Memorándum explicativo sobre el nuevo programa de gTLD

Conducta Malintencionada Atenuante

Fecha de publicación: 3 de Octubre del 2009

Antecedentes - Nuevo programa de gTLD

Desde la fundación de ICANN diez años atrás como organización multilateral compuesta por partes interesadas sin ánimo de lucro, dedicada a la coordinación del sistema de direcciones de Internet, uno de sus principios fundamentales –reconocido por los Estados Unidos y otros gobiernos– ha sido 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 (gTLDs) permitirá una mayor innovación, opciones y cambios en el sistema de direcciones de Internet, representado ahora por 21 gTLDs.

La decisión de introducir nuevos gTLDs fue siguiente a un detallado y prolongado proceso de consulta con todos los constituyentes de la comunidad mundial de Internet representados por una amplia variedad de partes interesadas –gobiernos, individuos, sociedad civil, negocios, constituyentes de propiedad intelectual y la comunidad tecnológica. También contribuyeron el Comité Asesor Gubernamental (GAC) de ICANN, el Comité Asesor de Alcance (ALAC), la Organización de Apoyo para Nombres de Dominio con Códigos de País (ccNSO) y el Comité Asesor de Seguridad y Estabilidad (SSAC). El proceso de consulta resultó en una política sobre la introducción de Nuevos gTLDs concluidos por la Organización de Soporte de Nombres Genéricos (GNSO) en el 2007, y adoptada por la Junta de la ICANN en Junio del 2008. Se espera que el programa se lance en el año calendario 2010.

Este memorándum explicativo es parte de una serie de documentos publicados por la ICANN para asistir a la comunidad mundial de Internet en entender los requerimientos y procesos presentados en la Guía del Solicitante, actualmente en borrador. Desde finales del 2008, el personal de la ICANN ha estado compartiendo el progreso del desarrollo del programa con la comunidad del Internet a través de una serie de foros de comentarios públicos sobre los borradores de la guía del solicitante y documentos de soporte. Hasta la fecha, ha habido más de 250 días de consulta sobre los materiales cruciales del programa. Los comentarios recibidos continúan siendo evaluados cuidadosamente y utilizados para refinar adicionalmente el programa e informar el desarrollo de la versión final de la Guía del Solicitante.

Para información actual, cronogramas y actividades relacionadas al Nuevo Programa de gTLD, por favor vaya a http://www.icann.org/en/topics/new-gtld-program.htm.

Tenga en cuenta que se trata sólo de una versión preliminar del debate. Los aspirantes no deben confiar en ninguno de los detalles propuestos del nuevo programa de gTLD, ya que éste continúa siendo objeto de más consultas y revisiones.

Resumen de los puntos clave de este documento

ICANN busca comentarios sobre la propuesta para agregar medidas específicas para el nuevo acuerdo de registro gTLD, descrito a continuación, a ser requerido para todos los registros para poder atenuar una potencial conducta malintencionada.

Durante este estudio de conducta malintencionada, el personal de ICANN solicitó y recibió comentarios de múltiples fuentes externas, incluyendo el APWG (Grupo de Trabajo Anti-Suplantación de Identidad), RISG (Grupo de Seguridad de Registro de Internet), el SSAC (Comité Asesor de Estabilidad y Seguridad), CERTs (Equipos de Respuesta de Emergencia Informática) y miembros de la banca/finanzas y comunidades de seguridad de Internet. Estas partes describieron algunos problemas potenciales de conducta malintencionada y alentaron a la ICANN a considerar maneras en las que estas se podrían tratar o atenuar en los nuevos acuerdos de registro de gTLD. Se intenta que estas medidas recomendadas incrementen los beneficios a la seguridad y estabilidad general de los registrantes y confianza de todos los usuarios de estas nuevas zonas gTLD.

Los comentarios recibidos sobre la versión 2 del Borrador de la Guía de Solicitante, durante la convención de Sídney y en las consultas desde Sídney recomendaron que las medidas y controles para atenuar la conducta malintencionada sean incorporadas como requerimientos dentro del borrador del acuerdo de registro base para los nuevos gTLDs. El siguiente es un resumen de la aportación considerada y el proceso seguido al preparar estas recomendaciones.

Las recomendaciones proporcionan atenuaciones concretas de los riesgos de conducta malintencionada en nueve áreas:

1. Operadores de registro vetados
2. Plan demostrado para la implementación DNSSEC
3. Prohibición de comodines
4. Eliminación de registros de interconexión huérfanos cuando un ingreso de servidor de nombre se elimina de la zona
5. Requerimiento para registros de identificación marcada
6. Centralización de acceso a archivos de zona
7. Contactos y procedimientos documentados de abuso a nivel de registro
8. Participación en un proceso Expedido de Solicitud de Seguridad de Registro
9. Borrador de Marco de Trabajo para Verificación de Zonas de Alta Seguridad

Juntos, creemos que estas medidas ayudarán considerablemente a ayudar a atenuar el riesgo creciente de conducta malintencionada que surge de nuevos gTLDs. La política de trabajo sobre estas cuestiones los pasos tomados para atenuar la conducta malintencionada continuarán. ICANN también puede explorar la formación de un grupo de trabajo combinando a miembros dentro de la industria de la seguridad y comunidad de ICANN para ayudar a desarrollar y evaluar soluciones e implementaciones específicas de medidas de atenuación propuestas.

