# Guía sobre la Identificación y Mitigación de Colisiones de Nombres para Profesionales de Tecnología de la Información

1 de agosto de 2014
Versión 1.1

## Índice

# 1. Introducción

Luego de que los nuevos nombres de dominio de alto nivel entran en la raíz del DNS global, las organizaciones pueden ver que las consultas para resolver algunos de los nombres "internos" específicos de sus redes devuelven valores diferentes, lo que da a los usuarios y programas resultados distintos. Existen 2 cuestiones básicas: Los nombres "internos" que se están filtrando en la Internet global y los espacios de nombres privados que están definidos en conflicto con el espacio de nombres del DNS global.

La causa de tales resultados diferentes en una consulta al DNS que un administrador de red intentó resolver en forma local mediante la utilización de un espacio de nombres interno, ahora, está siendo resuelta mediante la utilización de los datos de los nuevos dominios de alto nivel en el DNS global. Bajo estas circunstancias, las consultas que nunca se habían previsto que dejaran la red interna ahora obtienen los resultados en el DNS global y éstos resultados son distintos. Como mínimo, los nombres filtrados que producen resultados diversos pueden ser molestos para los usuarios (por ejemplo, pueden causar un retraso en el acceso a las páginas web). También pueden presentar problemas de seguridad (como por ejemplo, correos electrónicos que se envían a destinatarios erróneos).

Este documento engloba las estrategias para la mitigación y prevención de los tipos más comunes de espacios de nombres privados utilizados por organizaciones. Este documento describe lo que una organización puede encontrar cuando los nombres internos se filtran al DNS global y específica prácticas recomendadas para su mitigación. La descripción y el asesoramiento que se detallan aquí están destinados a los profesionales de TI (administradores de red, administradores de sistema y personal del departamento de tecnología de la información) que comprenden en general cómo funciona el DNS y cómo funcionan sus propios sistemas de nombres internos. Los lectores que quieran conocer mejor el trasfondo deben consultar los documentos en el Anexo A. Aquellos lectores con inquietudes en relación a la seguridad deben consultar, en particular, los informes emitidos por el Comité Asesor de Seguridad y Estabilidad de la ICANN (SSAC).

La ICANN, la organización que administra los contenidos de la raíz del DNS global, ha preparado este documento con la ayuda de expertos en cuestiones de espacio de nombres para asistir a las organizaciones cuyos espacios de nombres privados pueden estar en conflicto con la raíz del DNS global. La ICANN ha publicado otros documentos que describen cómo se organiza el DNS global, cómo se incorporan nuevos nombres a la raíz del DNS, etc. El Anexo A del presente documento enumera las referencias a distintos tópicos para consulta. Además, la ICANN recientemente ha comenzado a asistir a las organizaciones que utilizan espacios de nombres privados para que sepan cuando esos espacios de nombres comenzarán a tener colisiones; esto se describe en la Sección 1. 4 y la Sección 6.

Nótese que, aunque este documento aborda medidas de mitigación para la colisión de nombres, sólo debate sobre los problemas que pueden encontrar las organizaciones cuando al momento de resolver nombres. No aborda otras cuestiones relacionadas con la operación del DNS global en sí mismo. Por ejemplo, los servidores de nombres raíz del DNS global siempre han sido inundados con consultas que nunca debían ser procesadas por el DNS global (véase *SAC 045* en el Anexo A), pero los servidores de nombres raíz siempre también siempre han contado con los recursos suficientes para poder abordar estas consultas adicionales. Este documento no ahonda en las cuestiones relacionadas con los servidores de nombres raíz. Sólo aborda las consecuencias de las consultas que se filtran de forma inadvertida en los servidores de nombres raíz del DNS global.

La ICANN ha desarrollado un sitio web que brinda material informativo referido a la colisión de nombres y que se encuentra disponible en http://www.icann.org/namecollision. La página también incluye un proceso para informar daños severos comprobables como consecuencia de las colisiones de nombres causadas por los nuevos Dominios genéricos de Alto Nivel (gTLD).

# *1. 1 Colisiones de Nombres*

El DNS global es un espacio de nombre jerárquico y los nombres en el DNS se componen de una o más etiquetas que componen un nombre completo. En la parte superior de la jerarquía se encuentra la zona raíz del DNS que contiene un conjunto de nombres, como, por ejemplo, `com`, `ru`, `asia`, etcétera; éstos son los TLD (dominios de alto nivel), por lo general denominados simplemente "los TLD". Un ejemplo de un nombre de dominio entero (a menudo denominado nombre de dominio completo o FQDN) podría ser `www.ourcompany.com`.

La mayor parte de los espacios de nombres privados son también jerárquicos. Existen tres clases principales de espacios de nombres privados:

- **Espacios de nombres que se ramifican fuera del DNS global** - Los espacios de nombres privados que se ramifican por fuera del DNS global tienen raíz bajo un nombre que se puede resolver en el DNS global, pero toda la estructura del directorio bajo ese nombre es administrada en forma local bajo nombres que los administradores de TI nunca deberían ver en el DNS global. Por ejemplo, consideremos un espacio de nombre privado con raíz bajo `winserve.ourcompany.com`:los nombres en ese espacio de nombres privado (`winserve`) son administrados por un servidor de nombres privados y no son visibles en el DNS global.

- **Espacios de nombres que utilizan sus propias raíces con TLD privados**-La raíz del espacio de nombres privado es una etiqueta única que no es un TLD global. Toda la estructura del directorio, inclusive la del TLD privado, es administrada por servidores de nombres privados que no son visibles en el DNS global. Por ejemplo, si el espacio de nombres privado tiene raíz en `ourcompany`, entonces los servidores de nombres privados también son responsables de`www.ourcompany`, `region1.ourcompany`, `www.region1.ourcompany`, etc. Existen muchos tipos diferentes de espacios de nombres que utilizan sus propias raíces con TLD privados. Los ejemplos incluyen el Directorio Activo de Microsoft (en algunas configuraciones), DNS *multicast* (RFC 6762) y servicios de directorio LAN más antiguos que aún se utilizan en algunos rincones de Internet.

- **Espacios de nombres que se crean mediante el uso de listas de búsqueda-** Una lista de búsqueda es una característica de un resolutor de nombres local (ya sea para un espacio de nombres privado o un resolutor recursivo para el DNS global). Una lista de búsqueda permite al usuario ingresar nombres más breves, según su conveniencia; durante la resolución, el servidor de nombres anexa nombres configurados a la derecha del nombre en una consulta. (Estos nombres configurados también se denominan sufijos).

Los espacios de nombres que se ramifican fuera del DNS global sólo causan colisiones de nombres cuando se combinan con listas de búsqueda. Toda consulta que implique un FQDN que provenga del DNS global, por definición, nunca tendrá una colisión de nombres con un nombre diferente en el DNS global. Tal consulta podría causar colisiones de nombres cuando, de forma inadvertida, se crea mediante el uso de listas de búsqueda.

El concepto de "espacios de nombres privados" confunde a muchas personas que se encuentran mayormente acostumbradas al uso común de Internet, es decir, personas que sólo están familiarizadas con la denominación del DNS global y que pueden sorprenderse al saber que algunas

solicitudes de resolución de nombres no resultan, o no deberían resultar, en una consulta al DNS global. Incluso pueden sorprenderse aún más al enterarse que ciertas consultas sobre nombres están intencionalmente creadas para iniciarse en el espacio de nombres privado, pero terminar en el DNS global. Una razón por la cual las colisiones de nombres pueden ocurrir es que las consultas destinadas a un servidor de nombres de un espacio de nombres privado se inicia de forma incorrecta en el DNS global.

## *1.2 Colisiones de Nombres a Causa de TLD Privados*

Las colisiones de nombres ocurren como resultado de dos eventos. En primer lugar, una consulta de un nombre de dominio completo que tiene raíz en un TLD privado se filtra de una red privada al DNS global. En segundo lugar, la consulta localiza en el DNS global exactamente el mismo nombre que existe en la red privada bajo el TLD privado.

Una causa común de tales colisiones de nombres es la utilización de un nombre en un sistema como el Directorio Activo de Microsoft que no es un TLD en el DNS global al momento que el tema se configura, pero es luego agregado al DNS global. Este tipo de colisión de nombres ya ha sucedido en muchas oportunidades anteriormente y se espera que continúe con la introducción de los nuevos TLD en el DNS global (véase Introducción al Programa de Nuevos TLD en el Anexo A).

