

**SAC 050**

**Bloqueo de DNS: Daños Versus Beneficios, Un Asesoramiento del Comité Asesor para la Seguridad y Estabilidad sobre el Bloqueo de Dominios de Nivel Superior en el Sistema de Nombres de Dominios**



Un Asesoramiento del  
Comité Asesor  
para la Seguridad y Estabilidad  
(SSAC) de ICANN  
14 de junio de 2011

## **Prefacio**

Este es un Asesoramiento del Comité Asesor para la Seguridad y Estabilidad (SSAC). El SSAC asesora a la comunidad ICANN y a la Junta Directiva sobre asuntos relacionados con la seguridad e integridad de los sistemas de adjudicación de nombres y direcciones en Internet. Esto incluye asuntos operativos (relativos a la operación correcta y confiable del sistema de nombres raíz), asuntos administrativos (relativos a la adjudicación de direcciones y de números de Internet), y asuntos de registro (relativos a los servicios de registro y de registradores). El SSAC realiza constantes evaluaciones de amenazas y análisis de riesgos de los servicios de adjudicación de nombres y direcciones para evaluar dónde residen las amenazas principales a la estabilidad y seguridad, y asesora a la comunidad de ICANN de acuerdo con esas investigaciones. El SSAC no tiene autoridad oficial para regular, imponer o adjudicar. Esas funciones corresponden a otros y el asesoramiento ofrecido aquí debe ser evaluado según sus méritos.

La lista de los que contribuyeron a este Asesoramiento, la referencia a las biografías de los miembros del comité y sus declaraciones de interés y las objeciones de los miembros del comité a los hallazgos o recomendaciones que figuran en este Asesoramiento, figuran al final de este documento.

## **Tabla de Contenidos**

**TOC**

## 1. Bloqueo de DNS: Daños versus Beneficios

El bloqueo o la alteración de respuestas a consultas sobre el Sistema de Nombres de Dominios (DNS) es cada vez más importante. El filtro a direcciones de nombres de Dominio o Protocolo de Internet (IP) (o evitar de otra manera el acceso al contenido de la web como política de seguridad) puede ser visto por algunas organizaciones como una extensión natural de los históricos controles de la telefonía, que apuntaban a bloquear su uso dentro de las organizaciones, para que las personas no incurrieran en un aumento de los gastos.

Los enfoques técnicos del bloqueo de DNS tienen por finalidad afectar a los usuarios dentro de un dominio administrativo dado, tal como una red pública o privada de operaciones. Impedir la resolución del nombre de dominio en una dirección IP evitará la conexión inmediata al servidor nombrado, aunque determinadas técnicas puedan permitir de todos modos la conexión con el sistema dado (esto incluye el simple acceso al sitio vía dirección IP más bien que vía un Nombre de Dominio Plenamente Válido (FQDN). Un operador de red o resolvidor DNS puede incluso re-escribir una respuesta DNS que contenga una dirección IP mediante una representación de las opciones del operador, sea re-escribiendo una respuesta para un Dominio No Existente (NXDOMAIN) o re-escribiendo la respuesta DNS para un FQDN existente, con los efectos potencialmente dañinos sobre la Extensión de Seguridad del DNS (DNSSEC) de los servidores de nombres de respaldo y sus usuarios. Un enfoque particularmente grueso es que un operador descarte silenciosamente respuestas DNS, aunque esto da como resultado un comportamiento no determinista y puede en sí mismo ser problemático.

Sea cual fuere el mecanismo usado, las organizaciones que implementen el bloqueo deben aplicar estos principios:

1. La organización impone una política a la red y sus usuarios, sobre la cual ejerce el control administrativo (es decir, es el administrador de un dominio de política).
2. La organización determina que la política es benéfica para sus objetivos y/o los intereses de sus usuarios.
3. La organización implementa la política usando una técnica que sea lo menos perjudicial posible para sus operaciones de red y usuarios, a menos que leyes o regulaciones especifiquen ciertas técnicas.
4. La organización realiza un esfuerzo concertado para no hacer daño a la red o a usuarios externos a su dominio de política como consecuencia de la implementación de la política.

Cuando estos principios no se apliquen, el bloqueo usando el DNS puede causar mucho más daño colateral o consecuencias no intencionadas y puede no haber remedio disponible para las partes afectadas.

