VERSIÓN PRELIMINAR mayo de 2023

Documento de asesoramiento: Cumplimiento de las obligaciones sobre el uso indebido del DNS en el Acuerdo de Acreditación de Registradores y el Acuerdo de Registro

El presente Documento de asesoramiento ofrece orientación sobre la interpretación y el cumplimiento de las enmiendas del [FECHA] al Acuerdo de Acreditación de Registradores (RAA) y al Acuerdo de Registro (RA) base de Dominios Genéricos de Primer Nivel (gTLD) en relación con las obligaciones de mitigación del uso indebido del DNS (Enmiendas sobre el uso indebido del DNS).

A menos que se modifiquen específicamente con las Enmiendas sobre el uso indebido del DNS, todas las obligaciones del RAA y del RA que estaban en vigencia antes de estas Enmiendas siguen vigentes y aplicables.

Todos los términos en mayúscula que no se definen en el presente Documento de asesoramiento tienen el significado que se les atribuye en el RAA y el RA.

Los registradores y registros que utilicen las prácticas que se establecen el presente Documento de asesoramiento probablemente cumplirán las obligaciones establecidas en las Enmiendas sobre el uso indebido del DNS, pero la adhesión a una o más de estas prácticas no dará lugar automáticamente a la determinación de que el registrador u operador de registro ha cumplido sus obligaciones. Los ejemplos que se exponen a continuación son únicamente ilustrativos y no tienen por objeto limitar las posibles acciones de mitigación. En todos los casos, siempre que el departamento de Cumplimiento Contractual de la ICANN inicie una investigación, los registradores y operadores de registro deberán aportar pruebas que demuestren el cumplimiento de los requisitos pertinentes del RAA y del RA.

Información de referencia

La organización de la ICANN celebra contratos con los registros para operar gTLD a través de un RA. El RA especifica las responsabilidades del operador de registro, que incluyen el mantenimiento de la base de datos autoritativa de todos los nombres de dominio registrados en el gTLD y la publicación de la zona del DNS para el gTLD.

La ICANN también celebra un RAA con cada registrador, que le permite ofrecer servicios de registración de nombres de dominio en los gTLD. El RAA describe las responsabilidades del registrador, como la verificación de la información del registratario (o titular del nombre registrado) y el mantenimiento de datos precisos.

Las funciones y obligaciones de los registradores y los registros son distintas y se reflejan en sus respectivos acuerdos, el RAA y el RA.

La ICANN está facultada para exigir el cumplimiento de las normas relativas a los nombres de dominio y a los servicios de registración de nombres de dominio, conforme a lo que se establece en el RAA y en el RA. Este Documento de asesoramiento se centra en los nombres de dominio (o nombres registrados) en gTLD que se utilizan como vehículos o mecanismos para el uso indebido del DNS. Los requisitos de las Enmiendas sobre el uso indebido del DNS en el RAA y el RA se basan en las medidas que los registradores y los operadores de registro, respectivamente, pueden adoptar para minimizar el alcance y la intensidad del daño y la victimización que genera el uso indebido del DNS. Estos requisitos también tienen en cuenta que los registradores y los operadores de registro representan solo una parte del ecosistema del DNS, que está compuesto por muchos actores[1]. En función de las circunstancias específicas de un caso de uso indebido del DNS, el actor más adecuado para detectar, evaluar, verificar y detener la actividad abusiva puede variar y, en ocasiones, puede ser un actor distinto de un registrador u operador de registro.

Uso indebido del DNS

A efectos del RAA, el RA y el presente Documento de asesoramiento, *uso indebido del DNS* se refiere a malware, botnets, phishing, pharming y spam (cuando el spam se utiliza como mecanismo de entrega para cualquiera de los otros cuatro tipos de uso indebido del DNS), conforme a lo que se define en estos términos en la Sección 2.1 del Informe del Comité Asesor de Seguridad y Estabilidad sobre un Enfoque interoperable para abordar la gestión del uso indebido en el DNS (SAC 1152):

> El **malware** es software malicioso instalado y/o ejecutado en un dispositivo sin el consentimiento del usuario, que interrumpen el funcionamiento del dispositivo, recopilan información sensible y/o acceden a sistemas informáticos privados. El malware incluye virus, spyware, ransomware y otros programas informáticos no deseados.
>
> Los **botnets** son conjuntos de computadoras conectadas a Internet que han sido infectadas con malware y se les puede ordenar que realicen actividades

bajo el control de un atacante remoto.