Prefacio

Desde la fundación de ICANN diez años atrás como una organización multilateral compuesta por partes interesadas sin fines de lucro, dedicada a la coordinación del sistema de direcciones de Internet, uno de sus principios fundamentales, reconocido por muchos gobiernos y otras partes interesadas, ha sido promocionar la competencia en el mercado de nombres de dominio sin descuidar la seguridad y la estabilidad de Internet. La expansión dará lugar a la innovación, opción y cambios positivos para el sistema de direcciones del Internet. En un mundo con una diversidad de 1.500 millones de usuarios de Internet, la variedad de opciones y la competencia son claves para la continuidad del éxito y del alcance de la red global.

La decisión de lanzar estas nuevas series de solicitudes de gTLD siguió a un proceso de consulta extenso y meticuloso con la participación de todas las unidades constitutivas de la comunidad global de Internet. Representantes de una amplia variedad de partes interesadas (gobiernos, individuos, sociedades civiles, empresas y representantes del sector de propiedad intelectual, así como de la comunidad tecnológica) han participado en discusiones durante más de dieciocho meses. En octubre de 2007, la Organización de apoyo para nombres de dominio (GNSO), uno de los grupos que coordina la política global de Internet en ICANN, completaba su trabajo de desarrollo de políticas sobre los nuevos gTLD y aprobaba un conjunto de recomendaciones. Este proceso de desarrollo de políticas culminó con la decisión de la Junta Directiva de ICANN de adoptar la política elaborada por la comunidad en la reunión en París de este organismo, en junio de 2008. Puede hallar un resumen detallado del proceso de la política y los resultados en http://gnso.icann.org/issues/new-gtlds/.

Este documento forma parte de una serie de informes que servirán como documentos explicativos publicados por ICANN para ayudar a la comunidad de Internet a comprender mejor la solicitud de propuesta (RFP), también denominada Guía del Solicitante. Un período de comentario público para la Guía del Solicitante y estos documentos darán un informe de revisión detallado y enmiendas de estas ideas. Dichos comentarios se utilizarán para revisar los documentos con el objeto de preparar una Guía de Solicitante Final.

Tenga en cuenta que se trata sólo de una versión preliminar del debate. Los aspirantes no deben confiar en ninguno de los detalles propuestos del nuevo programa de gTLD, ya que éste continúa siendo objeto de más consultas y revisiones.

Aportes de la Comunidad con respecto a la Cuestión de Conducta Malintencionada

ICANN ha recibido numerosos comentarios públicos abarcando múltiples áreas en respuesta a su anuncio proponiendo una expansión del espacio TLD para delegar nuevos TLDs incluyendo TLDs de IDN. Una de las cuestiones identificadas por algunas partes fue el creciente potencial de conducta malintencionada que podría surgir de nuevos gTLDs. Para tratar esta cuestión, ICANN buscó comentarios de parte de expertos al responder a conductas malintencionadas y de parte de partes interesadas impactadas por conducta malintencionada en gTLDs existentes.

El aporte recibido en las versiones anteriores 1 y 2 del Borrador de la Guía del Solicitante sirve como una fuente principal importante en el desarrollo de las recomendaciones que

se incluyen en la versión 3 del Borrador de la Guía del Solicitante.

Una segunda fuente de aporte en esta cuestión es la estructura de informes emitidos por SSAC en formatos de conducta malintencionada. Específicamente, **SAC038: Punto de Contacto de Abuso del Registrador (pdf)** y SAC040: Medidas para Proteger a los Servicios de Registro de Dominio contra la Explotación o el Mal Uso (pdf). Estos informes y otros trabajos realizados por la SSAC proporcionan una guía con respecto a las mejores prácticas de seguridad para registrados y registradores, las cuales han guiado los cambios propuestos en el Borrador de la Guía del Solicitante y nuevos acuerdos de registro gTLD.

Una tercera fuente es el informe borrador preparado por el APWG (Grupo de Trabajo Anti-Suplantación de Identidad), una asociación de la industria enfocada en eliminar el robo de identidad y fraude que resulta del problema creciente de suplantación de identidad y falsificación de IP de correo electrónico. Este informe se coordinó con el IPC (Comité de Políticas de Internet), el cual incluye más de 90 miembros representando a todo el espectro de la membresía de APWG. Vale la pena notar que muchas partes interesadas de la ICANN, incluyendo los registros gTLD y ccTLD y los registradores, proveedores de servicios de Internet, propietarios de propiedad intelectual e instituciones de seguridad y financieras son miembros de la APWG y la APWG IPC, ver http://www.antiphishing.org/sponsors.html. El IPC de la APWG ve la expansión planificada de los gTLDs como un evento importante con un impacto potencial sobre el espacio de crimen electrónico. El informe APWG IPC proporciona un aporte amplio y constructivo para la ICANN sobre numerosas cuestiones de conducta malintencionada que el IPC de la APWG cree que ameritan atención y planificación durante la implementación de los nuevos gTLDs.