## *1.3 Colisiones de Nombres a Causa de las Listas de Búsqueda*

Otra causa de colisiones de nombres es el procesamiento de listas de búsqueda. Si una consulta no es un FQDN, es un nombre de dominio breve e incompleto. Una lista de búsqueda contiene uno o más sufijos. Éstas son anexadas de forma interactiva a la parte derecha de la consulta. Cuando un resolutor no puede resolver un nombre de dominio breve e incompleto, anexa sufijos de la lista conforme intenta resolver el nombre hasta que se encuentra un nombre que coincide. Una lista de búsqueda es una característica útil; no obstante, el procesamiento legalista de búsqueda acomoda la utilización de nombre de dominio breve e incompletos que no son FQDN y por lo tanto crea, de forma inadvertida, espacios de nombres que no tienen raíz en el DNS global. En este caso, ocurre la colisión de nombres cuando una cadena de caracteres que el usuario intenta utilizar como nombre de dominio breve e incompleto es, por el contrario, completada por la lista de búsqueda y resuelta como un FQDN.

Por ejemplo, supongamos que un resolutor de nombres tiene una lista de búsqueda que consiste en los sufijos `ourcompany.com` y `marketing.ourcompany.com`. Además supongamos que el usuario ingresa `www` al programa que utiliza para resolver. El resolutor podría, entonces, buscar primero `www`,y sino devolviese un resultado, podría, entonces buscar `www.ourcompany.com` y `www.marketing.ourcompany.com`.

Nótese la utilización de la palabra "podría" en la descripción de este ejemplo. Las reglas sobre cómo se deben aplicar las listas de búsqueda cuando se realiza una resolución de un nombre varían según los sistemas operativos o las aplicaciones. Algunos sistemas siempre tratarán de resolver un nombre, ya sea en el espacio de nombres privados o en el DNS global, antes de aplicar una lista de búsqueda. No obstante, otros sistemas utilizarán la lista de búsqueda en primer lugar si la cadena de caracteres que se busca no contiene un caracter "`.`" Aun así, otros sistemas utilizarán la lista de búsqueda en si la cadena de caracteres que se busca finaliza con un caracter "`.`" Algunos sistemas operativos y aplicaciones (como por ejemplo los buscadores web) han cambiado sus reglas de lista de búsqueda en varias oportunidades. Por lo tanto, resulta poco práctico predecir cuándo las listas de búsqueda se utilizarán o no, qué es o no un nombre de dominio breve e incompleto, y por lo tanto, si esos nombres de dominio breves e incompletos tienen probabilidad de filtrarse en el DNS global. Véase *Inquietudes*

*sobre Nuevos gTLD: Nombres sin Punto y Colisiones de Nombres* en el Anexo A para obtener más información sobre la diversidad del procesamiento de listas de búsqueda.

Esta descripción de las listas de búsqueda puede sorprender a algunos lectores porque son muy comunes en lugares en los que, a primera vista, no parecen crear "espacios de nombres privados". Cada sufijo en una lista de búsqueda define otro espacio de nombres que puede ser consultado durante la resolución de un nombre. Esto crea un espacio de nombre privado que opera de forma confiable únicamente cuando un cliente consulta los resolutores particulares para este espacio de nombres. Dependiendo de la implementación de las listas de búsqueda, algunos resolutores de nombres pueden incluso probar el nombre de dominio breve e incompleto ingresado por el usuario o configurado en el software antes de anexar cualquiera de los nombres en la lista de búsqueda. Por ejemplo, escribir `www.hr` en un lugar en Internet podría arrojar un resultado desde el resolutor del DNS, pero al escribirlo en otra ubicación diferente puede dar un resultado distinto. Cuando esto sucede, uno de esos espacios de nombres es "privado" en relación al otro.

La utilización de listas de búsqueda en lugar de resolver FQDN mediante el DNS global contribuye a la incertidumbre en la resolución de nombres. Las colisiones de nombres producidas por las listas de búsqueda son difíciles de predecir porque estas listas son muy comunes. Son parte del mismo software resolutor en muchos sistemas operativos, equipos de red, servidores, etcétera. El software del resolutor actúa de manera diferente en un sistema o en otro, entre diferentes versiones de un mismo sistema operativo, e incluso como una función de la visualización del sistema operativo o de la aplicación de dónde, en la red, proviene la consulta. La implementación de un servicio de resolución de nombres que resuelva nombres mediante la utilización únicamente del DNS global es la mejor garantía contra tales incertidumbres y resultados impredecibles.

## *1.4 Asistencia en la Detección de Colisiones de Nombres en los Nuevos gTLD*

A partir del 18 de agosto de 2014 en adelante, cuando se delegue un TLD desde la zona raíz del DNS, el TLD deberá realizar un servicio de interrupción controlada durante 90 días. Durante el periodo de interrupción controlada, se envían respuestas, que se pueden identificar con facilidad, desde los servidores de nombres autoritativos para el nuevo gTLD para una variedad de consultas al DNS. El propósito de esta respuesta es alertar a las organizaciones que experimentarán colisiones de nombres que deben tomar acción inmediata a fin de prevenir un posible daño debido a las consultas infiltradas.

Además, a partir de dicha fecha, algunos gTLD que ya se encuentran en la zona raíz deberán realizar un servicio de interrupción controlada durante 90 días antes de delegar nombres de segundo nivel en el DNS global. El propósito aquí es el mismo que el mencionado anteriormente: alertar a las organizaciones que filtran consultas privadas sobre la necesidad de mitigar el posible daño a la mayor brevedad posible.

Nótese que las reglas sólo se aplican a los gTLD, no a los TLD que son para códigos de país (usualmente denominados "ccTLD"). Cuando se agrega un ccTLD a la zona raíz, su operador puede elegir realizar una interrupción controlada, pero no está obligado a hacerlo.

# 2. Problemas Causados por las Colisiones de Nombres

Las colisiones de nombres basadas en las consultas que se filtran al DNS global desde las redes privadas pueden tener muchas consecuencias no deseadas. Cuando una consulta obtiene una respuesta positiva, pero con una respuesta que proviene del DNS global en lugar del espacio de nombres privado, la aplicación que realiza la consulta intentará conectar con un sistema que no es parte de la red privada, y puede tener éxito. Dicha conexión podría ser una molestia (al producir un retraso durante la resolución de nombres). También podría resultar en una cuestión de seguridad, es decir, podría crear una vulnerabilidad que podría explotarse con fines maliciosos, dependiendo de lo que haga la aplicación luego de que se conecte.

## *2.1 Direccionamiento a Sitios Web no Esperados*

Supongamos que un usuario ingresa `https://finance.ourcompany`en un buscador web mientras se encuentra en una red privada y que la red privada tiene un espacio de nombres cuyo TLD privado es `ourcompany`. Si la consulta del buscador para el nombre`finance.ourcompany`se resuelve tal como se espera, el buscador obtiene una dirección IP para el servidor web interno del departamento de finanzas. Imaginemos, no obstante, que el TLD `ourcompany` es también parte del DNS global y que ese TLD posee un nombre de dominio de segundo nivel (SLD) `finance`. Si la consulta se filtra, se resolverá en una dirección de IP distinta de aquella a cuando la consulta se resolvió en un nombre de espacio privado. Ahora imaginemos que esta dirección de IP diferente podría alojar un servidor web. El buscador podría intentar conectarse a un servidor web en la Internet pública, no en una red privada.

Tal como se indicó anteriormente, el mismo problema puede suceder incluso en redes que no tienen TLD privados, pero que utilizan listas de búsqueda. Consideremos un buscador que se utiliza normalmente en una red donde los usuarios tienen una lista de búsqueda con el nombre `ourcompany.com`, y que los usuarios ingresan el nombre `www.finance` a fin de obtener el host `www.finance.ourcompany.com`. Ahora imaginemos que el buscador está siendo utilizado por un empleado desde un dispositivo móvil en una cafetería. Si esa consulta se filtra en Internet y existe un TLD llamado `finance`,la consulta podría resolverse en una dirección de IP diferente, por ejemplo un host totalmente diferente cuyo nombre en el DNS global sea `www.finance`. Dicha consulta haría que el buscador intente conectarse a un servidor web en una parte pública de Internet completamente diferente de la que lo hubiera hecho si la consulta hubiese ido al resolutor en la red privada.

Una respuesta al usuario común para este escenario es que el usuario reconocería que este es un sitio web erróneo y simplemente lo abandonaría inmediatamente. Sin embargo, un buscador puede exponer gran cantidad de información al servidor web si el buscador "confía" en el servidor web porque tiene el mismo nombre de dominio que el servidor que ha visitado anteriormente. El buscador puede automáticamente ingresar datos de registro u otros datos confidenciales y, por lo tanto, exponer esta información a la captura o el análisis por fuera de la organización. En otras circunstancias (por ejemplo, un ataque cuidadosamente formulado en contra de la organización), el buscador podría conectarse a un sitio que aloje códigos maliciosos que instalen programas peligrosos en la computadora.

