SAC132

El Sistema de Nombres de Dominio se ejecuta en software libre y de código abierto (FOSS)

Informe del Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN
25 de septiembre de 2025

Prefacio

Este es un informe dirigido a la Junta Directiva de la ICANN, la organización de la ICANN, la comunidad de la ICANN y, en términos más generales, a la comunidad de Internet, elaborado por el Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN, sobre las formas en que el Sistema de Nombres de Dominio (DNS) depende del software libre y de código abierto (FOSS).

El SSAC se centra en cuestiones relativas a la seguridad y la integridad de los sistemas de asignación de nombres y direcciones de Internet. Esto incluye las cuestiones operativas (por ejemplo, las relacionadas con el funcionamiento correcto y fiable del sistema de publicación de la zona raíz), cuestiones de administración técnica (por ejemplo, las relativas a la distribución de direcciones y asignación de números en Internet) y cuestiones de registración (por ejemplo, las relacionadas con los servicios de registro y registrador). El SSAC participa en la evaluación continua de amenazas y análisis de riesgos de los servicios de distribución de nombres y direcciones en Internet, para entender dónde residen las principales amenazas a la estabilidad y la seguridad, y asesora a la comunidad de la ICANN en consecuencia. El SSAC no tiene la facultad de regular, ejecutar o adjudicar. Esas funciones pertenecen a otras partes, y el asesoramiento que aquí se brinda debe evaluarse según sus propios méritos. Los miembros del SSAC participan a título individual, no como representantes de sus empleadores u otras organizaciones. El consenso del SSAC sobre un documento se produce cuando los autores que figuran en la lista están de acuerdo sobre el contenido y las recomendaciones sin objeciones finales del resto del SSAC, con la excepción de las abstenciones incluidas al final del documento.

Índice

Lista de figuras

Lista de tablas

Resumen ejecutivo

El Sistema de Nombres de Dominio (DNS) es un sistema distribuido, jerárquico y descentralizado a nivel mundial cuya información sustenta casi todas las interacciones en línea. Su objetivo principal es asignar nombres de dominio fáciles de usar a las direcciones IP necesarias para localizar recursos en la red. Ya sea para navegar por la web, enviar un correo electrónico o utilizar una aplicación móvil, todas las conexiones en línea dependen de la información que se origina y se estructura en el DNS.

La conclusión principal de este informe es que el DNS se basa y se sustenta en software libre y de código abierto (FOSS). No se trata de una práctica minoritaria, sino de la realidad dominante. FOSS es la regla general para los componentes esenciales de la infraestructura del DNS. Por ejemplo, al menos nueve de las doce organizaciones independientes que gestionan el sistema de servidores raíz (RSS) de Internet utilizan exclusivamente implementaciones de FOSS, y nueve de los diez mayores proveedores de servicios para dominios de alto nivel (TLD) utilizan FOSS. Este dominio proviene de las fortalezas inherentes al modelo de desarrollo de FOSS, que combina la eficiencia económica y la adopción sin fricciones con la transparencia, la seguridad colaborativa y la resiliencia operativa esenciales para la infraestructura crítica.

Aunque el modelo de desarrollo de FOSS es fundamentalmente diferente al del software propietario, FOSS no es intrínsecamente más o menos seguro. La seguridad de todo proyecto de software está determinada por la calidad de sus procesos de desarrollo y mantenimiento, no por la visibilidad de su código fuente. A diferencia del software comercial, FOSS es un esfuerzo colaborativo y global que se funda en cuatro libertades esenciales: usar, estudiar, compartir y modificar. Este ecosistema depende de una red global de encargados del mantenimiento y colaboradores que, a menudo, son voluntarios que no reciben remuneración alguna. Si bien muchos son voluntarios no remunerados, el espacio del DNS es único ya que también depende de un grupo de organizaciones de mantenimiento de larga trayectoria. Esto crea un modelo basado en la colaboración de la comunidad, en lugar de los contratos comerciales que definen la cadena de suministro tradicional del software, lo que introduce riesgos únicos relacionados con la sostenibilidad financiera de las organizaciones de mantenimiento y el agotamiento de los voluntarios que se encargan del mantenimiento.

Estas características únicas significan que los marcos normativos diseñados para el software propietario pueden no ser adecuados para FOSS y, por lo tanto, podrían tener graves consecuencias no deseadas para la estabilidad de la infraestructura crítica de Internet. Para sortear estas complejidades y fomentar un ecosistema digital seguro, el Comité Asesor de Seguridad y Estabilidad (SSAC) ofrece las siguientes pautas a los responsables de la formulación de políticas:

- **Reconocer el rol fundamental de FOSS:** Los responsables de la formulación de políticas deben reconocer explícitamente en cualquier legislación o normativa pertinente que la infraestructura crítica de Internet depende de FOSS y que su uso es una fortaleza que debe preservarse.