Una cuarta fuente de aportes fue proporcionada por el RISG (Grupo de Seguridad de Registro de Internet), un grupo mundial de organizaciones responsables relacionadas al Internet quienes trabajan de modo cooperativo para combatir el robo de identidad en internet, particularmente la suplantación de identidad y la distribución de software malicioso. Este informe del RISG (pdf) proporciona una enumeración de algunas cuestiones, que pueden resultar por un incremento en el número de registrados.

Una quinta fuente de aporte recibida sobre la cuestión de conducta malintencionada es una serie de comentarios recibidos por la comunidad Bancaria y Financiera. Una serie de asociaciones de la industria incluyendo el Programa de Reducción de Fraudes BITS, la Asociación Americana de Bancos, *FS-ISAC* (Centro de Análisis y Reparto de Información de Servicios Financieros) y el FSTC (Consorcio de Tecnología en Servicios Financieros) contribuyeron con su experiencia. Con su perspectiva y experiencia únicas en asegurar tanto redes como información sensitiva, esta comunidad proporcionó específicas recomendaciones valiosas para medidas que los registros deben implementar, incluyendo la adopción de prácticas comerciales seguras, incrementar la confianza del usuario y reducir el riesgo de compromiso por ataques malintencionados.

Una sexta fuente de aportes en las medidas para atenuar la conducta malintencionada dentro de los nuevos gTLDs es el trabajo hecho por el IRT (Equipo de Recomendación de Implementación). Aunque la ICANN ha identificado una protección de marca registrada y un potencial de abuso malintencionado como cuestiones separadas de gran alcance a ser tratadas en el establecimiento de nuevos gTLDs, existe una intersección significativa en los intentos de remediación que se proponen para tratar estas inquietudes. El trabajo del IRT fue resumido en la "Carta Abierta del IRT Introduciendo Nuestro Trabajo," de fecha 29

de Mayo del 2009. El IRT fue formado por la Constitución de Propiedad Intelectual del ICANN en conformidad con la resolución de la Junta Directiva de la ICANN del 6 de Marzo del 2009 (link) a solicitud de la comunidad que busca soluciones para riesgos potenciales a los dueños de marcas registradas en la implementación de nuevos gTLDs. El informe proporcionado por el equipo del IRT (pdf) refleja la experiencia y diversidad geográfica de sus 18 miembros y sus dos alternos.

Fuentes adicionales de aportes vienen de miembros de la comunidad de primera respuesta en seguridad de Internet. Los miembros de organizaciones tales como el FIRST (Foro mundial de Respuesta a Incidentes y Equipos de Seguridad), el cual consiste de equipos de respuesta de emergencia a redes e informática de 180 corporaciones, cuerpos gubernamentales, universidades y otras instituciones dispersas a lo largo de las Américas, Asia, Europa y Oceanía y que ayudan a guiar los esfuerzos del mundo para combatir el cyber-crimen, proporcionaron valiosos consejos. Miembros de varias agencias para el cumplimiento de la ley proporcionaron asistencia al definir cuestiones de importancia y sugerencias de cambios en operaciones de registro, lo que ayudaría en combatir al crimen con base en el Internet.

Además de las fuentes ya mencionadas, el ICANN incorporó aportes de participantes en consultas públicas realizadas en Sídney, New York, Londres, Hong Kong y Abu Dabi. Estas consultas incluyeron sesiones dedicadas enfocadas en la cuestión de atenuar el potencial de la conducta malintencionada y nuevos gTLDs.

ICANN mantiene un wiki en el sitio web icann.org dedicado a las soluciones potenciales solicitadas para tratar la conducta malintencionada en los nuevos gTLDs. Los informes referidos anteriormente han sido publicados en este wiki y se ha invitado a una participación y comentarios públicos.

Cuestiones clave identificadas

Se identificó un número de cuestiones relacionadas al potencial de la conducta malintencionada por parte de este diverso grupo de participantes en el proceso ICANN. Aunque muchas de las cuestiones exponen vulnerabilidades técnicas únicas y complejas y requieren una variedad de controles y consideraciones, éstas pueden ser resumidas bajo las siguientes categorías de temas claves:

A. ¿Cómo aseguramos que los malos intervinientes no hagan funcionar Registros?

Las fuentes han pedido que ICANN tome pasos para reducir el riesgo de que un número expandido de registros pudiera conducir a que operadores no confiables o criminales ingresen en la comunidad y permitan que ocurra una conducta malintencionada.

B. ¿Cómo aseguramos la integridad y utilidad de la información de registro?

Las fuentes alentaron a ICANN a que aproveche la creación de nuevos gTLDs para mejorar la calidad de registro de nombre de dominio y servicios de resolución de nombres de dominio en una manera que limitaría las oportunidades para la conducta malintencionada.

C. ¿Cómo aseguramos un esfuerzo más efectivo para combatir el abuso identificado?

Dada la conducta malintencionada que ya existe y afecta a todos los TLDs, las fuentes han solicitado a ICANN que continúe dentro del establecimiento de nuevas mejoras TLDs a los procesos y herramientas disponibles para reducir el crimen virtual continuo y abuso del DNS y sistemas de registro de dominio.