[1] Se puede encontrar información adicional en el informe elaborado por el Grupo de Interés Especial sobre el Uso Indebido del DNS en .FIRST que también incluye asesoramiento para los equipos de respuesta ante incidentes sobre las organizaciones con las que se podría contactar de forma productiva en diferentes fases de respuesta a incidentes para diferentes técnicas de uso indebido del DNS. Además, la Red de Políticas de Internet y Jurisdicción (https://www.internetjurisdiction.net/) ha proporcionado más orientación sobre estas formas de uso indebido del DNS en sus "Enfoques operativos, normas, criterios y mecanismos"

[2] SAC 115 del Comité Asesor de Seguridad y Estabilidad de la ICANN, Sección 2.1, páginas 12 y 13, 19 de marzo de 2021

El **phishing** ocurre cuando un atacante engaña a la víctima para que revele información personal, corporativa o financiera sensible (por ejemplo, números de cuenta, ID de inicio de sesión, contraseñas), ya sea mediante el envío de correos electrónicos fraudulentos o imitados, o atrayendo a los usuarios finales hacia copias falsas de sitios web. Algunas campañas de phishing pretenden persuadir al usuario para que instale malware.

El **pharming** es la redirección de usuarios, sin saberlo, a sitios o servicios fraudulentos, generalmente a través del secuestro o envenenamiento del DNS. El secuestro del DNS se puede producir cuando los atacantes utilizan malware para redirigir a las víctimas al sitio del perpetrador en lugar del sitio solicitado inicialmente. El envenenamiento del DNS hace que un servidor o resolutor del DNS responda con una dirección de Protocolo de Internet falsa que contiene software malicioso. El phishing se diferencia del pharming en que el pharming implica la modificación de las entradas del DNS, mientras que el phishing engaña a los usuarios para que introduzcan información personal.

El **spam** es correo electrónico masivo no solicitado, en el que el destinatario no ha otorgado permiso para que se envíe el mensaje y cuando el mensaje se envía como parte de un conjunto de mensajes, todos con un contenido sustancialmente idéntico. El spam solo se considera uso indebido del DNS cuando se utiliza como mecanismo de entrega de al menos uno de los otros tipos de uso indebido del DNS descritos anteriormente.

Obligaciones del registrador

Sección 3.18 del RAA

Antes de la promulgación de las Enmiendas sobre el uso indebido del DNS, la Sección 3.18 exigía a los registradores que mantuvieran y publicaran los datos de contacto para recibir informes de uso indebido, incluida la Actividad ilegal. Esta disposición también esbozaba los requisitos relativos a la investigación y respuesta a las denuncias de usos indebidos que afectan a Nombres registrados patrocinados por un registrador, y los registros relacionados que debe mantener un registrador. Los requisitos de la Sección 3.18 del RAA se han modificado de la siguiente manera:

Requisitos relativos a la publicación y mantenimiento de contactos de uso indebido (RAA 3.18.1)

Donde denunciar el uso indebido[3]
Para facilitar la presentación de denuncias de cualquier parte que alegue uso indebido y/o Actividad Ilegal, el registrador debe publicar una dirección de correo electrónico o formulario web que sea fácilmente accesible en la página de inicio del sitio web del registrador[4]. Los formularios web no deben requerir un inicio de sesión para enviar denuncias de uso indebido.

Se considerará conforme la página de inicio de un registrador que muestre claramente un enlace a una página de "Denuncia de uso indebido" o de "Contacto" (que incluya claramente el contacto para usos indebidos) y que permita a los denunciantes enviar fácilmente las denuncias desde la página enlazada.

Confirmación de recepción de una denuncia por uso indebido
Además, el registrador debe proporcionar al denunciante de usos indebidos una confirmación de la recepción de la denuncia. Este acuse de recibo puede enviarse al denunciante de usos indebidos o mostrarse en la pantalla al finalizar el envío al registrador. Este acuse de recibo debe contener información suficiente para que el denunciante pueda demostrar que ha enviado la denuncia de uso indebido. Como mínimo, el acuse de recibo debe identificar al registrador, el nombre o nombres registrados denunciados y la fecha de presentación de la denuncia.

Contactos para los organismos de cumplimiento de la ley
Los requisitos relacionados con los contactos dedicados a recibir informes de los Organismos de cumplimiento de la ley (LEA) y otras autoridades dentro de la jurisdicción del registrador, previamente descritos en la Sección 3.18.2 del RAA, se encuentran ahora en la Sección 3.18.3 del RAA; estos requisitos permanecen sin cambios.

Requisitos relacionados con la adopción de medidas de mitigación tras la recepción de denuncias procesables de uso indebido del DNS (RAA 3.18.2)

La Sección 3.18.2 del RAA, modificada por las Enmiendas sobre el uso indebido del DNS, ahora establece lo siguiente:

> *Cuando el Registrador tenga evidencia procesable de que un Nombre Registrado patrocinado por el Registrador está siendo utilizado para el uso indebido del DNS, el Registrador debe adoptar de inmediato la medida o medidas de mitigación apropiadas que sean razonablemente necesarias para detener, o de otra manera, impedir que el Nombre Registrado se utilice para el uso indebido del DNS. La medida o medidas pueden variar en función de las circunstancias, teniendo en cuenta la causa y la gravedad del perjuicio derivado del uso indebido del DNS y la posibilidad de daños colaterales asociados.*

[3] Para evitar dudas, los requisitos relacionados con la publicación de la dirección de correo electrónico y el número de teléfono de contacto de uso indebido del registrador a través del Servicio de Directorio de Datos de Registración (RDDS) permanecen inalterados.

[4] Este sitio web debe estar ubicado en el mismo localizador uniforme de recursos (URL) que el registrador muestra como valor para el campo "URL del registrador" a través de su RDDS, proporcionado a la ICANN y al operador de registro para su publicación en el RDDS del operador de registro.

Pruebas procesables
Las pruebas deben ser *procesables*. Esto significa que la información que esté a disposición del registrador debe ser suficiente para permitir que el registrador determine razonablemente si el Nombre registrado se está utilizando para una o más formas de uso indebido del DNS. Se recomienda a los registradores que supervisen de forma proactiva los Nombres registrados que patrocinan para identificar posibles usos indebidos del DNS. La evaluación por parte de un registrador de las pruebas procesables variará en función de las circunstancias de cada caso.

Obtención de pruebas procesables de una parte externa
La Cámara de Partes Contratadas (CPH) publicó pautas para ayudar con la presentación de informes sobre uso indebido completos y procesables a los registradores (Pautas de la CPH). Las Pautas de la CPH describen las pruebas que tienden a hacer que un informe de uso indebido sea procesable. Por ejemplo, una captura de pantalla que muestre un intento de phishing con una indicación de a qué va dirigido el ataque (una institución financiera, por ejemplo); y el URL completo donde se encuentra el uso indebido (por ejemplo, example[.]tld/badpage[.]html)5. Se recomienda a los denunciantes de usos indebidos que consulten y sigan las Pautas de la CPH y que proporcionen tanta información como sea posible en sus denuncias, para permitir al registrador llevar a cabo una investigación sobre un posible uso indebido del DNS.

En los casos en que un registrador reciba una denuncia de uso indebido que no contenga toda la información necesaria para ser considerada prueba procesable de uso indebido del DNS, el registrador deberá investigar conforme a la Sección 3.18 del RAA. En algunos casos, el registrador puede tener acceso a información que no fue proporcionada por un denunciante de uso indebido, pero que es necesaria o útil para determinar que el Nombre registrado está siendo utilizado para un uso indebido del DNS. En dichos casos, el registrador debe considerar la información a la que pueda acceder razonablemente y que sea pertinente para la investigación (por ejemplo, servidores de nombres, información y actividad de la cuenta, y contenido de al menos la página web principal o el URL específico en el informe de uso indebido, si se proporciona).

Tras la obtención de pruebas procesables, se requiere una acción inmediata
Una vez obtenidas las pruebas procesables, el registrador debe *adoptar de inmediato las medidas de mitigación apropiadas* que sean razonablemente necesarias para detener, o interrumpir de otro modo, el

[5] Este URL se muestra en un formato conocido como “URL desactivado” Un URL desactivado es legible para el ojo humano, pero no se puede hacer clic en él. Por lo tanto, si usted o el destinatario de su informe de uso indebido hace clic en el URL por error, no le dirigirá a usted o al destinatario a un sitio potencialmente malicioso.

Nombre registrado de su utilización para el uso indebido del DNS. Para determinar las medidas de mitigación que son inmediatas y apropiadas, el registrador considerará las circunstancias específicas del caso, que pueden incluir el equilibrio entre el alcance y la intensidad del perjuicio causado por el uso indebido del DNS y la posibilidad de daños colaterales asociados.

El daño colateral es una consideración particularmente importante cuando un nombre de dominio legítimo o benigno se utiliza como vector para el uso indebido del DNS sin el conocimiento o consentimiento del registratario. Esto se conoce a menudo como un "dominio afectado" y, en ocasiones, es el resultado de la explotación del sistema de gestión de contenidos de un sitio web. En estas situaciones de afectación, la suspensión directa del dominio por parte del registrador u operador de registro puede no ser la mitigación adecuada, dado que la suspensión cortará el acceso a todo el contenido legítimo, además de hacer inaccesibles cualquier correo electrónico asociado y otros servicios con el dominio[6]. Lo mismo ocurre cuando el uso indebido del DNS está asociado a un dominio de tercer nivel o subdominio. Los registradores y registros pueden actuar únicamente a nivel de dominio de segundo nivel. Por lo tanto, si suspenden el dominio de segundo nivel, se suspenderán también todos los dominios de tercer nivel, no solo el asociado al uso indebido del DNS. En estas situaciones, un registrador puede optar por enviar una notificación al registratario, al operador del sitio y/o al proveedor de alojamiento web.

Qué hace que una acción sea inmediata

Como se señaló anteriormente, la acción de mitigación apropiada para detener o interrumpir una instancia de uso indebido del DNS variará en función de las circunstancias específicas. En consecuencia, la cantidad de tiempo adecuada para investigar y adoptar medidas también variará, por lo que es imposible prescribir una cantidad de tiempo fija para que una acción se considere "inmediata". En cambio, los registradores deben demostrar una atención continua a las denuncias de nombres patrocinados que se utilizan para el uso indebido del DNS. La atención debe ser proporcional al perjuicio potencial que el uso indebido del DNS causa a las víctimas.

En consecuencia, en respuesta a una consulta de Cumplimiento Contractual de la ICANN, los registradores deberán explicar por qué las acciones fueron inmediatas teniendo en cuenta las circunstancias específicas. A continuación, Cumplimiento Contractual de la ICANN revisará la explicación y las circunstancias pertinentes para determinar caso por caso si las acciones fueron razonablemente inmediatas. Los plazos de los ejemplos incluidos en el presente Documento de asesoramiento no son requisitos contractuales, sino que se incluyen únicamente a modo ilustrativo. El hecho de que un registrador tarde más tiempo en investigar y adoptar medidas en un caso similar a los ejemplos no será necesariamente una indicación de incumplimiento. Por el contrario, otras circunstancias pueden requerir que el registrador actúe con mayor

rapidez, como los casos de uso indebido del DNS que conllevan el potencial de causar un perjuicio inminente a los usuarios finales. Se prevé que un registrador investigue y adopte medidas lo antes posible tras el intento razonable del registrador de confirmar un caso de uso indebido del DNS.

[6] Encontrará más información sobre daños colaterales y consideraciones de proporcionalidad cuando se actúa a nivel del DNS en la publicación de la Red de Políticas de Internet y Jurisdicción titulada "Conjunto de herramientas: Acción a nivel del DNS para abordar usos indebidos"

Recapitulación – Ejemplos de cumplimiento por parte de los registradores
Los ejemplos que figuran a continuación ilustran las medidas de mitigación razonables e inmediatas adoptadas para impedir que el Nombre registrado se utilice para el uso indebido del DNS (Primer escenario) y para interrumpir el curso del uso indebido del DNS en relación con el Nombre registrado (Segundo escenario). Estos escenarios contienen circunstancias fácticas específicas. En circunstancias diferentes, los registradores individuales pueden adoptar medidas diferentes y dentro de un marco temporal diferente para detener, o interrumpir de otro modo, casos individuales de uso indebido del DNS. En todos los casos, los registradores deben ser capaces de demostrar que cualquier enfoque adoptado cumple con los requisitos pertinentes de la Sección 3.18 del RAA.

Primer escenario: Un registrador recibe un informe de uso indebido completo y procesable en el que se alega que un Nombre registrado patrocinado por el registrador se utiliza para phishing. El informe incluye pruebas de que un URL que contiene el Nombre registrado patrocinado por el registrador se envía por correo electrónico o SMS representándose a sí mismo como un gran banco que solicita a los destinatarios que desbloqueen sus cuentas. El registrador inicia una investigación teniendo en cuenta toda la información relevante incluida en el informe de uso indebido. La investigación del registrador revela que el nombre registrado no tiene un sitio web disponible públicamente y solo muestra un URL directo con lo que parece ser una pantalla de inicio de sesión de un banco importante. El mismo URL es el que se envía por correo electrónico o SMS. El registrador también considera que el cliente es nuevo y que el Nombre registrado se registró cinco días antes.

Medidas de mitigación apropiadas: El registrador concluye razonablemente que el Nombre registrado está siendo utilizado para el uso indebido del DNS y detiene el uso indebido del DNS suspendiendo el Nombre registrado, aplicando el código de estado clientHold del Protocolo de Aprovisionamiento Extensible (EPP)[7]. La investigación y la medida de mitigación se producen en un plazo de dos días hábiles a partir de la recepción del informe de uso indebido. El registrador también puede decidir aplicar un bloqueo de transferencia al Nombre registrado para evitar que el registratario intente eludir la acción de mitigación y reanude el uso indebido del DNS, siempre que el registrador cumpla los requisitos aplicables de la Política de transferencia de la ICANN.

Segundo escenario: Un registrador recibe un informe de uso indebido completo y procesable en el que se alega que un Nombre registrado patrocinado por el registrador, autobrand.tld, se utiliza para phishing. El informe de uso indebido incluye pruebas de que se está utilizando un URL específico para el phishing. El registrador investiga, teniendo en cuenta toda la información pertinente incluida en el informe de uso indebido, así como la información a la que el registrador puede acceder de forma fácil y razonable.

[7] Haga clic aquí para obtener más información de la ICANN sobre los códigos de estado de EPP

La investigación confirma que el URL que figura en la denuncia de uso indebido se está utilizando para phishing. La investigación también revela que el URL pertenece a un subdominio (city.autobrand.tld), y parece ser utilizado por un franquiciado. El registrador reconoce que el nombre registrado autobrand.tld se registró hace tres años y tiene un sólido conjunto de contenidos para una franquicia de concesionarios de automóviles. El registrador puede confirmar que el Nombre registrado se utiliza para los correos electrónicos corporativos de Autobrand y subdominios para múltiples franquiciados.

Medidas de mitigación apropiadas: El registrador concluye razonablemente que el Nombre registrado está siendo utilizado para el uso indebido del DNS, pero que es probable que sea el resultado de un dominio afectado y que el registratario no está utilizando con pleno conocimiento el Nombre registrado para el uso indebido del DNS. El registrador evalúa el daño colateral potencial que tendría la suspensión del nombre de dominio, y concluye razonablemente que no es una acción de mitigación apropiada en este momento. En su lugar, el registrador interrumpe el uso indebido del DNS notificando a Autobrand, el registratario de autobrand.tld, solicitándole que elimine el contenido de phishing en una fecha determinada razonablemente por el registrador. La investigación y la acción de mitigación tienen lugar dentro de los tres días hábiles siguientes a la recepción del informe de uso indebido.

Requisitos relacionados con el mantenimiento y el suministro a la ICANN de registros

Los requisitos relativos a la documentación y suministro de registros relacionados con la recepción y respuesta a los informes de uso indebido descritos anteriormente en la Sección 3.18.3 del RAA se encuentran ahora en la Sección 3.18.4 del RAA; estos requisitos permanecen inalterados. Estos requisitos también se aplican a la respuesta a los informes de uso indebido del DNS en virtud de la Sección 3.18.2.

Obligaciones del Operador de Registro

Sección 4, Especificación 6 del RA:

La Especificación 6, Sección 4 del RA exige la publicación, y puesta a disposición de la ICANN, de los datos de contacto para gestionar las consultas relacionadas con conductas maliciosas en el dominio de alto nivel (TLD). También incluye requisitos relacionados con la eliminación de registros de pegado huérfanos cuando se utilicen en relación con conductas maliciosas. Los requisitos de esta Especificación se han modificado de la siguiente manera:

Requisitos relativos a la publicación y mantenimiento de contactos de uso indebido (RA base, Especificación 6, Sección 4.1)

Donde denunciar el uso indebido
Para facilitar la presentación de denuncias de cualquier parte que alegue una conducta maliciosa en el TLD, incluido el uso indebido del DNS, el operador de registro debe publicar una dirección de correo electrónico o un formulario web, una dirección postal y un contacto principal para la gestión de dichas denuncias.

Se considerará conforme la página de inicio de un operador de registro que muestre claramente un enlace a una página de "Denuncia de uso indebido" o de "Contacto" (que incluya claramente el contacto para usos indebidos) donde se pueda enviar denuncias sin impedimentos.

Confirmación de recepción de una denuncia por uso indebido
Una vez recibida la denuncia de uso indebido, el operador de registro confirmará su recepción al denunciante. Este acuse de recibo puede enviarse al denunciante del uso indebido o mostrarse en la pantalla al finalizar el envío al operador de registro. Este acuse de recibo debe contener información suficiente para que el denunciante pueda demostrar que ha presentado la denuncia de uso indebido. Como mínimo, el acuse de recibo debe identificar el operador de registro, el nombre o nombres registrados denunciados y la fecha en la que se presentó la denuncia.

Requisitos relacionados con la adopción de medidas de mitigación tras la recepción de denuncias procesables de uso indebido del DNS (RA base, Especificación 6, Sección 4.2)

La Sección 4.2 de la Especificación 6, modificada por las Enmiendas sobre el uso indebido del DNS, ahora establece lo siguiente:

> *Cuando un Operador de Registro determine razonablemente, basándose en pruebas procesables, que un nombre de dominio registrado en el TLD se está utilizando para un uso indebido del DNS, el Operador de Registro deberá adoptar de inmediato las medidas de mitigación apropiadas que sean razonablemente necesarias para contribuir a poner fin al uso indebido del DNS o a impedirlo. Dichas medidas deben, como mínimo, incluir lo siguiente: (i) la remisión de los dominios que se estén utilizando para el uso indebido del DNS, junto con las pruebas pertinentes, al registrador patrocinador; o (ii) la adopción de medidas directas por parte del Operador de Registro, cuando éste lo considere oportuno. La medida o medidas pueden variar en función de cada*

caso, teniendo en cuenta la gravedad del perjuicio derivado del uso indebido del DNS y la posibilidad de daños colaterales asociados.

Pruebas procesables

Las pruebas deben ser *procesables*. Esto significa que la información que esté a disposición del operador de registro debe ser suficiente para permitir que el operador de registro determine razonablemente si el Nombre registrado se está utilizando para una o más formas de uso indebido del DNS. Los operadores de registro pueden obtener pruebas procesables revisando la información a la que puedan acceder de forma razonable e independiente, ya sea junto con una denuncia de uso indebido o como parte de sus propias iniciativas en virtud de la Especificación 11(3)(b) del Acuerdo de Registro, realizando análisis técnicos para identificar los dominios que se están utilizando para el uso indebido del DNS. Las pruebas procesables también pueden ser presentadas al operador de registro por una parte externa, como los Organismos de cumplimiento de la ley (LEA), las fuentes de confianza o reconocidas del operador de registro pertinente, o cualquier otra parte o fuente. Se recomienda a los denunciantes de usos indebidos a que proporcionen toda la información posible para contribuir a garantizar que el operador de registro disponga de información suficiente para llevar a cabo una investigación sobre un posible uso indebido del DNS. Para evitar dudas, una denuncia de uso indebido que el operador de registro considere incompleta podrá considerarse procesable si el operador de registro tiene acceso a información suficiente para llevar a cabo razonablemente una investigación con el fin de determinar si el Nombre registrado denunciado se utiliza para el uso indebido del DNS.

Tras la obtención de pruebas procesables, se requiere una acción inmediata

Una vez obtenidas las pruebas procesables, el operador de registro debe adoptar de inmediato las medidas de mitigación adecuadas que sean razonablemente necesarias para contribuir a detener, o interrumpir de otro modo, el uso indebido del DNS en relación con el nombre de dominio. Para determinar las medidas apropiadas, el operador de registro considerará las circunstancias específicas del caso, que pueden incluir un equilibrio entre el alcance del perjuicio y la victimización que provoca el uso indebido del DNS y la posibilidad de daños colaterales asociados. La importancia de los daños colaterales en la situación de dominios afectados descrita anteriormente para los registradores se aplica igualmente a los registros.

El operador de registro también considerará si él mismo, el registrador patrocinador y/u otra parte son las partes mejor preparadas para revisar y adoptar las medidas de mitigación apropiadas y proporcionadas. Por ejemplo, en el caso de un único Nombre registrado que se utilice para el uso indebido del DNS, el registrador puede ser la parte más indicada para revisar y abordar el uso indebido del DNS con su cliente. Del mismo modo, en el caso de sistemas afectados, el Titular del nombre registrado o el proveedor de alojamiento que mantiene el acceso administrativo a los sistemas afectados pueden estar en mejores condiciones para abordar los problemas, y el operador de registro debe remitirlos primero al registrador, dado que suspender el dominio aplicando clientHold o serverHold puede causar daños colaterales en el contenido benigno o

legítimo. Por otro lado, el operador de registro puede ser la parte más indicada para abordar amenazas a gran escala que abarcan a muchos titulares de nombres registrados o registradores, como los algoritmos de generación de dominios utilizados para propagar botnets.

Las medidas de mitigación que se adopten de inmediato deben ser razonablemente necesarias para lograr uno de los siguientes resultados: *contribuir a detener* o *impedir* que el Nombre registrado sea utilizado para el uso indebido del DNS. Como mínimo, el operador de registro debe:

1) Informar el o los Nombres registrados y proporcionar las pruebas pertinentes al Registrador o Registradores patrocinadores; o bien
2) Adoptar medidas directas sobre el o los Nombres registrados cuando el operador de registro lo considere apropiado.

Qué hace que una acción sea inmediata

Como se señaló anteriormente para los registradores, la acción de mitigación apropiada para mitigar o interrumpir una instancia de uso indebido del DNS variará en función de las circunstancias específicas.

En consecuencia, la cantidad de tiempo adecuada para investigar y adoptar medidas apropiadas también variará, por lo que es imposible prescribir una cantidad de tiempo fija para que una acción se considere "inmediata". En cambio, los operadores de registro deben demostrar una atención continua a las denuncias de nombres patrocinados que se utilizan para el uso indebido del DNS. La atención debe ser proporcional al perjuicio potencial que el uso indebido del DNS causa a las víctimas.

En consecuencia, en respuesta a una consulta de Cumplimiento Contractual de la ICANN, un operador de registro deberá explicar por qué las acciones fueron inmediatas teniendo en cuenta las circunstancias específicas. A continuación, Cumplimiento Contractual de la ICANN revisará la explicación y las circunstancias pertinentes para determinar caso por caso si las acciones fueron inmediatas. Los plazos de los ejemplos incluidos en el presente Documento de asesoramiento no son requisitos contractuales, sino que se incluyen únicamente a modo ilustrativo. El hecho de que un operador de registro se tome más tiempo en un caso concreto no es necesariamente una indicación de incumplimiento. Por el contrario, otras circunstancias pueden exigir que el operador de registro actúe con mayor rapidez, como los casos de amenazas a gran escala que puedan causar un daño inminente a una gran cantidad de usuarios finales. Se prevé que un operador de registro investigue y adopte medidas lo antes posible tras el intento razonable del operador de registro de confirmar un caso de uso indebido del DNS.

Los ejemplos que figuran a continuación ilustran las medidas de mitigación razonables adoptadas con prontitud para contribuir a impedir que el Nombre registrado se utilice para el uso indebido del DNS (Segundo escenario) y para contribuir a interrumpir el curso del uso indebido del DNS en relación con el Nombre registrado (Primer y tercer escenario). Estos escenarios contienen circunstancias fácticas específicas. En circunstancias diferentes, los operadores de registro individuales pueden adoptar medidas diferentes con duraciones de tiempo diferentes para contribuir a detener, o

interrumpir de otro modo, casos individuales de uso indebido del DNS. En todos los casos, los operadores de registro deben ser capaces de demostrar que cualquier enfoque adoptado cumple con los requisitos pertinentes de la Sección 4.2 de la Especificación 6 del RA.

Sección 3(b), Especificación 11 del RA

Esta sección se modificó para sustituir el término definido de uso indebido del DNS, tal como se establece en las enmiendas a la Especificación 6, Sección 4, para "amenazas a la seguridad".

Recapitulación – Ejemplos de cumplimiento por parte de los operadores de registro

Primer escenario: Un operador de registro recibió una notificación de una cooperativa de crédito (Example Credit Union) a través de su formulario web de uso indebido que indicaba que alguien había registrado el dominio <loginexamplecreditunion[.]TLD> hace seis días y la cooperativa de crédito alega que el dominio está involucrado en phishing.
La cooperativa de crédito proporciona una captura de pantalla que muestra una página web en el dominio que recopila credenciales de inicio de sesión.

Medidas de mitigación apropiadas: Siguiendo su proceso interno, el operador de registro procesa y revisa el informe en un plazo de dos días hábiles. Al concluir su investigación, el operador de registro determina razonablemente que el Nombre registrado se estaba utilizando para un uso indebido del DNS. Por lo tanto, el operador de registro interrumpe el curso del uso indebido del DNS y notifica y proporciona toda la información pertinente al registrador patrocinador. El operador de registro incluye una solicitud con un plazo para que el registrador investigue y tome las medidas de mitigación razonablemente necesarias para detener, o interrumpir de otro modo, el uso indebido del DNS. En el plazo establecido, el operador de registro puede confirmar que el registrador suspendió el Nombre registrado mediante la aplicación del código de estado de EPP clientHold.

Segundo escenario: Un organismo de cumplimiento de la ley (LEA) se pone en contacto con un operador de registro y proporciona pruebas de que una serie de dominios están, o estarán, implicados en un algoritmo de generación de dominios asociado a una botnet. La botnet involucra algunos Nombres registrados existentes, pero predominantemente dominios que aún no están registrados.

Medidas de mitigación apropiadas: En las seis horas siguientes a la conclusión de su investigación y a la confirmación razonable del uso indebido del DNS, el operador de registro contribuye a poner fin al uso indebido del DNS adoptando las medidas indicadas o acordadas con el organismo de cumplimiento de la ley. En este caso, el operador de registro ha acordado que para los Nombres registrados pertinentes, el registro delegará a otros servidores de nombres (por ejemplo, redirigir los servidores de nombres o pozo de captura) a solicitud del organismo de cumplimiento de la ley. El operador de registro también crea directamente los dominios para los que previamente los dominios no

registrados asociados con la botnet según lo solicitado por el organismo de cumplimiento de la ley. Teniendo en cuenta que la creación de dominios por parte del operador de registro normalmente requiere permiso a través de la Exención de respuesta de seguridad de la ICANN (SRW)[8]. El operador de registro también realizará una solicitud oportuna para obtener una exención contractual. No obstante, cabe señalar que una SRW también puede

[8] Encontrará información sobre las Exenciones de Respuesta de Seguridad en esta página.

solicitarse tan pronto como sea razonablemente posible después del hecho, y la organización de la ICANN podrá responder con una exención retroactiva si procede, para no retrasar el apoyo a la operación del organismo de cumplimiento de la ley[9].

Tercer escenario: Como parte de su análisis técnico en busca del uso indebido del DNS conforme a la Especificación 11(3)(b), un operador de registro descubre que una subpágina de un dominio se está utilizando para distribuir malware, mientras que el resto del sitio del dominio parece ser contenido legítimo o benigno. El nombre de dominio ha estado registrado tres años.

Medidas de mitigación apropiadas: En las tres horas siguientes a la determinación de que el Nombre registrado está siendo utilizado para el uso indebido del DNS y está afectado, el operador de registro contribuye a interrumpir el curso del uso indebido del DNS notificando y proporcionando toda la información pertinente al registrador patrocinador y realizando una solicitud de acción con un plazo determinado para que el registrador informe al respecto. A continuación, el registrador notifica directamente al registratario, que resuelve el problema actualizando su sistema de gestión de contenidos para eliminar el malware.

