ICANN | GAC
Governmental Advisory Committee

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

# Mitigación del Uso Indebido del DNS

## Sesiones 2, 8

## Contenidos

## Objetivos de la Sesión

El GAC debatirá sobre los desarrollos recientes relacionados con el uso indebido del DNS, en particular en el contexto de la crisis generada por el COVID-19, en relación con una Sesión Plenaria Intercomunitaria planificada sobre este tema durante la Reunión ICANN68. Esta sesión también constituirá una oportunidad para revisar y deliberar sobre los desarrollos relevantes en la prevención y mitigación del uso indebido del DNS y las amenazas a la seguridad.

## 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.). 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, 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 incluía 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

[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

Maliciosas (3 de octubre de 2009). En el Informe de la ICANN sobre las Protecciones del Programa de Nuevos gTLD (18 de julio de 2016), se evaluó su efectividad en la preparación para la Revisión de Competencia, Confianza y Elección de los Consumidores (CCT) estipulada en los estatutos, cuyas recomendaciones se entregaron el 8 de septiembre de 2018.

- 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 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 del GAC.**

- **El Comité Asesor de Seguridad y Estabilidad (SSAC)** emitió recomendaciones para 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) en el que se elaboran 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

de WHOIS amplio, centralizar el acceso a los archivos de zona, requerir contactos y procedimientos documentados sobre el uso indebido a nivel de registro.

[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)

indebido del DNS en los gTLD que surge de la Revisión de CCT (9 de agosto de 2017), han puesto de relieve las tendencias persistentes en relación con el uso indebido, prácticas comerciales conducentes al uso indebido y evidencia de que existe un "*ámbito para el desarrollo y la mejora de las medidas y protecciones de mitigación actuales", así como el potencial para el desarrollo de políticas futuras* [4].

Además, la inquietud referida a la capacidad de mitigar eficazmente el uso indebido del DNS se ha incrementado en los círculos de los organismos de cumplimiento de la ley, seguridad cibernética, protección del consumidor y protección intelectual[5] como consecuencia de la entrada en vigor del Reglamento General de Protección de Datos (GDPR) de la Unión Europea y los esfuerzos posteriores para modificar el sistema WHOIS, una herramienta clave de investigación de delitos y usos indebidos a fin de cumplir con el GDPR. Más recientemente, la emergencia sanitaria internacional causada por el COVID-19 reflejó los desafíos que existen dado que hubo un incremento de las registraciones de nombres relacionados, lo que incluye un pequeño porcentaje que avala propósitos fraudulentos oportunistas.

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.

Véanse 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 Móvil (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 (que se documentan en detalle en este resumen informativo) para que se pueda avanzar hacia una prevención y mitigación más eficaces del uso indebido.

## Propuesta del Liderazgo para la Acción del GAC durante la Reunión ICANN68

1. **Revisar las lecciones aprendidas** hasta el momento **sobre el uso indebido del DNS en relación con el COVID-19**, según lo informado por las partes interesadas, incluidas las autoridades públicas, los registradores, los operadores de ccTLD y la organización de la ICANN, y **prepararse para interactuar con la comunidad de la ICANN según corresponda**, comenzando con la Sesión Plenaria Intercomunitaria sobre Uso Indebido del DNS y Registraciones Maliciosas durante la Crisis del COVID-19 agendada para el 22 de junio de 2020 como parte de la Reunión ICANN68.

2. **Deliberar sobre los posibles próximos pasos para abordar cuestiones generales de política pública relacionadas con el uso indebido del DNS** como se identificó en las contribuciones anteriores del GAC, y **en particular considerar el seguimiento** con el Consejo de la GNSO, el ALAC, la ccNSO y posiblemente la Junta Directiva de la ICANN sobre **posibles vías para abordar las recomendaciones de la Revisión de CCT sobre el uso indebido del DNS antes del lanzamiento de rondas futuras de nuevos gTLD** de conformidad con el Asesoramiento contenido en el Comunicado del GAC pronunciado en Montreal (6 de noviembre de 2019).