D. ¿Cómo proporcionamos un marco de trabajo de control mejorado para los TLDs con un potencial intrínseco de abuso?

Algunos nuevos TLDs pueden involucrar que las transacciones de servicios electrónicos requieran de una infraestructura de alta confiabilidad (por ejemplo servicios financieros electrónicos o voto electrónico) y pueden involucrar activos e infraestructura crítica (tales como aquellas que apoyan las infraestructuras de energía o servicios médicos) la cual debe permitir una protección mayor de los actores quienes ya conducen conducta malintencionada utilizando el sistema de nombre de dominio. Las fuentes han recomendado que ICANN tome pasos para crear un sistema para permitir una confianza mejorada en las operaciones de dichas zonas.

Medidas de Atenuación Propuestas:

Para tratar la conducta malintencionada resumida anteriormente, el ICANN cree que deberían tomarse una combinación de medidas como parte de la implementación planificada de los nuevos gTLDs. Además de las mayores obligaciones por parte de los nuevos registros gTLD en sus contratos con ICANN, se recomienda que estos nuevos registros negocien normas más fuertes para los negocios y prácticas de seguridad con registradores acreditados. Específicamente, un nuevo registro gTLD tendrá la capacidad de requerir a los registradores que implementen medidas específicas para reducir la conducta malintencionada para poder registrar marcas dentro de sus zonas.

Adicionalmente, ICANN continuará trabajando con la comunidad para complementar un desarrollo de política existente y esfuerzos de grupos de trabajo para tratar medidas de atenuación a ser implementadas en la interfaz registrador-registrado.

Las siguientes son las categorías generales de pasos de atenuación propuestos para ser implementados en la versión actual del Borrador de la Guía del Solicitante:

1. Operadores de registro vetados
2. Plan demostrado para la implementación DNSSEC
3. Prohibición de comodines
4. Eliminación de registros de interconexión huérfanos cuando un ingreso de servidor de nombre se elimina de la zona
5. Requerimiento para registros de identificación marcada
6. Centralización de acceso a archivos de zona
7. Contactos y procedimientos documentados de abuso a nivel de registro
8. Participación en un proceso Expedido de Solicitud de Seguridad de Registro
9. Borrador de Marco de Trabajo para Verificación de Zonas de Alta Seguridad

Relación de cuestiones para medidas de atenuación

A. ¿Cómo aseguramos que los malos intervinientes no hagan funcionar Registros?

1. Operadores de registro vetados

B. ¿Cómo aseguramos la integridad y utilidad de la información de registro?

2. Requerimiento de implementación DNSSEC
3. Prohibición de Comodines
4. Alentar la eliminación de Registros de Interconexión Huérfanos

C. ¿Cómo aseguramos esfuerzos más efectivos para combatir el abuso identificado?

5. Requerimiento para IDENTIFICACIÓN Marcada
6. Centralización de acceso a archivos de zona
7. Registro Documentado y Contacto y Políticas de Abuso a Nivel de Registradores
8. Disponibilidad de Procesos Acelerados de Solicitud de Seguridad de Registro

D. ¿Cómo proporcionamos un marco de trabajo de control mejorado para los TLDs con un potencial intrínseco de conducta malintencionada?

9. Programa de Verificación de Zonas de Alta Seguridad

Medidas Específicas a ser implementadas en nuevos Contratos de Registro

Las siguientes medidas se incluyen en la Guía del Solicitante y reflejan procedimientos requeridos para todos los nuevos registros. Se identifica la ubicación de lenguaje dentro del borrador de la Guía de Solicitante. Se incluye una breve descripción de la racionalidad para cada medida específica (en itálicos).

1. Operadores de registro vetados

La pregunta del solicitante (anexo al módulo 2) dice:

ICANN puede negar una solicitud de otro modo calificada por cualquiera de las siguientes razones:

Solicitante, o cualquier funcionario, socio, director, o gerente u otro afiliado, o cualquier persona y entidad que posea (o que posea como beneficiaria) quince por ciento o más de solicitante:

a. dentro de los últimos diez años, ha sido convicto de un crimen o de algún delito menor relacionado a una conducta mal intencionada de gobernabilidad corporativa o financiera, o ha sido juzgado por un tribunal por haber cometido fraude o incumplimiento de deber fiduciario, o ha sido objeto de una determinación judicial que ICANN haya considerado como el equivalente sustantivo de cualquiera de lo anterior;

b. en los últimos diez años, ha sido disciplinado por parte del cuerpo regulatorio de

cualquier gobierno o industria por conducta que involucre deshonestidad o uso ilícito de fondos de terceros;

c. está involucrado actualmente en cualquier demanda judicial o regulatoria que podría resultar en una condena, juicio, determinación o disciplina del tipo especificado en (a) o (b);

d. es el tema de una descalificación impuesta por la ICANN que está en vigencia al momento en que se considera la solicitud; o

e. i ncumplió en proporcionar a la ICANN la información de identificación necesaria para confirmar la identidad en el momento de la solicitud

f. es el tema de un patrón de decisiones indicando responsabilidad por, o práctica repetida de mala fe con respecto a registros de nombres de dominio, incluyendo:

(i) adquirir nombres de dominio principalmente para el propósito de vender, alquilar o de otro modo transferir los registros de nombres de dominio al propietario de una marca registrada o marca de servicio o a un competidor, por consideración valiosa en exceso de costos externos documentados directamente relacionados al nombre del dominio; o

(ii) registrar nombres de dominio para poder prevenir que el propietario de una marca registrada o marca de servicio refleje la marca en un nombre de dominio correspondiente; o

(iii) registrar nombres de dominio principalmente para el propósito de perturbar el negocio de un competidor; o

(iv) utilizar nombres de dominio con la intención de atraer, ganancias comerciales, usuarios de Internet a un sitio web u otra ubicación en línea, creando una similitud o confusión con una marca registrada o marca de servicio con respecto a la fuente, patrocinio, afiliación o endoso del sitio web o ubicación o de un producto o servicio en el sitio web o ubicación.

