

Seguridad, Estabilidad y Resiliencia de Internet en la Región de LACNIC



Gillermo Cicileo / guillermo @ lacnic.net
César Díaz / cesar @ lacnic.net
Carlos M. Martinez / carlos @ lacnic.net

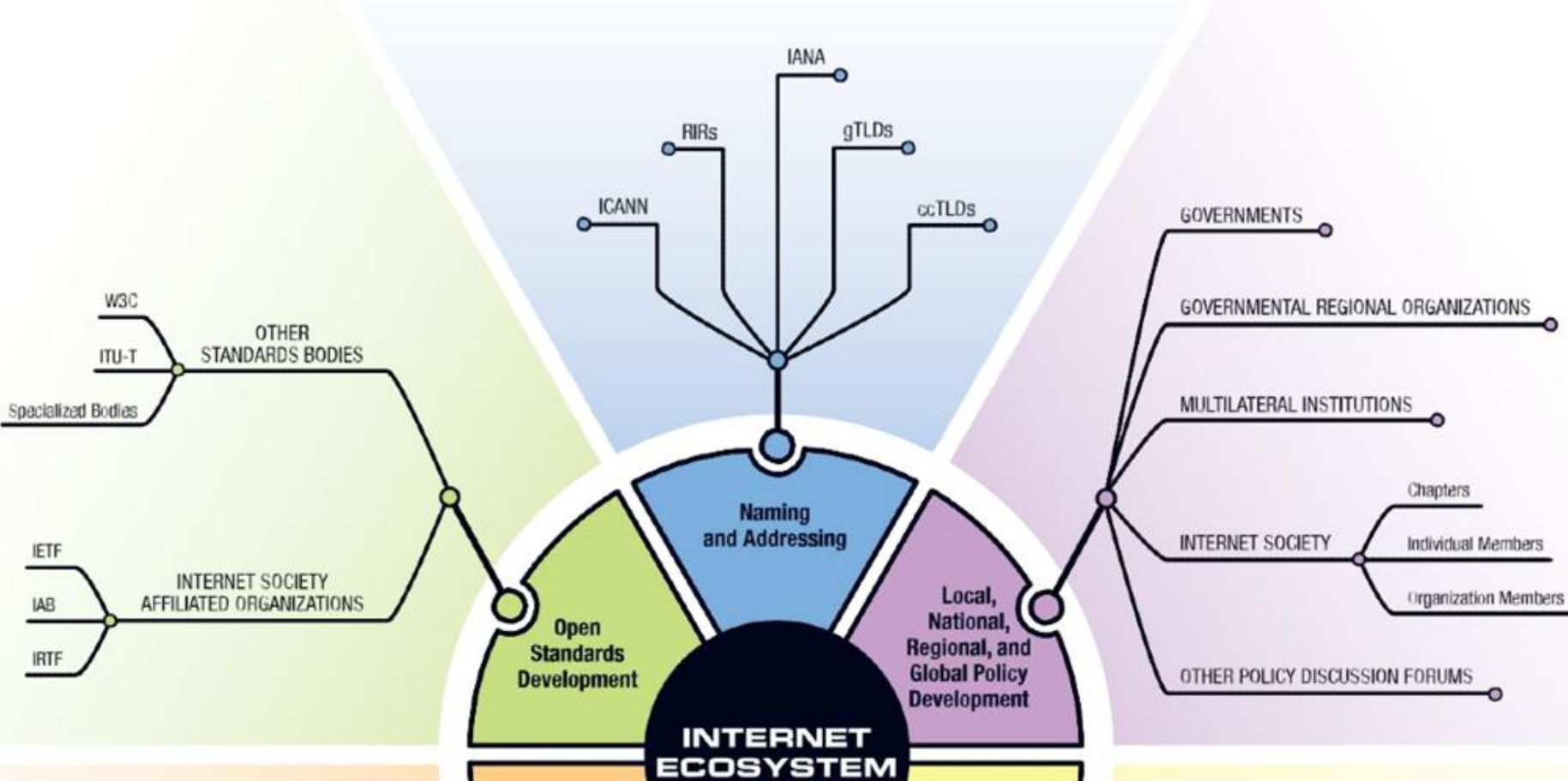
Visión de LACNIC como organización

“Liderar la creación de sinergias e iniciativas para la construcción de una Internet abierta, estable y segura al servicio del desarrollo económico, social y cultural de América Latina y el Caribe”

