ICANN | GAC
Governmental Advisory Committee

ICANN 65 POLICY FORUM
MARRAKECH
24–27 June 2019

Mitigación del uso indebido del DNS

Sesión 5.1

Índice

Objetivos de la sesión

- Revisar los desarrollos recientes y los debates sobre la definición, detección y mitigación del uso indebido del DNS, y el impacto del cumplimiento de WHOIS con los esfuerzos del GDPR.
- Discutir posiciones y posibles pasos a seguir para el Grupo de Trabajo sobre Seguridad Pública (PSWG) del GAC y el GAC.

Información de referencia

La actividad maliciosa en Internet amenaza y afecta a los registratarios de nombres de dominio y usuarios finales al aprovecharse de las vulnerabilidades en todos los aspectos de los ecosistemas de Internet y del DNS (protocolos, sistemas informáticos, transacciones personales y comerciales, procesos de registración de dominios, etc.). Algunas de estas actividades nefastas amenazan la seguridad, la estabilidad y la flexibilidad de las infraestructuras del DNS y la del DNS en su conjunto.

Estas amenazas y actividades maliciosas generalmente se conocen, dentro de la comunidad de la ICANN, como "uso indebido del DNS". Por lo general, se entiende que el uso indebido del DNS incluye la totalidad o parte de actividades como los ataques de denegación de servicio distribuido (DDoS), spam, suplantación de identidad (phishing), malware, botnets y la distribución de materiales ilegales. Si bien todos parecen estar de acuerdo en que el uso indebido es un problema y debe abordarse, existen diferencias de opinión sobre en quién debe recaer la responsabilidad. En particular, a los registros y a los registradores les preocupa que se les pida hacer más, ya que esto afecta su modelo de negocios y su resultado final.

Como parte de esta conversación, se debe tener en cuenta que, incluso, la definición exacta de "uso indebido del DNS" es un tema de debate.[1]

No obstante, en los últimos años se han logrado algunos avances. Aquí se presenta un resumen de los esfuerzos realizados anteriormente en la comunidad de la ICANN para abordar el uso indebido del DNS, algunos de los cuales han contado con la participación del GAC:

- La **Organización de Apoyo para Nombres Genéricos (GNSO)** de la ICANN creó el Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones en 2008. Identificó un conjunto de cuestiones específicas, pero no desarrolló resultados de políticas, ni llevó a cabo un debate posterior sobre las mejores prácticas no vinculantes para Registros y Registradores (lo que incluye talleres durante las reuniones ICANN41 e ICANN42).

- **Como parte del Programa de Nuevos gTLD**, una serie de nuevos requisitos [2] adoptados por la organización de la ICANN, según su memorándum sobre mitigación de conductas maliciosas (3 de octubre de 2009). Su efectividad finalmente se evaluó en el Informe de la ICANN sobre las Protecciones en el Programa de Nuevos gTLD (18 de julio de 2016), en preparación para la Revisión obligatoria establecida por los estatutos (Revisión de la CCT).

[1] Como quedó demostrado durante el debate sobre el uso indebido de DNS y la protección de los consumidores durante la Cumbre de la GDD (7 y 8 de mayo de 2019).

[2] Examinar a los operadores de registro, que requieren un plan demostrado para la implementación de las DNSSEC, prohibir el uso de comodines, eliminar registros de pegado huérfanos cuando se elimina una entrada del servidor de nombres de la zona, requerir el mantenimiento de registros de WHOIS amplio, centralizar el acceso a los archivos de zona, requerir contactos y procedimientos documentados sobre el uso indebido a nivel de registro.

- Antes de la creación del Grupo de trabajo sobre Seguridad Pública del GAC (PSWG), **los representantes de los organismos de cumplimiento de la ley (LEA)** asumieron un papel de liderazgo en la negociación del Acuerdo de Acreditación de Registradores de 2013 [3], así como en el desarrollo del asesoramiento del GAC en relación con las Amenazas a la Seguridad, que condujeron a nuevas disposiciones en el Acuerdo de Base de Nuevos gTLD, que describían las responsabilidades de los registros. Estas disposiciones se complementaron posteriormente con un Marco no vinculante para que los Operadores de Registro respondan a las amenazas a la seguridad (20 de octubre de 2017) negociado entre la **organización de la ICANN, los Registros y el PSWG.**

- **El Comité Asesor de Seguridad y Estabilidad (SSAC)** emite recomendaciones a la comunidad de la ICANN en particular en el documento SAC038: Punto de Contacto del Registrador para casos de Uso Indebido (26 de febrero de 2009) y el documento SAC040: Medidas para proteger los servicios de registración de dominios contra la explotación o el uso indebido (19 de agosto de 2009).

- **La Organización de la ICANN,** a través de su **Equipo de Seguridad, Estabilidad y Flexibilidad (SSR),** capacita de forma regular a las comunidades de seguridad pública y ayuda a responder a los incidentes cibernéticos a gran escala, incluso a través del Proceso de Solicitud Acelerada de Seguridad de Registro (ERSR). Más recientemente, la **Oficina del Director de Tecnologías (CTO)** de la ICANN ha dirigido el proyecto de Informe de Actividades de Uso Indebido de Dominios (DAAR) que produce informes sobre uso indebido en forma mensual. Esta herramienta ha sido apoyada activamente por el GAC y por varios Equipos de Revisión Específicos como una forma de crear transparencia e identificar las fuentes de problemas, que luego podrían abordarse a través del cumplimiento o, cuando sea necesario, mediante una nueva política.

