Guía de compras del DNS para funcionarios de adquisiciones gubernamentales

ICANN Office of the Chief Technology Officer

David Huberman
OCTO-013
24 de julio de 2020

ICANN

ÍNDICE

El presente documento forma parte de la serie de documentos de la OCTO. Consulte la página de publicaciones de la OCTO
para obtener una lista de documentos en las series. Si tiene preguntas o sugerencias sobre cualquiera de estos documentos, envíelas a octo@icann.org.

1 Introducción

Esta guía tiene por objeto ayudar a los funcionarios de adquisiciones gubernamentales a tomar buenas decisiones de adquisición de nombres de dominio y del Sistema de Nombres de Dominio (DNS) para ayudar a garantizar la seguridad, la estabilidad y la flexibilidad de los servicios de nombres y servidores de las redes de su gobierno. No se requiere experiencia en el DNS para usar esta guía. Está redactada en un lenguaje accesible para ayudarlo a trabajar tanto con su departamento de TI como con tus proveedores.

El presente documento es publicado por la Corporación para la Asignación de Números y Nombres en Internet (ICANN). La ICANN es una corporación de beneficio público sin fines de lucro que, en nombre de la comunidad de Internet, supervisa la coordinación técnica del nivel más alto del Sistema de Nombres de Dominio (DNS) de Internet y ayuda a garantizar su seguridad, estabilidad y flexibilidad.

En esta guía se sugieren buenas prácticas y tecnologías operativas. No todos los proveedores proporcionarán cada servicio o tecnología que incluimos en esta guía. Pero para ayudarle a tomar una decisión de adquisición totalmente informada, debe saber cuáles de nuestras tecnologías recomendadas admiten y cuáles no.

La presente guía se centra en tres fases para la obtención y la puesta en funcionamiento de los nombres de dominio:

- Elección de un nombre de dominio
- Registro de nombre de dominio
- Operaciones del DNS: alojamiento para su nombre de dominio

2 Elección de un nombre de dominio

Los nombres de dominio terminan en un sufijo. Entre algunos ejemplos de estos sufijos, se incluyen *.com*, *.gov*, *.uk* y *.asia*. Existen más de 1300 sufijos como estos en el DNS y se llaman dominios de alto nivel o *TLD*. Cuando se elige un nombre de dominio, primero hay que decidir qué TLD utilizar, ya sea un nombre genérico (sufijos como ".com" o ".asia" que tienen un significado genérico) conocido como *gTLD*, o un dominio de alto nivel con código de país de dos letras, denominado *ccTLD*, de un territorio reconocido (sufijos como *.fr* para Francia o *.za* para Sudáfrica, en los que cada sufijo corresponde a códigos de territorio enumerados en la norma ISO-3166-2).[1]

En muchos casos, y a fin de seguir las normas y políticas locales establecidas, es posible que los organismos gubernamentales tengan que utilizar un nombre de dominio en el ccTLD de su país (por ejemplo, *go.jp* para un organismo gubernamental de Japón). Los distintos gobiernos operan sus ccTLD de maneras diferentes. Le recomendamos que hable con el operador de servicios de nombres de dominio de su gobierno, pregunte acerca de las políticas vigentes y compruebe su funcionalidad, características de seguridad y planes de continuidad de

[1] Consulte https://www.iso.org/iso-3166-country-codes.html para obtener más información sobre la norma ISO-3166-2. La ICANN **no** asigna códigos de ISO-3166; esa es la función de la Agencia de Mantenimiento de la Norma ISO-3166.

operaciones (como se describe a continuación) para que pueda compararlos con cualquier otra opción de TLD que pueda tener a su disposición. La información de contacto de los administradores de cada TLD, incluso de cada ccTLD, se publica en un directorio situado en https://www.iana.org/domains/root/db (para acceder a la información de contacto, hay que hacer clic en el enlace del TLD).