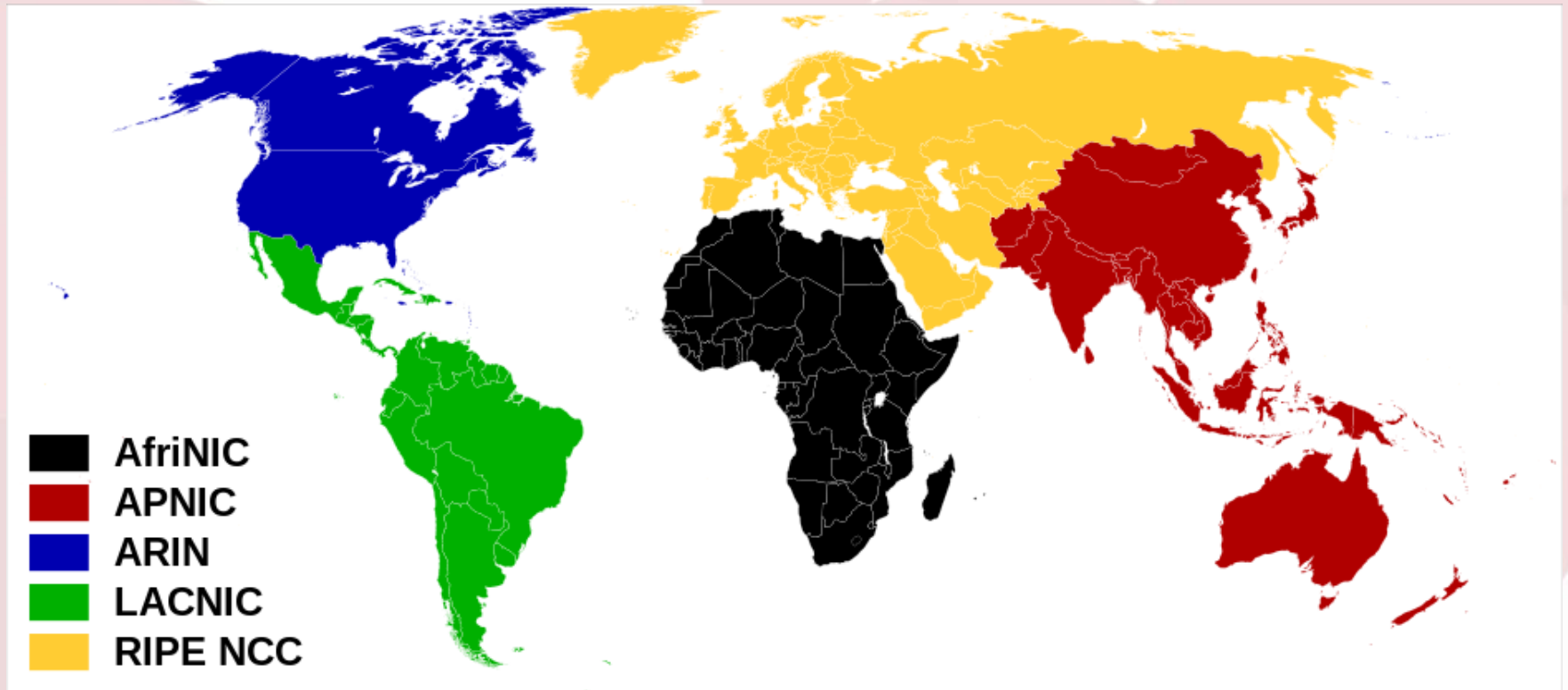
Seguridad, Estabilidad y Resiliencia

- Para LACNIC los conceptos conocidos como “SSR” forman parte de un conjunto
- Seguridad
 - *Libre de riesgos y peligros*
- Estabilidad
 - *Permanencia, continuidad y predecibilidad en el tiempo*
- Resiliencia
 - *Capacidad de recuperación y de auto-reparación*

