Programa de gTLD nuevos
Actualización al Memorando explicativo
Mitigación de las conductas maliciosas

Antecedentes - Programa de gTLD nuevos

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 primer nivel (gTLD) permitirá mayor innovación, opciones y cambios en el sistema de direcciones de Internet, actualmente representado por 21 gTLD.

La decisión de introducir gTLD nuevos se tomó después de un proceso de consulta extenso y meticuloso con la participación de todas las unidades constitutivas de la comunidad global de Internet representada por una amplia variedad de partes interesadas: gobiernos, particulares, la sociedad civil, el sector empresarial y el de la propiedad intelectual, así como la comunidad tecnológica. También contribuyeron con esta labor: 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 dio lugar a una política sobre la introducción de gTLD nuevos completada por la Organización de apoyo para nombres genéricos (GNSO) en 2007 y adoptada por la Junta directiva de ICANN en junio de 2008. Se espera que el programa se lance en el año calendario 2010.

Este memorando explicativo forma parte de una serie de documentos publicados por ICANN con el objeto de ayudar a la comunidad global de Internet a comprender los requisitos y los procesos presentados en la Guía del solicitante, que actualmente se encuentra en borrador. Desde fines de 2008, el personal de ICANN ha compartido el progreso del desarrollo del programa con la comunidad de Internet a través de una serie de foros de comentarios públicos sobre los borradores de la guía del solicitante y los comprobantes. Hasta el momento, ha habido más de 250 días de consulta sobre materiales fundamentales del programa. Los comentarios recibidos se siguen evaluando minuciosamente y se utilizan para perfeccionar aún más el programa e informar el desarrollo de la versión final de la Guía del solicitante.

Para obtener información actual, cronogramas y actividades relacionadas con el programa de gTLD nuevos, visite

http://www.icann.org/en/tlds/select.htm

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

Resumen

Se ha hecho un progreso significativo en el abordaje de las inquietudes de la comunidad con respecto a la mitigación de la posibilidad de que aumenten los casos de conducta maliciosa en relación con el programa de gTLD nuevos.

Las soluciones aquí descritas darán como resultado mejoras importantes en el entorno de DNS: proporcionando protecciones para los registrantes, un entorno más estable y herramientas para detectar y combatir el posible comportamiento malicioso. Mientras que en esta área siempre se requieren mejoras continuas, estas mejoras contribuirán al lanzamiento estable del proceso de gTLD nuevos. El abordaje de las cuestiones de seguridad, estabilidad y flexibilidad en desarrollo seguirá siendo una inquietud continua, de alta prioridad para ICANN a medida que el programa de gTLD nuevos avanza hacia el lanzamiento, la eventual implementación y mucho más.

Se ha realizado una cantidad importante de excelente trabajo, principalmente a cargo de voluntarios de la comunidad en foros de comentarios o en grupos de trabajo. Se los elogiará por mejorar significativamente el entorno de DNS. ICANN se lo agradece.

Este documento es una actualización del memorando original "Mitigación de las conductas maliciosas" ("memorando de las conductas maliciosas") publicado el 3 de octubre de 2009. El memorando original está disponible en el siguiente vínculo:

http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

En el memorando original de las conductas maliciosas, ICANN buscó comentarios sobre la propuesta de agregar medidas específicas al acuerdo de registro de gTLD nuevos, para que se exijan todos los registros con el fin de reducir la posibilidad de conductas maliciosas dentro de los gTLD nuevos.

Para facilitar este proceso, ICANN realizó un estudio de conductas maliciosas, cuando se relacionaban con las conductas dentro del espacio de TLD. Durante el estudio, el personal de ICANN solicitó y recibió comentarios de múltiples fuentes externas, que incluyen: la Unidad constitutiva de propiedad intelectual (IPC), el Grupo de seguridad para registros de Internet (RISG), el Comité asesor de seguridad y estabilidad (SSAC), los Equipos de respuesta de emergencias informáticas (CERT) y los miembros de las comunidades bancarias o financieras y de seguridad de Internet. Estas partes describieron diversas cuestiones de conductas maliciosas posibles y alentaron a ICANN a considerar las formas en que estas podrían abordarse o mitigarse dentro de los acuerdos de registro de gTLD nuevos, o como un componente del proceso de solicitud. Estas medidas recomendadas pretendían aumentar los beneficios para la estabilidad y la seguridad general de los registrantes y la confianza de todos los usuarios de estas zonas de gTLD nuevos.