La ICANN tiene un contrato con cada gTLD que especifica muchas reglas. En concreto, los gTLD deben cumplir los términos y condiciones del acuerdo de registro de la ICANN del que son signatarios.[2] Estos términos y condiciones imponen ciertos requisitos técnicos y de políticas a los administradores de gTLD, con el fin de mejorar la salud del ecosistema del DNS y proteger a los titulares de nombres de dominio. En cambio, los ccTLD no tienen acuerdos firmados con la ICANN. Cualquier recurso legal que pueda necesitar el titular de un nombre de dominio dependerá probablemente de la jurisdicción legal en la que opere el registro de ccTLD.

Tanto si se registra un nombre de dominio en un ccTLD como en un TLD genérico, hay cuatro características que un TLD puede ofrecer y que consideramos importantes: compatibilidad con DNSSEC, compatibilidad con IPv6, implementación de algún tipo de bloqueo de registro y la reputación del TLD.

2.1 Compatibilidad con DNSSEC

Los usuarios están mejor protegidos si los nombres de dominio están firmados criptográficamente por el propietario del nombre de dominio, es decir, su organización. Su organización puede firmar digitalmente sus nombres de dominio a través de una tecnología denominada Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC). El documento de la ICANN titulado “DNSSEC: Protección del DNS” proporciona más información sobre la importancia de las DNSSEC.[3]

Para firmar su dominio, el TLD que usted elija debe admitir la *firma de las DNSSEC*. La buena noticia es que la mayoría de los TLD (incluidos los TLD genéricos) admiten DNSSEC. Sin embargo, si la compatibilidad con DNSSEC no aparece como opción en el TLD de su elección, debería consultar acerca de su compatibilidad actual o planificada para esta opción. Cabe admitir que enterarse en qué medida un TLD admite las DNSSEC no siempre es sencillo. Algunos TLD publicarán esta información en su sitio web; otros no lo harán. Es posible que pueda realizar algunas búsquedas web para encontrar esta información o que incluso tenga que enviarles un correo electrónico o llamarlos para hablar al respecto.

2.2 Compatibilidad con IPv6

Las máquinas en Internet utilizan las direcciones del Protocolo de Internet (IP) para identificarse ante otras máquinas. Existen dos tipos de direcciones IP: IPv4 e IPv6. Las direcciones IPv4 son los tipos más comunes de direcciones IP. IPv6 es un nuevo tipo de dirección IP diseñado para ayudar a que Internet siga creciendo a medida que se agregan más y más dispositivos.

[2] Existen diversas versiones del Acuerdo de Registro de la ICANN y distintos TLD son signatarios de versiones diferentes. La versión actual se conoce como "el acuerdo de registro básico de 2017", y se encuentra en el siguiente enlace: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html

[3] Véase https://www.icann.org/en/system/files/files/octo-006-en.pdf

Debido a que algunos gobiernos tienen requisitos para que la infraestructura de Internet sea compatible con el direccionamiento IPv4 e IPv6, consulte con el operador del TLD para asegurarse de que sus servidores del DNS sean compatibles con las direcciones IPv4 e IPv6. En concreto, el operador del TLD necesita brindarle el soporte para que usted pueda tener servidores de nombres autorizados que tengan direcciones IPv6. Si su operador de TLD no admite IPv6, el mundo no podrá llegar a los sitios de su dominio.

2.3 Bloqueo de registro

Otra consideración importante a la hora de elegir un TLD es preguntar al operador del TLD si admite una función denominada *bloqueo de registro*.

El operador de un TLD administra "un registro" que contiene todos los dominios de segundo nivel, como ejemplo.tld, dentro del TLD.[4] Registry lock allows domain name owners, known as registrants, to tell the TLD operator to “lock” the domain name, just like locking your car doors. Cuando su dominio está bloqueado, nadie puede realizar cambios en él, borrarlo ni transferirlo a otro registratario sin algún tipo de proceso de autorización que usted haya definido con el operador del TLD. Sin embargo, tenga en cuenta que no hay estándares de toda la industria para la implementación del bloqueo de registro, por lo que debe preguntar al operador del TLD si ofrece el bloqueo de registro y, si lo hace, cómo funciona.