Ecosistema de Gobernanza de Internet



Gestión de los Recursos Numéricos de Internet

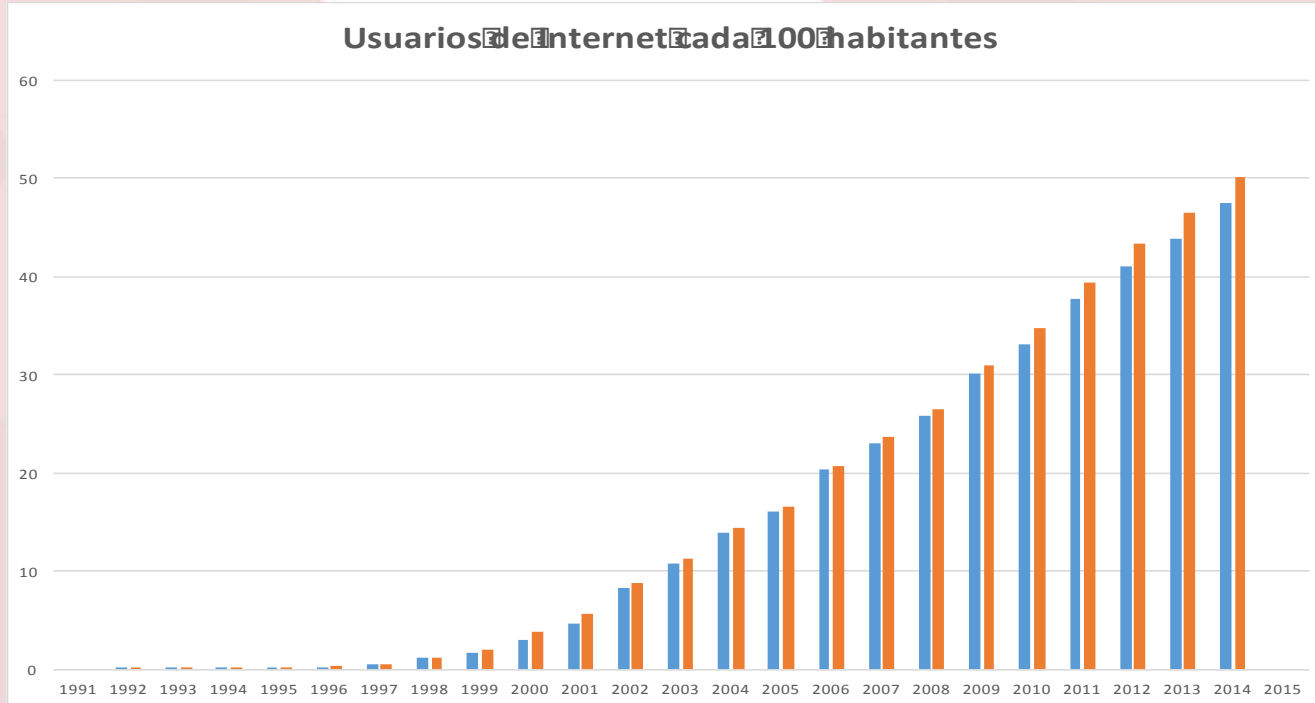


Alcance de nuestra comunidad

- La comunidad de LACNIC (y de los RIRs) es una comunidad abierta, donde cualquier persona u organización con un interés en la evolución y futuro de Internet puede participar
- Naturalmente, la mayor parte de los miembros de la comunidad surgen de
 - Proveedores de servicio de Internet
 - Proveedores de contenido
 - IXPs
 - Sector académico

Banda ancha en América Latina

- La penetración de la banda ancha en América Latina ha crecido dramáticamente durante los últimos años



Fuente: Banco Mundial

[<http://datos.bancomundial.org/indicador/IT.NET.USER.P2>]

- Esto introduce nuevos desafíos que no existían durante la era del dialup y de las redes *'narrowband'*

