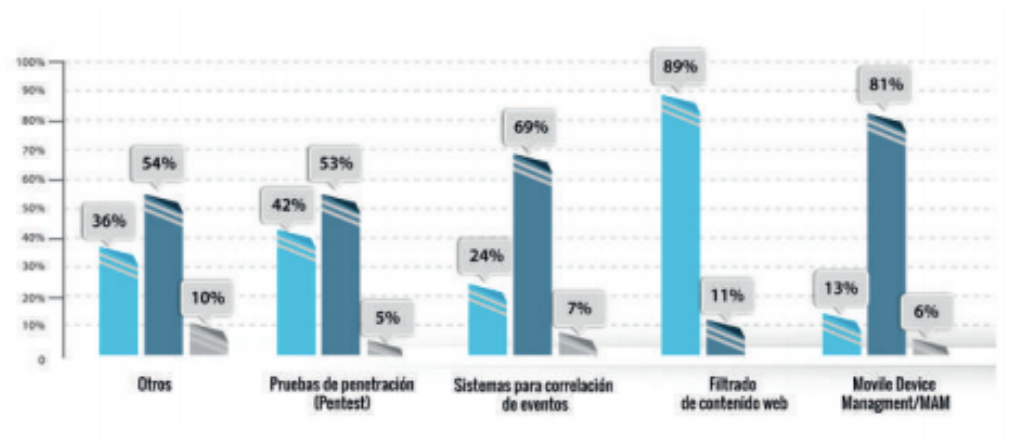
- Pruebas de penetración (Pentest)
- Sistemas para correlación de eventos
- Filtrado de contenido web
- Mobile Device Management/MAM
- DLP
- UTM
- Autenticación con mecanismos biométricos
- Cifrado de archivos
- Control de acceso (passwords)
- Buenas prácticas para desarrollo de software
- Https para sitios web
- Firma electrónica/pki
- Seguridad perimetral (fw, ngfw, ips, ids)
- Análisis de vulnerabilidades
- Gateway Anti-spam
- Software Antimalware
- Otros

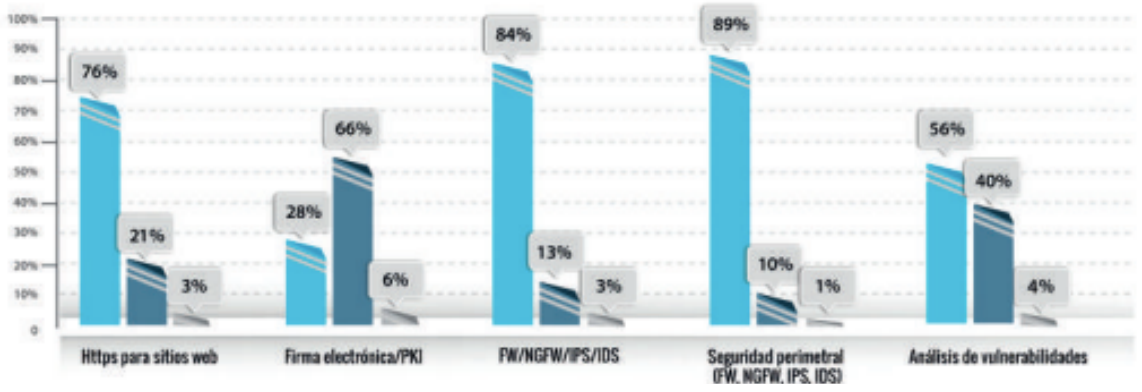
http://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2018.pdf