En general, creemos que el mejor proceso para autorizar los cambios implica una autorización "fuera de banda", en la que todas las partes no dependen de la comunicación centrada en Internet, sino que dependen de las llamadas telefónicas o algún otro método en el que los atacantes tendrían dificultades para penetrar. Los cambios en las características básicas de un nombre de dominio deben ser muy poco frecuentes, por lo que es aceptable confiar en un proceso más lento como la autorización fuera de banda. Al mismo tiempo, sin embargo, probablemente sea bueno asegurarse de que su operador de TLD tenga un procedimiento de escalonamiento claramente redactado en el caso aún menos común de que algunos datos del DNS necesiten cambiarse en caso de emergencia.

Recomendamos encarecidamente a todos los registratarios que utilicen TLD que admitan el bloqueo de registro, dado que así se evitan los ataques conocidos que pueden comprometer dominios enteros.

2.4 Reputación

Por último, antes de elegir un TLD, considere investigar su reputación. Según la empresa antiabuso, Spamhaus,[5] un TLD tiene mala reputación si demasiados de los nombres de dominio registrados en él están relacionados con actividades como la distribución de spam y malware. Si bien siempre habrá algunos nombres de dominio maliciosos registrados en cada TLD, las empresas como Spamhaus miden carteras enteras de nombres de TLD para determinar el grado de "maldad" o "bondad" de un TLD.

[4] Confusamente, un operador de TLD también puede denominarse registro

[5] Véase https://www.spamhaus.org/

Lo importante es elegir un TLD que no tenga un número significativo de registraciones maliciosas. Cuando un TLD tiene mala reputación en la comunidad técnica, puede ser bloqueado por los proveedores de servicios de Internet (ISP) y los operadores de redes empresariales. Si el TLD que usted utiliza tiene mala reputación, es posible, por ejemplo, que no pueda enviar correo electrónico utilizando su dominio, dado que muchos servidores de correo están configurados automáticamente para bloquear los correos electrónicos procedentes de los dominios que figuran en las listas de bloqueo.

Existen varias empresas antiabuso que publican listas de clasificación de la reputación de los TLD, entre ellas, Spamhaus y SURBL.[6]

3 Elección de un registrador de nombres de dominio

Una vez que haya elegido un TLD para su agencia, entonces registra un nombre de dominio en él. Puede registrar nombres de dominio en algunos ccTLD directamente a través del operador de TLD. Sin embargo, para muchos ccTLD y la mayoría de los gTLD, usted registra un nombre de dominio a través de un "registrador" de nombres de dominio. [7]En esta sección, enumeramos algunos criterios que le sugerimos que investigue cuando elija un posible registrador de nombres de dominio.

3.1 Acreditación

La ICANN ofrece a los registradores una acreditación oficial. La obtención y el mantenimiento satisfactorios de la acreditación significan que el registrador ha demostrado que cumplía todos los criterios técnicos, operacionales y financieros necesarios para calificar como empresa registradora.[8] Es importante señalar que el registrador está obligado a cumplir los términos y condiciones del Acuerdo de Acreditación de Registradores,[9] que incluye muchas protecciones para los registratarios de nombres de dominio.

Si está registrando un nombre de dominio en un gTLD, asegúrese de elegir un registrador acreditado por la ICANN. En el sitio web de la ICANN, se incluye un listado de registradores acreditados.[10] El acuerdo que los registradores firman con la ICANN también les permite trabajar con "revendedores", que son empresas externas que ofrecen servicios de registración de nombres de dominio en representación de un registrador. Sin embargo, en el caso de los dominios de alto valor, recomendamos trabajar directamente con los registradores acreditados

6 Véase http://www.surbl.org/
7 Puede ver la distinción entre registro y registrador como similar a la distinción entre mayorista y minorista, es decir, al igual que las personas compran cosas en los minoristas que se abastecen de los mayoristas, los registratarios compran nombres de dominio a los registradores que obtienen su inventario de los registros.
8 Se puede obtener una descripción de las calificaciones de acreditación en el siguiente enlace https://www.icann.org/resources/pages/policy-statement-2012-02-25-es#IIA
9 El RAA actual está publicado en el siguiente enlace: https://www.icann.org/resources/pages/registrars/registrars-en
10 Véase https://www.icann.org/registrar-reports/accreditation-qualified-list.html

cuando sea posible, dado que así se reduce la cantidad de partes implicadas si es necesario abordar una cuestión urgente.

Si está registrando un nombre de dominio en un ccTLD, asegúrese de que está utilizando un registrador o revendedor que esté autorizado por el registro de ccTLD.

3.2 Funciones básicas de seguridad

Cualquier registrador de nombres de dominio que elija debe admitir contraseñas seguras (generalmente, cadenas de caracteres largas con alguna combinación de una letra mayúscula, una letra minúscula y al menos un símbolo) y ofrecer autenticación de factor múltiple (una contraseña más algún tipo de identificador de seguridad, que suele ser un código SMS que se envía a un teléfono móvil) para los usuarios que se conecten a los portales de sus cuentas.

También debe verificar con el registrador o revendedor que esté utilizando que los portales de cuentas de clientes se ejecutan en un sitio web para el cual la comunicación esté encriptada mediante HTTPS. Esto ayuda a asegurar la confidencialidad de las comunicaciones electrónicas entre su personal de TI y el registrador o revendedor.

3.3 Compatibilidad con DNSSEC

Si ha hecho el esfuerzo de asegurarse de que su registro admita DNSSEC, es importante que elija un registrador que le permita suministrar la información necesaria relacionada con las DNSSEC y, si usted no administra sus zonas directamente, que firme sus zonas con DNSSEC. Los registradores generalmente publican los servicios de las DNSSEC que admiten en su sitio web. También es posible que desee que su personal técnico analice con el registrador el nivel de compatibilidad con las DNSSEC que se ofrece para garantizar que se cumplan sus requisitos técnicos.

3.4 Compatibilidad con IPv6

El registrador de nombres de dominio debe admitir el uso de direcciones IPv4 e IPv6, es decir, permitirle gestionar los registros de recursos de direcciones ("A" y "AAAA") de todos los dispositivos que desee nombrar dentro de su nombre de dominio.

3.5 Exportación de datos

Pensando a largo plazo, no querrá quedar atrapado en el uso de ese registrador de nombres de dominio para siempre. Sus necesidades tecnológicas pueden cambiar o el servicio del registrador puede degradarse o puede ocurrir algo más en el futuro que le indique que debe transferir sus nombres de dominio a un registrador diferente. Por lo tanto, sería útil que el registrador le permitiera "exportar sus datos de zona", es decir, que le permitiera descargar todos los datos del DNS asociados a sus nombres de dominio. Esto le proporciona control sobre los datos del DNS de sus dominios y permite al personal de TI transferir rápidamente los servicios a un nuevo registrador.

3.6 Reputación

Cualquier registrador de nombres de dominio que usted elija debe tener tanto una buena reputación en la lucha contra el abuso como un historial probado de trabajo en cooperación con los organismos nacionales e internacionales de cumplimiento de la ley cuando se les denuncie el uso indebido del DNS. Por ejemplo, usted debería asegurarse de que el registrador esté ejecutando un programa antifraude sólido que le permita detectar y detener las registraciones de nombres de dominio que impliquen el uso de información de tarjetas de crédito robadas.

4 Operaciones del DNS: Alojamiento externo para su nombre de dominio

Una vez que haya registrado un nombre de dominio, es necesario que esté alojado en algún lugar. Puede estar alojado por el departamento de TI de su gobierno o puede ser posible, o incluso necesario, elegir un proveedor externo para alojar sus nombres de dominio en sus centros de datos. Este alojamiento puede ser ofrecido como parte de un paquete de servicios que usted adquiere de un proveedor de TI. Esta sección se centra en ayudarle a elegir un proveedor externo y sugiere algunos aspectos que consideramos importantes.