- **Consultar a la comunidad de FOSS:** El desarrollo de la legislación y la normativa debe basarse en la consulta a todas las partes del ecosistema de FOSS, desde los encargados del mantenimiento individuales hasta las organizaciones sin fines de lucro y las empresas.
- **Aprovechar los casos contemporáneos en la regulación de FOSS:** Los responsables de la formulación de políticas pueden consultar los estudios de casos recientes incluidos en el informe sobre enfoques contemporáneos que incorporan las características únicas del modelo de desarrollo de FOSS.
- **Incentivar la sostenibilidad de FOSS:** Fomentar los aportes del sector público y privado a proyectos críticos de FOSS como una forma de inversión en un bien público compartido.
- **Abordar los riesgos sistémicos de manera colectiva:** Fomentar y financiar soluciones colaborativas para todo el ecosistema con el fin de mitigar los riesgos derivados de las dependencias compartidas, en lugar de sobrecargar a los encargados del mantenimiento individuales.

1 Introducción

Este informe está impulsado por la creciente participación de los responsables de la formulación de políticas en los esfuerzos de la industria por reducir las vulnerabilidades del software en la infraestructura digital. A medida que los gobiernos y los organismos reguladores de todo el mundo tratan de garantizar la seguridad de la cadena de suministro de software, es fundamental que estos esfuerzos se basen en una comprensión clara de cómo se construyen y mantienen realmente los sistemas más fundamentales de Internet. Entre los ejemplos recientes de intervenciones normativas (propuestas) para reducir la vulnerabilidad del software en la infraestructura digital se incluyen:

- Código voluntario de prácticas de seguridad de software para proveedores de software en el Reino Unido.[1]
- Auto certificación de la industria sobre prácticas de desarrollo de software seguro para su uso por parte del Gobierno de los Estados Unidos.[2]
- Requisitos de acceso al mercado ("Reglamento de Ciberresiliencia (CRA)") para productos digitales (incluido el software) en la UE.[3]
- Gestión de riesgos y obligaciones de notificación para los proveedores de infraestructura digital en la UE ("NIS2 IA").[4]
- Las comunidades de código abierto se incluyen como objetivo de desarrollo en el plan quinquenal de China para TI.[5,6]

Aunque el software libre y de código abierto (FOSS) es la práctica dominante en el desarrollo de software hoy en día, sus características particulares suelen pasarse por alto en el discurso sobre políticas. Si los responsables de la formulación de políticas introducen intervenciones reguladoras sin comprender el modelo único de desarrollo y suministro de FOSS, corren el riesgo de poner en peligro la seguridad y la estabilidad de la infraestructura crítica que depende

[1] "Software Security Code of Practice." [*Código de prácticas de seguridad de software*]. Departamento de Ciencia, Innovación y Tecnología del Reino Unido, 7 de mayo de 2025. https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice.
[2] "Secure Software Development Attestation Form" [*Formulario de certificación de desarrollo de software seguro*]. Agencia de Seguridad Cibernética y de Infraestructuras de EE. UU., https://www.cisa.gov/secure-software-attestation-form.
[3] "Reglamento de Ciberresiliencia: Los diputados del Parlamento Europeo aprueban planes para reforzar la seguridad de los productos digitales", comunicado de prensa del Parlamento Europeo, 12 de marzo de 2024, https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products
[4] "Reglamento de Ciberresiliencia: Los diputados del Parlamento Europeo aprueban planes para reforzar la seguridad de los productos digitales". Comunicado de prensa. Parlamento Europeo, 12 de marzo de 2024. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products.
[5] "14.º Plan quinquenal para la industria de servicios de software y tecnología de la información". Consejo de Estado de la República Popular China, Ministerio de Industria y Tecnología de la Información, diciembre de 2021. https://www.gov.cn/zhengce/zhengceku/2021-12/01/5655205/files/a44b507d67c74591ad4f5e55b98c4518.pdf.
[6] "Traducción: 14.º Plan quinquenal para la informatización nacional". Proyecto DigiChina, Universidad de Stanford, 24 de enero de 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

de él, incluidos los sistemas de dominios y enrutamiento de Internet. El presente informe tiene por objeto proporcionar ese contexto necesario.

A diferencia de lo que suele ocurrir en otros sectores, gran parte del software que hace funcionar Internet está disponible bajo licencias de derechos de autor de FOSS. Estas licencias no se refieren principalmente al costo, sino a la libertad. Específicamente, las licencias de FOSS otorgan a los operadores de infraestructuras cuatro libertades esenciales: usar, estudiar, modificar y compartir el software, modificado o no, con todo el mundo. Se trata de un modelo de desarrollo, no solo de software "gratuito",[7] y es la base del esfuerzo colaborativo y global que construye y mantiene gran parte de la infraestructura crítica de Internet.

Se elabora este informe para proporcionar a los responsables de la formulación de políticas una comprensión exhaustiva del rol que desempeña el software libre y de código abierto (FOSS) en el Sistema de Nombres de Dominio (DNS) y en el ecosistema de registración de nombres de dominio.