El resultado de este estudio, y el período para comentarios públicos correspondiente, generó nueve recomendaciones diseñadas para proporcionar áreas de interés, a partir de las cuales se podrían crear controles que reducirían la posibilidad de conductas maliciosas dentro de los gTLD. Se implementarán nueve recomendaciones en el programa:

1. ***Operadores de registro revisados***: Esta recomendación requiere que se revise adecuadamente a los operadores de registro del solicitante de gTLD nuevos, con el fin de determinar si el operador de registro del solicitante tiene antecedentes delictivos o maliciosos.

2. ***Plan demostrado para implementación de DNSSEC:*** Esta recomendación requiere que sea obligatorio para un solicitante de gTLD nuevos que demuestre un plan para la implementación de DNSSEC, con el fin de reducir el riesgo de registros de DNS falsos.
3. ***Prohibición del uso de comodines***: Esta recomendación requiere controles adecuados en relación con el uso de comodines de DNS que reducirían el riesgo de redirección de DNS a un sitio malicioso.
4. ***Eliminación de los registros de interconexión huérfanos***: Esta recomendación requiere que los gTLD eliminen los registros de servidores de nombres, cuando se elimina un sistema del gTLD, con el fin de reducir el riesgo de uso de estos registros remanentes por un actor malicioso.
5. ***Requisito para registros de WHOIS extensos***: Esta recomendación requiere que los gTLD nuevos mantengan registros de "WHOIS extensos", con el fin de mejorar la precisión y la integridad de los datos de WHOIS. El uso de registros de WHOIS extensos proporciona un mecanismo clave para combatir el uso malicioso de los gTLD nuevos, al suministrar una cadena de contactos más completa dentro del TLD. A su vez, esto debe permitir una búsqueda de datos y una resolución de las actividades de conducta maliciosa más rápidas, a medida que se identifican.
6. ***Centralización del acceso a archivos de zona:*** Esta recomendación requiere que las credenciales de acceso para obtener datos de archivos de la zona de registro se otorguen a través de una fuente centralizada, lo que permite una identificación más precisa y más rápida de los puntos de contacto clave dentro de cada TLD. Esto reduce el tiempo necesario para realizar acciones correctivas dentro del TLD que experimenta la actividad maliciosa.
7. ***Contactos y procedimientos documentados de 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 designadas para combatir el uso indebido. Estos requisitos se consideran pasos fundamentales al permitir esfuerzos exitosos para combatir las conductas maliciosas dentro de los gTLD nuevos.
8. ***Participación en un proceso de solicitud acelerada de seguridad de registro:*** Esta recomendación contempla que se permita que los nuevos gTLD tomen medidas rápidas y eficaces en vista de las amenazas sistemáticas al DNS al establecer un proceso dedicado para revisión y solicitudes aceleradas de seguridad aprobadas.
9. ***Marco preliminar para la verificación de zonas de seguridad alta***: Esta recomendación sugirió la creación de un programa voluntario diseñado para designar TLD que deseen establecer y probar un nivel de seguridad y una confianza mejorados. El objetivo global del programa es proporcionar un mecanismo para los TLD que deseen distinguirse como seguros y fiables, para modelos comerciales 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 suministra el estado actual y/o las actualizaciones (si corresponde) de las nueve recomendaciones diseñadas para reducir la posibilidad de conductas maliciosas en los gTLD nuevos, según se presentaron en el memorando original de las conductas maliciosas (consulte el "Resumen de los puntos clave del documento" descrito anteriormente). Cada recomendación se divide en una sección de "estado actual y/o actualización", que detalla las actualizaciones significativas de la recomendación, y "mejoras específicas recomendadas para el proceso de los gTLD nuevos" como una referencia al material publicado en el memorando de las conductas maliciosas del 3 de octubre de 2009.