La evolución de la tecnología de Internet se basa en una adaptación del primer principio de la práctica médica: *primum no nocere* (primero, no hacer daño), que requiere que proveedores de asistencia médica evalúen el posible daño que podría causar una intervención. En el caso de Bloqueo de DNS, y sin tener en cuenta si el bloqueo se aplica a Dominios de Nivel Superior (TLDs) (tal como .example) o de segundo nivel (tal como example.example) y tercer nivel (tal como example.example.example), "no hacer daño" significa no crear circunstancias en que los usuarios de Internet de fuera del dominio de política de la organización sean adversamente afectados por la política de la organización o su implementación.

Todos los enfoques técnicos al bloqueo de DNS, y más aún los intentos de eludir ese bloqueo, tendrán cierto impacto sobre la seguridad y/o estabilidad de los usuarios y aplicaciones, y sobre la coherencia o solvencia del espacio de nombre global. El SSAC no puede establecer una línea entre "buenos bloqueos de DNS" y "malos bloqueos de DNS", en ningún nivel de TLD, aunque el Comité puede ofrecerse a investigar los impactos observables de los diversos enfoques de bloqueo, y puede sugerir qué pautas usar al evaluar los enfoques que puedan producir la menor cantidad de consecuencias no intencionadas y que puedan hacer el menor daño posible fuera del dominio bloqueado. Por ejemplo, los impactos negativos al bloqueo de DNS de dominios específicos o nombres de servidores sobre la seguridad del DNS han sido descritos en un documento reciente.<sup>1</sup>

El SSAC comprende que el tema del bloqueo de DNS surge a raíz del agregado de los XXX TLD Genéricos (gTLD) a la raíz. El SSAC no tiene suficiente información como para tomar una posición respecto de esta acción; no obstante, el Comité desea dejar claro que, más allá de si el bloqueo se aplica a TLDs o a sub-niveles, minimizar el daño requiere un esfuerzo concertado para no crear circunstancias en que los usuarios de Internet defuera del dominio de la política de la organización sean adversamente afectados por la política de la organización o su implementación. Extender este marco ético basado en el ámbito de las organizaciones al de las naciones soberanas requiere una comprensión del paisaje político mayor de la que SSAC tiene actualmente. Pero también podemos decir con certeza que el bloqueo a nivel nacional de los TLDs completos interfiere fundamentalmente con la meta de proporcionar un sistema de nombres único y unificado para los recursos de Internet. Si se lo implementa sin cierto marco ético destinado a minimizar el daño a partes externas, el bloqueo puede producir efectos más adversos de lo previsto en comunidades más amplias, exacerbando los problemas que tal bloqueo pretende resolver. Además, bloquear dominios en los niveles segundo y tercero así como en el nivel TLD puede dar lugar a sistemas de nombres alternativos y/o raíces, que podrían ser desestabilizantes y perjudiciales para Internet.

---

<sup>1</sup> See <[http://www.redbarn.org/files\\_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf](http://www.redbarn.org/files_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf)>.

## **2. Reconocimientos, Declaraciones de Interés, Objeciones y Abstinenias**

Estas secciones proporcionan al lector información sobre tres aspectos de nuestro proceso. La sección Reconocimientos lista a los miembros que contribuyeron a este documento en particular. La sección de Declaraciones de Interés contiene biografías de los miembros del Comité y cualquier conflicto de intereses, real, aparente o potencial, que pudiera tener que ver con el material de este documento. La sección de Objeciones y Abstinenias proporciona un lugar para que miembros individuales presenten su desacuerdo con el contenido de este documento o con el proceso de su preparación.

### **2.1 Reconocimientos**

El comité desea agradecer a los siguientes miembros de SSAC y otros contribuyentes por su tiempo, contribuciones y aportes para producir este Informe.

KC Claffy  
Steve Crocker  
Patrik Fältström  
Jim Galvin  
Warren Kumari  
Jason Livingood  
Danny McPherson  
Ram Mohan  
Dave Piscitello  
Bruce Tonkin  
Paul Vixie

### **2.2 Declaraciones de Interés**

La información biográfica de los miembros de SSAC y sus Declaraciones de Interés están disponibles en: <http://www.icann.org/en/committees/security/biographies-25mar11-en.htm>.

### **2.3 Objeciones y Abstinenias**

No hubo objeciones ni abstinenias.