- La sección 2 ofrece una introducción de carácter no técnico al DNS, en la que se explican los componentes y funciones clave de esta infraestructura crítica.
- La sección 3 detalla el modelo de FOSS, en la que se explican sus características clave, fortalezas inherentes y riesgos únicos en comparación con el software propietario.
- La sección 4 presenta la investigación fundamental del Comité Asesor de Seguridad y Estabilidad (SSAC) sobre la preponderancia de FOSS, lo que demuestra su predominio en las partes más críticas del DNS.
- La sección 5 examina varios casos contemporáneos de Estados Unidos, Reino Unido y la Unión Europea que ilustran cómo los responsables de la formulación de políticas están adaptando las regulaciones relativas a la ciberseguridad a las realidades únicas del ecosistema de FOSS.
- La sección 6 consolida el análisis central del informe en una serie de conclusiones que constituyen la base empírica de las pautas que se recogen en la sección 7.
- La sección 7 proporciona pautas directas y aplicables para los responsables de la formulación de políticas.

[7] FOSS se puede utilizar para cualquier fin y no tiene restricciones, como la caducidad de la licencia o limitaciones geográficas. Cualquiera puede estudiar su código, sin acuerdos de confidencialidad ni restricciones similares. Se puede compartir y copiar prácticamente sin costo alguno. Además, FOSS puede ser modificado por cualquier persona, y estas mejoras pueden compartirse públicamente. La ausencia o el debilitamiento de, al menos, una de estas libertades significa que una aplicación es propietaria, es decir, que no es software de código abierto. Las cuatro libertades son otorgadas por una licencia de software. Las licencias de software definen las condiciones bajo las cuales un programa puede ser utilizado y reutilizado. Para que sea software libre, el texto de la licencia debe contener al menos las cuatro libertades. Free Software Foundation (https://www.gnu.org/licenses/license-list.html), Open Source Initiative (https://opensource.org/licenses) y el Proyecto Debian (https://wiki.debian.org/DFSGLicenses) mantienen listas de licencias revisadas y aprobadas. Por lo general, una aplicación no puede considerarse FOSS si su licencia no aparece en una de estas listas.

2 Introducción al DNS

Cuando uno envía un correo electrónico, navega por una página web, chatea con amigos, etc., el dispositivo (por ejemplo, computadora, teléfono o tableta) envía y recibe miles de datos. Se puede pensar en esto como una postal digital, con una dirección de remitente, una dirección de destinatario y contenido. Cada dispositivo conectado a Internet tiene asociada al menos una dirección de Protocolo de Internet (IP) única. Para los seres humanos, es más fácil recordar nombres que números. El DNS es como la libreta de direcciones de Internet. Conecta la dirección IP con el nombre de dominio para que todo el mundo pueda navegar más fácilmente por Internet.[8,9] El DNS es un sistema crítico que resulta vital para mantener una Internet global estable, segura e interoperable.

El DNS proporciona una asignación entre nombres de dominio fáciles de usar (por ejemplo, icann.org) y direcciones IP numéricas fáciles de usar para las computadoras (por ejemplo, 192.0.43.7 o 2001:db8::1). Estas asignaciones conforman colectivamente un espacio de nombres global. Para tener un sitio web o una cuenta de correo electrónico accesible a través de un nombre de dominio, el titular del dominio debe publicar las asignaciones para ese servicio. Esta publicación en el DNS pone a disposición de cualquier usuario de Internet la conexión entre el nombre de dominio y la dirección IP del servicio.

Como se ilustra en la figura 1, el ecosistema del DNS tiene tres partes principales:

- Registración de nombre de dominio (cuadro celeste): Este es el marco administrativo y contractual para la adquisición de nombres de dominio.
- Infraestructura del DNS (cuadro verde): Estos son los sistemas técnicos que hacen que los nombres de dominio funcionen en Internet al traducirlos a direcciones IP.
- Servicios para usuarios finales y contenidos (cuadros naranja y azul oscuro): Estos son los servicios que la gente utiliza en última instancia, como sitios web y correo electrónico.

El presente informe se centra en la registración de nombres de dominio y la infraestructura del DNS, que juntos conforman una capa de la infraestructura crítica de Internet. La búsqueda de información en el espacio de nombres de dominio global no suele monetizarse y se ofrece "gratuitamente", sin cargo alguno, a los clientes. La infraestructura que permite este servicio global y distribuido como un "bien público no explotable" es lo que este informe denomina "infraestructura del DNS". El sistema está ampliamente distribuido por Internet y consta de diversos componentes, operados por numerosas organizaciones independientes que desempeñan diferentes funciones específicas en este sistema. Estos sistemas interoperan porque los detalles técnicos necesarios de sus interfaces y comunicaciones están estandarizados a través del Grupo de Trabajo en Ingeniería de Internet (IETF).

[8] ICANN. "El Sistema de Nombres de Dominio", 13 de septiembre de 2022. https://www.icann.org/resources/pages/dns-2022-09-13-en.
[9] Cloudflare. "¿Qué es DNS? | Cómo funciona", https://www.cloudflare.com/learning/dns/what-is-dns/.

