Consultoría para la Implementación de un IXP Nacional para la Republica del Paraguay

Política de Uso Aceptable IXP-PY (PUAIX)

V1.0 – Agosto/2016

Asunción, Paraguay, 5 de agosto de 2016

Introducción (por ISOC)

El establecimiento de un IXP requiere la colaboración de multiples actores, muchos de los cuales son competidores que intercambiarán tráfico en el IXP. Inicialmente, algunos operadores podrían sentirse reticentes a colaborar con sus potenciales competidores. Resolver este desafío implica la construcción de comunidades locales de Internet y confianza entre los participantes. De hecho, la mayor parte del tiempo y el esfuerzo necesarios para instalar un IXP se invierte en desarrollar confianza, un entendimiento común y acuerdos dentro de la comunidad local. Los aspectos técnicos de un punto de intercambio de Internet suelen ser muy sencillos; sin embargo, dado que el desarrollo de las relaciones entre las partes interesadas es tan importante para el éxito de un IXP, suele decirse que la creación de un IXP requiere “80 por ciento de ingeniería social y 20 por ciento de ingeniería técnica”.

Contenido cursado por el IXP

- El IXP es neutral y transparente. No hace la verificación del contenido del trafico.
- Los participantes son responsables por cumplir con lo dispuesto en las leyes, normativas e regulaciones que se aplican, y por esta Política de Uso Aceptable (PUA)
- Por el hecho de no controlar el contenido generado por los Participantes, el IXP no tiene ninguna responsabilidad por el mismo. El IXP es responsable solamente por su propio contenido.

Reglas Generales

- Equipamientos de rede disponibles de modo justo a todos los Participantes, sin impedimentos accidentales o deliberados

- Los Participantes deberán controlar y monitorear sus conexiones, para preservar la operación del IXP

- Esta PUA podrá ser modificada a cualquier tiempo por el CEIXP-PY, quedando la última versión disponible en la página Web del IXP

Prevención de inundación de la red (flooding) y ataques DOS

- Los Participantes deben monitorear sus redes 24 x 7 para evitar o mitigar ataques originados en sus redes

- Para reducir la probabilidad de ocurrencia de ataques, los Participantes deberán obedecer a todas las disposiciones contenidas en la Política de Requisitos Técnicos del IXP (PRTIX)

Accesos no autorizados

- Ningún uso del IXP podrá ser efectuado con propósitos ilegales y/o no éticos que violen a las leyes
- Los Participantes deberán tomar medidas para evitar accesos no autorizados
- Los Participantes no deberán divulgar informaciones de terceros o confidenciales
- Violaciones de sistemas y de la seguridad de las redes son prohibidas. El IXP ayudará a las autoridades locales a solucionar el problema legal
- El IXP se reserva el derecho de desconectar las puertas involucradas en actividades maliciosas