1. Operadores de registro revisados

- **Estado actual y/o actualizaciones**

  La recomendación de requerir una "revisión" o verificación de antecedentes de los operadores de registro ha sido un principio rector en la mejora del proceso de solicitud para los solicitantes de nuevos gTLD. El proceso de solicitud de nuevos gTLD actualmente contiene criterios específicos que requieren que el solicitante de nuevos gTLD se someta a diversas verificaciones de antecedentes como un componente del proceso de solicitud. Además, como se mencionó en el memorando original de las conductas maliciosas, el Módulo 2 del borrador de la Guía del solicitante contiene una referencia específica al derecho de rechazar a los solicitantes calificados de otro modo, en caso de que no aprueben un proceso de revisión específico. Los detalles de los criterios y las referencias del Módulo 2 del borrador de la Guía del solicitante se pueden encontrar a continuación o en el siguiente vínculo:

  http://www.icann.org/en/topics/new-gtlds/draft-evaluation-criteria-30may09-en.pdf

2. Requerir la implementación de DNSSEC

- **Estado actual y/o actualizaciones**

  La evidencia de un plan para la implementación de DNSSEC sigue siendo un componente obligatorio del proceso de solicitud de nuevos gTLD y un componente de prueba anterior a la delegación para cada gTLD nuevo. Puede encontrar la documentación sobre el requisito en el Módulo 5 del borrador de la Guía del solicitante. Como en el memorando original de las conductas maliciosas, la Especificación 6 de la versión 3 del Acuerdo de registro contiene referencias con respecto a DNSSEC (vea a continuación). La primera frase de la Sección 6 de la versión 3 se modificó a: "El operador de registro firmará sus archivos de zona de TLD implementando las Extensiones de seguridad del sistema de nombres de dominio ("DNSSEC")".

  NOTA: La RFC 4310 (como se menciona a continuación) se actualizó a la RFC 5910.

3. Prohibición del uso de comodines

- **Estado actual y/o actualizaciones**

La referencia relacionada con la prohibición de los comodines de DNS sigue siendo parte de la Especificación 6 de la versión 3 del Acuerdo de registro (consulte "Estado del memorando original de las conductas maliciosas" a continuación). Además, ICANN publicó el 24 de noviembre de 2009 un memorando explicativo llamado "Harms and Concerns Posed by NXDOMAIN Substitution (DNS Wildcard and Similar Technologies) at Registry Level" (Daños e inquietudes planteados por la sustitución de NXDOMAIN, comodines de DNS y tecnologías similares, en el nivel de registro). Este memorando explicativo describe los daños y las inquietudes planteados por la sustitución de NXDOMAIN (implementado comúnmente por el uso de comodines de DNS) en el nivel de registro. El documento es una recopilación de hallazgos publicados por expertos en la materia. El memorando real se puede consultar en el siguiente vínculo:

http://www.icann.org/en/announcements/announcement-2-24nov09-en.htm

La Junta directiva de ICANN resolvió que los nuevos dominios de primer nivel no deben utilizar la redirección de DNS ni la sintetización de respuestas de DNS, en su reunión pública en Sydney en junio de 2009.

En respuesta a la resolución de la Junta, el personal de ICANN incluyó una prohibición contra la redirección y la sintetización de respuestas de DNS en el borrador del Acuerdo de registro para nuevos gTLD. Además, ICANN incluyó un compromiso similar como parte de la solicitud de nuevos ccTLD de IDN en los Términos y condiciones propuestos y en las tres opciones de relación propuestas entre ICANN y el administrador de ccTLD de IDN.

Finalmente, la Junta también indicó al personal de ICANN que informe sobre los daños y las inquietudes planteados por el uso de redirección y sintetización de respuestas de DNS, en forma colectiva, sustitución de NXDOMAIN.