Esta infraestructura crítica es independiente del contenido que se transmite a través de ella. Registrar un nombre de dominio no es lo mismo que crear un sitio web. Publicar un nombre de dominio en el DNS para que pueda ser encontrado no es lo mismo que publicar el contenido de un sitio web. Este informe analiza el software básico que hace funcionar la libreta de direcciones, no la información escrita en las páginas de dicha libreta.

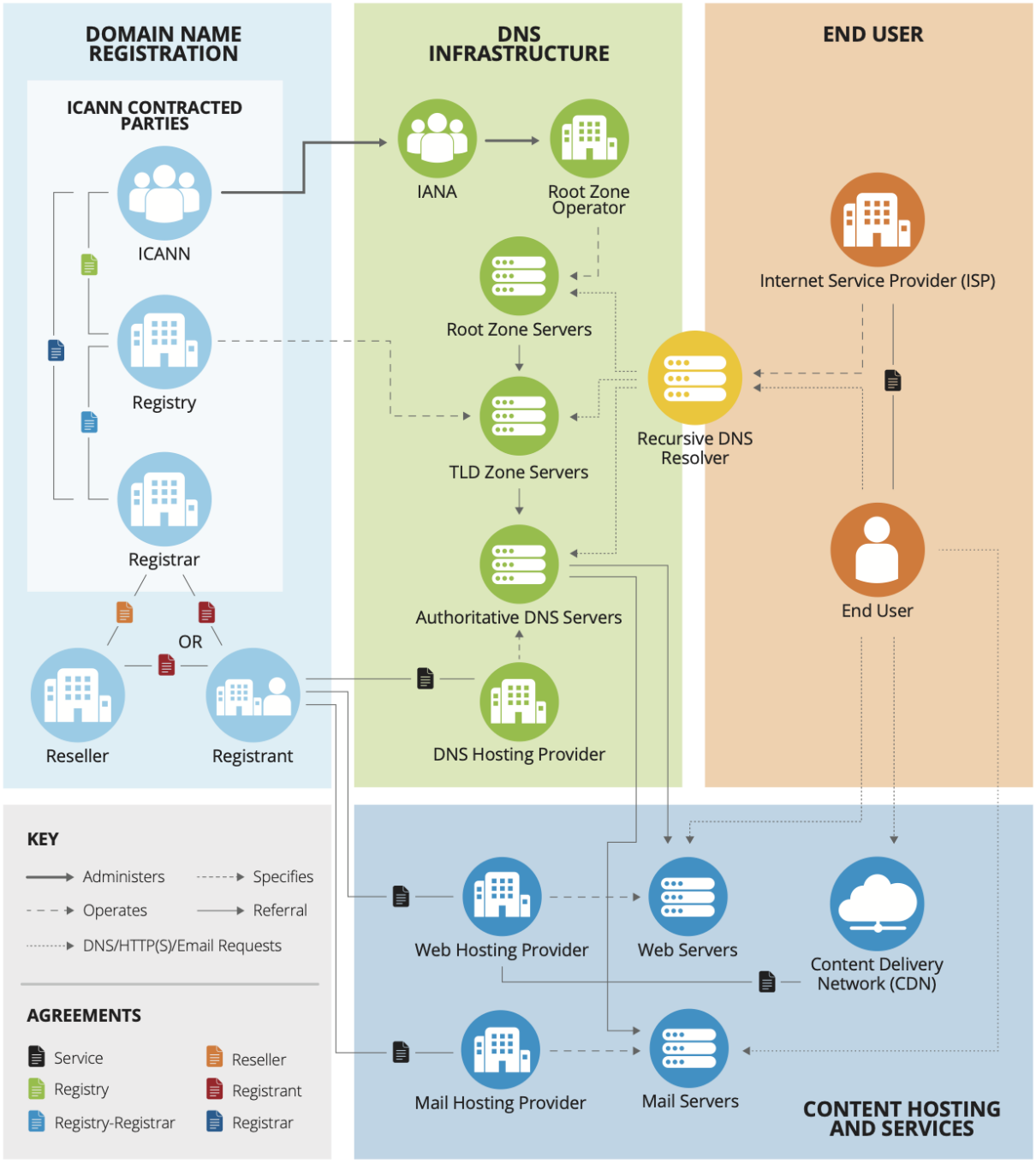

Figura 1: *El ecosistema de Internet.* Drazek, Keith. "DNS Security: Ongoing Community Work to Mitigate Domain Name System (DNS) Security Threats." ["*Seguridad del DNS: Trabajo continuo de la comunidad para mitigar las amenazas a la seguridad del Sistema de Nombres*

de Dominio (DNS)]. Blog de Verisign, 7 de diciembre de 2021. https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/.

2.1 Jerarquía del DNS

El DNS es un sistema distribuido, jerárquico y descentralizado a nivel global. Este sistema, que se muestra como la "Infraestructura del DNS" en la Figura 1, está diseñado para ser resiliente, lo que garantiza que no haya un punto único de falla para la Internet global.

