Programa de Nuevos Dominios Genéricos de Alto Nivel (gTLD)
Memorando Explicativo

Mitigación de Conductas Maliciosas

Fecha de publicación: 12 de noviembre de 2010

Antecedentes – Programa de Nuevos Dominios Genéricos de Alto Nivel (gTLD)

Creada hace diez años, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) es una organización sin fines de lucro integrada por múltiples partes interesadas que se dedica a la coordinación del sistema de direcciones de Internet. Uno de sus principios fundacionales, reconocido por los Estados Unidos y por otros Gobiernos, consiste en promocionar la competencia en el mercado de nombres de dominio sin descuidar la seguridad y la estabilidad de Internet. La expansión de los dominios genéricos de alto nivel (gTLD) permitirá seguir innovando, proporcionar nuevas opciones e introducir cambios en el sistema de direcciones de Internet.

La decisión de introducir nuevos gTLD se tomó después de un extenso y meticuloso proceso de consulta, el cual contó con la participación de representantes de toda la comunidad global de Internet: Gobiernos, particulares, empresas, el sector de la propiedad intelectual, la comunidad tecnológica y la sociedad civil. También contribuyeron las siguientes entidades de ICANN: el Comité Asesor Gubernamental (GAC), el Comité Asesor At-Large (ALAC), la Organización de Apoyo para Nombres de Dominio con Código de País (CCNSO) y el Comité Asesor de Seguridad y Estabilidad (SSAC). El proceso de consulta dio como resultado una política para la introducción de nuevos gTLD, la cual fue elaborada por la Organización de Apoyo para Nombres de Dominio (GNSO) en 2007 y adoptada por la Junta Directiva de ICANN en junio de 2008.

Este memorando explicativo forma parte de una serie de informes publicados por ICANN con el fin de ayudar a la comunidad global de Internet a comprender los requisitos y los procesos que se presentan en la *Guía para el Solicitante*. Desde fines de 2008, el personal de ICANN comparte el desarrollo del programa con la comunidad de Internet a través de una serie de foros de consulta pública que permiten realizar comentarios sobre los borradores de la *Guía para el Solicitante* y sobre la documentación de respaldo. Todos los comentarios recibidos se evalúan detenidamente y se utilizan para optimizar el Programa.

Tenga en cuenta que este documento es solo una versión borrador para el debate. Los posibles solicitantes no deben dar por sentado ninguno de los detalles propuestos para el Programa de Nuevos Dominios Genéricos de Alto Nivel (gTLD), ya que este continúa en proceso de consulta y revisión.

Resumen de los puntos clave de este documento

- Si bien ya se han incorporado a la Guía nueve recomendaciones para la mitigación de conductas maliciosas, se está trabajando en su implementación.

- Las soluciones detalladas en estos memorandos generarán mejoras significativas en el entorno del Sistema de Nombres de Dominio (DNS) al incrementar los mecanismos de protección para registrantes, al proporcionar un entorno más seguro y al desarrollar e implementar herramientas que permitan detectar y combatir posibles conductas maliciosas.

Resumen

ICANN ha publicado dos versiones de este Memorando Explicativo, que describen las nueve mejoras introducidas en la *Guía para el Solicitante* con el fin de combatir la conducta maliciosa en los nuevos gTLD. El primer memorando fue publicado el 3 de octubre de 2009 y el segundo memorando, el 31 de mayo de 2010.

Esta actualización procura describir los trabajos de implementación adicionales que se han realizado en estas áreas. Si bien las recomendaciones ya se han incorporado a la Guía, se está trabajando en su implementación.

Las soluciones detalladas en estos memorandos generarán mejoras significativas en el ámbito del Sistema de Nombres de Dominio (DNS) al incrementar los mecanismos de protección para registrantes, al proporcionar un entorno más seguro y al desarrollar e implementar herramientas que permitan detectar y combatir posibles conductas maliciosas. ICANN y la comunidad siguen trabajando juntos en la elaboración de medidas e iniciativas que contribuyan al lanzamiento estable del proceso de nuevos gTLD. La seguridad, la estabilidad y la flexibilidad continuarán siendo cuestiones de alta prioridad para ICANN durante el avance del Programa de Nuevos gTLD hacia su lanzamiento e implementación.

Este documento destaca el considerable volumen de excelente trabajo realizado, principalmente, por voluntarios de la comunidad a través de foros de consulta pública y de distintos grupos de trabajo. ICANN valora y agradece el compromiso mostrado por los voluntarios y su participación en distintas iniciativas que mejorarán considerablemente el entorno del Sistema de Nombres de Dominio (DNS).