Cuestiones

Las iniciativas anteriores todavía no han logrado una reducción efectiva del uso indebido del DNS; más bien, está claro que queda mucho por hacer. A pesar de la atención de la comunidad de la ICANN y las mejores prácticas existentes en la industria para mitigar el uso indebido del DNS, los compromisos de la comunidad liderados por el GAC, así como el Análisis estadístico del uso indebido del DNS en los gTLD que surge de la revisión de la CCT (9 de agosto de 2017), han puesto de relieve las tendencias persistentes en relación al uso indebido, prácticas comerciales conducentes al uso indebido y evidencia de que existe un "*ámbito para el desarrollo y la mejora de*

[3] Véanse las recomendaciones sobre verificación de antecedentes para el cumplimiento de la ley (octubre de 2019) y las 12 recomendaciones para el cumplimiento de la ley (1 de marzo de 2012)

las medidas y protecciones de mitigación actuales", así como el potencial para el desarrollo de políticas futuras [4].

Además, como consecuencia de la entrada en vigor del Reglamento General de Protección de Datos (GDPR) de la Unión Europea y los esfuerzos para poner en conformidad el sistema de WHOIS, una herramienta clave de investigación de delitos y usos indebidos, se han expresado inquietudes con respecto a la capacidad para mitigar efectivamente el uso indebido del DNS en los círculos de aplicación de la ley, ciberseguridad, protección del consumidor y protección intelectual.[5]

En este contexto, el departamento de Cumplimiento Contractual y el Departamento de Protección al Consumidor de la ICANN han informado que los comités asesores de la ICANN, en particular el GAC, el SSAC y el ALAC, y varios terceros afectados, han realizado un llamado a la Organización y la Comunidad de la ICANN para que tomen más medidas[6].

Dicha acción adicional requeriría que la comunidad de la ICANN llegue a algún tipo de consenso en torno a una serie de preguntas abiertas. Las discusiones sobre la mitigación del uso indebido y el posible trabajo de política en la comunidad de la ICANN giran en torno a:

- **La definición de uso indebido del DNS:**
  ¿Qué constituye uso indebido considerando el alcance de la ICANN y sus contratos con los Registros y Registradores?
- **La detección y el informe del uso indebido del DNS (perspectivas de conocimiento y transparencia):**
  ¿Cómo garantizar que el uso indebido del DNS sea detectado y conocido por las partes interesadas relevantes, incluidos los consumidores y los usuarios de Internet?
- **Prevención y mitigación del uso indebido del DNS (perspectiva de efectividad):**
  ¿Qué herramientas y procedimientos pueden utilizar la organización de la ICANN, los actores de la industria y las partes interesadas para reducir la incidencia del uso indebido y responder adecuadamente cuando esto ocurre? ¿Quién es responsable de qué partes del rompecabezas y cómo pueden cooperar mejor los diferentes actores?

El GAC, en sus esfuerzos por mejorar la seguridad y la estabilidad en beneficio de los usuarios de Internet en general, podría desear participar activamente en el avance de la discusión sobre estos

---

Véase el Comentario del GAC (19 de septiembre de 2017) sobre el Informe final del Análisis estadístico del uso indebido del DNS en los gTLD.

Véase las Secciones III.2 y IV.2 en el Comunicado del GAC pronunciado en Barcelona (25 de octubre de 2018) que señala las encuestas sobre el impacto en la aplicación de la ley en la sección 5.3.1 en el Informe Preliminar del Equipo de Revisión de RDS (31 de agosto de 2018) y en una publicación de los grupos de trabajo Anti- Phishing y Anti-Abuso vía Mensajes, Malware y Móviles (18 de octubre de 2018).

[6] Véase el debate sobre el uso indebido del DNS y las medidas de protección al consumidor llevado a cabo durante la Cumbre de la GDD (7 y 8 de mayo de 2019)

temas para que se pueda avanzar hacia una prevención y mitigación más eficaces del uso indebido.

Propuesta de liderazgo para la acción del GAC

Durante la reunión ICANN65 a celebrarse en Marrakech, el GAC tal vez desee:

1. **Convocar a un proceso para aclarar qué constituye el uso indebido del DNS** en relación con la misión de la ICANN y establecer su propia posición sobre el tema. Esto sería útil para avanzar en las discusiones en curso en la comunidad de la ICANN sobre la existencia de tal definición, las recomendaciones del Equipo de Revisión de CCT sobre el uso indebido del DNS, su consideración por parte de la Junta Directiva de la ICANN, así como las iniciativas en curso de la función de la Protección al Consumidor de la ICANN.

2. **Considerar la necesidad y la oportunidad para el desarrollo de políticas**, en relación con la discusión reciente de tal posibilidad durante la Cumbre de la GDD[7], y tomar nota de las posiciones anteriores adoptadas por el GAC sobre este asunto[8].