La Figura 2 muestra cómo el espacio de nombres del DNS es jerárquico.

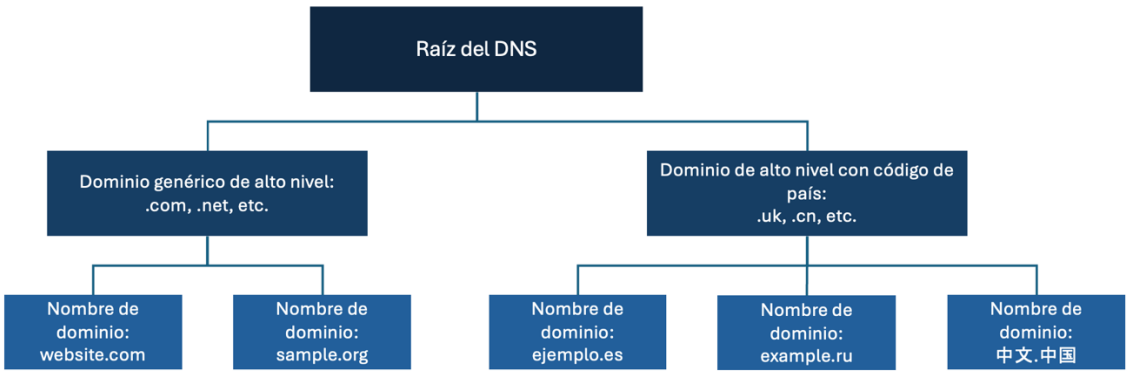

Figura 2: *Jerarquía del DNS*

En la parte superior de la jerarquía se encuentra la raíz del DNS (.), que es gestionada por el sistema de servidores raíz (RSS).[10] La raíz apunta a los servidores autoritativos para varios dominios de alto nivel (TLD). Los TLD son las terminaciones de los nombres de dominio y se clasifican, en términos generales, en dos tipos:

- TLD genéricos (gTLD): Son dominios de uso general como .com, .org, .xyz y .shop.[11]
- TLD con código de país (ccTLD): Están reservados para su uso por países, territorios y ubicaciones geográficas identificados en la lista de códigos de país ISO 3166-1.[12] Los ccTLD pueden basar sus nombres en los códigos de país de dos letras definidos por la

[10] El sistema de servidores raíz está compuesto por servidores distribuidos por todo el mundo y gestionados por 12 organizaciones independientes. Para obtener más información sobre los operadores de servidores raíz, consultar "RSSAC023v2: History of the Root Server System." [*RSSAC023v2: Historia del sistema de servidores raíz*]. Comité Asesor del Sistema de Servidores Raíz (RSSAC) de la ICANN, 17 de junio de 2020. ahttps://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf.

[11] ICANN. "Acrónimos y términos, dominio genérico de alto nivel (gTLD)", https://www.icann.org/en/icann-acronyms-and-terms/generic-top-level-domain-en.

[12] Organización Internacional de Normalización. "ISO 3166 — Country Codes,"[*ISO 3166 — Códigos de país*], https://www.iso.org/iso-3166-country-codes.html.

norma ISO 3166-1 (por ejemplo, .jp para Japón, .fr para Francia, .ke para Kenia), o pueden representar el nombre de un país o territorio en un alfabeto distinto de los caracteres ASCII.[13] Esto se conoce como nombres de dominio internacionalizados (IDN), un concepto que la ICANN ha implementado desde 2009.

Debajo de los TLD se encuentran los nombres de dominio individuales. Un nombre de dominio consiste en dos o más segmentos de texto separados por puntos. Como se muestra en la Figura 3, un nombre de dominio se construye de derecha a izquierda, comenzando por el TLD. Por ejemplo, en icann.org, el TLD es .org y el dominio de segundo nivel es icann. Juntos, forman el nombre de dominio único. En el segundo ejemplo, bbc.co.uk, el TLD es .uk y el dominio de segundo nivel es .co. Este sistema jerárquico y descentralizado permite una Internet global sólida y resiliente.

Un nombre de dominio es un nombre único que forma la base de los localizadores uniformes de recursos (URL) que las personas usan para buscar recursos en Internet. El propio nombre de dominio identifica una dirección específica en Internet que pertenece a una entidad, como una empresa, organización, institución o persona.[14]

[13] ICANN. "Acrónimos y términos, dominio de alto nivel con código de país (ccTLD)". https://www.icann.org/en/icann-acronyms-and-terms/country-code-top-level-domain-en.
[14] ICANN. "Acrónimos y términos, nombre de dominio". https://www.icann.org/en/icann-acronyms-and-terms/domain-name-en.