4. Promover la eliminación de los registros de interconexión huérfanos

- **Estado actual y/o actualizaciones**

El Comité asesor de seguridad y estabilidad (SSAC) formó un grupo de trabajo para estudiar esta cuestión. Actualmente, el grupo de trabajo está examinando los archivos de zona para todos los gTLD actuales con el fin de hacer un censo de los servidores de nombres huérfanos y, de ser posible, determinar el grado en el cual estos huérfanos se utilizan con fines maliciosos o delictivos. Las recomendaciones generadas por el grupo de trabajo del SSAC pueden ofrecer una guía adicional para los registros relativos a cómo manejar los registros huérfanos y se evaluarán para su inclusión en los procesos de gTLD clave.

Como se menciona en el memorando original de las conductas maliciosas, los registros deben brindar una descripción de cómo eliminarán los registros de interconexión huérfanos en el momento en que se elimina un servidor de nombre de la zona (vea a continuación).

5. Requisito para WHOIS extensos

- **Estado actual y/o actualizaciones**

Ahora está establecida la recomendación de hacer que los registros "WHOIS extensos" sean un requisito para todos los gTLD nuevos. Todos los gTLD nuevos deberán implementar requisitos de WHOIS extensos, según el último Acuerdo de registro.

Además, una nueva cláusula con respecto a la "capacidad de búsqueda" de WHOIS se ha agregado al borrador del acuerdo de registro de manera provisional para recibir comentarios. La cláusula contiene lo siguiente:

"Para ayudar a los reclamantes con la UDRP para determinar si un registrante particular ha demostrado un patrón de 'mala fe', la información de WHOIS estará disponible en una base de datos de acceso público, sujeta a las políticas de privacidad pertinentes, que se podrá buscar por nombre de dominio, nombre del registrante, dirección postal del registrador, nombres de los contactos, ID de contacto de los registradores y dirección del Protocolo de Internet sin límites arbitrarios. Para proporcionar una base de datos WHOIS eficaz, se pueden ofrecer las capacidades de Boolean Search".

La cláusula brinda una herramienta adicional a aquellas personas involucradas en identificar y confrontar la conducta maliciosa en el espacio de nombres, siempre que los métodos y estándares utilizados para realizar búsquedas tengan una estructura de control diseñada para disminuir el uso malicioso de la capacidad de búsqueda misma. Esta cláusula forma parte de algunos acuerdos de registro actuales (.ASIA, .MOBI, .POST, etc.) y está incluida en este borrador del acuerdo de registro de gTLD nuevos con fines de debate. Como punto de referencia, .NAME (http://www.icann.org/en/tlds/agreements/name/appendix-05-15aug07.htm) ha tenido una función de búsqueda "WHOIS de gran alcance", disponible desde el comienzo. La función de búsqueda se basa en un modelo de acceso escalonado que ayuda a reducir el posible uso malicioso de la función. Se invita a las personas a hacer comentarios particularmente sobre cómo este requisito podría ayudar a abordar ciertos tipos de conducta maliciosa y sobre las soluciones alternativas mediante las que el uso de datos Whois para los nombres registrados sea una herramienta eficaz en el contexto de mitigar la conducta maliciosa en los nuevos gTLD. Si se respalda el requisito, también se pedirán sugerencias sobre el desarrollo de una especificación técnica uniforme para la función de búsqueda.

6. Centralización del acceso a archivos de zona

- **Estado actual y/o actualizaciones**

La recomendación para 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 llamado el "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 archivos de zona. El ZFA AG finalizó su trabajo sobre la propuesta estratégica y se puede consultar en el siguiente vínculo:

http://www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf

El paso siguiente para la centralización del acceso a archivos de zona es implementar las recomendaciones descritas en la propuesta.

7. Contactos y políticas documentadas de uso indebido del nivel de registro

- **Estado actual y/o actualizaciones**

La recomendación de requerir que los nuevos gTLD documenten un contacto específico de uso indebido del registro y que brinden una descripción de sus políticas específicas contra el uso indebido es un requisito para todos los gTLD nuevos. Esto no se ha modificado desde el memorando original de las conductas maliciosas (vea a continuación).