3. **Revisar las acciones tomadas en las Recomendaciones de la Revisión del CCT** relacionadas con el uso indebido del DNS (Recomendaciones 14 a 19), incluida su consideración por parte de la Junta Directiva de la ICANN y el trabajo que ordenó a la Organización de la ICANN, así como una consideración más amplia por parte de los grupos y procesos relevantes de la ICANN.

4. **Considerar mostrar las mejores prácticas de la industria en el espacio de nombres de ccTLD**, como el de .DK presentado durante la reunión ICANN64[9], y su aplicación a la industria de gTLD.

---

[7] Véase el debate sobre el uso indebido del DNS y las medidas de protección al consumidor llevado a cabo durante la Cumbre de la GDD (7 y 8 de mayo de 2019)

En particular, en su comentario (19 de septiembre de 2017) sobre el Informe final del Análisis estadístico del uso indebido del DNS en los gTLD, el GAC observó que:

- *"El estudio de uso indebido del DNS hace referencia brevemente a un hallazgo de que ciertas URL se utilizan más ampliamente para distribuir material de abuso infantil [...] Sería útil si el informe pudiera explicar, elaborar y / o cuantificar más claramente esta declaración para que las partes interesadas puedan comprender hasta qué punto el estudio examinó este tema, así como para informar cualquier posible consideración de políticas futuras ".*
- *"Las correlaciones establecidas entre políticas de registración más estrictas y menos recuentos de casos de uso indebido sugieren posibles áreas para el desarrollo futuro de políticas".*
- *"El uso del análisis estadístico debe informar las políticas futuras sobre uso indebido del DNS y se debe realizar un análisis adicional para considerar cómo esta información podría reforzar los esfuerzos de la ICANN y de sus equipos de cumplimiento contractual y seguridad para responder de manera efectiva al uso indebido del DNS y prevenir mejor la repetición de estos abusos en el futuro".*

[9] Véase Sección de Lecciones aprendidas: Cómo .DK redujo con éxito los dominios indebidos (13 de marzo de 2019) y la discusión posterior del PSWG (17 de abril de 2019)

Desarrollos relevantes

Definición de Uso Indebido del DNS: ¿Consenso sobre el Uso Indebido de la Infraestructura?

Como se destacó más recientemente durante la Cumbre de la GDD (del 7 al 9 de mayo de 2019), **no hay un acuerdo general a nivel de la comunidad sobre lo que constituye el 'uso indebido del DNS',** en parte debido a las inquietudes planteadas por algunas partes interesadas de que la ICANN se exceda su mandato, los impactos en los derechos de los Usuarios, y el efecto en las finanzas de las partes contratadas[10].

Sin embargo, según el Equipo de Revisión de la CCT, existe un consenso sobre lo que constituye '**Uso indebido de la Seguridad del DNS' o 'Uso indebido de la Seguridad del DNS de la infraestructura del DNS'** que incluye "*formas más técnicas de actividad maliciosa* ", como malware, phishing y botnets, así como el correo no deseado "*cuando se utiliza como un método de entrega para otras formas de uso indebido*"[11].

Recientemente, el **Departamento de Cumplimiento Contractual de la ICANN se ha referido al 'Uso indebido de la infraestructura del DNS'** en sus comunicaciones sobre auditorias de registros y registradores con respecto a la implementación de las disposiciones contractuales en el Acuerdo de Registro de Nuevos gTLD (Especificación 11 3b), que se refiere a " *amenazas a la seguridad tales como como pharming, phishing, malware y botnets* " - y en el Acuerdo de Acreditación de Registradores (Sección 3.18) - que se refiere a "*contactos de uso indebido*" e " *informes de uso indebido*" sin proporcionar una definición de los términos "*uso indebido*" específicamente, pero que incluye la "Actividad Ilegal" dentro de su alcance.

Desde la perspectiva del GAC , la definición de 'amenazas a la seguridad' en el Acuerdo de Registro de Nuevos gTLD es, de hecho, la transcripción exacta de la definición que figura en el **Asesoramiento referido a las Protecciones del GAC sobre las 'Verificaciones de seguridad'** que se aplica a todos los nuevos gTLD en el Comunicado pronunciado en Pekín (11 de abril de 2013).).

Tras la resolución de la Junta Directiva (1 de marzo de 2019), que ordena a la organización de la ICANN *" facilitar los esfuerzos de la comunidad para desarrollar una definición de 'uso indebido' a*

[10] De hecho, la definición de Mitigación del Uso Indebido puede tener consecuencias en términos del alcance de la actividad supervisada por las políticas y contratos de la ICANN. Si bien los gobiernos y otras partes interesadas están preocupados por el impacto del uso indebido del DNS en el interés público, incluida la seguridad pública y la violación de los derechos de propiedad intelectual, los Registros y Registradores muestran inquietud por las restricciones en sus actividades comerciales, la capacidad de competir, el aumento en los costos de las operaciones y la responsabilidad por las consecuencias en las que los registratarios pueden incurrir cuando se toman medidas con respecto a los dominios indebidos. Por su parte, las partes interesadas no comerciales plantean inquietudes relacionadas con la violación de la libertad de expresión y los derechos de privacidad de los registratarios y los usuarios de Internet, y comparten con las partes contratadas las inquietudes sobre una extra limitación por parte de la ICANN en su misión.