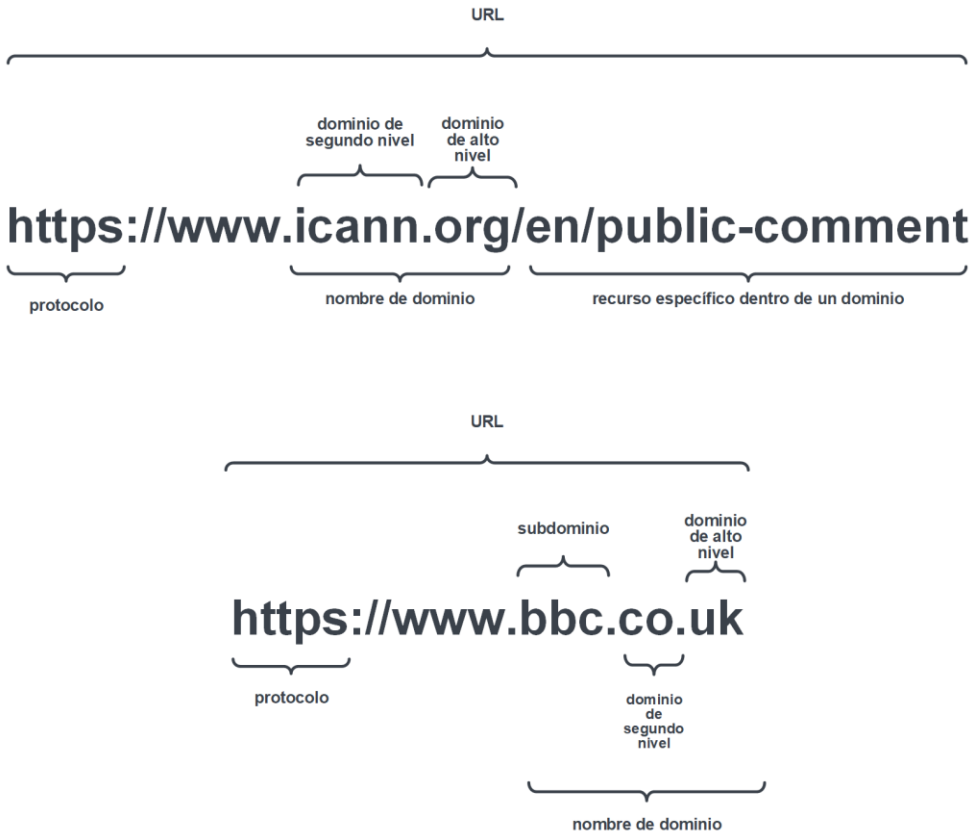

Figura 3: *Componentes de un URL y un nombre de dominio*

2.2 Registración y publicación de nombres de dominio

La infraestructura de registración de nombres de dominio se refiere a los sistemas que facilitan la adquisición de un nombre de dominio único. Este proceso, ilustrado en la parte "Registración de nombres de dominio" de la Figura 1, implica varios actores clave y dos procesos distintos: la registración y la publicación.

La registración es el proceso de reservar un nombre de dominio. Un registratario es la persona física u organización que registra y posee los derechos sobre un nombre de dominio específico. Para registrar un nombre de dominio bajo un TLD específico, el registratario debe utilizar un registrador. El registrador es una organización abierta al público que actúa como minorista de nombres de dominio. Los registradores son, en la práctica, el canal de distribución de las registraciones, y se encargan de gestionar los pagos, las renovaciones y otra información administrativa. Luego, el registrador interactúa con un registro. El registro es la base de datos maestra y autorizada de todos los nombres de dominio dentro de ese TLD. La organización que mantiene esta base de datos se denomina operador de registro. Para automatizar los millones de transacciones entre ellos, los registradores y los registros utilizan el Protocolo de Aprovisionamiento Extensible (EPP), un protocolo estandarizado para la registración, la renovación y la transferencia de nombres de dominio.

El resultado de una registración exitosa es la publicación de los registros del DNS del dominio en los servidores autoritativos que forman parte de la infraestructura del DNS, lo que hace que el dominio sea accesible en Internet. La publicación es el proceso técnico que consiste en hacer que los registros del DNS de un dominio estén disponibles en servidores de nombres autoritativos. Estos servidores contienen los listados de nombres de dominio fácilmente identificables por los usuarios y sus correspondientes direcciones IP, que son fundamentales para localizar y verificar la autenticidad de sitios web, servidores de correo y otros recursos de Internet.

2.3 Resolución del DNS

Cuando se escribe un nombre de dominio como www.ejemplo.com en un navegador web, se inicia un proceso denominado "resolución del DNS". Este proceso se basa en dos tipos de componentes de infraestructura del DNS que funcionan conjuntamente: resolutores recursivos y servidores autoritativos (véase la Figura 4).

Figura 4: *Resolución tradicional del DNS*

Los servidores autoritativos son los componentes que publican la información del dominio. Mantienen el registro oficial definitivo de un dominio específico y lo ponen a disposición para su recuperación. Los servidores de nombres autoritativos son operados por personas, empresas, universidades, proveedores de servicios y entidades gubernamentales. Los servidores de nombres de TLD, por ejemplo, publican los datos técnicos de todos los dominios individuales dentro de su registro. Muchas organizaciones cuentan con servicios de DNS locales que solo proporcionan información relevante para su organización interna, como la ubicación de los sitios web departamentales en una intranet. Esta es una gran parte del DNS que no es visible desde la Internet abierta.