Las nueve recomendaciones propuestas para los nuevos gTLD, actualmente incluidas o mencionadas en la Versión Final Propuesta de la Guía para el Solicitante, son las siguientes:

1. ***Revisión de operadores de registros***: Esta recomendación requiere que se investigue adecuadamente a los operadores de registros que soliciten nuevos gTLD, a fin de determinar si el solicitante tiene antecedentes penales o de conducta maliciosa.
2. ***Presentación de un plan para la implementación de DNSSEC***: Esta recomendación requiere la presentación obligatoria por parte del solicitante de nuevos gTLD de un plan para la implementación de Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), a fin de reducir el riesgo de registros falsos en el Sistema de Nombres de Dominio (DNS).
3. ***Prohibición del uso de comodines***: Esta recomendación requiere la implementación de controles adecuados en relación con el uso de comodines de DNS, lo que reduciría el riesgo de redireccionamiento de DNS a sitios maliciosos.
4. ***Eliminación de los registros de pegado huérfanos***: Esta recomendación requiere que los gTLD eliminen los registros de servidor de nombres cuando se elimine un sistema del gTLD, a fin de reducir el riesgo de que actores maliciosos utilicen estos registros remanentes.
5. ***Requisito de registros de WHOIS extensos***: Esta recomendación requiere que los nuevos gTLD tengan registros "WHOIS extensos" y que brinden acceso a ellos, con el fin de mejorar la precisión y la integridad de los datos de WHOIS. El uso de registros de WHOIS extensos constituye un mecanismo clave para combatir el uso malicioso de los nuevos gTLD, al suministrar una cadena de contratos [sic] más completa dentro del TLD. A su vez, esto permitiría buscar datos en forma más rápida y abordar las actividades de índole maliciosa a medida que se identifican.
6. ***Centralización del acceso a los archivos de zona***: Esta recomendación requiere que las credenciales de acceso para obtener datos de archivos de zona de registro se otorguen a través de una fuente centralizada, a fin de identificar de manera más rápida y precisa los

puntos de contacto clave dentro de cada TLD. Esto reduce el tiempo necesario para implementar acciones correctivas dentro de los TLD víctimas de actividad maliciosa.

7. ***Contacto y procedimientos sobre uso indebido del nivel de registro:*** Esta recomendación requiere que los gTLD establezcan un punto de contacto único responsable del manejo de reclamaciones por uso indebido y que los registros proporcionen una descripción de sus políticas antiabuso. Estos requisitos se consideran pasos fundamentales para combatir con éxito las conductas maliciosas dentro de los nuevos gTLD.
8. ***Participación en un proceso de solicitud acelerada de seguridad del registro***: Esta recomendación requiere que los nuevos gTLD puedan tomar medidas rápidas y eficaces ante amenazas sistémicas al DNS mediante un proceso dedicado que revise y apruebe solicitudes aceleradas de seguridad.
9. ***Marco preliminar para la verificación de zonas de alta seguridad***: Esta recomendación sugirió la creación de un programa voluntario diseñado para designar TLD que deseen establecer y probar un nivel optimizado de seguridad y confianza. El objetivo global del programa es proporcionar un mecanismo para los TLD que deseen distinguirse como seguros y fiables, para modelos empresariales de TLD que se beneficiarían de esta distinción.

El resto de este memorando abordará el estado de trabajo específico en relación con cada recomendación.

Estado de las nueve recomendaciones sobre conducta maliciosa

Esta sección informa el estado actual de las nueve recomendaciones ideadas para reducir la posibilidad de conductas maliciosas en los nuevos gTLD.

1 Revisión de operadores de registros

- **Estado actual**

  La recomendación de requerir una "revisión" o verificación de antecedentes de los operadores de registros ha sido un principio rector en la mejora del proceso de solicitud para solicitantes de nuevos gTLD. El proceso de solicitud de nuevos gTLD contiene criterios específicos que deben verificarse para cada solicitante de un nuevo gTLD. En respuesta a los comentarios recibidos, la Versión Final Propuesta de la Guía para el Solicitante ha sido modificada a fin de añadir mayor detalle y precisión. La referencia específica al terrorismo fue eliminada (así como también la lista excesivamente simplificada de áreas de verificación de antecedentes). La verificación de antecedentes se llevará a cabo en solo dos áreas: antecedentes penales y de conducta empresarial general, y antecedentes de ocupación ilegítima de dominios.