Nótese que el uso del TLS y certificados digitales podría no ayudar a evitar el daño debido a las colisiones de nombres; en realidad, podría empeorarlo al brindar a los usuarios un falso sentido de seguridad. Muchas de las autoridades de certificados (CA) que emiten certificados para nombres en el DNS global también emiten certificados para nombres de dominio breves e incompletos en espacios

de direcciones privados, de modo que es posible que un usuario que es direccionado de manera errónea a un sitio web aún vea un certificado válido. Véase el documento SAC 057 en el Anexo A para más información sobre los certificados con nombres de espacios de nombres privados.

## *2.2 Direccionamiento de Correo Electrónico a Destinatarios Erróneos*

Las consecuencias posibles que surgen a partir de la colisión de nombres no se limitan a los buscadores web. Un correo electrónico dirigido a un destinatario puede enviarse a otro destinatario si los nombres del host en las direcciones del destinatario son las mismas; por ejemplo, un correo electrónico para `chris@support.ourcompany` podría enviarse a una cuenta de usuario totalmente diferente si`ourcompany` se transforma en un TLD en el DNS global. Incluso si el mensaje no se envía a un usuario de correo electrónico en particular, puede existir un intento de enviarlo y dichos intentos podrían exponer el contenido del correo electrónico a que sea capturado o analizado fuera de una organización.

Muchos dispositivos de red como, por ejemplo, los firewall, enrutadores e incluso impresoras pueden configurarse para enviar notificaciones o datos de registro por correo electrónico. Si el nombre del destinatario que se ingresó para las notificaciones de correo electrónico luego está sujeto a una colisión de nombres en el DNS global, la notificación podría enviarse a un destinatario completamente diferente. Los datos del evento o registro en el cuerpo del mensaje que pueden revelar la configuración de la red o la conducta del host podrían filtrarse hacia un destinatario no deseado. El rendimiento de la red de rutina o el análisis del tráfico por parte del personal de TI podría interrumpirse si el destinatario deseado nunca recibe los datos de registro, o los eventos que desencadenaron las notificaciones no se pueden investigar o mitigar.

## *2.3 Reducciones en materia de Seguridad*

Los incidentes de colisiones de nombres que no son mitigados pueden exponer a los sistemas en las redes privadas a una conducta no deseada o daño. Los sistemas que confían en la resolución de nombres para la correcta operación y que también realizan funciones de seguridad pueden funcionar de manera confiable cuando utilizan FQDN y los resuelven desde el DNS global.

Por ejemplo, en los firewalls, las reglas de seguridad, a menudo, se basan en el origen o destino del flujo de paquetes. El origen y destino de los paquetes son direcciones de IPv4 o IPv6, pero muchos firewalls, permiten que se los ingrese como nombres de dominio también. Si los nombres de dominio breves e incompletos se utilizan y no se realiza la resolución de nombres como se espera, las reglas pueden no bloquear o permitir el tráfico como el administrador deseado. De manera similar, los registros de firewalls generalmente utilizan nombres de dominio y la utilización de nombres de dominio breves e incompletos que se resuelven de forma impredecible pueden interferir con el control de los eventos, análisis o respuesta. El personal de TI que analiza estos registros podría, por ejemplo, malentender la severidad de un evento ya que un nombre de dominio breve e incompleto en el registro podría identificar diferentes hosts dependiendo de donde se creó el archivo de registro (es decir, en el archivo de registro, el mismo nombre de dominio breve e incompleto podría aparecer asociado con dos o más direcciones de IP diferentes). Este problema puede complicarse por el hecho de que la mayoría de los firewalls pueden actuar como sus propio resolutores de DNS o permitir a los administradores utilizar o configurar listas de búsqueda.

## *2.4 Sistemas Afectados por las Colisiones de Nombres*

Todo sistema relacionado a una red debería verificarse en relación al uso de nombres del host que tienen raíz en un TLD privado o nombres del host que se basan en listas de búsqueda. Todas estas instancias "de uso" tendrán que ser actualizadas para utilizar un FQDN del DNS global. Una lista no exhaustiva de sistemas o aplicaciones a verificar incluiría:

- **Buscadores**- Los buscadores web permiten a los usuarios especificar la ubicación de los *proxies* HTTP y éstos se encuentran generalmente en las redes privadas. Verificar si un usuario o personal de TI ha creado páginas de inicio personalizadas, marcadores o motores de búsqueda: éstos pueden tener enlaces a servidores en la red privada. Algunos buscadores también poseen opciones de configuración respecto de dónde obtener información de revocación sobre certificados SSL/TLS que podrían apuntar a nombres del host en la red privada.

- **Servidores Web** -Los servidores web ofrecen contenido HTML que posee enlaces y meta datos incluidos en los nombres del host. Verificar si los servidores web en una red privada poseen contenido con nombres de dominio breves e incompletos. Verificar si los archivos de configuración para el servidor web tienen nombres de dominio breves e incompletos de otros hosts en la red privada.

- **Agentes Usuarios de Correo Electrónico-** Los clientes de correo electrónico como Outlook y Thunderbird poseen todos opciones de configuración respecto de a dónde recibir un correo electrónico utilizando protocolos POP o IMAP y donde enviar correos electrónicos mediante el protocolo SUBMIT; todos éstos pueden utilizar nombres del host en la red privada. Verificar si estas aplicaciones están configuradas para obtener información de revocación sobre los certificados SSL/TLS de los nombres de dominio breves e incompletos asignados a los hosts.

- **Servidores de Correo Electrónico**- Verificar si los servidores de correo electrónico tienen configuraciones que enumeren los nombres de dominio breves e incompletos de otros hosts locales, como por ejemplo, puertas de accesos de correo electrónico con copia de seguridad, servidores de almacenamiento fuera de línea, etcétera.

- **Certificados**-Verificar si las aplicaciones emplean certificados X509, tales como programas de telefonía y mensajería instantánea, poseen datos de configuración que utilizan nombres de dominio breves e incompletos para identificar dónde obtener la información de revocación sobre los certificados SSL/TLS.

- **Otras Aplicaciones**-Las aplicaciones personalizadas pueden tener parámetros de configuración donde se podrían almacenar los nombres del host. El espacio más obvio sería los archivos de configuración, pero los nombres del host podrían aparecer en muchos tipos de datos de aplicaciones, enlaces a las redes sociales o sitios Wiki, o incluso código duro en código fuente. Verificar los siguientes datos de configuración para los nombres de dominio breves e incompletos.

- **Dispositivos de Red**-Verificar los dispositivos con infraestructura de red-firewalls, información en materia de seguridad y sistemas de gestión de eventos (SIEM), enrutadores,interruptores, dispositivos para el monitoreo de redes, sistemas de prevención o detección de intrusiones, servidores VPN, servidores de DNS, servidores DHCP, servidores de registro-para determinar si están configurados con nombres de dominio breves e incompletos de otros dispositivos en la red privada.

- **Administración de Clientes**-Verificar si las herramientas de administración de clientes centralizadas, como por ejemplo aquellas que configuran estaciones de trabajo de una organización y dispositivos de red, poseen nombres de dominio breves e incompletos en su configuración (particularmente listas de búsqueda) que son controladas y reiniciadas por los sistemas.

- **Dispositivos Móviles-**Los dispositivos de los consumidores tales como teléfonos y tabletas tienen opciones de configuración similares a alguna de las aplicaciones mencionadas anteriormente y, por lo tanto, posiblemente posean opciones de configuración que podrían contener nombres de dominio breves e incompletos de la red local.

Todos estos sistemas deberían verificarse para corroborar los datos de configuración que almacenan nombres de dominio breves e incompletos a fin de asegurar que dichos nombres puedan cambiarse cuando cambie la raíz del espacio de nombres privado o cuando ya no se utilicen las listas de búsqueda.

# 3. Cuándo Implementar Medidas para Mitigar las Colisiones de Nombres

A veces, los nombres se agregan a la zona raíz del DNS global, como por ejemplo cuando cambia el nombre de un país o cuando la ICANN delega un nuevo TLD.  Ambas clases de dominios de alto nivel se han agregado casi todos los años durante más de dos décadas. Se han agregados nuevos TLD en 2013 y 2014 y ciertamente se agregarán más en los próximos años.