[11] Véase pág. 88 del Informe Final de la Revisión del CCT (8 de septiembre de 2018)

fin de informar nuevas medidas sobre esta recomendación"[12], y la creación de actividades de la función de Protección al consumidor de la organización de la ICANN, se esperan nuevas **conversaciones sobre la definición de uso indebido en la reunión de la ICANN66** a celebrarse en Montreal (de 2 al 7 de noviembre de 2019).

[12]Véase la pág.5 del tablero de control de la Acción de la Junta Directiva sobre las recomendaciones finales del CCT

Definición de uso indebido del DNS: Diálogo sobre la Protección al Consumidor

Desde la extensión de la función de Cumplimiento Contractual de la ICANN para incluir la Protección al Consumidor en 2017[13], el GAC participó en varios desarrollos relacionados:

- Una presentación del Director de Medidas de Protección al Consumidor de la ICANN (27 de junio de 2017) que debatió el establecimiento de un diálogo informal en toda la comunidad para crear conciencia y comprensión de la comunidad, e identificar formas para que la organización de la ICANN fortalezca su desempeño de las funciones de Cumplimiento Contractual y Protección al Consumidor.

- Un debate mediante seminario web sobre Cumplimiento Contractual y Protección al Consumidor (25 de septiembre de 2017), al que asistieron casi 100 miembros de la comunidad, incluida la discusión de un Resumen de Protecciones dentro del ámbito de la ICANN(11 de septiembre de 2017) y luego se enviaron preguntas para obtener comentarios de la Comunidad en un blog posterior (11 de octubre de 2017):
    - ¿Cuál debería ser el rol de la ICANN al abordar el uso indebido del DNS?
    - ¿Existen brechas entre el uso indebido del DNS y la autoridad de la ICANN para abordar ese uso indebido?
    - ¿Qué herramientas o datos adicionales serían útiles para evaluar el uso indebido del DNS?
    - ¿Hay áreas donde las medidas voluntarias podrían ser útiles?
    - ¿Cómo debería colaborar la ICANN con otras partes interesadas para abordar el uso indebido?
    - ¿Existe una amenaza de intervención gubernamental si la comunidad de la ICANN no pudiese abordar satisfactoriamente el uso indebido del DNS?

- Se organizó una reunión de representantes de la comunidad en Washington DC (11 de enero de 2019) para debatir más a fondo estos temas sobre la posible participación de toda la comunidad en las reuniones de la ICANN.

Más recientemente, durante la Cumbre de la GDD (9 de mayo de 2019), el departamento de Cumplimiento Contractual y Protección al Consumidor llevó adelante una sesión para continuar el diálogo ya iniciado:

- **Algunas partes contratadas consideran que sus prácticas voluntarias contra el uso indebido son adecuadas y se oponen a que se conviertan en obligaciones**, en parte debido a la limitación en el mandato de la ICANN, así como a la carga que representan los informes

[13]con la contratación del Director de Medidas de Protección al Consumidor de la ICANN (23 de mayo de 2017) encargado de "*incrementar el conocimiento sobre las protecciones actuales de la ICANN, facilitar el debate entre las partes interesadas sobre otras formas en las que la ICANN podría mejorar sus mecanismos de protección*"

de uso indebido no procesables (a menudo presentados por partes no informadas sobre el alcance limitado de las mitigaciones disponibles para los Registros[14] y Registradores).

- Otros representantes sugirieron que **la ICANN tiene el deber de establecer reglas e incentivos adecuados** para desalentar a los malos actores sin dañar a los actores responsables (**principio del "contaminador-pagador**") y que las **partes responsables del uso indebido deben mencionarse** en los informes relevantes de la ICANN.
- **La organización de la ICANN presentó la idea de un proceso de desarrollo de políticas de la GNSO** para alinear los contratos con las expectativas de los comités asesores y terceros, así como para prevenir el impacto de futuras legislaciones heterogéneas que podrían implementarse en lugar de la política de la ICANN.
- Esta sugerencia se encontró con **una fuerte oposición y exige formas alternativas para abordar el problema,** incluida la conciliación de las definiciones existentes en partes relevantes de la comunidad o la celebración de negociaciones del Acuerdo de Registro de manera similar a lo que se hizo para el RAA de 2013.
- Las **partes contratadas** solicitaron que la **organización de la ICANN facilite los esfuerzos para educar a la comunidad de la ICANN** en su nombre durante la reunión ICANN66 en Montreal, lo que incluye una presentación de las mejores prácticas y datos que muestren la prevalencia de reclamos no procesables.