3. Debatir el estado de la consideración e implementación de las **recomendaciones relacionadas con el Uso Indebido del DNS emitidas a partir de las Revisiones de CCT y RDS-WHOIS2**, a la luz de la Acción de la Junta Directiva de la ICANN como se informa en:
    a. Tabla de Clasificación de las Acciones de la Junta Directiva en relación con las recomendaciones surgidas de la revisión de CCT (1 de marzo de 2019)
    b. Tabla de Clasificación de las Acciones de la Junta Directiva en relación con las recomendaciones surgidas de la revisión de RDS-WHOIS2 (25 de febrero de 2020)

4. **Considerar el avance de los esfuerzos clave en la mitigación del uso indebido del DNS de manera más general, en la comunidad de la ICANN** y, en particular, por parte de las partes contratadas, los operadores de ccTLD y la organización de la ICANN, incluso con el fin de promover altos estándares en las prácticas y los contratos:
    a. Implementación de medidas voluntarias por parte de registradores y registros de gTLD según el Marco Dirigido por la Industria para Abordar el Uso Indebido
    b. **Implementación de medidas proactivas contra el uso indebido por parte de los operadores de ccTLD** que podrían informar las prácticas de los registros de gTLD
    c. **Auditoria de los Registradores realizada por el Departamento de Cumplimiento Contractual** con respecto a las amenazas a la seguridad del DNS, la cual se esperaba siguiera la conclusión de una auditoria similar de Registros.
    **d. Mejoras en el Informe de Actividades de Uso Indebido de Dominios (DAAR) de la ICANN,** tal como lo debatieron previamente los Registros, el GAC y el SSAC

## Desarrollos Relevantes

**Generalidades de los acontecimientos recientes**

- **La crisis ocasionada por el COVID-19 ha dado lugar a una participación entre el GAC y las partes interesadas afectadas,** que ha puesto de manifiesto varios **esfuerzos para responder y coordinar la respuesta** contra actividades fraudulentas y delictivas:
    - El Liderazgo del GAC informó acerca de una deliberación(9 de abril) que fue pedida por los líderes del Grupo de Partes Interesadas de Registradores (RrSG), y discutió el asunto posteriormente durante una llamada conjunta con los líderes (3 de junio de 2020) en preparación para la Reunión ICANN68.
    - Como parte de su respuesta a las posibles actividades fraudulentas relacionadas con el COVID-19, los **Registradores** informan sobre los desafíos que enfrentan al evaluar la fraudulencia en la jurisdicción relevante y solicitaron asistencia de las autoridades públicas. El RrSG ha documentado enfoques compartidos de los Registradores con respecto a la crisis del COVID-19 en beneficio de sus miembros
    - **Los miembros del GAC han sido invitados a compartir los recursos** correspondientes que establecieron sus respectivas autoridades públicas, como los que comparten los organismos encargados del cumplimiento de la ley (FBI en los Estados Unidos, NCA del Reino Unido, Europol) y las agencias de protección al consumidor (FTC de Estados Unidos)
    - La Comisión Europea informó sobre los esfuerzos en curso en colaboración con los Estados Miembros de la UE, Europol, los ccTLD y los registradores para facilitar los informes, su revisión y su derivación a la jurisdicción correspondiente mediante la adopción de un formulario estandarizado para informar el dominio/contenido relacionado con el COVID-19 y el establecimiento de un único punto de contacto para las autoridades pertinentes de los Estados Miembros.
    - Los operadores de ccTLD de todo el mundodeben informar al GAC(4 y 5 de junio de 2020) sobre las lecciones que aprendieron de sus operaciones durante la crisis.
    - Se espera que en un resumen del GAC por parte de la **Oficina del Director de Tecnologías (OCTO) de la ICANN** que se está planificando antes de la Reunión ICANN68, se ilustren las iniciativas y los recursos de la ICANN dedicados a apoyar la respuesta de las partes contratadas

- **Mientras tanto, las Partes Contratadas, el Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN y la organización de la ICANN han iniciado un nuevo trabajo** relacionado con las Amenazas a la Seguridad:
    - Según lo informado por el Grupo de Trabajo sobre Seguridad Pública del GAC durante la Reunión ICANN67, el Grupo de Partes Interesadas de Registradores publicó una Guía para los Informes sobre Uso Indebido de Registradores

- El Marco para Abordar el Uso Indebido del DNS (17 de octubre de 2019) propuesto como una iniciativa voluntaria por parte de los principales interesados de la industria del DNS, ahora registra 56 signatarios al 29 de marzo de 2020.
- El **SSAC** inició un Grupo de Trabajo sobre Uso Indebido del DNS en el que se invitó a participar a un representante del PSWG.
- La **organización de la ICANN,** como parte de la implementación del Plan Estratégico para los Años Fiscales 2021 a 2025 (FY21-25), anunció el lanzamiento de un Grupo de Estudio Técnico sobre Iniciativas para Facilitar la Seguridad del DNS(6 de mayo de 2020) para "*explorar ideas sobre lo que la ICANN puede y debe hacer a fin de incrementar el nivel de colaboración y compromiso con las partes interesadas del ecosistema del DNS para mejorar el perfil de seguridad del* mismo".