La historia nos dice que ciertas colisiones de nombre sucedieron cuando se agregaron TLD al DNS. También señala que los nombres de los espacios de nombres privados se han filtrado durante varios años, en algunos casos, con una frecuencia muy alta; véase el documento SAC 045 en el Anexo A para más información. La historia demuestra que los espacios de nombres y la resolución de nombres destinada para las redes privadas nunca son segregadas tan detalladamente como creen los administradores y que las consultas de nombres que los administradores intentan resolver mediante servidores de nombres internos son, por el contrario, a veces enviadas a los resolutores en el DNS global.

Los administradores de red a menudo realizan elecciones de nombres sobre la base de sus suposiciones de que la lista de nombres en la raíz del de DNS global es inmutable, pero dicha lista en realidad ha cambiado y lo seguirá siendo a lo largo del tiempo. Por ejemplo, cuando el TLD `cs`se agregó hace casi 25 años para el país Checoslovaquia, muchas universidades utilizaban listas de búsqueda que permitía al usuario ingresar un nombre con terminación `cs`para el departamento de Informática que calificaría completamente con el nombre de dominio de la Universidad y estas decisiones resultaron en una incertidumbre en la resolución de nombres cuando se agregaba el nuevo TLD en la zona raíz porque los nombres que finalizaban en `cs`, ahora, eran FQDN en el de DNS global. Incluso cuando los actuales nombres en la raíz del DNS global, generalmente, no se superponen con aquellos en el espacio de nombres privado (ya sea un TLD privado o lista de búsqueda), los administradores de red, por lo general, olvidan actualizarse en relación a los nombres que se encuentran en la raíz del DNS global.

Se recomienda que el departamento de TI comience con los esfuerzos de mitigación tan pronto como sea factible. Adoptar una postura de "sólo tendremos que mejorar nuestro firewall" puede reducir algunas colisiones, pero nunca las erradicará por completo. De igual modo, decir "nos aseguraremos de que nuestros usuarios utilicen nuestros servidores de nombre" o "haremos que los trabajadores remotos utilicen VPN", probablemente reduzca algunas colisiones, pero esto podría hacer que las colisiones restantes sean más difíciles de diagnosticar.

Las colisiones de nombres pueden ocurrir independientemente de los caracteres en el nombre; no obstante, el uso de caracteres no ASCII como por ejemplo `ä` y `中` y `й` en TLD privados complica el análisis de las colisiones.  Los resolutores pueden enviar consultas para éstos de manera que sean difíciles de predecir y pueden no coincidir con los estándares de Internet, de modo que determinar cuándo ocurrirá una colisión de nombres se torna mucho más dificultoso.

Aunque la raíz del DNS global terminará siendo más grande de lo que ha sido en los últimos años, la adición de nombres a la raíz realmente no es tan inusual. Para cada nuevo TLD que se agrega, existe una posibilidad de que haya una colisión de nombres con los espacios de nombres privados que se han estado filtrando en Internet, en su mayoría, sin ser notados. Las organizaciones han estado utilizando nombres y han asumido el riesgo de colisiones durante años.

Nótese que el agregado de nuevos nombres a la raíz del DNS no es, y nunca será, un problema para las organizaciones que utilizan FQDN del DNS global en sus redes. Estas organizaciones no verán diferencia en el uso de sus propios nombres de DNS porque no hay colisiones de nombres. Los problemas sólo surgen para aquellas organizaciones que utilizan TLD privados u organizaciones que utilizan listas de búsqueda que permiten la entrada de nombres de dominio breves e incompletos cuando el nombre abreviado, en sí mismo, podría ser un nombre válido en el DNS global.

## *3.1. Determinación de la Posibilidad de Colisiones*

A fin de poder determinar si habrá colisiones de nombres o no con el espacio de nombres privados de su organización, es necesario identificar y catalogar todos los espacios de nombres privados y listas de búsqueda de DNS que utiliza su organización y luego compilar una lista de nombres de alto nivel en estas fuentes. Para la mayoría de las organizaciones, básicamente existe sólo un espacio de nombre con sólo un nombre de alto nivel, pero algunas organizaciones, en particular aquellas que se han combinado con otras que también utilizaban espacios de nombres privados (por ejemplo, como resultado de una fusión comercial o adquisición) poseen múltiples nombres de alto nivel privados.

Luego, es necesario determinar tanto los contenidos actuales como los esperados de la zona del DNS global. Los nombres en la zona raíz actual para el DNS global se pueden encontrar en http://data.iana.org/TLD/tlds-alpha-by-domain.txt Para determinar si un nombre de un espacio de nombres privados se considera para distribución mediante el actual programa de nuevos gTLD:

1. Véase https://gtldresult.icann.org/application-result/applicationstatus
2. Hacer clic en la flecha en la columna "cadena de caracteres"
3. Desplácese por las páginas hasta encontrar el rango que contiene el nombre de su espacio de nombres privado

Si hay alguna superposición entre la lista de TLD privados que usted acaba de hacer y la lista de nombres en la zona del DNS, existe la posibilidad de que haya colisiones de nombres y, por lo tanto, se requieren medidas de mitigación.

Nótese que luego de que la ronda actual de nuevos TLD se ingrese en la zona raíz, se pueden proponer más; en particular, la lista de nuevos TLD puede cambiar y es posible que ocurran colisiones de nombres entre los espacios de nombres privados y los futuros nuevos TLD. También, las organizaciones con TLD privados que consisten en dos caracteres (como por ejemplo `ab`) deberían tener en cuenta que los nombres de dominio de alto nivel de dos caracteres están reservados para su uso como código de país y que se agregan a la zona raíz mediante un procedimiento totalmente diferente.

## *3.2 gTLD del DNS Global cuya Delegación se Demora Indefinidamente*

La ICANN ha señalado que demorará de forma indefinida la delegación de tres TLD: .corp, .home y .mail. Estos gTLD aún se encuentran aún en uso común en los espacios de nombres privados y, por lo tanto, representan un riesgo significativamente mayor de colisiones que otros TLD. No se garantiza que esta demora sea para siempre, de modo que toda organización que utilice uno de los nombres como espacio de nombres privado debe todavía cumplir las directivas señaladas en la Sección 4 o Sección 5 para la mitigación en el espacio de nombres privado. No obstante, dichas organizaciones tienen mucho más tiempo para realizar la mitigación que otras organizaciones que han utilizado un nombre diferente que podría aparecer en la raíz del DNS global en un futuro predecible.

# 4. Pasos para Mitigar los Problemas Asociados con un TLD Privado

Durante décadas, la utilización de TLD privados no se ha recomendado como buena práctica. En realidad las instrucciones que vienen con los productos de Servidor y Directorio Activo de Microsoft han explícitamente no recomendado el uso de TLD privados durante muchos. La formas de mitigación más efectiva para las colisiones de nombres debido a nombres que terminan filtrándose desde un TLD privado al DNS global consiste en pasar de la utilización de un TLD privado a uno que tenga raíz en el DNS global.

Los pasos mencionados en esta sección se aplican a toda red que, por sus propias razones, haya elegido utilizar un TLD privado como su raíz y utilizar listas de búsqueda para resolver los nombres de dominio breves e incompletos en lugar de colocar su raíz en el espacio de nombres en el DNS global y consultar al DNS global para la resolución de sus FQDN. Esta sección se aplica a toda organización que utilice un TLD privado, no solamente aquellos que ya están filtrando consultas de nombres en Internet global. Si su organización utiliza lo que usted percibe como un TLD privado "seguro", es decir, un nombre cuya delegación en la raíz del DNS global ya no se solicita o aprueba, debería, aún así, considerar seriamente cambiar a un nombre con raíz en el DNS global. Si trabaja en una gran organización con más de un TLD privado (como por ejemplo una compañía que se ha fusionado con otra y que no han fusionado sus dos espacios de nombres ), se deben realizar los pasos establecidos en esta sección para cada TLD privado.

Las posibilidades son que cuando una organización elige utilizar un TLD privado, lo haya hecho con una convención de nombres particular en mente. Los pasos aquí establecidos pueden estar en conflicto con ese modelo original.  A fin de mitigar de manera confiable el problema asociado con las colisiones de nombre debido a TLD privados, es necesario que los usuarios y sistemas cambien la forma en la que utilizan los nombres de dominio y los servidores de nombres locales tienen que ser re-configurarlos de una manera que a ciertos usuarios puede resultarles no conveniente. Utilice las explicaciones de las consecuencias no intencionales o no deseadas que pueden afectar a su organización a fin de conscientizar y fomentar la aceptación entre su comunidad de usuarios.

**Nota importante:** Simultáneamente, conforme se implementan los pasos establecidos en esta sección, probablemente también necesitará mitigar colisiones de nombres causadas por las listas de búsqueda, lo que se explica en la Sección 5. Muchos de los pasos en dicha sección son los mismos que éstos y se pueden realizar al mismo tiempo.