Nota: La información recolectada durante el curso de estas verificaciones de antecedentes incluyendo registros de actividad criminal pasada será considerada durante el proceso de solicitud.

El proceso de solicitud incluirá verificaciones de antecedentes y referencias normalizadas y detalladas para compañías e individuos (por ejemplo funcionarios clave). Este paso atenuará el riesgo de que criminales conocidos, miembros de organizaciones criminales o aquellos con historias de malas operaciones comerciales se involucren en operaciones de registro u obtengan posesión o control de apoderados de los registros.

2. Requerimiento de implementación DNSSEC

Se requerirá que los Operadores de Registro proporcionen un plan documentado para inscribir su archivo de zona y tengan la implementación de DNSSEC en su sitio al inicio de las operaciones.

Se ha agregado el siguiente idioma a la Especificación 6 de la versión 3 del Acuerdo de Registro, sujeto a una revisión técnica:

"El Operador del Registro implementará DNSSEC (Extensiones de Seguridad de Sistema de

Nombre de Dominio por sus siglas en inglés)." Durante el término, el Operador de Registro cumplirá con la 4033, 4034, 4035, 4509 y 4310 de RFC y sus normas sucesivas, y seguirá las mejores prácticas descritas en RFC 4641 y sus sucesores. Si el Operador del Registro implementa una Negación de Existencia Autenticada con la función Hash para las Extensiones de Seguridad DNS, deberá cumplir con la RFC 5155 y sus normas sucesivas. El Operador de Registro aceptará material clave público de los nombres de dominios jóvenes de una manera segura en conformidad a las mejores prácticas de la industria. El Registro también publicará en su sitio web el documento de práctica y política (también conocido como la Declaración de Política DNSSEC o DPS) describiendo el almacenamiento de material clave, acceso y uso para sus propias claves y el material anclaje de confianza de los registrantes."

Las ventajas proporcionadas por la implementación del DNSSEC a la seguridad total y estabilidad del Internet están bien documentadas. ICANN está comprometida a la inscripción de la zona raíz durante el 2009 y asegurará que el establecimiento de nuevos gTLDs permita el uso de este importante medio de mejorar la seguridad DNS.

3. Prohibición de Comodines

El informe SAC041 de SSAC (aprobado por la Junta Directiva de ICANN) e informes de otras organizaciones de comentarios han aconsejado a ICANN que debería prohibirse a los nuevos TLDs el utilizar el redireccionamiento de DNS y respuestas DNS sintetizadas.

Dada la actual tendencia de software malicioso asociado con sitios que promueven publicidad, la redirección de dominios a sitios de publicidad representa el potencial para una mayor conducta malintencionada. Para los nombres de dominio que estén ya sea o no registrados por un Registrante, o el Registrante que no haya proporcionado registros válidos tales como registros NS para alistarse en el archivo de zona DNS, o su status no les permita ser publicados en el DNS, el uso de Registros de Recurso de Comodines DNS como se describió en RFC 4592 o cualquier otro método o tecnología para sintetizar Registros de Recursos DNS o que utilicen redirección dentro del DNS por el Registro está prohibido. Específicamente, cuando se consulta por dichos nombres de dominio los servidores de nombres autoritativos deben devolver la respuesta "Error de Nombre" (también conocida como NXDOMAIN), RCODE 3 como se describió en RFC 1035 y RFCs relacionados.

Esta estipulación aplica para todos los archivos de zona DNS en todos los niveles del árbol DNS para el cual el Operador de Registro (o un afiliado comprometido en proporcionar Servicios de Registro) mantiene información, organiza dicho mantenimiento o deriva ingresos por dicho mantenimiento.

Se ha agregado la siguiente prohibición en comodines a la Especificación 6 de la versión 3 del Acuerdo de Registro:

"Para los nombres de dominio que estén ya sea o no registrados por un Registrante, o el Registrante no haya proporcionado registros válidos tales como registros NS para alistarse en el archivo de zona DNS, o su status no les permita ser publicados en el DNS, el uso de Registros de Recurso de Comodines DNS como se describió en RFC 4592 o cualquier otro método o tecnología para sintetizar Registros de Recursos DNS o que utilicen redirección dentro del DNS por el Registro está prohibido. Cuando se consulta por dichos nombres de dominio los servidores de nombres autoritativos deben devolver la respuesta "Error de Nombre" (también conocida como NXDOMAIN), RCODE 3 como se describió en RFC 1035 y RFCs relacionados. Esta estipulación aplica para todos los archivos de zona DNS en

todos los niveles del árbol DNS para el cual el Operador de Registro (o un afiliado comprometido en proporcionar Servicios de Registro) mantiene información, organiza dicho mantenimiento o deriva ingresos por dicho mantenimiento.

El informe SAC041 pdf) por la SSAC e informes de otras organizaciones de comentarios han aconsejado a ICANN que debería prohibirse a los nuevos TLDs el utilizar el redireccionamiento de DNS y respuestas DNS sintetizadas. Los peligros inherentes en redirección respuestas sintetizadas no sólo en TLDs sino también en niveles subordinados del DNS. Esta estipulación en nuevos contratos de registro está diseñada para tratar esta cuestión a nivel de registro.

4. Alentar la eliminación de Registros de Interconexión Huérfanos

Como parte de sus políticas de anti-abuso publicadas, los registrados deben proporcionar una descripción de cómo eliminará los registros de interconexión huérfanos en el momento en que el ingreso de nombre de servidor sea eliminado de la zona. Lo siguiente es escogido de la Guía de Solicitud en Borrador, módulo 2 preguntas de solicitante:

"Prevención de Abuso y Atenuación: Los solicitantes deben describir las políticas y procedimientos propuestos para minimizar el registro abusivo y otras actividades que tengan un impacto negativo en los usuarios de internet...Las respuestas deben incluir una bajada rápida o sistema de suspensión, y medidas propuestas para la administración y eliminación de registros de interconexión huérfanos para nombres eliminados de la zona."

Un estudio APWG estimó que aproximadamente 3% de los dominios utilizados para usurpación de identidad estaban utilizando registros de "servidor de nombre huérfano", por ejemplo restos de un dominio que fuera previamente eliminado de un registro. Esto puede crear un ingreso potencial de servidor de nombre "de protección" en el archivo de zona TLD que los abusadores puedan utilizar para apoyar a registros de dominio criminal.

5. Requerimiento para IDENTIFICACIÓN Marcada

El Operador de Registro debe mantener y proporcionar un acceso público a información de registro utilizando un modelo de datos de Identidad Marcada como lo requiere la Especificación 4 a versión 3 del acuerdo de registro de formato.

"Servicio WHOIS. Hasta que ICANN especifique un formato y protocolo diferente, el Operador de Registros prestará un servicio de publicación de datos de registro disponible a través del puerto 43 y un sitio web en <whois.nic.(TLD)>, en conformidad con RFC 3912 proporcionando acceso público gratuito basado en consultas a por lo menos los elementos que se indican a continuación en el formato siguiente: ICANN se reserva el derecho a especificar formatos y protocolos, incluyendo el "IRIS" –(Servicio de Información de Registro de Internet por sus siglas en inglés)("RFC 3981 y RFCs relacionados), y luego de dicha especificación, el Operador de Registro implementará dicha especificación alternativa tan pronto como se pueda aplicar de modo razonable."

ICANN ha propuesto la modificación a los requerimientos de Identificación en el nuevo acuerdo de registro propuesto para requerir a todos los registrados ofrecer una respuesta de Identificación Marcada como se describió en un memorándum explicativo anterior (pdf). Además, el reporte en borrador (pdf) del Equipo de Recomendaciones de Implementación formado por los Miembros de Propiedad Intelectual de la ICANN declara que "el IRT cree que el proporcionar información de Identificación a nivel del registro bajo el modelo de Identificación Marcada es esencial para la protección de economía de los

consumidores y propietarios de propiedad intelectual." La implementación de Identificación Marcada ayudará a atenuar una conducta malintencionada asegurando una accesibilidad mayor y una estabilidad mejorada del acceso a registros.

6. Centralización de acceso a archivos de zona

ICANN requerirá que los registrados permitan el acceso a información de archivo de zona para el propósito de hacerla disponible por medio de un proveedor centralizado.

Una versión sugerida o propuesta de la Especificación 4 del Acuerdo de Registro (sujeta a revisión técnica) estipula que el operador del registro hará que esta información esté disponible a la comunidad en general:

"2.2.1. **Acceso General.** El Operador de Registro proporcionará un acceso en bruto a los archivos de la zona para el registro para el TLD a la ICANN o su designado en una base continua en la manera en la cual ICANN pueda especificar razonablemente de un momento a otro.

"2.2.2. **Repositorio Central de Archivos de la Zona.** En el caso de que la ICANN o su designado establezcan un repositorio central para los archivos de la zona, el Operador del Registro proporcionará toda la información de archivos de la zona a ICANN o a un operador tercero de dicho repositorio designado por ICANN luego de una solicitud por ICANN. Si se estableciera dicho repositorio central de archivos de la zona, ICANN puede no aplicar, a discreción exclusiva de ICANN, el cumplimiento con la Sección 2.1 de esta Especificación 4. [La presente Sección 2.2.2 está incluida para propósitos de discusión de la comunidad como resultado de previas discusiones de la comunidad con respecto a la atenuación de conducta malintencionada. Bajo esta estipulación, un representante de la ICANN podría asumir la responsabilidad actualmente llevada por los operadores del registro de vetar y controlar el acceso a la información de archivos de zona por partes responsables para propósitos legítimos.]"