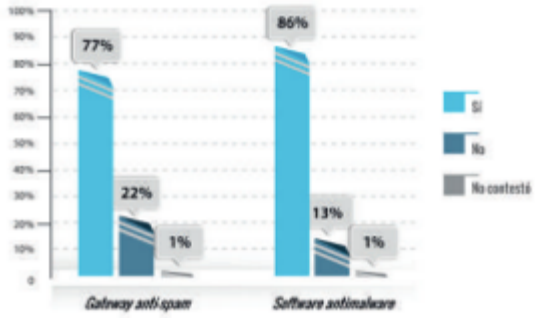
MANRS

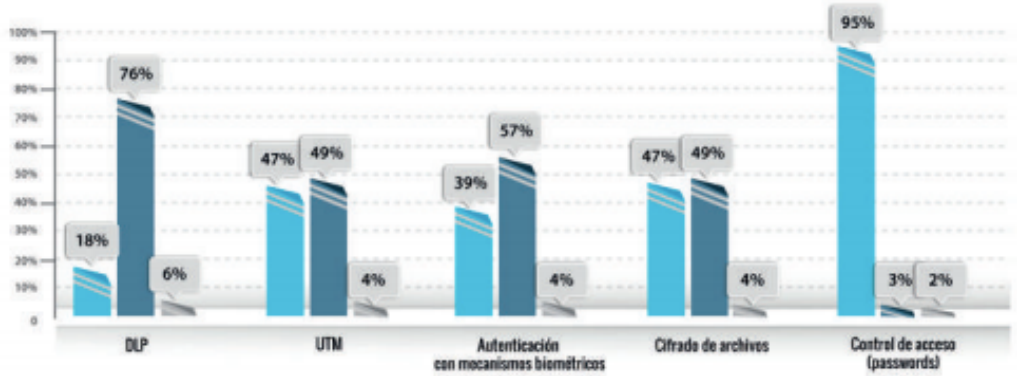
Indicadores: Mecanismos para proteger la infraestructura y los sistemas de información

Figura 2.5.12 Mecanismos para proteger la infraestructura y los sistemas de información









http://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2018.pdf

Hallazgos y Áreas de Oportunidad

- El 34% de las Universidades de México que respondieron la encuesta, cuentan con ASN.
- No se cuentan estadísticas sobre los mecanismos de seguridad en el ruteo.
- Se cuenta con una comunidad de operadores de red de universidades en México, en el que se encuentran expertos en buenas prácticas de ruteo.
- Universidades que solo requieren perfeccionamiento de filtrado y antispoofing, pero con desconocimiento de la importancia de RPKI y actualización de información del WhoIs.
- Desconocimiento de MANRS en la comunidad de Operadores de Red de las Universidades

Propuesta

Propuesta:

- Incluir reactivos en la encuesta ANUIES-TIC 2019 sobre Seguridad en el Ruteo.
- Taller: MANRS para Operadores de Red de Universidades
  - Cinco sesiones virtuales con frecuencia mensual: duración de una hora.
  - Un taller presencial con duración de 8 horas.

Propuesta: Incluir reactivos en la encuesta ANUIES-TIC 2019 sobre Seguridad en el Ruteo

¿Su Universidad aplica alguno de los siguientes mecanismos para la seguridad en el ruteo BGP?

- Filtrado BGP: Prefix-list, AS-PATH
- Prefijos definidos en el RFC1918
- Anti-spoofing BCP38 (RFC 2827)
- Buenas prácticas para la configuración del plano de control del ruteador perimetral - RFC6192
- Información de contacto actualizada a nivel mundial en bases de datos de enrutamiento comunes: Whois
- Recursos de Internet Certificado: RPKI (Resource Public Key Infraestructure)
- ROAs (Route Origination Authorizations)
- Registro en un IRR (Internet Routing Registry

Indique qué tipo de incidentes de enrutamiento se han presentado en los últimos 12 meses:

- Route Hijacking (secuestro de rutas
- Route Leak (fuga de rutas)
- IP Address Spoofing (Falsificación de direccionamiento ip)

Inclusión en la pregunta 5.9 "Indique cuáles son las necesidades de sus administradores en cuanto a TI y seguridad":

- Seguridad de Ruteadores
- Configuración BGP/RPKI

MANRS

Enfrentemos en conjunto …

- Los operadores de red tienen la responsabilidad de garantizar una infraestructura de enrutamiento segura y robusta a nivel mundial.
- La seguridad de la red depende de una infraestructura de enrutamiento que elimine a los malos actores: configuraciones erróneas y accidentales que puedan causar estragos en Internet.
- Cuantos más operadores de red trabajen juntos, menos incidentes habrá y menos daño podrán hacer.

lacnic

Internet Society

lacnog

Red CLARA

NIC MÉXICO

ANUIES

ANUIES - TIC

cudi

Corporación Universitaria para el Desarrollo de Internet A.C.