## *4.1. Monitorear las solicitudes que provienen de servidores de nombres autoritativos*

A fin de mitigar los problemas con un TLD privado, enumere todas las computadoras, equipos de red y cualquier otro sistema que utilice el actual TLD privado en cualquier solicitud. Cuando cambie los nombres que se utilizan, todos los dispositivos que usan nombres privados antiguos de manera automática tendrán que ser actualizados

Existen tres formas comunes de realizar esta supervisión y enumeración de sistemas:

- El servidor de nombres autoritativo (como por ejemplo Directorio Activo) pueden tener una función de registro. Active la función de registro para recabar detalles de todas las consultas para los nombres privados.

- Muchos firewalls modernos pueden también configurarse para detectar y registrar las consultas para nombres privados. Esto puede no ser tan efectivo como registrarse a partir del sistema de nombres en sí mismo, dependiendo de la topología de su red. Por ejemplo, si una consulta no atraviesa el firewall, este no puede verla y por lo tanto se perderá.

- Si nada de lo anteriormente expresado se puede utilizar, supervise y recabe el tráfico enviado al servidor de nombres autoritativo y emitido por éste mediante la utilización de un programa de captura de paquetes, como por ejemplo, Wireshark. Sin embargo, este método requiere que la captura de datos se procese con un programa a fin de encontrar las consultas para sólo los nombres privados.

Algunas organizaciones optarán (y deberían hacerlo) por implementar más de una de las sugerencias antes mencionadas para incrementar las posibilidades de hallar todas las solicitudes Nótese que este paso puede producir resultados confusos. Los dispositivos tales como las computadoras y teléfonos poseen aplicaciones en las cuales los usuarios escriben nombres; estos dispositivos aparecerán en la encuesta incluso aunque no haya ninguna versión almacenada de los antiguos nombres privados. Para este paso, sólo es necesario saber todos los lugares en su red donde el antiguo nombre privado se almacenaba y era utilizado para las aplicaciones.

## *4.2. Crear un inventario de cada sistema que utiliza el TLD privado de manera automática*

Necesita un resumen de los datos de registro obtenidos en el paso anterior. Este resumen debe ser una lista de todos los dispositivos y todos los nombres consultados en lugar de todas las instancias en las cuales el dispositivo efectúa una búsqueda. La razón por la cual se requieren todos los nombres que se consultan es que ciertos dispositivos tendrán múltiples aplicaciones que deberán ser adaptadas. En consecuencia, el resumen debe incluir todos los sistemas y todas las aplicaciones en cada sistema que utilizan el TLD privado. Este resumen se transforma en un manifiesto para los dispositivos que se deben cambiar.

## *4.3. Determinar dónde se administran los nombres del DNS global*

Es probable que ya tenga un nombre de DNS global para su organización y que el nombre de dominio pueda utilizarse para la raíz de su espacio de nombres privado. Es necesario determinar quién está a cargo de los nombres de DNS y qué procesos utilizan para crear y actualizar los nombres en el DNS. Esto puede realizarse dentro de su departamento de TI o mediante un proveedor de servicios (por lo general, la misma compañía que provee la conectividad a Internet).

## *4.4. Cambiar la raíz de su espacio de nombres privado para utilizar un nombre del DNS global*

Una estrategia común para utilizar un nombre del DNS global como raíz de su espacio de nombres privados es tener un nombre públicamente accesible delegado del DNS global, pero luego utilizar el servidor de nombres autoritativo existente para administrar todos los nombres que dependen de él. Por ejemplo, si su compañía posee el nombre de dominio global `ourcompany.com`, podría elegir `ad1.ourcompany.com` como el nombre raíz.

Si su organización cuenta con más de un nombre de dominio en el DNS global, debería colocar sus nombres en una raíz que sea más fácilmente accesible por el personal de TI en su organización. En

algunos casos,otras entidades controlan los nombres adicionales, como por ejemplo el departamento de marketing.  Si es posible, es mejor colocar el nombre en una raíz bajo un nombre sobre el cual tenga control el departamento de TI.

Los pasos para efectuar este cambio dependen del software del servidor de nombres privado que se tenga, la versión específica de dicho software, la topología de los servidores de nombres en su red privada y la configuración existente del servidor de nombres. Estos detalles están más allá del alcance de este documento, no obstante, deberían estar contenidos en las instrucciones del proveedor del sistema actual.  También, en muchas organizaciones, este cambio requerirá autorización de parte de algunos niveles de administración, en particular, si la administración del nombre del DNS global difiere de la administración del espacio de nombres privado

Como parte de este paso, si posee certificados para cualquier host que utilice nombres en el espacio de nombres privado, será necesario crear certificados para estos hosts mediante la utilización de nuevos nombres (completos). Los pasos para la obtención de estos certificados dependen de su CA y, en consecuencia, se encuentran fuera del alcance del presente documento

## *4.5. Asignar nuevas direcciones de IP para hosts, si es necesario*

Si posee certificados TLS que se basen en el nombre del TLD privado antiguo, será necesario obtener nuevos certificados para los nuevos nombres. Si su servidor web no admite la extensión de la Indicación del Nombre del Servidor (SNI) a TLS que permiten servir más de un nombre de dominio bajo el TLS en la misma dirección IP, será necesario agregar direcciones de IP al host para que el host admita el nombre privado antiguo en la dirección de IP original y el nuevo nombre en la nueva dirección de IP. De forma alternativa, puede actualizar el software del servidor web a una versión que admita las extensiones SNI correctamente.

## *4.6. Crear un sistema para monitorear la equivalencia entre los nombres privados nuevos y antiguos*

Cuando cambia todos los nombres privados para utilizar la nueva raíz, continuará designando direcciones y registrando consultas para sus nombres privados antiguos a fin de verificar aquellos sistemas que no se encuentran en el inventario y que no fueron actualizados para la utilización de nombres con raíz en el DNS. Debido a esto, es necesario asegurarse que los nombres privados nuevos y antiguos tengan los mismos valores para las direcciones de IP.

Cierto tipo de software de espacio de nombres privado le permite mantener dos árboles en paralelo, pero si posee un software más antiguo o servidores de nombres autoritativos múltiples, es probable que tenga que realizar el monitoreo de las equivalencias con herramientas personalizadas. Estas herramientas personalizadas requieren consultar todos los nombres en el espacio de nombres antiguo y de nombres generalmente y alertarlo en caso de que exista una falta de coincidencia para que pueda determinar qué sistema cambió sin un cambio paralelo en el otro sistema.

Si fue necesario añadir direcciones de IP en el paso anterior por tener certificados SSL / TLS, es necesario permitir la falta de coincidencia mediante el software de monitoreo de equivalencias.

## *4.7. Capacitar usuarios y administradores de sistema para utilizar el nuevo nombre*

Además de cambiar los sistemas en los cuales los nombres se ingresan en configuraciones, es necesario cambiar las formas de pensar de los usuarios a fin de que cambien de los antiguos nombres privados a los nuevos. Esta capacitación debería realizarse antes de implementar los siguientes pasos para que los usuarios tengan la posibilidad de acostumbrarse a los nuevos nombres, pero dicho entrenamiento debería dejar en claro que se acerca el cambio y que se debería comenzar a pensar en términos de los nuevos nombres. También es una buena oportunidad para capacitar a los usuarios en relación a la utilización de FQDN. Utilice las explicaciones de las consecuencias no intencionales o no deseable que pueden afectar a su organización a fin de crear consciencia y fomentar la aceptación.

## *4.8. Cambiar todo sistema afectado a los nuevos nombres*

Este es el punto donde la mitigación de los nombres privados antiguos a los nuevos se materializa para todos los sistemas (PC, dispositivos de red, impresoras, etc.) en la red. Los nombres privados se reemplazan por los nuevos nombres del DNS sistema por sistema. Se busca toda instancia del antiguo nombre privado en todo el software del sistema y se reemplaza por el nuevo nombre del DNS. Al mismo tiempo, deberá eliminar el uso de los nombres de dominio breves e incompletos en las listas de búsqueda.

El monitoreo que se comenzó anteriormente es excepcionalmente importante en este paso. Es poco probable que pueda determinar todas las aplicaciones en todos los sistemas que posean nombres privados, antiguos incorporados en las mismas. Por el contrario, se debe consultar el sistema de monitoreo luego de que se cambie cada sistema para determinar si el sistema todavía realiza solicitudes para los nombres privados, antiguos.