Para facilitar acceso a la información de registro de archivo de zona, la cual es actualmente manejada por registros individuales (o parcialmente designados por ICANN para realizar esta función) ICANN recolectaría información de archivos de zona de nuevos registros gTLD y proporcionaría a los suscriptores un acceso electrónico a la información. Esto también incluiría un sólo contrato para firmarse por las partes que deseen acceso a los archivos de zona para los registros regulados por ICANN, ICANN establecería los contratos de acceso basada en el modelo actual y administraría/daría soporte al sistema de transferencia.

Esta coordinación central permitirá a la comunidad anti-abuso el obtener eficientemente actualizaciones de nuevos dominios a medida que se creen dentro de cada zona.

7. Registro Documentado y Contacto y Políticas de Abuso a Nivel de Registradores

El Operador del Registro proporcionará un sólo punto de contacto de abuso para todos los dominios dentro del TLD. Este contacto de abusos será responsable de tratar y proporcionar una respuesta oportuna a las quejas de abuso recibidas por partes reconocidas, tales como otros registros, registradores, organizaciones de cumplimiento de la ley y miembros reconocidos de la comunidad de anti-abuso. Los registros también deben proporcionar una descripción de sus políticas para combatir el abuso.

El Operador de Registro puede requerir de todos los registros con quienes contrata servicios que éstos proporcionen un punto de contacto de abusos. Este paso es consistente con las recomendaciones del informe SAC038 de SSAC (pdf). Los registros también pueden requerir que los registradores publiquen una política de abuso documentada que sea consistente con la política de abuso del Registro. En ambos niveles, la política trata los procedimientos por los cuales:

1. Suspenderá dominios identificados como involucrados en abuso de marca registrada, identidad falsa, distribución voluntaria de software malicioso y otra actividad ilegal o fraudulenta.
2. Tratará cuestiones relacionadas a revendedores y otros distribuidores de servicios bajo su control
3. Eliminará los registros de interconexión huérfanos asociados con conducta malintencionada
4. Identificará el punto de contacto de abuso y cómo se espera que ocurran las comunicaciones con dicho punto de contacto

Se ha agregado el siguiente idioma a la Especificación 6 de la versión 3 del Acuerdo de Registro para tratar este punto:

"El Operador de Registro proporcionará en su sitio web sus detalles de contacto exactos incluyendo una dirección de correo físico y correo electrónico validas así como también un contacto principal para manejar consultas relacionadas con conducta malintencionada en el TLD, y proporcionará a la ICANN una notificación oportuna de cualquier cambio a dichos detalles de contacto."

Además, el siguiente extracto de una pregunta del módulo 2 se incluye en el Borrador de la Guía de Solicitud, versión 3:

"...Se requerirá que cada operador de registro establezca y publique en su sitio web un solo punto de contacto de abuso responsable de tratar cuestiones que requieran una atención más rápida, proporcionando una respuesta oportuna a quejas de abuso con respecto a todos los nombres registrados en el TLD por medio de todos los registradores de registros, incluyendo aquellos que involucran a un revendedor."

La implementación de nuevos registros, posiblemente en gran escala, necesita de nuevos controles bien definidos y roles definido en el proceso de registro de dominio. Los contactos de abuso y políticas tanto a nivel del registro como del registrador serán un paso fundamental en permitir esfuerzos futuros para combatir la conducta malintencionada y para continuar y escalar con la adición de nuevos operadores.

8. Disponibilidad de Procesos Acelerados de Solicitud de Seguridad de Registro

ICANN ha desarrollado un procedimiento adicional http://www.icann.org/en/announcements/announcement-01oct09-en.htm, en consulta con los registros gTLD, registradores y expertos en seguridad, basado en lecciones aprendidas en responder al virus Conficker, **para proporcionar un proceso para que los registros informen a ICANN de una situación presente o inminente de seguridad que involucre a un gTLDD y para solicitar una no aplicación contractual por acciones que el registro tal vez tome o deba tomar para atenuar o eliminar las inquietudes de seguridad.**

Se define una situación de seguridad como una o más de las siguientes:

a. Actividad malintencionada que involucra el DNS de escala y severidad que amenaza la seguridad sistemática, estabilidad y capacidad del DNS;

b. Divulgación potencial o real no autorizada, alteración, inserción o destrucción de datos del registro o el acceso no autorizado o la divulgación de información o recursos de Internet por sistemas que operan en conformidad con todas las normas aplicables;

c. Las consecuencias potenciales o reales no deseadas que pueden causar o amenazan causar una falla temporal o de largo plazo a uno o más de las funciones críticas de un registro gTLD como lo define el Plan de Continuidad de Registro gTLD de ICANN (**pdf**).

El ERSR es exclusivamente para incidentes que requieren de una acción inmediata por el registro y una respuesta acelerada (dentro de 24 a 48 horas) por la ICANN. No se intenta que este proceso reemplace las solicitudes que se deben hacer a través de la RSEP (Política de Evaluación de Servicios de Registro) (**link**).