  Se esperan recomendaciones para mayo de 2021.

- Desde la reunión ICANN66, en **varios procesos de la comunidad de la ICANN se han considerado nuevas recomendaciones relacionadas con el uso indebido del DNS**, algunas de las cuales han recibido aportes del GAC y otras pueden estar sujetas al seguimiento de dicho comité:
  - Luego, las Recomendaciones Finales del **Equipo de Revisión RDS-WHOIS2** (3 de septiembre de 2019), cuya relevancia para la mitigación del uso indebido del DNS se resaltó en un comentario del GAC (23 de diciembre de 2019), fueron analizadas por la Junta Directiva según Tabla de Clasificación de las Acciones de la Junta Directiva (25 de febrero de 2020 ) y como parte de sus resoluciones 2020.02.25.01 - 2020.02.25.06: Se aceptaron 15 recomendaciones, 4 se colocaron en estado pendiente, 2 pasaron a la GNSO y 2 fueron rechazadas.
  - El **Equipo de Revisión de SSR2** entregó un Informe Preliminar (24 de enero de 2020) con un enfoque significativo en medidas para prevenir y mitigar el uso indebido del DNS. El comentario del GAC (3 de abril de 2020) respaldó muchas de las recomendaciones y, en particular, aquellas relacionadas con la mejora del Informe de Actividades de Uso Indebido de Dominios y el fortalecimiento de los mecanismos de cumplimiento. Las recomendaciones finales del SSR2 RT ahora se esperan para octubre de 2020 (según deliberaciones recientes)
  - **El Grupo de Trabajo para el Proceso de Desarrollo de Políticas sobre Procedimientos Posteriores a la Introducción de los Nuevos gTLD de la GNSO** informó recientemente (29 de abril de 2020) que *"no planea efectuar ninguna recomendación con respecto a la mitigación del uso indebido de nombres de dominio además de afirmar que cualquier esfuerzo futuro debe aplicarse tanto a los gTLD existentes como a los nuevos (y potencialmente a los ccTLD*)." Esto es a pesar de las recomendaciones relevantes que le dirigió el Equipo de Revisión de CCT, con el apoyo adicional de la Acción de la Junta Directiva de la ICANN a estas recomendaciones, así como el Asesoramiento contenido en el Comunicado del GAC

pronunciado en Montréal (6 de noviembre de 2019) y otros aportes del GAC, según lo registrado en el Comunicado del GAC pronunciado durante la Reunión ICANN67 (16 de marzo 2020). En una reunión del Consejo de la GNSO reciente (21 de marzo de 2020) se discutió la posibilidad de iniciar un Grupo de Trabajo Intercomunitario (CCWG) y posiblemente un PDP de la GNSO posterior si fueran necesarios nuevos requisitos contractuales. No se discutió una propuesta informal del Liderazgo del GAC (12 de mayo de 2020) de considerar llevar a cabo un debate especializado entre expertos relevantes, incluidos los operadores de ccTLD, a fin de dar marco a todo esfuerzo de políticas futuro.

**Cuestiones - Definición de Uso Indebido del DNS:**

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 exceda su mandato, los impactos en los derechos de los Usuarios, y el efecto en las finanzas de las partes contratadas[7].

Sin embargo, según el Equipo de Revisión de 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*"[8].

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*" [9] - 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 fin de informar nuevas medidas sobre esta recomendación"*[10], 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 durante la reunión ICANN66** a celebrarse en Montreal.

---

[7] 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.

[8] Véase la página 88 del Informe Final de la Revisión de CCT (8 de septiembre de 2018) como se destacó más recientemente en la Declaración del GAC sobre el Uso indebido del DNS (18 de septiembre de 2019)

[9] El Documento de Asesoramiento sobre la Especificación 11 (3) (b) contenida en el Acuerdo de Registro de Nuevos gTLD (8 de junio de 2017) proporciona una definición de *"Amenazas a la seguridad" que incluye "pharming, phishing, malware, botnets y otros tipos de amenazas a la seguridad"*.