2 Implementación de DNSSEC

- **Estado actual**

  La presentación de un plan para la implementación de DNSSEC es un componente obligatorio del proceso de solicitud de nuevos gTLD y permite probar cada nuevo gTLD antes de su delegación. La Especificación 6 del Acuerdo de Registro dispone que: "El operador de registro firmará sus archivos de zona del TLD implementando extensiones de seguridad para el sistema de nombres de dominio (DNSSEC)". Desde la activación de DNSSEC en la zona raíz el 15 de julio de 2010, sesenta y cuatro TLD (hasta el 11 de noviembre de 2010) han firmado sus zonas.

3 Prohibición del uso de comodines

- **Estado actual**

  La referencia a la prohibición de los comodines de DNS sigue siendo parte de la Especificación 6 del Acuerdo de Registro. Esta prohibición no ha sufrido modificaciones desde que la Junta Directiva de ICANN resolvió, en su reunión pública realizada en Sydney en junio de 2009, que los nuevos dominios de alto nivel no deben utilizar redireccionamiento de DNS ni sintetización de respuestas de DNS.

4 Registros de pegado huérfanos

- **Estado actual**

  El Comité Asesor de Seguridad y Estabilidad (SSAC) formó un grupo de trabajo para estudiar esta cuestión. Se ha realizado un profundo análisis de zonas y registraciones de TLD a fin de obtener un panorama más claro respecto de cuán comunes son los registros huérfanos en los principales TLD. El grupo de trabajo examinó los archivos de zonas de todos los gTLD actuales y analizó con qué frecuencia se utilizan los registros huérfanos con fines maliciosos. El SSAC ha elaborado un borrador del Informe del Grupo de Trabajo, el cual se encuentra bajo revisión final

por parte del grupo de trabajo. Las recomendaciones generadas por el grupo de trabajo del SSAC pueden ofrecer orientación adicional para los registros [sic] respecto de cómo manejar los registros huérfanos, y serán evaluadas para su inclusión en los procesos clave referentes a gTLD. Como se indica en la Resolución 2.8 de la Junta Directiva de ICANN con fecha 25 de septiembre de 2010, “Las disposiciones actuales de la Guía exigen que cada solicitante explique cómo manejará y eliminará los registros de pegado huérfanos correspondientes a nombres eliminados de la zona. Este requisito debe seguir vigente y será modificado si el SSAC hace una nueva recomendación en su informe sobre este tema.”.

5 Registros de WHOIS extensos

- **Estado actual**

El estado de esta recomendación no ha cambiado, y los registros de “WHOIS extensos” son un requisito para todos los gTLD nuevos. Todos los gTLD nuevos deberán cumplir con los requisitos de registros WHOIS extensos, según la Especificación 4 del Acuerdo de Registro. En el Memorando Explicativo sobre WHOIS publicado el 30 de mayo de 2010, se brinda más información sobre esta recomendación.

Asimismo, el sistema de evaluación y puntaje de la Versión Final Propuesta de la Guía para el Solicitante ha sido modificado a fin de incluir un punto adicional que se otorgará a aquellos solicitantes que especifiquen que tendrán una función de búsqueda WHOIS.

6 Centralización del acceso a los archivos de zona

- **Estado actual**

La recomendación de crear un mecanismo que respalde la centralización del acceso a los registros de archivos de zona fue aceptada por ICANN, y se creó un grupo asesor denominado “Grupo Asesor de Acceso a Archivos de Zona” (ZFA AG), con el mandato de trabajar con la comunidad para desarrollar una propuesta para un mecanismo que respalde la centralización del acceso a los archivos de zona. El ZFA AG finalizó su trabajo y los detalles fueron publicados en su Propuesta de Estrategia el 13 de mayo de 2010.

En resumen, el ZFA AG recomendó un modelo híbrido (el “Modelo”), que combina el modelo bilateral optimizado y el modelo *clearinghouse* (centro de intercambio de información) descriptos en su propuesta. El Modelo ofrece un único punto de contacto para los solicitantes que buscan acceso a los archivos de zona y preserva en gran medida los roles y las funciones operativas existentes de los proveedores de datos. El Modelo introduce dos cambios en el sistema actual de acceso a archivos de zona. Primero, estandariza la relación entre los proveedores de datos de archivos de zona (es decir, los operadores de registros) y los consumidores (por ejemplo, organizaciones antiabuso y para la protección de marcas, investigadores, académicos, etc.) dividiéndola en tres categorías: estándares de aplicación, estándares de acceso y estándares de formato de archivo/registro. Segundo, introduce un *clearinghouse* ligero para el manejo de la identidad en el sistema de acceso a archivos de zona, a fin de proveer un punto único de contacto para los consumidores que buscan acceso a los archivos de zona.

ICANN está elaborando un plan para encontrar un proveedor de servicio adecuado que implemente la recomendación descripta en la propuesta.