8. Participación en un proceso de solicitud acelerada de seguridad de registro

- **Estado actual y/o actualizaciones**

Según el resumen en el memorando original de las conductas maliciosas, ICANN publicó un memorando explicativo llamado "Expedited Registry Security Request Process Posted" (Proceso publicado de solicitud acelerada de seguridad de registro) (vea a continuación). Este memorando explicativo define un proceso llamado proceso de "solicitud acelerada de seguridad de registro" (ERSR). Representa el resultado de un esfuerzo colaborativo entre ICANN y los registros de gTLD para desarrollar un proceso de rápida acción en casos donde los registros de gTLD:

- informan a ICANN sobre un incidente de seguridad existente o inminente en sus TLD y/o DNS, y
- solicitan una renuncia contractual por medidas que pudieron tomar o que han tomado para mitigar o eliminar el incidente.

Una renuncia contractual es una excepción al cumplimiento de una disposición específica del Acuerdo de registro durante un período necesario para responder al incidente.

El procedimiento de presentación de ERSR basado en la Web está actualmente disponible y se puede consultar en el apéndice A o a través del siguiente vínculo:

http://www.icann.org/en/registries/ersr/.

Los registros de gTLD emplearán este nuevo proceso exclusivamente para incidentes que requieran una acción inmediata del registro con el fin de evitar efectos deletéreos para la estabilidad o la seguridad de DNS. Para garantizar la estabilidad de DNS, este proceso se activó inmediatamente el 1° de octubre de 2009. Puede acceder a información adicional sobre el proceso de ERSR en el siguiente vínculo:

http://www.icann.org/en/announcements/announcement-01oct09-en.htm

9. Marco preliminar para la verificación de zonas de seguridad alta

- **Estado actual y/o actualizaciones**

  La recomendación de crear un marco preliminar para la verificación de zonas de seguridad alta fue realizada por los grupos de partes interesadas financieras y bancarias, como BITS, y se creó una iniciativa llamada Programa de dominios de nivel superior de zonas de seguridad alta ("Programa HSTLD"). La iniciativa es realizar una versión preliminar de un marco de controles propuestos para la verificación de zonas de seguridad alta. Para analizar enfoques posibles a tal marco y avanzar hacia una propuesta para la revisión de la comunidad, ICANN formó el Grupo asesor de dominios de nivel superior de zonas de seguridad alta ("HSTLD AG"). El mandato del HSTLD AG es trabajar con la comunidad, a través de un modelo de desarrollo exhaustivo, para proponer enfoques de un programa voluntario compuesto por estándares e iniciativas de control para aumentar la seguridad y la confianza en los TLD que optan por participar en dicho programa.

  Actualmente, el HSTLD AG está formado por miembros de la comunidad que han expresado un interés en ayudar con el programa, además de personas que son expertos en el tema en disciplinas relacionadas con el programa (por ejemplo, seguridad, auditoría, programas de certificación, representantes de servicios financieros) respaldado por los miembros del personal de ICANN. El HSTLD AG se reúne regularmente para contribuir con los conceptos introducidos en el documento original de octubre de 2009, los elementos de control preliminares y los requisitos del programa, y planifica la publicación de un programa actuable para revisión y consideración de la comunidad. El HSTLD AG lleva a cabo sus actividades y el desarrollo del programa a través de un proceso abierto y transparente. En el siguiente vínculo, se encuentra disponible información adicional que incluye a los participantes del grupo y las grabaciones de las reuniones semanales del HSTLD AG:

  http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

  ICANN no operará el programa. Una entidad independiente establecerá los criterios y certificará los TLD según esos criterios. Estarán a cargo de la supervisión y la renovación de las certificaciones, además de la publicación de las certificaciones.

Apéndice A

Proceso de solicitud acelerada de seguridad de registro

El proceso de solicitud acelerada de seguridad de registro (ERSR) se desarrolló con el fin de proporcionar un proceso para los registros de gTLD que informan a ICANN sobre un incidente de seguridad existente o inminente (en lo sucesivo, en este documento, se denominará "incidente") en sus TLD y/o DNS para solicitar una renuncia contractual por medidas que pudieron tomar o que han tomado para mitigar o eliminar el incidente. Una renuncia contractual es una excepción al cumplimiento de una disposición específica del Acuerdo de registro durante un período necesario para responder al incidente. La ERSR se diseñó para permitir el mantenimiento de la seguridad operativa en relación con un incidente mientras permanecen informadas las partes relevantes (por ejemplo, ICANN, otros proveedores afectados, etc.), según corresponda.

Un incidente podría ser una o más de las siguientes opciones:

- Actividad maliciosa que involucra al DNS de un nivel y gravedad que amenaza la seguridad sistemática, la estabilidad y la flexibilidad de un TLD o del DNS.
- Divulgación, alteración, inserción o destrucción no autorizada de datos del registro o el acceso no autorizado o la divulgación de información o recursos de Internet por sistemas que operan de acuerdo con todas las normas aplicables.
- Un suceso con el potencial de causar una falla temporal o prolongada de una o más funciones críticas de un registro de gTLD, según se define en el Plan de continuidad de registros de gTLD de ICANN [PDF, 96K].

La ERSR es exclusivamente para incidentes, es decir, que requiere medidas inmediatas del registro y una respuesta acelerada de ICANN dentro de los 3 días hábiles. Este proceso no pretende reemplazar las solicitudes que se deben realizar a través de la Política de evaluación de servicios de registros (RSEP).

Se reconoce que en algunos casos extraordinarios puede ser necesario que los registros tomen medidas inmediatas para prevenir o tratar un incidente. En los casos en que tales incidentes ocurran, los registros deben presentar una ERSR lo antes posible de modo que ICANN pueda responder con una renuncia retroactiva, si corresponde.

Los registros pueden presentar una ERSR al completar el formulario de solicitud que se encuentra en http://www.icann.org/cgi/registry-sec. La solicitud presentada se procesa de la siguiente manera:

- Automáticamente, la ERSR se enviará al equipo de respuesta de seguridad de ICANN y se proporcionará una copia al solicitante. El equipo de respuesta de seguridad incluye personal de los siguientes departamentos: Seguridad, Coordinación de registro de gTLD, Consejero general y Cumplimiento.

- Para cada caso en particular, un miembro designado del Equipo de respuesta de seguridad será responsable de comunicarse con el registro en el plazo de un día hábil para confirmar el incidente y solicitar información adicional si es necesario.
- El equipo de respuesta de seguridad puede solicitar información adicional si es necesario para revisar y considerar la ERSR y se pedirá al solicitante que proporcione dicha información prontamente.
- Se convocará al equipo de respuesta de seguridad en el plazo de dos días hábiles de la recepción de la solicitud (y cualquier información adicional requerida) para revisar y determinar una respuesta.
- ICANN responderá al solicitante o a su representante designado, verbalmente y por escrito, en el plazo de tres días hábiles de la recepción de la ERSR.
- Un miembro designado del equipo de respuesta de seguridad se mantendrá en comunicación con el contacto principal del registro durante todo el transcurso del incidente.
- Si la solicitud se recibe después de que el registro respondió a un incidente, ICANN procurará responder en el plazo de 10 días hábiles para proporcionar por escrito una renuncia retroactiva a la solicitud, si corresponde.
- Después de una respuesta a una ERSR, el equipo de respuesta de seguridad junto con el registro afectado desarrollarán un informe posterior a la acción (AAR) que puede ponerse a disposición de la comunidad. Si se publica un AAR, ICANN y el registro afectado revisarán en conjunto qué secciones de la solicitud ERSR y el AAR deben redactarse para garantizar que se proteja la información confidencial y patentada. ICANN y el registro pueden redactar tal información, que se considera razonablemente confidencial o patentada.