[10] Véase la pág.5 de la Tabla de clasificación de la Acción de la Junta Directiva sobre las Recomendaciones Finales de CCT

En particular, durante un seminario web previo a Reunión ICANN66 el 15 de octubre de 2019, **el PSWG y las Partes Contratadas discutieron temas actuales y prácticas de la industria.** En preparación para este seminario web, el Grupo de Partes Interesadas de Registros había emitido una carta abierta (19 de agosto de 2019) en la que analizaba los puntos de vista de los registros sobre la definición de uso indebido del DNS, las limitadas opciones que tienen los registros para actuar en relación con las amenazas a la seguridad y sus inquietudes en relación al Informe de Actividades de Uso Indebido de Dominios de la ICANN. En respuesta, el GAC emitió una Declaración sobre el Uso indebido del DNS (18 de septiembre), y también la Unidad Constitutiva de Negocios (28 de octubre).

**Cuestiones - Conocimiento y Transparencia: Participación de la comunidad sobre el Uso indebido del DNS**

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**. Más recientemente, los líderes de los Comités Asesores y de las Organizaciones de Apoyo de la ICANN (SO/AC) y el ALAC mantuvieron intercambios con mucha participación sobre el asunto.

- 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: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 [11].

- Durante la Reunión ICANN66 celebrada en Montreal (6 de noviembre de 2019), la comunidad de la ICANN llevó a cabo una sesión Plenaria Intercomunitaria sobre el Uso indebido del DNS.

- Durante la reunión virtual ICANN67 (9 de marzo de 2020), el ALAC celebró dos sesiones a las que asistieron de forma remota muchos participantes de la comunidad de la ICANN, una de las cuales proporcionó una introducción al uso indebido del DNS (que incluía un video educativo) y otra que revisó en la práctica la ejecución del Cumplimiento Contractual en respuesta a los típicos Casos de Uso indebido del DNS

**Cuestiones - 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 [12] 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 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.

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 seinformaron (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:

[11] 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)

[12] 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 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.

El 17 de octubre de 2019, una consultora (Interisle Consulting Group) lanzó un estudio sobre el Uso Indebido Delictivo de las Registraciones Masivas de Nombres de Dominio y el Acceso a la Información de Contacto que tiene relevancia directa para los debates de la comunidad que están en curso y exploró:

- Cómo los delincuentes cibernéticos aprovechan los servicios de registración masiva para "militarizar" grandes cantidades de nombres de dominio para efectuar sus ataques.
- Efectos de la política interina de la ICANN de omitir la información del punto de contacto de Whois a fin de cumplir con el GDPR en las investigaciones sobre delitos informáticos
- Recomendaciones de política para la organización de la ICANN y las consideraciones de la comunidad

**Cuestiones - 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).[13]

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 deinformes 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.[14]

[13]Véanse las sesiones intercomunitarias dirigidas por el PSWG del GAC durante las reuniones ICANN57 (noviembre de 2016), ICANN58 (marzo de 2017) e ICANN60 (octubre de 2017), así como las preguntas a la Junta Directiva de la ICANN sobre la efectividad de las Protecciones en relación al uso indebido del DNS en el Comunicado pronunciado en Hyderabad (8 Noviembre de 2016), las preguntas de seguimiento contenidas en el Comunicado del GAC pronunciado en Copenhague (15 de marzo de 2017) y un conjunto de respuestas preliminares (30 de mayo de 2017) de la organización ICANN.

[14] Para más información, véase https://www.icann.org/octo-ssr/daar-faqs

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 carta reciente del Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil (M3AAWG)[15] 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.