Conocimiento y transparencia: Participación de la comunidad liderada por el GAC

El GAC y su Grupo de trabajo sobre Seguridad Pública (PSWG) han liderado varias sesiones de participación intercomunitarias en las reuniones de la ICANN durante los últimos años, con el **objetivo de crear conciencia y explorar soluciones con expertos relevantes**, en particular:

- Durante la reunión ICANN57 realizada en Hyderabad (5 de noviembre de 2016), el PSWG del GAC dirigió una sesión de temas de alto interés sobre la mitigación del uso indebido en los gTLD, que se diseñó como un intercambio de puntos de vista en la comunidad de la ICANN y destacó:
  - la falta de una comprensión compartida de lo que constituye el uso indebido del DNS;
  - la diversidad de modelos de negocios, prácticas y habilidades que influyen en los enfoques para mitigar el uso indebido; y
  - la necesidad de una mayor cooperación en la industria, que sea avalada por datos compartidos sobre amenazas a la seguridad.
- Durante la reunión ICANN58 en Copenhague (13 de marzo de 2017), el PSWG del GAC moderó una sesión intercomunitaria sobre la Mitigación efectiva del Uso Indebido del DNS:

[14] Véase, por ejemplo, las *categorías de acciones por registros en respuesta a amenazas a la seguridad* en el marco voluntario para que los operadores de registro respondan a amenazas a la seguridad

Prevención, Mitigación y Respuesta donde se discutieron las tendencias recientes en el uso indebido del DNS, en particular el phishing, así como el comportamiento, como el salto de dominios entre registradores y TLD, que pueden requerir respuestas más coordinadas y sofisticadas en la industria. La sesión también sirvió para destacar:
    - la iniciativa emergente del Informe de Actividades de Uso Indebido de Dominios (DAAR),
    - La colaboración continua entre las funciones de Cumplimiento Contractual de la ICANN y SSR, y
    - la oportunidad de aprovechar los ingresos de las subastas de nuevos gTLD para financiar las necesidades de mitigación del uso indebido

- Durante la reunión ICANN60 llevada a cabo en Abu Dabi (30 de octubre de 2017), el PSWG organizó una sesión intercomunitaria sobre el informe de uso indebido del DNS para la formulación de políticas basadas en hechos y la mitigación efectiva a fin de discutir el establecimiento de mecanismos de informe de uso indebido del DNS confiables, públicos y procesables para la prevención y mitigación del uso indebido, y para permitir la formulación de políticas fundadas en evidencia. La sesión confirmó la necesidad de publicar datos detallados y confiables sobre el uso indebido del DNS, según lo contenido en la herramienta de Informe de Actividades de Uso Indebido de Dominios (DAAR). El PSWG consideró continuar desarrollando los posibles principios del GAC [15].

Conocimiento y transparencia: Estudios de uso indebido del DNS

Se incorporaron una serie de medidas de seguridad en relación al uso indebido del DNS en el Programa de Nuevos gTLD mediante nuevos requisitos [16] adoptados por la organización de la ICANN, según su memorándum sobre la mitigación de conductas maliciosas (3 de octubre de 2009) y el Asesoramiento en materia de medidas de protección del GAC sobre verificaciones de seguridad.

Sobre la base de la evaluación de la organización de la ICANN en torno a la efectividad de estas Protecciones en el Programa de Nuevos gTLD (18 de julio de 2016), a las que el GAC había contribuido (20 de mayo de 2016), el Equipo de Revisión de la CCT buscó un análisis comparativo más completo de las tasas de uso indebido en gTLD nuevos y heredados, incluido el análisis estadístico inferencial de hipótesis, como las correlaciones entre los precios minoristas de nombres de dominio y las tasas de uso indebido.

[15] Véase el Anexo 1: Principios de mitigación del uso indebido en el resumen informativo del GAC durante la Reunión ICANN60 sobre el uso indebido del DNS e informe de la sesión del Comunicado del GAC pronunciado en Abu Dabi (p.3)

[16] Examinar a los operadores de registro, que requieren un plan demostrado para la implementación de las DNSSEC, prohibir el uso de comodines, eliminar registros de pegado huérfanos cuando se elimina una entrada del servidor de nombres de la zona, requerir el mantenimiento de registros de WHOIS amplio, centralizar el acceso a los archivos de zona, requerir contactos y procedimientos documentados sobre el uso indebido a nivel de registro.

Los hallazgos de este Análisis estadístico del uso indebido del DNS en gTLD (9 de agosto de 2017) se enviaron para comentario público. Las contribuciones de la comunidad se informaron (13 de octubre de 2017) como constructivas y acogieron con satisfacción el rigor científico del análisis y se solicitó que se realicen más estudios de este tipo.

En sus comentarios (19 de septiembre de 2017), el GAC destacó, entre otras conclusiones, que:

- El estudio dejó en claro que hay problemas significativos con respecto al uso indebido en el DNS:
    - En ciertos nuevos gTLD, más del 50% de las registraciones son indebidas
    - Cinco nuevos gTLD representaron el 58.7% del total de dominios en lista negra objeto de phishing en los nuevos gTLD
- El uso indebido se correlaciona con las políticas de los operadores de registro:
    - Los operadores de registro de los nuevos gTLD con más casos de uso indebido compiten sobre la base del precio;
    - Los malos actores prefieren registrar dominios en los nuevos gTLD estándar (abiertos para la registración pública), en lugar de en los nuevos gTLD de la comunidad (restricciones sobre quiénes pueden registrar nombres de dominio)
- Hay potencial para el desarrollo de políticas futuras con respecto a:
    - Rondas posteriores de nuevos gTLD, en relación con la evidencia de que el riesgo varía con las categorías de TLD, además del rigor de la política de registración.
    - La mejora de las medidas de mitigación actuales y las protecciones contra el uso indebido, según lo informado por dicho análisis estadístico.
- La ICANN debe continuar y ampliar el uso del análisis estadístico y los datos para medir y compartir información con la comunidad sobre los niveles de uso indebido del DNS.