En la Sección 2 de la Especificación 4 del Acuerdo de Registro, se hace referencia al acceso a archivos de zona.

7 Contacto y políticas sobre uso indebido del nivel de registro

- **Estado actual**

La recomendación de requerir que los nuevos gTLD consignen un contacto específico para casos de uso indebido del registro y que brinden una descripción de sus políticas antiabuso específicas es un requisito para todos los gTLD nuevos. Esto no se ha modificado desde el memorando original sobre conductas maliciosas. La disposición se detalla en la Sección 5.4.1 del Módulo 5.

8 Participación en un proceso de solicitud acelerada de seguridad del registro (ERSR)

- **Estado actual y/o actualizaciones**

El 1 de octubre de 2009, ICANN anunció que se encontraba disponible el proceso de solicitud acelerada de seguridad del registro (ERSR). Este proceso será utilizado por los registros de gTLD exclusivamente para incidentes que requieran acción inmediata por parte del registro a fin de evitar efectos nocivos en la estabilidad o en la seguridad del DNS.

La ERSR, un procedimiento de comunicación basado en la Web, es el resultado de una iniciativa conjunta entre ICANN y los registros de gTLD para el desarrollo de un proceso que permita actuar con rapidez en casos en que dichos registros:

- informen a ICANN sobre un incidente de seguridad existente o inminente en sus TLD y/o DNS, y
- soliciten una exención contractual por medidas que hayan tomado o pudieran tomar para mitigar o eliminar el incidente.

Una exención contractual exime al solicitante de cumplir con una cláusula específica del Acuerdo de Registro durante el tiempo necesario para responder al incidente.

9 Marco preliminar para la verificación de zonas de alta seguridad

- **Estado actual**

La recomendación de crear un marco preliminar para la verificación de zonas de alta seguridad fue realizada por grupos bancarios y de servicios financieros, como BITS (un consorcio de instituciones de servicios financieros de los Estados Unidos), y esto dio origen a una iniciativa denominada Programa de Dominios de Alto Nivel en Zona de Alta Seguridad (Programa HSTLD). La iniciativa tiene por objetivo elaborar un marco de controles para la verificación de zonas de alta seguridad. A fin de analizar posibles enfoques a dicho marco y avanzar hacia una propuesta que será sometida a revisión por parte de la comunidad, ICANN formó el Grupo Asesor de Dominios de Alto Nivel en Zona de Alta Seguridad (HSTLD AG). El mandato del HSTLD AG es trabajar con la comunidad, a través de un modelo de desarrollo consultado con las bases, para proponer distintos enfoques para el desarrollo de un programa voluntario compuesto por estándares de control e incentivos tendiente a aumentar la seguridad y la confianza en los TLD que opten por participar en dicho programa. ICANN no operará el programa de HSTLD. Una entidad independiente establecerá los criterios y certificará los TLD según esos criterios.

El 16 de junio de 2010, ICANN publicó el Informe de Estado de HSTLD N.º 2 para análisis

público. Este informe presenta un marco común de principios, criterios y estándares de control que permitirá a los operadores de registros de TLD que deseen obtener la certificación de "Dominio de Alto Nivel en Zona de Alta Seguridad" respaldar e implementar prácticas y políticas de seguridad optimizadas. El marco actual constituye la base para los requisitos básicos del Programa HSTLD y se trata en el Anexo A del Informe de Estado.

El período de comentarios públicos sobre el Informe de Estado finalizó el 21 de julio de 2010. El resumen y análisis de los comentarios se publicará junto con la Versión Final Propuesta de la Guía para el Solicitante. Asimismo, ICANN y el HSTLD AG consideran que sería útil implementar una Solicitud de Información (RFI) respecto del programa. El propósito de la RFI es ayudar a la comunidad ICANN a comprender los posibles marcos y enfoques para la evaluación de los registros TLD según los criterios HSTLD; determinar en qué áreas de los criterios preliminares y del programa en general sería necesario introducir mejoras a fin de garantizar su éxito; y evaluar la viabilidad del Programa HSTLD propuesto. ICANN anunció la publicación de la RFI el 22 de septiembre de 2010. El plazo de respuesta finaliza el 23 de noviembre de 2010.

Una vez finalizado el periodo de la RFI el 23 de noviembre de 2010, y después de que ICANN y el HSTLD AG hayan respondido las preguntas y resumido y analizado las respuestas, se determinarán los próximos pasos a seguir.

ICANN mantiene su compromiso de mitigar la conducta maliciosa en los nuevos gTLD y respalda el desarrollo del concepto de HSTLD como programa voluntario a cargo de una entidad independiente.