4.1 Administración de nombres de dominio

Es importante que tenga la capacidad de crear subdominios de forma rápida y sencilla. Un subdominio es un nombre de dominio que se parece a *correo.departmento.za* o *elecciones.gobierno.co.jp*, o algo similar. Debería consultar acerca de la facilidad de crear, modificar y eliminar subdominios, especialmente en grandes cantidades. También es importante que usted pueda crear tipos de registro del DNS modernos, por ejemplo, el tipo de registro Autenticación mediante TLS (TLSA) que es utilizado por una tecnología de seguridad llamada Autenticación Basada en el DNS de Entidades Nominadas (DANE).

4.2 Seguridad de las operaciones

Una de las consideraciones más importantes al adquirir servicios del DNS es la seguridad. Es fundamental que su organización mantenga en todo momento el control de todos sus nombres de dominio y los servicios alojados en ellos. La mejor manera de mantener este control es trabajar siempre con proveedores, desde el registrador de nombres de dominio hasta todos los proveedores de TI, que tengan una sólida cultura y compromiso con la seguridad. Cuando se pierde el control de cualquier parte de las tecnologías del DNS, los ataques pueden ocurrir muy rápidamente y pueden producirse filtraciones de datos.

En el caso de un proveedor de alojamiento externo, destacamos tres elementos de seguridad que son fundamentales para proporcionar una seguridad sólida:

- Deben ofrecer una autenticación de factor múltiple para los inicios de sesión de las cuentas. Si el acceso a las tecnologías está disponible a través de un solo factor (por ejemplo, una contraseña), no es seguro.
- El proveedor debería tener publicadas las prácticas y políticas de seguridad completas.

- El proveedor también debería ofrecer un monitoreo detallado de la seguridad de los elementos de la infraestructura y de los datos del DNS. Este monitoreo debería realizarse de forma periódica para asegurarse de que cualquier cambio que realice un atacante sea detectado rápidamente. Cuando se detecta una actividad anómala, el proveedor debería disponer de un sistema de alertas escalonadas para notificar al personal técnico.

Como práctica general, también es importante preguntar sobre la implementación del documento *BCP 38*.[11] BCP 38 is a document that specifies the operational practices that providers should follow to reduce the amount of network routing fraud on the Internet. Todos los proveedores de redes deberían implementar el BCP38. En algunos casos excepcionales, puede haber motivos por los cuales no se pueda implementar el BCP38, pero en el contexto de las organizaciones típicas de alojamiento de dominios, estos casos serían inusuales y usted debería pedir explicaciones detalladas al respecto.

4.3 Servicio de nombres autoritativos

El servicio de nombres autoritativos es la forma en que usted le dice al mundo que su nombre de dominio se resuelve en determinadas direcciones IP, qué servidor de correo está utilizando para el correo entrante, cómo está dispuesto el espacio de nombres de su organización, etc. Tanto si va a configurar sus propios servidores de nombres autoritativos como si va a pagar a un proveedor externo para que aloje los servidores de nombres autoritativos en su nombre, hay que tener en cuenta algunas consideraciones:

- La práctica recomendada consiste en disponer de servidores de nombres autoritativos múltiples y distintos en redes separadas, geográficamente y topológicamente distintas.
- Asegúrese de que cualquier servicio de alojamiento de servidores de nombres sea totalmente compatible con DNSSEC, incluida la carga de registros DNSKEY y/o DS en su registrador de nombres de dominio.
- Asegúrese de que haya buena compatibilidad para las adiciones, modificaciones o eliminaciones a gran escala de los datos del DNS, incluidos los registros de recursos y los subdominios.
- Comprenda las medidas que se utilizan para protegerse contra los ataques de denegación de servicio distribuido, independientemente de que decida operar sus propios servidores de nombre o configurarlos con un proveedor externo.

4.4 Compatibilidad con IPv6

Resulta cada vez más importante que el proveedor de alojamiento externo admita el IPv6 en su software y sus servicios. Los Registros Regionales de Internet (RIR), que son los asignadores al más alto nivel de direcciones IP, han elaborado una gran cantidad de material para ayudarlo a tomar buenas decisiones de adquisición relacionadas con los servicios que utilizan direcciones IP. Entre ellos:

- AFRINIC, el RIR de África, tiene una guía de IPv6 para los gobiernos.[12]

11 Véase https://datatracker.ietf.org/doc/bcp38/
12 Véase https://afrinic.net/guidebook-gov-ipv6

- ARIN, el RIR de América del Norte y partes del Caribe, ha realizado un video de 6 minutos en el que se explica qué es el IPv6 y por qué es importante.[13]
- LACNIC, el RIR de América Latina, publicó una guía de despliegue de IPv6 de 12 pasos para gobiernos y empresas.[14]
- RIPE NCC, el RIR de Europa y partes de Asia occidental, ha publicado una guía de requisitos de IPv6 para los equipos de TIC.[15]

5 Resumen

Hemos abarcado mucho material en esta guía. Por otra parte, no todos los vendedores podrán ofrecer cada uno de los servicios que hemos enumerado aquí y que creemos que son importantes. Pero los mensajes generales que esperamos transmitir son los siguientes:

- La seguridad es importante, y es mucho más que una simple contraseña bien elegida.
- La compatibilidad con DNSSEC y la compatibilidad con IPv6 deben ser un requisito básico.
- Las empresas con las que trabaje deberían comprometerse a mantener una buena reputación para mitigar los usos indebidos y gestionar los reclamos por uso indebido.

13 Véase https://youtu.be/bkLs5_geTM4
14 Véase https://www.lacnic.net/innovaportal/file/3635/1/10-12-steps-government-ipv6-v3.pdf
15 Véase https://www.ripe.net/publications/docs/ripe-554

Apéndice: Lista de verificación de adquisición

Elección de un registro de TLD

- ❑ Admite DNSSEC

  Los nombres de dominio registrados en este TLD pueden ser firmados por DNSSEC
- ❑ Admite tanto IPv4 como IPv6

  Los registros del servidor de nombres del TLD pueden ser emitidos con direcciones IPv4 e IPv6
- ❑ Ofrece bloqueo de registro

  Tiene un proceso para bloquear los registros y requiere autorización fuera de banda para realizar cambios en los registros bloqueados
- ❑ Tiene una buena reputación

  El TLD combate activamente los dominios abusivos registrados en el TLD

Elección de un registrador de nombres de dominio

- ❑ Es un registrador acreditado o autorizado

  Si un gTLD está acreditado por la ICANN y si un ccTLD está autorizado a ofrecer dominios
- ❑ Practica una buena higiene cibernética

  Requiere una autenticación de factor múltiple para los inicios de sesión de las cuentas de usuario y las páginas web utilizan HTTPS
- ❑ Admite DNSSEC

  Los nombres de dominio pueden ser firmados por DNSSEC
- ❑ Permite que los nombres de dominio sean alojados por terceros

  Admite solo la registración de nombres de dominio y no lo obliga a alojar el nombre de dominio en sus servidores web
- ❑ Permite la exportación de datos

  Su personal de TI puede exportar los datos del DNS para que usted pueda transferirlos fácilmente a un nuevo registrador
- ❑ Admite ambas direcciones IPv4 e IPv6

  Los registros del servidor de nombres pueden ser emitidos con direcciones IPv4 e IPv6
- ❑ Tiene una buena reputación

  Es proactivo en la prevención, detección y mitigación de los usos indebidos, y en la respuesta a los reclamos

Elección de un proveedor de alojamiento externo

- ❑ Admite tanto la administración masiva de subdominios como los tipos de registros modernos del DNS

  Puede agregar, modificar o eliminar subdominios de forma masiva y agregar registros de recursos como TLSA

- ❏ Tiene operaciones seguras

  Autenticación de factor múltiple para los inicios de sesión de los usuarios, prácticas y políticas de seguridad publicadas, monitorización proactiva de los datos del DNS e implementación del BCP38

- ❏ Admite servicios autoritativos de DNS

  Servidores de nombres geográficamente dispares, buena protección contra los ataques y más

- ❏ Admite ambas direcciones IPv4 e IPv6

  El acceso a los servidores del proveedor y las actualizaciones del servidor de nombres son compatibles tanto con IPv4 como con IPv6