Investigaciones de la organización de la ICANN sobre el cumplimiento de la nueva Sección 3.18.2 del RAA y la Sección 4.2 de la Especificación 6 del RA

¿Qué constituiría una respuesta completa, conforme y bien fundamentada? El departamento de Cumplimiento Contractual de la ICANN exigirá el cumplimiento de los requisitos explicados en el presente Documento de asesoramiento a través del procesamiento de los reclamos externos, el monitoreo proactivo y las actividades de auditoría. Cuando el departamento de Cumplimiento Contractual de la ICANN recibe un reclamo, revisará las pruebas presentadas por el denunciante, así como toda la información pertinente disponible, para determinar si debe iniciarse un caso de cumplimiento con el registrador u operador de registro correspondiente. Ante la ausencia de pruebas suficientes que respalden un reclamo de uso indebido del DNS, Cumplimiento Contractual de la ICANN cerrará el caso como no válido. Entre otras cosas, esta revisión considerará si la información a disposición del registrador patrocinador directamente o a través de un revendedor, o el operador de registro, según corresponda, es suficiente para determinar razonablemente que el Nombre registrado se está utilizando para una o más formas de uso indebido del DNS. La revisión también tendrá en cuenta si había alguna información adicional

[9] Para obtener más información sobre cómo los registros pueden trabajar con los organismos encargados del cumplimiento de la ley y la ICANN para abordar los algoritmos de generación de dominios, consulte "Marco sobre algoritmos de generación de dominios asociados con malware y botnets," publicado por el Grupo de Trabajo sobre Seguridad Pública del Comité Asesor Gubernamental y el Grupo de Partes Interesadas de Registros de gTLD.

que proporcionó el denunciante en respuesta a las solicitudes de información o pruebas adicionales por parte del registrador u operador de registro.

Además, según corresponda y sea pertinente para el caso específico, el departamento de Cumplimiento Contractual de la ICANN: (1) revisará los datos pertinentes de acceso público que se muestran a través del Servicio de Directorio de Datos de Registración, por ejemplo, fecha de creación, estado(s) del EPP o información sobre servidores de nombres; y (2) realizará búsquedas en el DNS para determinar si los Nombres registrados denunciados se resuelven en el DNS. Cumplimiento Contractual de la ICANN también puede llevar a cabo su propia investigación y revisar información adicional pertinente sobre un Nombre registrado en particular que presuntamente esté involucrado en el uso indebido del DNS.

Al iniciar un caso de cumplimiento con un registrador u operador de registro en virtud de la Sección 3.18.2 del RAA o la Sección 4.2 de la Especificación 6 del RA, respectivamente, el departamento de Cumplimiento Contractual de la ICANN proporcionará una lista detallada de toda la información y los registros necesarios para evaluar el cumplimiento en lo que respecta a los Nombres registrados denunciados y las formas del presunto uso indebido del DNS.

En respuesta a un caso de cumplimiento, el registrador y el operador de registro deberán, como mínimo:

- Explicar cómo y por qué el registrador u operador de registro llegó a determinar que las pruebas obtenidas no eran recurribles, según corresponda. Por ejemplo, un registrador puede explicar que, después de revisar la información y los registros presentados por la parte denunciante, y a través de su investigación, el registrador no pudo verificar que el uso indebido del DNS estuviera teniendo lugar en relación con el o los Nombres registrados denunciados. Cumplimiento Contractual de la ICANN podrá solicitar al registrador u operador de registro que aclare cualquier discrepancia clara entre la explicación proporcionada y cualquier información y datos capturados por Cumplimiento Contractual de la ICANN durante el proceso de validación de los reclamos.
- Proporcionar una explicación detallada, respaldada por los registros pertinentes, de las medidas de mitigación específicas adoptadas, cuándo se adoptaron las medidas y cómo se consideró que las medidas adoptadas fueron inmediatas y razonablemente necesarias para detener o interrumpir o contribuir a detener o interrumpir, en lo que respecta a las circunstancias específicas del caso (incluida cualquier explicación aplicable relacionada con la desproporcionalidad de las acciones a nivel del DNS y los daños colaterales). Los requisitos para que el registrador proporcione esta información seguirán aplicándose en los casos en los que el registrador opte por delegar la investigación del informe de uso indebido del DNS en un revendedor. En dichos casos, el registrador conserva la obligación de demostrar el cumplimiento de la Sección 3.18 del RAA[10] explicando las medidas que adoptó, así como las medidas de cualquier otra parte delegada, como los

revendedores, y proporcionando los registros relacionados.

[10] Véase la Sección 3.12 de la RAA

Las políticas y requisitos contractuales de la ICANN se aplican dentro de los límites de las leyes y reglamentos aplicables a cada registrador y operador de registro. Para evitar cualquier duda, ni a los registradores ni a los operadores de registro se les exigirá ni se esperará que adopten ninguna medida que contravenga las leyes y normativas aplicables.

La información sobre cuándo, cómo y dónde presentar los reclamos ante Cumplimiento Contractual de la ICANN está disponible aquí.