Resumen ejecutivo

El mito de la ciberseguridad:

Por qué las soluciones parciales no son suficientes y cómo EzIP ofrece un camino más sencillo y seguro.

Internet impulsa la sociedad moderna, pero sigue siendo vulnerable. Las recientes interrupciones globales en Cloudflare (noviembre de 2025) y las frecuentes fallas en Amazon Web Services ponen de manifiesto la fragilidad persistente, incluso entre los principales proveedores diseñados para mejorar la seguridad y la confiabilidad. Las iniciativas federales (FCC NPRM, 2024) y la Hoja de Ruta de la Casa Blanca para mejorar la seguridad del enrutamiento de Internet (2024) se centran en el Protocolo de Puerta de Enlace de Frontera (BGP) para un monitoreo y validación más rigurosos. Estas medidas son útiles, pero abordan los síntomas de un problema más profundo: la escasez original de direcciones IPv4. Para hacer frente a la limitación de direcciones:

- La asignación dinámica (DHCP) hizo que las direcciones IP fueran temporales.
- El DNS rastreaba los cambios.
- Las redes se fragmentaron en miles de dominios (Sistemas Autónomos), que dependían de BGP para conectarse entre sí.
- Las redes de distribución de contenido (CDN) centralizaron el tráfico para gestionar la complejidad..

Esta arquitectura genera confusión, puntos únicos de fallo y ventajas para los atacantes: las direcciones falsificadas son fáciles de usar y difíciles de rastrear, mientras que los usuarios legítimos dejan registros claros. Las redes de distribución de contenido (CDN) centralizadas se convierten en objetivos principales, y las actualizaciones de seguridad añaden más capas sin resolver la causa raíz. EzIP (Easy IPv4) soluciona este problema recuperando el bloque IPv4 240/4, reservado durante mucho tiempo, para proporcionar direcciones públicas estáticas y únicas a millones de ubicaciones, suficientes para dar servicio a regiones enteras sin reasignación dinámica ni una dependencia excesiva de protocolos problemáticos. Beneficios clave:

• Mayor seguridad intrínseca: Las direcciones estáticas permiten detectar la suplantación de identidad, mejoran la trazabilidad y reducen la superficie de ataque por diseño.
• Mayor fiabilidad: La menor complejidad reduce los riesgos de interrupciones; la geolocalización precisa facilita la gestión y la respuesta.
• Mínima interrupción: Se superpone a la infraestructura de Internet existente, se implementa gradualmente mediante enrutadores regionales mejorados y no requiere actualizaciones masivas de dispositivos.
• Ventajas adicionales: Reduce los riesgos de centralización, mejora la arquitectura de Internet y facilita la atribución de responsabilidades en la aplicación de la ley.

EzIP complementa IPv6 y las herramientas existentes al abordar la escasez fundamental que hacía que internet fuera vulnerable. Se alinea con los objetivos de una infraestructura digital más resiliente y equitativa. Para un análisis completo, visite:

https://avinta.com/gallery/CyberSecurityMyth-ES.pdf

Preparado por: Abraham Y. Chen / Avinta Communications, Inc.
Contacto: AYChen@Avinta.com / +1(650)248-1829
Enero de 2026