Muchos sistemas ejecutan algunas aplicaciones de inicialización cuando se activan por primera vez. Estas aplicaciones pueden tener nombres de sistemas incorporados en ellas y encontrarlos puede ser dificultoso. Luego de cambiar todos los nombres en un sistema de nombres privados antiguos a nombres nuevos de DNS, reinicie el sistema y utilice el software de monitoreo para supervisar las búsquedas de nombres. Si el sistema busca algún antiguo nombre privado, es necesario que determine cuál es el software que da origen a dicha solicitud y que lo cambie para utilizar los nuevos nombres.  Este proceso puede requerir algunos reinicios a fin de configurar completamente un sistema de forma correcta.

## *4.9. Comenzar a monitorear el uso de nombres privados en el servidor de nombres*

Debe configurar su servidor de nombres autoritativo para comenzar a monitorear todas las solicitudes de nombres que tengan la antigua raíz. Dado que sus usuarios ya no deberían utilizar estos nombres, el archivo de registro creado en el paso de supervisión puede no ser demasiado extenso; si lo es, tendrá que repetir algunos de los pasos antes mencionados en el caso de ciertos sistemas particulares en su red.

## *4.10. Configuración del monitoreo a largo plazo en los perímetros para buscar nombres privados, antiguos*

Con los pasos anteriores se deberían haber encontrado la mayor parte de los usos de nombres privados antiguos, sin embargo, los sistemas pueden aún estar utilizando algunos (posiblemente importantes) nombres privados antiguos, pero tal vez sólo en raras ocasiones. Una manera de detectar estas consultas es incorporar reglas a todos los firewalls en el borde de la red para buscar todas las consultas que se están filtrando. Estas reglas deberían tener una prioridad alta asociada a las mismas y se deberían configurar para generar notificaciones de eventos de modo tal que el personal de TI reciba la alerta oportunamente. Por otra parte, también podría hallar estos eventos en los archivos de registro del firewall, pero hacer esto tendría una mayor posibilidad de no detectarlo. Las alertas que se disparan cuando aparece una solicitud permitirán al personal detectar estos eventos afortunadamente ocasionales en la actualidad. Algunos firewalls sólo admiten este tipo de regla mediante la adición de funcionalidades adicionales a un costo extra; si este es el caso de su firewall, deberá evaluar si el beneficio de encontrar estas solicitudes dispersas merece el costo adicional.

## *4.11. Cambiar todos los nombres de la antigua raíz para que apunten a una dirección que no funcione*

Luego de haber entrenado a los usuarios, la forma más efectiva de asegurar que dejarán de utilizar los nombres privados antiguos antes de eliminarlos es hacer que todos esos nombres privados antiguos apunten a un servidor esté configurado para no responder a ningún tipo de servicio de solicitudes. Esto también contribuirá a eliminar todo sistema que todavía utilice el espacio de nombres antiguo y que no haya sido detectado en los pasos anteriores.

La dirección a la que se apunte debería ser un servidor que con seguridad no ejecute ningún servicio. Al hacer esto, no hay posibilidad de que ningún sistema que utilice un nombre privado antiguo obtenga información errónea y que las aplicaciones informen errores que deberían ser detectados o comprendidos con facilidad por los usuarios; como parte de esta capacitación informativa, puede recomendar a los usuarios que informen todos los errores de este tipo al departamento de TI. Conforme se implementa este paso, el sistema de monitoreo que busca equivalencias entre los nombres nuevos y antiguos (descritos anteriormente) necesita actualizarse con los cambios.

Los nombres se deben cambiar uno a la vez, probablemente con, al menos, algunas horas entre cada cambio o grupo de cambios. Es probable que este paso requiera al departamento de TI, de modo que organizar los cambios contribuirá a equilibrar la carga de llamadas conforme los nombres que aún estaban en uso dejen de funcionar.

## *4.12. Si los certificados fuesen emitidos para cualquier host bajo nombres privados antiguos, revocarlos*

Si su organización tuviese certificados SSL/TLS emitidos por cualquier servidor en su red que utilice nombre privados antiguos, dichos certificados se deberán revocar. Esto resulta bastante sencillo de realizar si su organización actúa como su propia CA. Si utilizara una CA comercial para emitir certificados para el espacio de nombres privado, necesitará determinar el proceso de dicha CA para solicitar la revocación; las CA diferentes podrían tener requisitos distintos para cada solicitud.

## *4.13. Operaciones a Largo Plazo con el Nuevo Nombre*

Nótese que el nombre privado antiguo y los dominios relacionados aún se encuentran en el servidor y continuarán así mientras ejecute el servidor de nombres. No hay razón para eliminarlos y, en muchos sistemas, como por ejemplo Active Directory, puede ser difícil eliminar el primer nombre que se configuró en el sistema.

En realidad, existe una buena razón para dejar el nombre así: esto le permite ver si hay indicios residuales del antiguo nombre privado en los sistemas de su red. Siempre y cuando todas las direcciones asociadas con todos los nombres bajo el TLD privado apunten a un host donde no se ejecuten servicios, puede utilizar ambos archivos de registros del servidor de nombres (y, para beneficio adicional, un sistema que registra todo el tráfico al servidor) para determinar un exacto fue en la eliminación del antiguo nombre privado.

# 5. Pasos para Mitigar las Colisiones de Nombres asociadas con las Listas de búsqueda

A fin de mitigar de manera confiable estos problemas asociados con las colisiones de nombres debido a las listas de búsqueda, los usuarios y sistemas necesitan cambiar la forma en la que utilizan sus nombres de dominio. Puede resultar de utilidad preparar a los usuarios por adelantado mediante las notificaciones de cambio, programas de concientización y de capacitación.

Nótese que si se está efectuando una administración centralizada, estas acciones resultan probablemente menos dificultosas de lo que podría imaginar. Mucha gente que normalmente utiliza listas de búsqueda sabe que también pueden escribir nombres completos si es necesario (como si estuviesen accediendo a un servidor por fuera de la red privada de la organización) y necesitará menos capacitación que aquellos que sólo comprenden los nombres de domino breves e incompletos.

## *5.1. Supervisar las solicitudes que ingresan al servidor de nombre*

A fin de mitigar los problemas ocasionados por las listas de búsqueda, es necesario conocer todas las computadoras, equipos de red y cualquier otro sistema que utilizan listas de búsqueda en cualquier solicitud. Será necesario actualizar todos los dispositivos que utilizan listas de búsqueda de forma automática.

Existen tres formas comunes de realizar esta supervisión y enumeración de sistemas:

- El servidor de nombres recursivo (como por ejemplo Active Directory) puede tener una funcionalidad de registro y usted puede activarla para obtener los detalles de todas las consultas que poseen nombres de dominio breves e incompletos.

- Muchos firewalls modernos pueden también configurarse para detectar y registrar las consultas de todos los nombres. Esto puede no ser tan efectivo como registrarse a partir del sistema de nombres en sí mismo, dependiendo de la topología de su red. Por ejemplo, si una consulta no atraviesa el firewall, este no puede verla y por lo tanto se perderá.

- Si nada de lo anteriormente expuesto se puede utilizar, el servidor de nombres puede monitorearse mediante la utilización de un programa de captura de paquetes como por ejemplo, Wireshark. Sin embargo, este método requiere que la captura de datos se procese con un programa a fin de encontrar las consultas para los nombres de domino breves e incompletos únicamente.

Nótese que este paso puede producir resultados confusos. Los dispositivos, tales como las computadoras y teléfonos, poseen aplicaciones en las cuales los usuarios escriben nombres; estos dispositivos aparecerán en la encuesta incluso aunque no haya ninguna versión almacenada de los nombres de dominio breves e incompletos. Para este paso, sólo es necesario conocer todos los lugares de su red donde se almacena el nombre de dominio breve e incompleto o donde es utilizado por las aplicaciones.

## *5.2. Crear un inventario de cada sistema mediante la utilización de nombres de dominio breves e incompletos de manera automática*

Necesita un resumen de los registros obtenidos en el paso anterior. Este resumen debe contener una lista de todos los positivos y todos los nombres breves e incompletos consultados en lugar de todas las instancias en las cuales el dispositivo efectúa una búsqueda. La razón por la cual se requieren todos los nombres que se consultan es que ciertos dispositivos tendrán múltiples aplicaciones que deberán adaptadas. Este resumen se transforma en un manifiesto para los dispositivos que se deben cambiar.

## *5.3. Capacitar a los usuarios y administradores de sistema en el uso de FQDN*

Además de cambiar los sistemas donde se ingresan los nombres de dominio breves e incompletos en toda configuración (ya sea una configuración de todo un sistema o la configuración de una aplicación en particular) será necesario cambiar las formas de pensar de los usuarios respecto de cómo obtenerlas para pasar de la utilización de nombres breves a nombres completos. Utilice las explicaciones de las consecuencias no intencionales o no deseadas que pueden afectar a su organización a fin de crear conciencia y promover su aceptación.