Recientemente, los registros informaron en una Carta Abierta (19 de agosto de 2019) que interactuaron con la Oficina del Director de Tecnologías de la ICANN *"para analizar el DAAR con el fin de recomendar mejoras a la OCTO para garantizar que el DAAR cumpla mejor su propósito previsto y brinde un recurso valioso a la comunidad de la ICANN."* Si bien los registros reconocieron que *"algunos miembros de la comunidad pueden confiar en los datos proporcionados en el Informe de Actividades de Uso Indebido de Dominios - o DAAR - para respaldar reclamos de Uso Indebido del DNS sistémico o generalizado", creen que "la herramienta tiene limitaciones significativas, que no se puede confiar en que informe de manera precisa y confiable las evidencias de amenazas a la seguridad, y que aún no cumple sus objetivos."*

**Cuestiones - Efectividad: Medidas de Protección actuales en relación al 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, **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

[15]Grupo de Trabajo Anti-Abuso vía Mensajes, Malware y Móvil

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 https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html - specification11 **En este documento de asesoramiento se propone un enfoque que los 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".*[16] 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*" En elinforme de la última auditoria (17 de septiembre de 2019), la ICANN concluyó que:

- La gran mayoría de los operadores de registro están comprometidos a abordar las amenazas a la seguridad del DNS.
- La prevalencia de las amenazas a la seguridad del DNS se concentra en un número relativamente pequeño de operadores de registro.
- Algunos operadores de registro interpretan el lenguaje contractual de la Especificación 11 3 (b) de una manera que hace difícil formar un juicio sobre si sus esfuerzos para mitigar las amenazas a la seguridad del DNS son efectivas y acordes.

**Las partes contactadas han considerado que estas auditorias** exceden el alcance de sus obligaciones contractuales.[17] La organización de la ICANN indicó que iniciará una auditoria de los registradores centrada en las amenazas a la seguridad del DNS.

[16]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

[17] 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*

**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 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 CCT aplazó la tarea de realizar una evaluación de la efectividad del Marco para una revisión[18] posterior ya que el tiempo de existencia del Marco no era suficiente para evaluar su efectividad.

**Efectividad: Medidas pro activas 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 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 pro activas 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

*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 "*

[18] 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.*

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)

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*".[19]

## Posiciones actuales

Las posiciones actuales del GAC se enumeran a continuación en orden cronológico inverso:

- Comentario del GAC (3 de abril de 2020) sobre el Informe Preliminar del Equipo de Revisión SSR2
- Comentario del GAC (23 de diciembre de 2019) sobre las Recomendaciones Finales de la Revisión RDS-WHOIS2
- Declaración del GAC sobre el Uso Indebido del DNS (18 de septiembre de 2019)
- Comentario del GAC (11 de diciembre de 2018) sobre las Recomendaciones Finales de la Revisión CCT
- Comentario del GAC (16 de enero de 2018) sobre lasNuevas Secciones del Informe Preliminar del Equipo de Revisión de CCT (27 de noviembre 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 sobre el Informe Inicial del SADAG (21 de mayo de 2018)
- 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)
- Comunicado pronunciado por el GAC en Copenhague (15 de marzo de 2017) que incluye el Asesoramiento sobre Mitigación del Uso Indebido que solicita respuestas a la tabla de clasificación de Seguimiento del GAC del Anexo 1 del Comunicado del GAC pronunciando en Hyderabad (págs. 11-32)
- 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 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)

[19]Véase la pág.5 de la tabla de clasificación de la Acción de la Junta Directiva sobre las Recomendaciones Finales del CCT

- 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 Nairobi (10):(10 de marzo de 2010), sección VI. Recomendaciones sobre averiguación de antecedentes para el cumplimiento de la ley.
- Recomendaciones de cumplimiento de la ley sobre las enmiendas al Acuerdo de Registrador (1 de marzo de 2012)
- Recomendaciones sobre averiguación de antecedentes para el cumplimiento de la ley (octubre 2009)

## Documentos de Referencia Clave

- Tabla de Clasificación de las Acciones de la Junta Directiva de la ICANN sobre las Recomendaciones Finales de la Revisión RDS-WHOIS2 (25 de febrero de 2020)
- Tabla de Clasificación de las Acciones de Junta Directiva de la ICANN sobre las Recomendaciones Finales del CCT (1 de marzo de 2019)
- Informe final y recomendaciones de la revisión del CCT (8 de septiembre de 2018), en particular la Sección 9 sobre Protecciones (pág.88)
- Análisis estadístico del uso indebido del DNS en los gTLD (9 de agosto de 2017)
- 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)

## Administración de la documentación

| | |
|---|---|
| **Reunión** | Foro de Política Virtual ICANN68, del 22 al 25 de junio de 2020 |
| **Título** | Mitigación del uso indebido del DNS |
| **Distribución** | Miembros del GAC (antes de la reunión) y público (después de la reunión) |
| **Fecha de distribución** | Versión 1: 3 de junio de 2020 |