Conocimiento y transparencia: Informe de Actividades de Uso Indebido de Dominios (DAAR)

El Proyecto de Informe de Actividades de Uso Indebido de Dominios de la organización de la ICANN surgió como un proyecto de investigación, al mismo tiempo que la Junta Directiva y la Comunidad de la ICANN se comprometieron con el GAC y el PSWG en relación a la eficacia de la mitigación del uso indebido del DNS, entre la Reunión ICANN57 (noviembre de 2016) y la Reunión ICANN 60 (noviembre de 2017) .

El objetivo general de DAAR es *"informar sobre actividades que amenazan la seguridad a la comunidad de la ICANN, la cual puede utilizar los datos para tomar decisiones informadas, incluidas las relacionadas con políticas".* Esto se logra desde enero de 2018 mediante la publicación de informes mensuales, fundados en la compilación de datos de registración de TLD con información proveniente de un gran conjunto de aportes de datos altamente confiables y de amenazas a la seguridad.

Como tal, el DAAR está contribuyendo al requisito identificado por el GAC para la publicación de *"datos confiables y detallados sobre el uso indebido del DNS"* en el Comunicado del GAC pronunciado en Abu Dabi (1 de noviembre de 2017). Sin embargo, como se destacó en una

reciente del Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil (M3AAWG)[17] a la organización de la ICANN (5 de abril de 2019), al no incluir la información sobre amenazas a la seguridad por registrador por TLD, el DAAR aún no está a la altura de las expectativas de los miembros del PSWG del GAC y sus socios de ciberseguridad con respecto a brindar información viable.

Efectividad: Medidas de protección actuales en relación con el uso indebido del DNS en los contratos de Registros y Registradores

Sobre la base de las recomendaciones de verificación de antecedentes para el cumplimiento de la ley (octubre de 2009), el GAC solicitó **la inclusión de las Protecciones para la mitigación del uso indebido del DNS en los contratos de la ICANN** con los registros y registradores:

- El Acuerdo de Acreditación de Registradores de 2013 (17 de septiembre de 2013) fue aprobado por la Junta Directiva de la ICANN (27 de junio de 2013) luego de incluir las disposiciones que abordan las 12 recomendaciones en materia de cumplimiento de la ley (1 de marzo de 2012)
- El Acuerdo de Registro de los Nuevos gTLD fue aprobado por la Junta Directiva de la ICANN (2 de julio de 2013) después de incluir disposiciones en línea con el Asesoramiento del GAC en materia de medidas de protección en el Comunicado pronunciado en Pekín (11 de abril de 2013), en consonancia con la Propuesta de la Junta Directiva de la ICANN para la Implementación de las Protecciones del GAC Aplicables a Todos los Nuevos gTLD (19 de junio de 2013)

Después de los primeros años de operaciones de los nuevos gTLD, durante la reunión ICANN57 (noviembre de 2016), **el GAC identificó una serie de disposiciones y protecciones relacionadas para las cuales no pudo evaluar la efectividad.** Como consecuencia, en su Comunicado pronunciado en Hyderabad (8 de noviembre de 2016), el GAC solicitó aclaraciones sobre su implementación a la Junta Directiva de la ICANN. Esto llevó a un diálogo entre el GAC y la organización de la ICANN, preguntas de seguimiento que se plasmaron en el Comunicado pronunciado por el GAC en Copenhague(15 de marzo de 2017) y un conjunto de respuestas preliminares (30 de mayo de 2017) que se discutieron en una conferencia telefónica entre el GAC y el Director Ejecutivo (CEO) de la ICANN (15 de junio de 2017). Se mantuvieron abiertas varias preguntas y se identificaron otras nuevas que se reflejaron en un documento de trabajo posterior (17 de julio de 2017).

Entre los temas destacados de interés para el GAC, el 8 de junio de 2017 se publicó un Documento de Asesoramiento sobre la Especificación 11 (3) (b) contenida en el Acuerdo de Registro de Nuevos gTLD en respuesta a las preguntas de algunos operadores de registro que buscan orientación sobre cómo garantizar el cumplimiento de la Sección 3b de la especificación 11 del Acuerdo de Registro de Nuevos gTLD **En este documento de asesoramiento se propone un enfoque que los**

[17]Grupo de Trabajo Anti-Abuso vía Mensajes, Malware y Móviles

operadores de registro pueden adoptar en forma voluntaria a fin de llevar a cabo dichos análisis técnicos para evaluar las amenazas a la seguridad y generar informes estadísticos de conformidad con la Especificación 11 (3)(b).

Como parte de las **auditorias efectuadas con regularidad por el Departamento Contractual de la ICANN** , una auditoria específica de 20 gTLD sobre sus " *procesos, procedimientos y manejo de la infraestructura del DNS"*, entre marzo y septiembre de 2018, reveló que *" hubieron análisis e informes de seguridad incompletos para 13 dominios de alto nivel (TLD), así como falta de procedimientos estandarizados o documentados sobre el manejo de casos de uso indebido y la falta de medidas para abordar las amenazas identificadas "*[18] .
Poco después, en noviembre de 2018, se lanzó una Auditoria para detectar el uso indebido de la infraestructura del DNS de casi todos los gTLD con el objeto de *"garantizar que las partes contratadas cumplan con sus obligaciones contractuales con respecto al uso indebido de la infraestructura del DNS y las amenazas a la seguridad*" Como se informó durante la Cumbre de la GDD (9 de mayo de 2019), la organización de la ICANN debe publicar el informe final de esta auditoria (originalmente previsto para mayo de 2019) y actualmente planea iniciar una auditoria similar de registradores a partir de julio de 2019.

Las partes contactadas han considerado que estas auditorias exceden el alcance de sus obligaciones contractuales[19] . **Se entiende que los Grupos de partes interesadas de Registros y Registradores están trabajando con el departamento de Cumplimiento Contractual de la organización de la ICANN** para garantizar que el informe final de la Auditoria de la Infraestructura del DNS de los Registros no carezca de claridad en cuanto al alcance de la ICANN (debido a las inquietudes que pueden dar lugar a convocatorias a la comunidad para dar inicio a un Proceso de Desarrollo de Políticas), y que las preocupaciones de los Registradores se tomen en cuenta antes del inicio de su auditoria.

Efectividad: Marco no vinculante para que los registros respondan a las amenazas a la seguridad

Como parte del Programa de Nuevos gTLD, la Junta Directiva de la ICANN resolvió (25 de junio de 2013) incluir las llamadas "verificaciones de seguridad" (Asesoramiento del GAC en materia de

[18]Como se informó en la publicación del blog del 8 de noviembre de 2018, Cumplimiento Contractual: Abordar el uso indebido en la infraestructura del DNS: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

[19] Véase la correspondencia de RySG (2 de noviembre de 2019) a la que la organización de la ICANN respondió (8 de noviembre), y en los comentarios publicados en la página de anuncios (15 de noviembre): los registros han considerado las preguntas de la auditoria como una acción de cumplimiento de la ley inminente que excede el ámbito de su obligaciones contractuales [en particular según lo dispuesto en la Especificación 11 3b] e indicaron su renuencia a *"compartir con la organización de la ICANN y con la comunidad información relevante con respecto a nuestros esfuerzos en curso para combatir el uso indebido del DNS [...] como parte de un esfuerzo de Cumplimiento de la ICANN que va más allá de lo permitido por el Acuerdo de Registro "*

medidas de protección contenido en el Comunicado pronunciado en Pekín) en la Especificación 11 del Acuerdo de Registro de Nuevos gTLD. Sin embargo, debido a que determinó que estas disposiciones carecían de detalles de implementación, decidió solicitar la participación de la comunidad para desarrollar un marco para que "*los Operadores de Registro respondan a los riesgos de seguridad identificados que representan un riesgo real de daño (...)".*
En julio de 2015, la ICANN formó un Equipo de Redacción compuesto por voluntarios de los Registros, Registradores y el GAC (incluidos los miembros del PSWG) que desarrollaron el Marco para que los Operadores de Registro Respondan a las Amenazas a la Seguridad publicado el 20 de octubre de 2017, luego de someterse a comentarios públicos.

Este marco es un instrumento voluntario y no vinculante diseñado para articular pautas sobre las formas en que los registros pueden responder a las amenazas a la seguridad identificadas, incluidos los informes de Cumplimiento de la Ley. Introduce una ventana de 24 horas, como máximo, para responder a solicitudes de alta prioridad (amenaza inminente para la vida humana, infraestructura crítica o explotación infantil) que provengan de un origen legítimo y creíble, como una autoridad gubernamental encargada de hacer cumplir la ley o una agencia de seguridad pública de jurisdicción apropiada.

Según su recomendación 19, el Equipo de Revisión de la CCT aplazó la tarea de realizar una evaluación de la efectividad del Marco para una revisión posterior [20].

Efectividad: Medidas proactivas y prevención del uso indebido sistémico

Sobre la base de su análisis del panorama sobre el uso indebido del DNS, incluida la consideración del Informe de la ICANN sobre las Protecciones del Programa de Nuevos gTLD (15 de marzo de 2016) y el Análisis Estadístico Independiente del uso indebido del DNS (9 de agosto de 2017), el Equipo de Revisión de la CCT recomendó, en relación con el uso indebido del DNS :

- La inclusión de **disposiciones en los Acuerdos de Registro para incentivar la adopción de medidas proactivas contra el uso indebido** (Recomendación 14)
- La inclusión de disposiciones contractuales dirigidas a **prevenir el uso sistémico de registradores o registros específicos** para el uso indebido de la seguridad del DNS, incluidos los umbrales de uso indebido en los que se activan automáticamente las consultas de cumplimiento y se considera una posible Política de resolución de disputas en materia de uso indebido del DNS (DADRP) si la comunidad determina que la organización de la ICANN, en sí, es inadecuada o no puede hacer cumplir tales disposiciones (Recomendación 15)

[20] Recomendación 19 de la revisión de CCT: *El próximo CCT debe revisar el "Marco para que los Operadores de Registro respondan ante amenazas a la seguridad" y deberá evaluar si el marco es un mecanismo suficientemente claro y eficaz para mitigar los usos indebido al proporcionar acciones específicas y sistémicas en respuesta a amenazas a la seguridad.*

La Junta Directiva de la ICANN resolvió (1 de marzo de 2019) colocar estas recomendaciones en estado "Pendiente", ya que ordenó a la organización de la ICANN " *facilitar a los esfuerzos de la comunidad a fin de desarrollar una definición de 'uso indebido' para informar otras acciones sobre esta recomendación*".[21]

Posiciones actuales

- Comunicado del GAC pronunciado en Nairobi (10):(10 de marzo de 2010), sección VI. Recomendaciones sobre averiguación de antecedentes para el cumplimiento de la ley.
- Comunicado del GAC pronunciado en Dakar (27 de octubre de 2011), sección III. Recomendaciones en materia de cumplimiento de la ley (LEA)
- Comunicado del GAC pronunciado en Pekín(11 de abril de 2013), en particular, las Protecciones de "verificaciones de seguridad" que se aplican a todos los Nuevos gTLD (pág.7)
- Comunicado del GAC pronunciado en Hyderabad (8 de noviembre de 2016) que incluye el Asesoramiento sobre la Mitigación del Uso Indebido que solicita respuestas al Anexo 1: Preguntas a la Junta Directiva de la ICANN sobre la Mitigación del Uso Indebido del DNS por parte de la ICANN y las Partes Contratadas (págs.14-17)
- Comunicado pronunciado por el GAC en Copenhague (15 de marzo de 2017) que incluye el Asesoramiento sobre Mitigación del Uso Indebido que solicita respuestas al tablero de control de Seguimiento del GAC al Anexo 1 del Comunicado del GAC pronunciando en Hyderabad (págs. 11-32)
- Comunicado del GAC pronunciado en Barcelona (25 de octubre de 2018), en particular, las secciones III.2 Grupo de trabajo sobre seguridad pública del GAC (pág.3) y IV.2 WHOIS y Legislación sobre Protección de Datos (pág. 5)
- Comentario del GAC sobre el informe inicial del SADAG (21 de mayo de 2018)
- Comentario del GAC sobre el análisis estadístico del uso indebido del DNS en los gTLD (19 de septiembre de 2017)
- Comentario del GAC sobre el Informe final del Equipo de Revisión de CCT y las Recomendaciones (11 de diciembre de 2018)

Documentos de referencia clave

- Recomendaciones sobre averiguación de antecedentes para el cumplimiento de la ley (oct. 2019)
- Recomendaciones de cumplimiento de la ley sobre las enmiendas al Acuerdo de Registrador (1 de marzo de 2012)

[21]Véase la pág. 5 del tablero de control de la Acción de la Junta Directiva sobre las recomendaciones finales del CCT

- 'Verificaciones de seguridad' del Asesoramiento del GAC en materia de Protecciones aplicable a Todos los Nuevos gTLD (pág. 7) en el Comunicado pronunciado en Pekín (11 de abril de 2013)
- Preguntas del GAC en relación a la mitigación del uso indebido y las respuestas preliminares de la ICANN (30 de mayo de 2017) según el asesoramiento contenido en el Comunicado del GAC pronunciado en Hyderabad (8 de noviembre de 2016) y seguimiento realizado en el Comunicado del GAC pronunciado en Copenhague (15 de marzo de 2017)
- Análisis estadístico del uso indebido del DNS en los gTLD (9 de agosto de 2017)
- Comentario del GAC sobre el análisis estadístico del uso indebido del DNS en los gTLD (19 de septiembre de 2017)
- Comentario del GAC (16 de enero de 2018) sobre las Nuevas Secciones del Informe Preliminar del Equipo de Revisión de CCT (27 de noviembre de 2017)
- Informe final y recomendaciones de la revisión del CCT (8 de septiembre de 2018), en particular la Sección 9 sobre Protecciones (pág.88)
- Comentario del GAC sobre el Informe final del Equipo de Revisión de CCT y las Recomendaciones (11 de diciembre de 2018)
- Tablero de control de la Junta Directiva de la ICANN sobre las recomendaciones finales del CCT (1 de marzo de 2019)

Información relacionada

- Sesión 11.1 del GAC durante ICANN65 sobre las Revisiones de la ICANN (que incluye información relevante sobre el estado de la Implementación de las Recomendaciones de la Revisión del CCT)
- Sesión 8.1 del GAC durante ICANN65 sobre WHOIS y la Política de Protección de Datos
- Sesión 4.1 del GAC durante ICANN65 sobre el PDP para Procedimientos Posteriores a la Introducción de los Nuevos gTLD

Administración de la documentación

Reunión	ICANN65 Marrakech, del 24 al 27 de junio de 2019
Título	Mitigación del uso indebido del DNS
Distribución	Miembros del GAC y público (después de la reunión)
Fecha de distribución	Versión 1: 6 de junio de 2019