Internet 2 - México

MANRS

Taller MANRS para Operadores de Red de Universidades

¿Porqué MANRS?
Redes de Educación e Investigación

- Mostrar liderazgo técnico y diferenciarse de los ISPs comerciales.
- Para ayudar a resolver los problemas de la red global. Las Redes Nacionales de Educación e Investigación (RNEI) son a menudo los primeros en adoptar nuevos desarrollos.
- Liderar con el ejemplo y mejorar la seguridad de enrutamiento para todos.
- Promover el cumplimiento de MANRS a clientes y proveedores centrados en la seguridad.

MANRS

Colaboración

- Agosto de 2018: Universidad Pública de México en MANRS
- Diciembre 2018: Propuesta de difusión de MANS en ANUIES
- Enero – Febrero 2019: Gestión del Proyecto con las partes interesadas. Reuniones, logística, ponentes, etc.
- Se suma RedClara.
- Marzo 2019: Invitación a CIOs de ANUIES, se solicita designar a Operador de Red.
- Abril 2019: Arranque de las sesiones.
- Respuesta: 50 participantes por sesión.
- Junio de 2019: MANRS Observatory beta testing

lacnic

Internet Society

lacnog

NIC MÉXICO

Red CLARA

ANUIES

ANUIES - TIC

cudi

Corporación Universitaria para el Desarrollo de Internet A.C.

Internet 2 - México

MANRS

Normas Mutuamente Acordadas para Enrutamiento Seguro en Internet para Operadores de Red de Universidades

El taller consta de **5 sesiones virtuales**

- Sesión 1: Jueves 25 de abril – Introducción a MANRS
- Sesión 2: Jueves 23 de mayo – MANRS: Acción 1 – Filtrado
- Sesión 3: Jueves 13 de junio – MANRS: Acción 2 – Anti-Spoofing
- Sesión 4: Jueves 11 de julio – MANRS: Acción 3 – Coordinación
- Sesión 5: Jueves 22 de agosto – MANRS: Acción 4 – Validación Global

La conclusión será con **una sesión presencial** en el marco de los eventos:

- Encuentro TICAL 2019, 2 – 4 de septiembre de 2019 en Cancún, México.
- Encuentro ANUIES-TIC 2019, 2 de octubre de 2019 en la UANL, Nuevo León, México.

ANUIES · ANUIES - TIC · cudi Corporación Universitaria para el Desarrollo de Internet A.C. Internet 2 - México · Red CLARA · Internet Society · lacnic · NIC MÉXICO

Ponentes

Estrategia de contenido en las sesiones

- Sensibilización: Antecedentes / Introducción
- Teoría con ejemplos de configuraciones: Acciones de MANRS
- Caso Práctico: Experiencia de participación en MANRS un Operador de Red de Universidad
- Referencias Bibliográficas

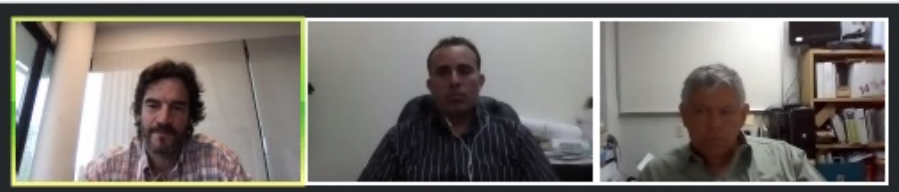
Las sesiones son grabadas, y posteriormente puesta a disposición en un repositorio junto con las presentaciones:

https://isoc.box.com/s/cz8iug9rte3afatiytor6vr9wteavt2h

Contenido de las sesiones

- Bienvenida, Reforzamiento de la Colaboración y Presentación de los Ponentes
- Sensibilización: Antecedentes / Introducción
- Teoría con ejemplos de configuraciones: Acciones de MANRS
- Caso Práctico: Experiencia de un Operador de Red
- Referencias Bibliográficas
- Preguntas y Respuestas
- Recordatorio de Próxima Sesión

Zoom



Recording

Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack*
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	*September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.*
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplificationattack reported by Akamai*

Participantes (56)

Escribir para filtrar...

- MG Miguel Gaspar - Paraguay Ciberseguro
- MR Miguel Rojas - UAM
- OM Omar Mtz (UG)
- PF Pedro Flores Montebello
- SEMS UDG
- SC Silvia Chávez
- TI Tobias INAOE
- U UADY
- U Uciel
- U UCTA
- V Victor
- X XDiaz
- JR Jesus Rmz (UAQ)

Zoom

Recording

MANRS Filtros con AS-PATH- Ejemplo

```
...
 neighbor 198.51.100.22 filter-list 11 out
...


ip as-path access-list 11 deny 64496$
ip as-path access-list 11 deny ^645
ip as-path access-list 11 permit _64497_64498_
...
```

Participantes (50)

Escribir para filtrar...

- Carmen Denis (coanfitrión, yo)
- Chris OFla (Anfitrión)
- Silvia Chávez
- Adrian Cinves
- Aleiandro Cuadra

Silenciar a todos | Activar todos | Más

Chatear

De mí para Chris OFla: (En privado)
Hola Christian, buenas tardes

De Chris OFla para mí: (En privado)
Hola Carmen!
Buenas tardes :-)
todo listo?

De mí para Chris OFla: (En privado)
Hola! Puedo apoyar como moderador, solo cuando me toque hablar no podré
Si, todo listo!

Para: Todos | Más

Escribir mensaje aquí...

MANRS

Repositorio

Internet Society

Log in to Box to save all files you view in your Recents and return to them at any time.

MANRS - Webinars

Name	Updated	Size
MANRS-Sesion-3-Anti-Spoofing.mp4	Yesterday by Israel Rosas	333.3 MB
MANRS-Sesion-3-Anti-Spoofing.pdf	Jun 13, 2019 by Israel Rosas	5.4 MB
MANRS-Sesion-2-Filtrado.pdf	May 27, 2019 by Israel Rosas	4.3 MB
MANRS-Sesion-1-Introduccion.pdf	May 27, 2019 by Israel Rosas	5 MB
MANRS-Sesion-2-Filtrado.mp4	May 27, 2019 by Israel Rosas	199.1 MB
MANRS-Sesion-1-Introduccion.mp4	May 27, 2019 by Israel Rosas	174.6 MB

Logística:
Consejos claves

- Minuta de seguimiento previa a las sesiones: revisar contenido de las presentaciones
- Fotografía y Reseña de los Ponentes
- Invitación al Taller de MANRS a través del CIO de la Organización: designar al Operador de Red que participará
- Sistema de Registro
- Difusión: Mail y Redes Sociales
- Grabaciones y Presentaciones: https://isoc.box.com/s/cz8iug9rte3afatiytor6vr9wteavt2h

MANRS

Difusión

InternetSocietyLAC @ISOC_... Apr 24
Nuevo día para participar del taller "Introducción a #MANRS" ➡️➡️
Jueves 25 de abril a las 18:00 UTC.
Regístrate aquí: ow.ly/QoKq50rsfxj
#Enrutamiento #Seguro #Internet

ANUIES-TIC @anuiestic
Recuerda inscribirte a la c
Sesión del taller "Introduc
#MANRS" en:
anuies.symposium.events/
sesio...
Este taller es gracias a Int
Society América Latina y e
@ISOC_LAC @lacnic @NIC
@RedCLARA y @RedCUDI
Conoce más de @RoutingMANRS en:
manrs.org

Red CUDI @RedCUDI Jun 12
¡Es mañana! Tercera Sesión del Taller sobre @RoutingMANRS | bit.ly/manrs-3-19-spf...

Los ponentes son: @Olmosv6 de @UDG_CGTI y @blackserr de @uady_mx.

Una colaboración de @ISOC_LAC @RedCLARA @NICMX @lacnic @anuiestic @udg_oficial @UADYoficial y @RedCUDI

RedCLARA @RedCLARA 3d
11 de julio: Taller #MANRS, de @ISOC_LAC, llega a su cuarta sesión, con el tema "Coordinación".
¡Regístrese ahora mismo y participe!
bit.ly/2LBmlDF

InternetSocietyLAC @ISOC_... May 22
¿Cuánto sabes sobre la #seguridad de #enrutamiento? Mañana, a las 18:00 UTC, hay un nuevo Taller sobre #MANRS 👉 ¡Todavía estás a tiempo de registrarte! ➡️
ow.ly/T8Ub50umJfY @RedCUDI @lacnic @ANUIES @RedCLARA @NICMX #Enrutamiento #Seguridad #Internet

MANRS

Preparación del Taller Presencial:

TICAL 2019

ANUIES-TIC 2019

s

Objetivos del Taller

- Despertar conciencia e impulsar acciones para mejorar la seguridad y la coordinación en el ruteo global de Internet reduciendo los problemas que afectan a la estabilidad y resiliencia del servicio.
- Proveer un marco para que los operadores de red de universidades entiendan y se ocupen de los temas relativos a la resiliencia y seguridad del sistema de enrutamiento global de Internet.
- Promover una cultura de responsabilidad colectiva para la resiliencia y seguridad del sistema de ruteo global de Internet.
- Guiar a los operadores de red de universidades en la utilización de RPKI, filtrados y otras técnicas que ayudan a prevenir problemas de ruteo.
- Demostrar la capacidad de los operadores de red de universidades para resolver los problemas de seguridad y resiliencia de Internet.
- Proporcionar las herramientas de autoevaluación disponibles para facilitar el camino de participación en MANRS.

Taller presencial el TICAL y ANUIES-TIC

Temario:

- Filtrado: prevención de la propagación de información de enrutamiento incorrecta.
- Anti-Spoofing: prevención del tráfico con direcciones IP de origen falsificadas.
- Coordinación -Facilitar la comunicación operacional y la coordinación global entre operadores de red.
- Validación global: facilitar la validaciónde la información de enrutamiento a escala global.
- Prácticas de las acciones 1, 2, 3 y 4 de MARNS.
- MANRS Observatory: acceso a la plataforma beta para consultar y analizar el estado del sistema de ruteo de las universidades participantes.

MANRS

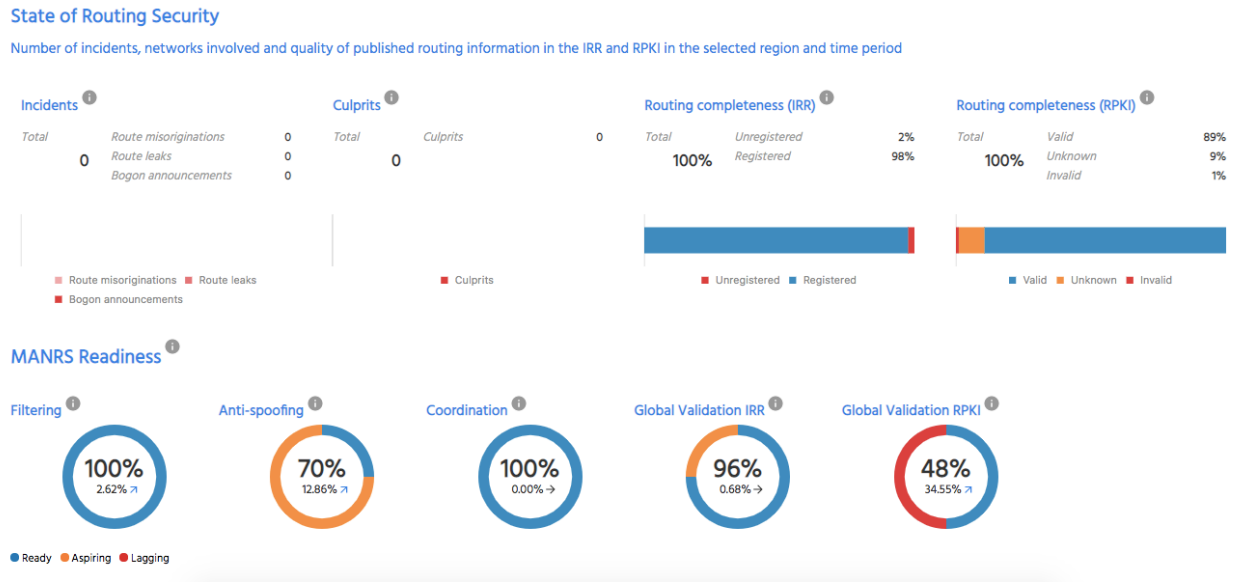
Herramientas de Autoevaluación en el Taller Presencial: MANRS Observatory

MANRS Observatory

- En el taller presencial se accederá a la plataforma beta para ayudar a analizar el estado de la seguridad y resilencia del sistema de ruteo de las universidades participantes, con el apoyo de Andrei Robachevsky, Senior Technology Programme Manager – ISOC.

Las siguientes compañias han contribuido grandemente en el desarrollo y operación de MANRS Observatory:

- Data sources:APNIC
- RIPE NCC
- CAIDA
- BGPMon/BGPStream
- Developers:Frontwerks
- NLNetLabs
- Operations:Internet Society



Herramientas adicionales de autoevaluación: Coordinación

Check that contacts are in the whois

- whois -h whois.lacnic.net prefix

Check that contact info is registered in the PeeringDB:

- https://www.peeringdb.com/asn/[ASN]

Herramientas adicionales de autoevaluación: Validation Global

Check that routing information is registered in an IRR or has ROA

- http://localcert.ripe.net:8088/bgp-preview
- https://milacnic.lacnic.net/lacnic/rpki/state

MANRS

Bibliografía

https://www.manrs.org/

https://www.manrs.org/wp-content/uploads/sites/14/2018/03/MANRS-BCOP-20170125.pdf

https://www.internetsociety.org/es/issues/manrs-es/

https://www.internetsociety.org/es/blog/2018/08/tech-companies-endorse-manrs-routing-security-actions/

https://www.lacnic.net/innovaportal/file/3512/1/bgp_buenas_practicas_2019a.pdf

https://www.lacnic.net/innovaportal/file/3512/1/20190510_marns_universidades_tutorial_peeringlacnic31.pdf

https://www.lacnic.net/innovaportal/file/3139/1/bgp-rosario-lacnic30.pdf

https://www.youtube.com/watch?v=eUSjVqj5ib4

MANRS

Bibliografía

- Understanding Unicast Reverse Path Forwarding
  - https://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html
- Security Configuration Guide: Unicast Reverse Path Forwarding
  - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_urpf/configuration/xe-3s/sec-data-urpf-xe-3s-book.html
- Configuring ACL Cisco:
  - https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html
- RFC 2267Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
  - https://www.ietf.org/rfc/rfc2267.txt
- Cisco Guide to Harden Cisco IOS Device:
  - https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Acciones Coordinadas

lacnic

Internet Society

lacnog

MANRS

NIC MÉXICO

Red CLARA

ANUIES

ANUIES - TIC

cudi

Preguntas

Gracias

Juan Herrera
Juan.hcorrea@gmail.com

Carmen Denis
Cdenis.polanco@gmail.com