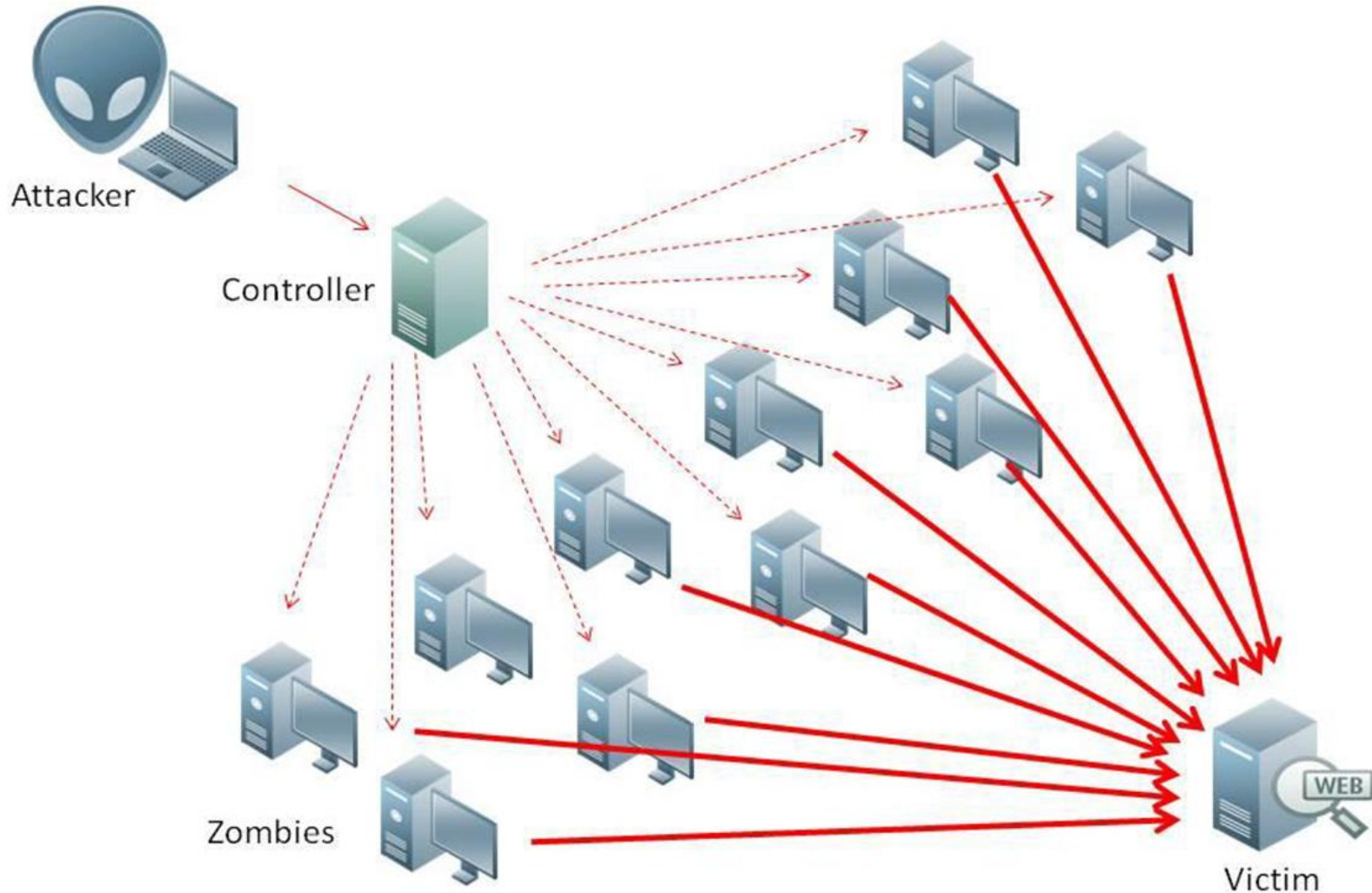
Evolución de los tipos de amenazas

- Prehistoria:
 - Virus ‘binarios’, propagados por intercambio de dispositivos de almacenamiento
- Año 1995-2000:
 - Surgimiento de los primeros ‘virus de macros’, asociados a documentos Word y similares, propagados por e-mail
 - *Spam*
- Año 2000: Gusanos / virus
 - SQL Slammer y similares, explosión de la ‘explotación remota’ (*remote exploits*)
 - *Spam*
- Año 2010:
 - Ataques masivos de denegación de servicio, botnets
 - *Spam*

Nuevos desafíos

- A medida que el grado de interconexión tanto
 - Física
 - A nivel de intercambio de información
- A medida que aumenta el uso de Internet como vehículo transaccional
 - eBanking, declaraciones impositivas
- ...
- El “valor” de un usuario o de un dispositivo para un atacante es cada vez mayor
- Surgen nuevas amenazas y nuevos usos maliciosos de la red