## *5.4. Cambiar todo sistema afectado al uso de FQDN*

Reemplazar todos los nombres de dominio breves e incompletos con su equivalente FQDN en cada uno de los sistemas. Se busca toda instancia de un nombre de dominio breve e incompleto en todo el software del sistema y es necesario reemplazarlo por el nombre de domino completo.

El monitoreo que se comenzó anteriormente es excepcionalmente importante en este paso. Es poco probable que pueda determinar todas las aplicaciones en todos los sistemas que posean nombres breves e incompletos incorporados en las mismas. Por el contrario, se debe consultar el sistema de monitoreo luego de que se cambie cada sistema para determinar si el sistema todavía realiza solicitudes para los nombres de dominio breves e incompletos.

Muchos sistemas ejecutan algunas aplicaciones de inicialización cuando se activan por primera vez. Estas aplicaciones pueden tener nombres de sistemas que se basan en esas listas de búsqueda incorporadas en ellos y encontrarlos puede ser dificultoso. Luego de cambiar todos los nombres en un sistema para utilizar FQDN, reinicie el sistema y utilice el software de monitoreo para monitorear las búsquedas de nombres. Si el sistema busca algún nombre breve e incompleto, es necesario que determine cuál es el software que da origen a dicha solicitud y que lo cambie para utilizar FQDN. Este proceso puede requerir algunos reinicios a fin de configurar completamente un sistema de forma correcta.

## *5.5. Desactivar las listas de búsqueda en los resolutores de nombres compartidos*

Este es el punto donde la mitigación fuera de los nombres breves e incompletos se hace real para todos los sistemas (PC, dispositivos de red, impresoras, etc.) en la red. Las listas de búsqueda pueden existir en cualquier sistema que realice resolución de nombres o que preste configuración a otro sistema, como por ejemplo un servidor DHCP. Estos sistemas generalmente son servidores de nombre independientes, pero también pueden ser firewalls u otros dispositivos de red. Independientemente del

tipo de sistema, es necesario desactivar las listas de búsqueda en cada uno de ellos a fin de evitar que los usuarios escriban nombres de dominios breves e incompletos dentro dentro de un determinado espacio de nombres.

## *5.6. Comenzar a monitorear el uso de nombres breves e incompletos en el servidor de nombres*

Debe configurar su servidor de nombres para comenzar a monitorear todas las solicitudes de nombres que tengan la raíz antigua. Si brinda capacitación y la suficiente antelación, sus usuarios no deberían utilizar estos nombres ya, de modo que el archivo de registro creado en el paso de supervisión puede no ser demasiado extenso; si lo es, tendrá que repetir algunos de los pasos antes mencionados en el caso de ciertos sistemas particulares en su red.

## *5.7. Configuración de monitoreo a largo plazo en los perímetros para buscar nombres breves e incompletos*

Con los pasos anteriores se deberían haber encontrado la mayor parte de los usos de los nombres privados antiguos, sin embargo, los sistemas pueden aún estar utilizando algunos nombres breves e incompletos, pero sólo tal vez en raras ocasiones. Una manera de detectar estas consultas es incorporar reglas a todos los firewalls en el borde de la red para buscar todas las consultas que se están filtrando. Estas reglas deberían tener una prioridad alta asociada a las mismas y se deberían configurar para generar notificaciones de eventos de modo tal que el personal de TI reciba la alerta oportunamente. Por otra parte, también podría hallar estos eventos en los archivos de registro del firewall, pero hacer esto tendría una mayor posibilidad de no detectarlo. Las alertas que se disparan cuando aparece una solicitud permitirán al personal detectar estos eventos afortunadamente ocasionales en la actualidad. Algunos firewalls sólo admiten este tipo de regla mediante la adición de funcionalidades adicionales a un costo extra; si este es el caso de su firewall, deberá evaluar si el beneficio de encontrar estas solicitudes dispersas merece el costo adicional.

# 6. Detección de Colisiones de Nombres en los Nuevos gTLD

A partir del 18 de agosto de 2014, la ICANN requiere que los gTLD que sean recientemente delegados en la zona raíz asistan a las organizaciones a detectar cuando se filtran consultas al DNS global de los nombres que entran en el nuevo TLD. Esta asistencia tendrá una duración de 90 días, muy probablemente, los primeros días en los que el nuevo gTLD se encuentre en la zona a raíz; luego de ello, el nuevo gTLD actuará como cualquier otro TLD en la zona raíz. La asistencia se proporciona mediante un servicio "de interrupción controlada" que se describe en esta sección.

Claramente, la organización que necesite mitigar las colisiones de nombre entre su espacio de nombres privados y el DNS global debería hacerlo antes de que el correspondiente nuevo TLD ingrese en la zona raíz: no debe esperar a este período de 90 días. (Esto es particularmente cierto para las organizaciones que eligen TLD de dos caracteres para sus nombres porque estos nombres no necesitan realizar una interrupción controla). Las interrupciones controladas tienen como objetivo ser una última advertencia para una organización respecto de que necesita rápidamente llevar a cabo una mitigación antes de que el TLD comience a dar respuestas "reales" a las consultas.

Esta sección describe cómo se implementa una interrupción controlada en un servidor de nombres autoritativo y como aparece en las respuestas a las consultas. También brinda asesoramiento a las organizaciones que tienen espacios de nombres privados para que determinen si los cambios operativos que observan se deben a la interrupción controlada y, si es así, qué deben hacer en relación a dichos cambios.

## *6.1 Descripción de las Interrupciones Controlas*

El servicio de interrupción controlada que requiere la ICANN para los nuevos gTLD agregados a la zona raíz con posterioridad al 18 de agosto de 2014 está diseñado para causar una interrupción en aquellos dispositivos cuyas solicitudes de nombres de dominio en los espacios de nombres privados se filtren en el DNS global. Actualmente, cuando tal consulta al DNS se infiltra en el DNS global, los servidores de nombre raíz envían una respuesta con un código que indica que el nombre de dominio no existe. (Técnicamente, este es el campo RCODE del encabezado de la respuesta que se ajusta a un valor de 3, mnemotécnicamente definido como una respuesta "NXDOMAIN").

Durante el período del servicio de dominio controlado, en lugar de un error NXDOMAIN en la respuesta, la respuesta no contiene indicación de error de un error, pero, en cambio, contiene datos con probabilidades muy elevadas de ser advertidos por el sistema que envía la solicitud.  Resulta imposible diseñar una respuesta que sea siempre advertida porque existen muchos tipos diferentes de software que efectúan solicitudes al DNS; no obstante, la interrupción controlada ordenada por la ICANN será observable en los sistemas con un registro de errores adecuado y en redes donde el tráfico de DNS pueda ser observado por administradores de red.

Los gTLD que operan en el modo de interrupción controlada responderán a una amplia variedad de consultas de DNS de una manera predecible. La Sección 6.2 explica cómo observar las conductas de los sistemas que obtienen respuesta de interrupción controlada a estas consultas del DNS.

- Por lejos, la consulta al DNS más común es sobre registros A, es decir, para la(s) dirección(es) de IPv4 asociadas con un nombre de dominio. Esas consultas siempre volverán con la dirección IPv4 127.0.53.53. Esta es una dirección *loopback* para el host que envió la consulta, por lo que si la aplicación utiliza esa dirección para iniciar cualquier tipo de contacto, se enviará el mensaje a sí misma. Esto, por supuesto, es probable que falle, ya que casi todos los

programas que realizan búsquedas de DNS tratan de utilizar la dirección en la respuesta al contactar a otro servidor.

- Otra consulta al DNS común es sobre registros que contienen texto, comúnmente conocidos como "registros TXT". En el servicio de interrupción controlada, la respuesta al registro TXT siempre será la cadena de caracteres exacta "su configuración de DNS requiere atención inmediata, véase https://icann.org/namecollision". Un sistema que muestra tales registros de texto brinda al observador información sobre colisiones de nombres.

- Para las consultas al DNS que son para servidores de correo (técnicamente, para intercambio de correo electrónico o registros MX), el servicio de interrupción controlada responderá con el nombre de dominio your-dns-needs-immediate-attention.<TLD>, donde "<TLD>" es el TLD en la solicitud al DNS. Este nombre de dominio puede ser visible en las respuestas de error del cliente o servidor de correo electrónico. La búsqueda de direcciones del nombre de dominio your-dns-needs-immediate-attention.<TLD> devolverá 127.0.53.53.