9. Programa de Verificación de Zonas de Alta Seguridad

Para poder facilitar la necesidad general de la comunidad de una confianza mejorada dentro de los gTLDs seleccionados, ICANN ha creado un borrador de un marco de trabajo para un programa de verificación gTLD. Como se propuso en la actualidad, este programa de verificación será totalmente opcional.

Una opción de no seguir una verificación en el momento de una solicitud de nuevo gTLD NO se refleja negativamente en el solicitante, ni afecta sus puntajes en el proceso de evaluación. El propósito del programa de verificación es establecer un grupo aceptable de normas y criterios que mejorarán la confianza en un gTLD verificado, a través de la aplicación de controles apropiados operacionales y de seguridad y midiendo las acciones de los registros gTLD y los registradores contra los controles. Los registros gTLD que elijan seguir una verificación podrán demostrar la verificación a través de algún método de exhibición pública, como por ejemplo un "sello" o una marca que se pueda verificar con una lista maestra de gTLDs verificados. ICANN mantendrá y publicará la lista maestra de los gTLDs verificados.

Adicionalmente para mantener la lista maestra de gTLDs verificados, el rol de la ICANN en el programa es ayudar a establecer, refinar y administrar la gobernabilidad del programa y trabajar con la comunidad para establecer normas y criterios del programa. La evaluación actual de un gTLD versus las normas y criterio del programa se realizará por entidades independientes.

Para lograr la verificación bajo el programa propuesto, las operaciones del registro deben ser consistentes con los siguientes principios (Ver Guía, Módulo2):

a. El registro demuestra que el operador mantiene controles efectivos para proporcionar la seguridad de que se mantengan la seguridad, disponibilidad, confidencialidad y privacidad de los sistemas y activos de información que dan soporte al TI de registro crítico y operaciones del negocio.

b. El Registro mantiene controles efectivos para proporcionar una seguridad de que el proceso de funciones de Registro centrales sean autorizadas, precisadas,

completadas y realizadas en manera oportuna en conformidad con políticas y normas establecidas. La identidad de las entidades participantes es establecida y autenticada.

c. El Registro mantiene controles efectivos para proporcionar una seguridad razonable de que el proceso de funciones centrales de registrador sea autorizado, precisado, completado y realizado en manera oportuna en conformidad con políticas y normas establecidas. La identidad de las entidades participantes es establecida y autenticada.

Los procesos requeridos para lograr la verificación incluyen la verificación tanto de operaciones de Registro como dar soporte a las operaciones del Registrador.

En caso de que un solicitante desee aplicar a la opción de verificación, lo hace en un proceso de dos fases.

Fase I

Previo a la delegación del nuevo gTLD, el solicitante participa en una evaluación, la cual incluirá lo siguiente:

- Información de antecedentes
- Procedimientos de administración/derribo de dominio
- Abuso de punto de contacto y respuesta
- Procedimientos para custodia de registros

Luego de que se haya delegado el nuevo gTLD e inicie las operaciones, se dará un período específico para que el solicitante implemente todos los procesos y controles pre-aprobados.

Fase II

La siguiente fase comprueba los procesos, controles y procedimientos documentados en la Fase 1 para validar que estén operando como se planificó. Si se identifican deficiencias, éstas serían comunicadas a ICANN por la agencia de evaluación independiente. El operador de registro tendrá un período definido para resolver el problema antes de que la solicitud para verificación del solicitante sea negada. El operador de registro puede volver a solicitar una verificación en lo posterior.

En el caso de que cualquier nueva solicitud de registro gTLD complete la evaluación y se delegue el TLD, el operador de registro puede escoger en ese momento solicitar una verificación y entonces completaría las pruebas anteriores en una sola fase. Esto significa, que un solicitante puede escoger tomar los pasos para obtener la verificación luego de que haya completado el proceso de evaluación y esté operando su nuevo gTLD, en lugar de un modo concurrente con el proceso de evaluación.

Los controles necesarios para dar soporte a la verificación son evaluados por medio de una auditoría en una base periódica, para retener el status verificado de gTLD.

ICANN cree que este programa de verificación permite un nivel de confianza mejorado dentro de los gTLDs certificados, a cuenta de los requerimientos adicionales para establecer la exactitud de los controles para registro, registrador y procesamiento de registrante así como también registro y operaciones de registrador. El equilibrio entre la

confianza y el costo/beneficio constituye la decisión de negocios clave que un registro de gTLD utilizará como la base para determinar si la Verificación es un proceso comercial apropiado de seguir.

El Programa de Verificación aplica a un conjunto propuesto de actividades necesarias para dar soporte a un nivel mejorado de confianza para las operaciones de registro. El enfoque del borrador del marco de trabajo está en los controles necesarios para reducir el potencial de una conducta malintencionada dentro de los registros gTLD que eligen buscar un sello de verificación de ICANN. El alcance está limitado a los controles y actividades a nivel de operaciones del registro y registrador y no se extiende a las operaciones de los registrantes. El Programa de Verificación tiene como propósito proporcionar una seguridad razonable, pero no absoluta de que los TLDs tienen controles de operación efectivos para cumplir con el criterio de verificación. Por lo tanto, el establecimiento del criterio de verificación y revisiones/auditorías independientes y periódicas de su efectividad a través del Programa de Verificación proporcionarán un nivel de confianza mayor.