Ataques de denegación de servicio



Estonia

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences



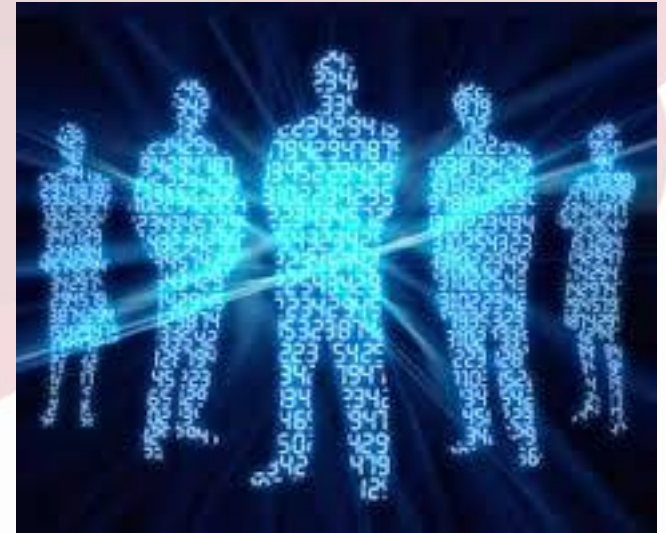
Diferentes planos

- Seguridad en infraestructura
 - Planta física
 - Integridad del DNS – sistema de nombre de dominios
 - Integridad del enrutamiento
 - Integridad en los servicios de directorio (WHOIS)



Diferentes planos (ii)

- Aspectos humanos
 - Conocimiento de los usuarios
 - Variedad y diversidad de aplicaciones
 - Modelos de seguridad
 - Modelos de distribución de software
 - Seguridad a nivel de las plataformas



Diferentes planos (iii)

- Aspectos de gobernanza de Internet
 - Reconocer a los diferentes *stakeholders* en sus roles específicos
- Interrelación entre diferentes actores
 - Agencias de '*law enforcement*'
 - Proveedores de servicio de Internet
 - Comunidad de usuarios



Programa de SSR para Internet de LACNIC

- Ejes principales
 - Fortalecimiento y protección de infraestructura
 - Creación de capacidades humanas
 - Difusión, cooperación e investigación

Fortalecimiento de Infraestructura

- SSR en enrutamiento
 - Proyecto de Certificación de Recursos (RPKI)
 - Emisión de firmas y certificados digitales para permitir validar anuncios de rutas
 - Fomento a la creación de puntos de intercambio de tráfico (IXP)
- Seguridad en el DNS
 - Despliegue de DNSSEC a nivel de la resolución **reversa**
 - Programa +Raíces, despliegue de copias de servidores raíz del DNS en nuestra región
- Despliegue de IPv6
 - *Una Internet basada dependiente de CGN sería más frágil*

Creación de capacidades humanas

- Cursos de capacitación virtuales y presenciales
 - DNSSEC
 - Enrutamiento con BGP y RPKI
 - Despliegue de IPv6
- Talleres sobre creación de grupos de respuesta a incidentes de seguridad (CSIRTs)
 - Talleres AMPARO

Difusión, cooperación e investigación

- LACNIC WARP, <http://warp.lacnic.net>
 - Servicio de mediación de incidentes (*incident brokering*)
 - Nos apoyamos en la fuerte relación que tenemos con nuestros miembros para hacerles llegar información sobre potenciales incidentes de seguridad que LACNIC recibe por otras vías
- Generación de reportes y estadísticas
- Colaboración con otras organizaciones en diferentes actividades

Reflexiones finales

- A medida que la red evoluciona hemos visto como también evolucionan las amenazas
 - Debemos aprovechar este conocimiento para tratar de estar un paso adelante de esta evolución
 - *Internet of Things ?*
- Los problemas técnicos pueden resolverse con mayor o menor esfuerzo, los problemas *humanos* son los más difíciles de resolver
- Todos los actores, en sus diferentes roles, tienen responsabilidad sobre el mantenimiento de una Internet abierta, estable y segura

Algunas referencias

- “Evolving Threat Landscape”, ENISA
 - <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014>
- “DDoS Attack Trends”, Imperva
 - https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf

¡Muchas Gracias!