- El servicio de interrupción controlada responderá a las consultas sobre registros de servicio (SRV) con el nombre de dominio your-dns-needs-immediate-attention.<TLD>. Las consultas sobre los registros SRV no son tan comunes como aquellas sobre las direcciones de IPv4, registros de texto y nombres de servidores de correo electrónico, pero se tornan cada vez más frecuente para las aplicaciones más nuevas tales como la mensajería instantánea y la transmisión mediante voz.

Un gTLD agregado a la zona raíz antes del 18 de agosto de 2014 también puede tener un servicio de interrupción controlada para un subconjunto de posibles dominios de segundo nivel en el TLD. Los registros devueltos en la interrupción controlada para estos nombres son idénticos a los registros descritos anteriormente. La ICANN solicitó el bloqueo de algunos SLD del TLD y dichos nombres podrían activarse rápidamente luego de la interrupción controlada de 90 días para los SLD.

## *6.2 Observación de las Interrupciones Controladas*

Es importante tener en cuenta que no hay garantía de una aplicación que recibe una respuesta de interrupción controlada actuará visiblemente diferente de lo que lo ha hecho antes de la interrupción controlada. No obstante, es muy probable que la aplicación se comporte de forma diferente y la diferencia muy probablemente será una falla; afortunadamente dicha falla tendrá mensajes de error asociados a ella y el usuario de la aplicación informará esto al administrador del sistema encargado de manejar esta cuestión. Si el mensaje de error contiene la dirección de IPv4 127.0.53.53, eso constituye una sólida indicación de que el error se debe a que un programa utiliza un nombre proveniente del espacio de nombres privados que se filtró en Internet pública.

Los errores debido al servicio de interrupción controlada aparecen cuando un programa que previamente obtenía respuestas NXDOMAIN a la consulta comienza a obtener respuestas reales. Desde luego, estos errores aparecerían posteriormente cuando el nuevo gTLD respondiese a los datos reales y el servicio de interrupción controlada probablemente durará sólo los 90 días indicados por la ICANN. Durante este tiempo, los errores serán más obvios porque los mensajes de error contienen la dirección de IPv4 127.0.53.53, el texto "Su configuración de DNS requiere atención inmediata, véase https://icann.org/namecollision" o un nombre de dominio que contiene "your-dns-needs-immediate-attention".

Las interrupciones controladas también se pueden observar en la red de una organización si el administrador de red está buscando activamente mensajes del DNS que contienen dichas respuestas. Tal búsqueda puede realizarse mediante un punto de conexión de red a los puntos de ingreso adecuados o puede hacerse en un firewall. Este tipo de observación no se basa en ver los mensajes

de error en la computadora afectada; por el contrario, el administrador de red puede determinar cuál es la computadora cuyas solicitudes de nombres en los espacios de nombres privados se están filtrando de la red de la organización.

Independientemente de cómo se descubra la interrupción controlada, el resultado debería ser que la computadora que obtiene la respuesta de la interrupción controlada debe estar configurada para sólo hacer consultas del DNS al servidor de nombres de la organización, no al DNS global. No existe una forma estandarizada para especificar tal configuración, aunque la configuración es normalmente parte del sistema operativo. Si la computadora obtiene su configuración de red a partir de un servidor en la red de la organización, comúnmente denominado "un servidor DHCP", dicho servidor requiere que se cambie su configuración para que las consultas del DNS vayan al servidor de nombres de la organización, no al DNS global.

Toda observación de una computadora que obtiene una respuesta de interrupción controlada es un signo de que otras computadoras en la red de la organización pueden también estar obteniéndolas. Un administrador de sistema inmediatamente debería verificar la configuración del DNS para todas las computadoras que se encuentran en la misma red, incluso si estas computadoras no muestran signos visibles de obtención de respuestas de interrupción controlada. Recuerde que la interrupción controlada dura sólo 90 días, por lo tanto, hay poco tiempo para encontrar aquellas computadoras que poseen configuraciones de DNS incorrectas.

Desde luego, realizar tales cambios sólo es una mitigación temporal para el problema de colisiones de nombres subyacente. Las Secciones 4 y 5 del presente documento brindan instrucciones respecto de cómo realizar mitigaciones permanentes.

# 7. Resumen

Las colisiones de nombres poseen el potencial para crear resultados no anticipados en aquellas organizaciones que utilizan espacios de nombres privados. Este documento enumera algunos de los posibles resultados y especifica las mejores prácticas para cambiar la forma en la que se utilizan los espacios de nombres privados.  El presente documento también describe la interrupción controlada como un medio para identificar dónde puede ser visible el efecto de las colisiones de nombres.

Para los espacios de nombre que utilizaban un TLD privado que se transforma (o ya se ha transformado) en un TLD en el DNS global, la mejor práctica de mitigación surge de migrar el espacio de nombres a un espacio de nombres que tenga raíz en el DNS global. Para los espacios de nombres que utilizan nombres breves con listas de búsqueda, la mitigación sólo se puede lograr al eliminar el uso de las listas de búsqueda. Los pasos para lograr estas mitigaciones también incluyen un monitoreo a largo plazo en la red privada para garantizar que todas las instancias de nombres que podrían ocasionar colisiones ya no se utilicen. Habrá medios para que las organizaciones expresen cuando van a experimentar colisiones de nombres conforme algunos nuevos TLD se deleguen en la zona raíz.

La mitigación generalizada para los problemas en relación a la colisión de nombres es la utilización de FQDN en todos los sitios donde se utiliza un nombre de dominio.  En una red que está utilizando el DNS global, esto implica no utilizar listas de búsqueda. En una red que utiliza un espacio de nombres privado, esto significa que el espacio de nombres privado debe tener su raíz en el DNS global, y no debe utilizar listas de búsqueda.

# Apéndice A: Para mayor información:

Los siguientes documentos fueron creados por varias organizaciones dentro de la ICANN. Otras organizaciones también brindan documentación que puede ser de utilidad. Lo más significativo es que el proveedor de su software de servidor de nombres y/o hardware puede tener información valiosa en su sitio web de soporte técnico.

## A.1 Introducción al Programa de Nuevos gTLD

Esta página describe la historia, implementación y progreso del programa para agregar cientos de nuevos gTLD al DNS global. http://newgtlds.icann.org/en/about/program

## A.2. Colisión de nombres en el DNS

La ICANN encomendó a Interisle Consulting Group, LLC crear este informe detallado sobre las posibles colisiones de nombres. Brinda un panorama general de las colisiones nombres, presenta datos en relación a los TLD no existentes que son actualmente consultados en los servidores raíz y proporciona una gran cantidad de información sobre el contexto en relación a los problemas que podrían implicar las colisiones de nombres. http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

## A.3. Plan de Gestión de Incidentes de Colisiones de Nuevos gTLD

Este es el plan adoptado por la ICANN en relación a cómo gestionar los incidentes de colisiones de nombres entre los nuevos gTLD y los espacios de nombres privados. También incluye varias referencias a los comentarios recibidos por la ICANN a propuestas anteriores que se relacionan con la colisión de nombres en la zona raíz. http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

## A.4. Marco de Gestión de Incidentes de Colisiones de Nombres

Este documento es parte del Plan de Gestión de Incidentes de Colisiones de Nuevos gTLD. Define las particularidades del servicio de interrupción controlada para los gTLD que se deleguen en la zona raíz del DNS a partir del 18 de agosto de 2014. http://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

## A.5. *Inquietudes sobre Nuevos gTLD:* Nombres Sin Punto y Colisiones de Nombres

Las listas de búsqueda en distintos sistemas pueden arrojar resultados diferentes según el nombre breve e incompleto que se esté consultando. Esta publicación se centra en las listas de búsqueda para los nombres de dominio sin punto (TLD que tienen registros de dirección en su ápice), pero la descripción del procesamiento de las listas de búsqueda es valiosa en muchos otros contextos también. https://labs.ripe.net/Members/gih/dotless-names

## A.6. SAC 045: Consultas Inválidas sobre Dominios de Alto Nivel a Nivel de la Raíz del Sistema de Nombres de Dominio

Este informe del Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN describe los tipos de consultas de TLD observadas por los servidores raíz al momento de su redacción. http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

## A.7. SAC 057: Asesoramiento del SSAC sobre Certificados de Nombre Internos

Este informe del Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN describe las implicaciones en materia de seguridad y estabilidad relacionadas con los certificados que contienen nombres (internos) privados. Identifica una práctica realizada por las CA que puede ser aprovechada por los atacantes y podría implicar un riesgo significativo para la privacidad e integridad de las comunicaciones seguras en Internet. http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf