ICANN | GAC
Governmental Advisory Committee

Distribución	Pública
Fecha	18 de septiembre de 2019

Declaración del GAC sobre el uso indebido del DNS

El Comité Asesor Gubernamental (GAC) de la ICANN espera con ansias el próximo debate intercomunitario sobre el uso indebido del DNS durante ICANN66 y agradece la carta abierta del Grupo de Partes Interesadas de Registros a la comunidad con fecha 19 de agosto de 2019 sobre este tema.

Proteger al público de las amenazas a la seguridad y del uso indebido del DNS es un tema importante en materia de política pública. El GAC ha emitido asesoramiento, brindado pautas y comentarios, organizado debates intercomunitarios y propuesto disposiciones contractuales más firmes para proteger al público. [1] Nuestras observaciones actuales brindarán más contexto sobre este tema al debatir sobre lo siguiente: 1) por qué el uso indebido del DNS es un tema vital; 2) las definiciones y obligaciones contractuales existentes respecto del uso indebido del DNS; y 3) las conclusiones y recomendaciones del Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores sobre el uso indebido del DNS. Mediante este debate, esperamos sentar las bases para un debate intercomunitario productivo e informado en Montreal.

Por qué el uso indebido del DNS es un tema vital

Con cada año que pasa, el costo global del ciberdelito aumenta, el cual alcanza un estimado de USD600 mil millones en 2018.[2] Los ciberdelincuentes explotan y usan indebidamente el DNS para cumplir con sus esquemas,[3] y el correo electrónico sigue siendo sin lugar a dudas el vector más común de compromiso inicial,[4] con un marcado aumento en ataques de phishing a los consumidores.[5]

Si el público debe confiar y depender de Internet para las comunicaciones y transacciones, aquellos encargados de administrar la infraestructura del DNS deben tomar medidas para garantizar que este recurso público sea seguro y esté protegido. Leyes de privacidad recientes, incluido el Reglamento General de Protección de Datos, han limitado la disponibilidad pública de información sobre los titulares de nombres de dominio, lo que ha creado desafíos para los profesionales a cargo del cumplimiento de la ley y de la ciberseguridad que tienen la tarea de combatir las amenazas a la seguridad y protección de Internet.[6]

---

1 El GAC ha brindado este aporte tanto independientemente como a través del Grupo de Trabajo de Seguridad Pública. *Véase por ej.,* los siguientes documentos: Comunicados del GAC: ICANN46 Pekín; ICANN 53 Buenos Aires, ICANN54 Dublín; e ICANN57 Hyderabad; presentaciones de la comunidad de la ICANN sobre uso indebido del DNS durante ICANN 57, 58 y 60; y Recomendaciones sobre el cumplimiento de la ley de 2009 (avaladas por el GAC durante ICANN 38).

2 Impacto económico del ciberdelito de McAfee – Sin desaceleración disponible en: https://www.csis.org/analysis/economic-impact-cybercrime; Costo del ciberdelito de 2019 de Accenture, disponible en https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

3 *Véase por ejemplo,* Informe sobre seguridad contra amenazas de Internet de Symantec (febrero de 2019) disponible en: https://www.symantec.com/security-center/threat-report.

4 Informe de investigaciones sobre filtración de datos de 2019 de Verizon disponible en https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations- report.pdf

5 Estado de Internet de 2019 de Akamai disponible en https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial- services-attack-economy-report-2019.pdf

6 *Véase por ejemplo,* Encuesta de usuarios de WHOIS y GDPR de la ICANN realizada por el Grupo sobre Phishing y el Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil disponible en https://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.html

Revisiones recientes y continuas de la ICANN, exigidas en virtud de los Estatutos destacan la importancia de:

- la **eficacia de los esfuerzos en seguridad para tratar los desafíos y amenazas reales y posibles a la seguridad y estabilidad del DNS**, y la medida en la que los **esfuerzos en seguridad son suficientemente sólidos para enfrentar futuros desafíos** y amenazas;[7]
- **protección del consumidor**, seguridad, estabilidad y flexibilidad, cuestiones de **uso indebido malicioso**, preocupaciones sobre la soberanía y derechos de protección anteriores o simultáneos a la autorización de un aumento en el número de nuevos dominios de alto nivel;[8]
- **mejora de la exactitud y el acceso a los datos de registración de dominios genéricos de alto nivel**, así como consideración de medidas de protección para dichos datos;[9]
- la **eficacia** del **servicio de directorio de registro de gTLD entonces en vigencia** y **si su implementación cubre las necesidades legítimas de cumplimiento de la ley, promoviendo la confianza del consumidor** y protegiendo los datos de los registratarios[10] [énfasis agregado]

Además, la ICANN está considerando los contornos para una segunda ronda de gTLD que brinda nuevas oportunidades de incluir dentro de los incentivos contractuales para la adopción de mejores prácticas mostradas a fin de reducir dicho uso indebido y aumentar el costo comercial a actores delictivos o que realizan usos indebidos.

En consecuencia, ahora es el momento correcto para considerar estas cuestiones y contemplar los mejores pasos a seguir en respaldo al compromiso de la ICANN respecto de preservar **y mejorar** la administración del DNS, incluidas la "estabilidad operativa, confiabilidad, seguridad, interoperabilidad mundial, flexibilidad y apertura del DNS y de Internet".[11]
En este respecto, los gobiernos y autoridades públicas se encuentran especialmente en una buena situación para brindar aportes.[12]

Definiciones existentes de uso indebido del DNS y obligaciones contractuales de la ICANN

El Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores (CCT), que estaba compuesto por partes interesadas de toda la comunidad de la ICANN, observó las definiciones existentes de uso indebido del DNS dentro de la comunidad de la ICANN cuando buscó examinar el uso indebido del DNS en nuevos gTLD en comparación con los gTLD existentes y evaluar si las medidas de protección existentes eran suficientes.[13] Teniendo en cuenta que las conclusiones de la ICANN demostraron que "existe consenso sobre qué constituye uso indebido de la seguridad del DNS o uso indebido de la seguridad del DNS de la infraestructura del DNS", **el Equipo de Revisión de CCT se refirió al uso indebido del DNS como "actividades intencionalmente engañosas, conspiradoras o no solicitadas que hacen uso activamente del DNS o los procedimientos usados para registrar nombres de dominio."**[14] El informe de CCT usó el término "uso indebido de la seguridad del DNS" para hacer referencia a formas más técnicas de actividad maliciosa, como malware, phishing y botnets, así como spam cuando se utilizan como un método de entrega para estas formas de uso indebido.[15]

Estas definiciones están en consonancia con los contratos estándar para registros y registradores de la ICANN. El Acuerdo de Registro estándar de la ICANN exigía que los operadores de registro de nuevos gTLD incluyesen disposiciones en sus Acuerdos entre Registro y Registrador.(RRA) que prohibieran a los registratarios:

> Distribuir malware, operar botnets de manera indebida, phishing, piratería, violación de derechos de autor o marca comercial, prácticas fraudulentas o engañosas, falsificar o participar de algún otro modo en actividades contrarias a la ley aplicable y proporcionar (en consonancia con la ley aplicable y cualquier proceso relacionado) consecuencias para dichas actividades incluida la suspensión del nombre de dominio.[16]

Además, los operadores de registro deben "llevar a cabo periódicamente un análisis técnico a fin de evaluar si los dominios en su TLD están siendo utilizados para perpetrar amenazas en contra de la seguridad, **tales como** pharming, phishing, malware y uso de botnets".[17] [énfasis agregado]. Señalamos que esta lista es ilustrativa y no exhaustiva. Como complemento de las disposiciones de los registros, el contrato estándar para registradores de la ICANN exige que los registradores oportunamente "investiguen y respondan de manera adecuada a cualquier informe de uso indebido".[18] En conjunto, estas fuentes, desarrolladas dentro de la comunidad de múltiples partes interesadas de la ICANN, comprenden un entendimiento fundacional común de qué comprende el uso indebido del DNS.

El Equipo de Revisión de CCT detecta el uso indebido del DNS concentrado entre ciertos registros y registradores y elabora recomendaciones

El Equipo de CCT observó que los nombres de dominio son generalmente un componente clave de los ciberdelitos, se usan para ayudar a la distribución de malware y comando y control de botnet, y que las campañas de spam generalmente se asocian con phishing y otros ciberdelitos.[19] En particular, el Equipo de Revisión señaló que

> [si] bien los contratos estándar para registros y registradores de la ICANN han ordenado el uso consistente de medidas de protección específicas, los esfuerzos para combatir el uso indebido de los nombres de dominio varían enormemente entre las partes contratadas. Algunas entidades no actúan hasta que se recibe un reclamo. En cambio, otros registradores toman medidas proactivas, como comprobar las credenciales de los registratarios, bloquear cadenas de caracteres de nombres de dominio similares a los objetivos de phishing conocidos e inspeccionar los revendedores de nombres de dominio. Los revendedores de nombres de dominio no son partes contratadas de la ICANN y, por ende, no están sujetos directamente a la autoridad de cumplimiento de la ley de la ICANN sobre los requisitos contractuales estándar. . . [20]

---

7 Estatutos de la ICANN, §4.6 (c), Revisión de Seguridad, Estabilidad y Flexibilidad.
8 Estatutos de la ICANN, §4.6 (d), Revisión de Competencia, Confianza y Elección de los Consumidores.
9 Estatutos de la ICANN, §4.6 (e), Revisión de los Servicios de Directorio de Registración.
10 *Id.*
11 Estatutos de la ICANN, §1.2(a) Compromisos.
12 Efectivamente reconocer el rol vital que los gobiernos y autoridades públicas tienen para contribuir cuando surjan cuestiones en materia de política pública es uno de los valores fundamentales de la ICANN. Estatutos de la ICANN, §1.2(b) Valores fundamentales.
13 *Véase* Informe Final de CCT (18 de septiembre de 2018) en páginas 88-109. Para obtener más información sobre cómo la comunidad de la ICANN ha caracterizado el uso indebido, véase el Informe Final del Grupo de Trabajo sobre políticas de uso indebido de registración (29 de mayo de 2010): https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf
14 Informe Final de CCT en pág. 88 y pies de página acompañantes. *Véase también* pág. 3 de "Medidas de protección del Programa de Nuevos gTLD contra el uso indebido del DNS: Informe revisado" (2016).
15 Informe Final de CCT en pág. 8.

A fin de comprender mejor la efectividad de las medidas de protección para nuevos gTLD, el Equipo de Revisión de CCT encargó un estudio que analizara los índices de distribución de spam y malware en el gTLD global desde 2014 a 2016 que distinguiese entre gTLD nuevos y existentes, y publicó el último informe.[21] De manera significativa, el estudio sobre el uso indebido del DNS deja en claro que hay cuestiones importantes sobre el uso indebido en el DNS. Respecto del Programa de Nuevos gTLD, el estudio señala que más del 50 % de las registraciones en ciertos nuevos gTLD tenía un uso indebido.[22] Otros aspectos destacados del estudio incluían lo siguiente:

- Los nuevos gTLD se han convertido en un objetivo creciente para los actores maliciosos;
- Los gTLD existentes tienen concentraciones más altas de dominios comprometidos mientras que los actores maliciosos generalmente eligen registrar nombres de dominios de manera maliciosa mediante el uso de uno de los nuevos gTLD;
- Los operadores de registro de los nuevos gTLD más usados de manera indebida compiten en el precio;
- Los índices de uso indebido de phishing y malware de nuevos gTLD están convergiendo con los índices de los gTLD existentes con el transcurso del tiempo;
- Cinco nuevos gTLD con la concentración más alta de dominios usados en ataques de phishing de acuerdo con la lista negra del Grupo de Trabajo Anti-Phishing contenían el 58,7 % de todos los dominios incluidos en la lista negra en los nuevos gTLD;
- Los nuevos gTLD experimentaron un porcentaje de spam significativamente más alto en el último trimestre de 2016 que los gTLD existentes (diez veces más que estos últimos);
- Los nombres de dominio registrados con fines maliciosos generalmente contenían cadenas de caracteres relacionadas a términos registrados como marca comercial
- Las cantidades de uso indebido se relacionan principalmente con los requisitos estrictos de registración: *es decir*, los actores maliciosos prefieren registrar dominios en nuevos gTLD estándar, los cuales generalmente están abiertos a la registración pública, en vez de en nuevos gTLD de la comunidad, donde los registros pueden imponer restricciones sobre qué personas o entidades pueden registrar nombres de dominio.

El Equipo de Revisión de CCT concluyó que factores tales como restricciones a la registración, precio y prácticas específicas a los registradores tenían más probabilidades de afectar a los índices de uso indebido.[23] En consecuencia, el Equipo de Revisión de CCT recomendó que:

- La organización de la ICANN negocie enmiendas a los acuerdos de registro existentes, o en consideración de los nuevos acuerdos de registro asociados a posteriores rondas de nuevos gTLD, **incluya disposiciones en los acuerdos para proporcionar incentivos, incluidos incentivos financieros para los registros, en especial, los registros abiertos, para adoptar medidas proactivas contra el uso indebido** [énfasis agregado];

---

16 Acuerdo de Registro de la ICANN, Especificación 11, 3(a).

17 Acuerdo de Registro de la ICANN, Especificación 11, 3(b). Esta disposición ha sido el tema repetido de las preguntas, inquietudes y asesoramiento del GAC que surgieron debido a que la implementación de esta medida de protección, si bien requería a los registros monitorear las amenazas a la seguridad, no obligaba a los operadores de registro actuar en respuesta a las amenazas a la seguridad. *Véase* Singapur (2014), Los Ángeles, Londres. El comunicado del GAC pronunciado en Pekín incluía no solo el deber de monitorear las amenazas a la seguridad sino también el deber de responder en el caso de que se detectasen ciertas terribles amenazas a la seguridad. El GAC recomendó que, en caso de amenazas a la seguridad que presentan un "riesgo de daño real", los operadores de registro notifiquen al registrador relevante y, si el registrador no toma una "acción inmediata", entonces "suspendan el nombre hasta que se resuelva el problema". Comunicado pronunciado en Pekín en pág. 7.

18 Acuerdo del Registrador de la ICANN, § 3.18.

19 Informe Final del Equipo de Revisión de CCT en pág. 93.

20 Informe Final del Equipo de Revisión de CCT en pág. 93.

21 *Véase* https://www.icann.org/news/announcement-2017-08-09-en

22 Informe Final del análisis estadístico del uso indebido del DNS (9 de agosto de 2017): https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

23 Informe Final de CCT en pág. 94., que cita el Estudio sobre el uso indebido del DNS en las páginas 24 y 25.

- La organización de la ICANN negocie enmiendas al Acuerdo de Acreditación de Registradores y los Acuerdos de Registro para incluir disposiciones dirigidas a evitar el uso sistemático de registradores o registros específicos para el uso indebido de la seguridad del DNS. En particular, la ICANN debería establecer umbrales de uso indebido en los cuales se activen automáticamente las consultas en materia de cumplimiento, con un umbral más alto en el cual se presuma que los registradores y los registros están en incumplimiento de sus acuerdos;
- Estudiar más exhaustivamente la relación entre operadores de registro específicos, registros y uso indebido de la seguridad del DNS al encargar la recopilación continua de datos, incluida, por ejemplo, la iniciativa de Informe de Actividades de Uso Indebido de Dominios (DAAR) de la ICANN. En pos de la transparencia, esta información debería publicarse de manera regular, idealmente en forma trimestral y en un plazo no superior al año, a fin de permitir la identificación de los registros y registradores que requieran mayor análisis, investigación y posible acción en pos del cumplimiento efectivo por parte de la organización de la ICANN. Al identificar los fenómenos de uso indebido, la ICANN debería implementar un plan de acción para responder a dichos estudios, corregir problemas identificados y definir la futura recopilación continua de datos; y
- La ICANN debería recopilar datos y publicar la cadena de partes responsables de las registraciones de nombres de dominio de gTLD.

Mejores prácticas de los registros de ccTLD

En años recientes, un número creciente de registros de ccTLD han adoptado medidas proactivas contra el uso indebido para abordar los delitos facilitados por el DNS y mantener su zona libre de uso indebido y repeler a los actores maliciosos al hacer que sus nombres de dominio sean tan poco atractivos para los actores maliciosos como sea posible. Estas medidas varían desde métodos de autenticación más estrictos, incluidas verificaciones de identidad, [24] hasta el uso de modelos de predicción de fraude basados en datos que combinan medidas de registración de datos e infraestructura a fin de identificar y predecir las registraciones de dominio realizadas con fines perniciosos. [25] Estas mejores prácticas comprobadas deberían ser implementadas por los registros y registradores de gTLD.

Conclusión

Esta comunidad está en una posición única para evaluar y elegir qué políticas deberían implementarse para proteger al público del uso indebido del DNS. Estamos de acuerdo con el Grupo de Partes Interesadas de Registros de que el éxito de su producto (y de hecho del DNS) depende de su capacidad de ofrecer un producto con buena reputación en el que los usuarios puedan confiar. A fin de lidiar eficazmente con el uso indebido del DNS y promover el DNS de manera más confiable, alentamos a la comunidad a considerar seriamente las recomendaciones descriptas anteriormente ya que proporcionan medidas prácticas que pueden *y deberían* ser implementadas para abordar el uso indebido del DNS. El GAC espera participar con otros grupos de la comunidad en este tema en ICANN 66 en Montreal.

[24] Véase, por ejemplo, Sesión sobre lecciones aprendidas en ICANN64: How .DK successfully reduced abusive domains y https://www.dk-hostmaster.dk/en/news/mandatory- identification-nemid y https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult

[25] Véase https://eurid.eu/en/news/identification-of-malicious-dns/