Algunos usuarios finales y pequeñas empresas dependen de los servicios autoritativos de su registrador de nombres de dominio o proveedor de alojamiento web para publicar la información de su dominio, pero es habitual que las empresas, los gobiernos y las organizaciones gestionen sus servidores autoritativos por separado, ya sea de forma interna o tercerizada. Las principales preocupaciones son la fiabilidad y la redundancia; por ello, los administradores de la información de la "zona" publicada bajo un dominio suelen adquirir "servicios del DNS secundarios autoritativos" de proveedores externos. Esos proveedores publican los mismos datos que los

servidores del DNS principales autoritativos. Muchas de las organizaciones que ofrecen estos servicios son las mismas que prestan servicios del DNS autoritativos para los TLD.

Los resolutores facilitan la recuperación de información del DNS. Actúan en nombre del dispositivo de un usuario (un "cliente", como su teléfono inteligente) para encontrar la dirección IP correcta. Para hacerlo de manera eficiente, los resolutores mantienen una base de datos constantemente actualizada de búsquedas recientes, llamada caché. En la práctica, es habitual que los resolutores respondan hasta el 90 % de las consultas desde su caché local, lo que es mucho más rápido que consultar servidores a través de Internet. Para las respuestas que no tienen almacenadas en caché, deben consultar servidores autoritativos. Los resolutores suelen ser sistemas muy ocupados y con una gran carga de trabajo, en parte porque un nivel de tráfico elevado y constante garantiza una caché que se actualiza constantemente.

Existen millones de resolutores en todo el mundo. La función de los resolutores puede ser local, dentro de la red del usuario o del proveedor de acceso, o en la nube, ya sea como un servicio independiente alojado en Internet o junto con otros servicios en la nube. Independientemente de cómo esté configurado el servicio, es importante garantizar que solo los usuarios deseados puedan realizar consultas al servicio. Si el servicio está abierto a cualquier persona en Internet, podría ser objeto de uso indebido, por ejemplo, ataques de denegación de servicio distribuido (DDoS). La configuración del dispositivo del usuario suele determinar el proveedor preferido. Muchas universidades, empresas y proveedores de servicios de Internet (ISP) proporcionan resolutores locales para los usuarios de sus redes, y existen servicios en la nube muy populares, como Google (8.8.8.8), Quad9 (9.9.9.9) y Cloudflare (1.1.1.1). Los factores clave a la hora de decidir qué proveedor de resolución utilizar incluyen la política de la organización, las políticas de filtrado o listas de bloqueo del resolutor y la disponibilidad de transportes del DNS cifrados. El proceso de resolución (Figura 4) muestra cómo estos componentes funcionan conjuntamente siguiendo la jerarquía del DNS.

3 El modelo de FOSS: Características clave e implicaciones

La sección anterior proporcionó una introducción al DNS y a la infraestructura de registración de nombres de dominio, los sistemas fundamentales que permiten a los usuarios navegar por Internet. En esta sección se explicará cómo se construye y mantiene esa infraestructura crítica. El software que sustenta gran parte de esta infraestructura es FOSS, que funciona con un modelo de desarrollo y económico fundamentalmente diferente al del software propietario tradicional. Un debate sobre políticas informado exige comprender estas características únicas.

3.1 Funciones clave en el ecosistema de FOSS

A diferencia del software tradicional de código cerrado, cuyo desarrollo es gestionado internamente por una única entidad jurídica, el modelo de FOSS es abierto y distribuido. Las

funciones no son mutuamente excluyentes y pueden ser desempeñadas por cualquier persona, en cualquier lugar. A los efectos del presente informe, se utilizarán los siguientes términos:

- **Encargado del mantenimiento:** Persona o grupo responsable de la dirección general de un proyecto de FOSS. Los encargados del mantenimiento tienen la autoridad de aceptar o rechazar contribuciones a la versión oficial del software, garantizando así la calidad y la coherencia. Son los administradores del proyecto.
- **Colaborador:** Persona u organización que ofrece mejoras a un proyecto, por ejemplo, enviando código, documentación o informes de errores. Estas colaboraciones son revisadas por un encargado del mantenimiento antes de ser incluidas en el proyecto oficial.
- **Usuario u operador:** Persona u organización que implementa y utiliza el software. En el contexto del DNS, un "operador" es una entidad que ejecuta componentes de la infraestructura del DNS, como servidores autoritativos o resolutores. Los usuarios y operadores son una parte fundamental del ecosistema, ya que aportan comentarios y dan sentido al proyecto.

Para evitar ambigüedades, este informe utiliza los términos específicos "encargado del mantenimiento" y "colaborador" en lugar del término más general "desarrollador", ya que una persona puede desarrollar código como encargado del mantenimiento, colaborador o de forma independiente.

3.2 Principios básicos del modelo de desarrollo de FOSS

El modelo de FOSS se define por los derechos otorgados por sus licencias de derechos de autor. Para que un programa se considere FOSS, su licencia debe otorgar a los usuarios cuatro libertades esenciales:[15,16]

- La libertad de ***usar*** el software para cualquier fin, sin restricciones tales como la caducidad de la licencia o limitaciones geográficas.
- La libertad de **estudiar** cómo funciona el programa, lo que requiere acceso al código fuente sin acuerdos de confidencialidad.
- La libertad de ***compartir*** el software, lo que significa que puede redistribuirse y copiarse prácticamente sin costo alguno.
- La libertad de ***modificar*** el programa y publicar esas mejoras al público.

La ausencia o el debilitamiento de cualquiera de estas libertades significa que el software es propietario, no FOSS. Estas libertades son la base de las características generales de FOSS, que difieren significativamente del software propietario. Organizaciones como Free Software

[15] Sistema operativo GNU. "¿Qué es el software libre?", https://www.gnu.org/philosophy/free-sw.html.
[16] Una definición alternativa y popular de lo que constituye una licencia de FOSS es la "Definición de código abierto" de Open Source Initiative. https://opensource.org/osd.

Foundation,[17] Open Source Initiative[18] y el Proyecto Debian[19] mantienen listas de licencias de software que han sido revisadas y aprobadas por cumplir estos criterios.

Estas cuatro libertades no son solo principios abstractos, sino que constituyen la base del modelo de desarrollo y las características económicas únicas de FOSS, que se describen en las siguientes subsecciones.

3.2.1 El modelo de FOSS permite el desarrollo colaborativo a nivel mundial

Dado que las licencias de FOSS otorgan a toda persona la libertad de estudiar, modificar y compartir el código, facilitan la colaboración global abierta en el desarrollo de software. No existe un conjunto arbitrario de condiciones previas que se apliquen a los colaboradores de FOSS, lo que permite a cualquier persona realizar contribuciones al software. Las colaboraciones pueden provenir de una amplia variedad de personas y organizaciones, a veces como parte del desarrollo corporativo de un producto, otras veces de forma voluntaria e individual.

El producto resultante se pone a disposición de cualquier persona de forma gratuita, no solo para cualquier uso (incluido el comercial), sino también para su desarrollo posterior. Esto reduce la fricción en la evolución del software, en particular cuando las modificaciones se integran de nuevo en el producto de software, lo que contribuye y acelera el desarrollo de funciones y la resolución de errores de software y problemas de seguridad. La naturaleza colaborativa de FOSS fomenta la transparencia y la innovación rápida. Además, las colaboraciones en sí mismas suelen ser también abiertas, lo que permite a otros inspeccionar las colaboraciones propuestas y comentar su idoneidad y las ventajas de integrarlas en el producto de software.

Sin embargo, no es habitual que todas estas colaboraciones sean aceptadas sin algún tipo de inspección y aceptación. El objetivo de estas comprobaciones es reducir el riesgo de que el software se vea comprometido por la inclusión de código incoherente, incorrecto o malicioso. Existen algunas condiciones comunes para la aceptación de colaboraciones, entre ellas, la necesidad de preservar los derechos de autor y las consideraciones relativas a la propiedad intelectual. Una práctica habitual en el ámbito de FOSS es que todas las contribuciones colaborativas no pueden imponer restricciones adicionales al uso del software más allá de las condiciones ya asociadas al mismo, ni pueden imponer restricciones adicionales en materia de derechos de autor o propiedad intelectual a la base de software existente.

Como alternativa a colaborar, las licencias de FOSS también permiten a los colaboradores iniciar su propio derivado (bifurcación), en lugar de trabajar con el proyecto original (upstream). Las bifurcaciones irrestrictas permiten una innovación rápida. Algunas bifurcaciones se han vuelto

[17] Sistema operativo GNU. "Varias licencias y comentarios sobre ellas". https://www.gnu.org/licenses/license-list.html.
[18] Open Source Initiative. “OSI Approved Licenses,” [*Licencias aprobadas por OSI*]. https://opensource.org/licenses.
[19] Página Wiki de Debian. “DFSGLicenses,” [*Licencias DFSG*], https://wiki.debian.org/DFSGLicenses.

más populares que el proyecto original del que derivan. Pero también pueden crear confusión, ya que se divide la capacidad de revisión disponible para detectar errores o adiciones maliciosas.

El software puede ser autónomo o puede depender de otras bibliotecas de software para construir la funcionalidad necesaria. Estas bibliotecas, que son esencialmente componentes de código externos, pueden cambiar de formas que resultan menos visibles para los desarrolladores del código, y esta situación puede dar lugar a comportamientos no deseados. FOSS tiene una barrera de entrada muy baja para su uso como componente en otro software (incluido el propietario), lo que hace que la frecuencia observada de aparición de dicho riesgo sea mayor, aunque no sea exclusivo de FOSS.

3.2.2 El modelo de FOSS funciona sin relaciones contractuales.

Una diferencia importante del modelo de suministro de FOSS es que estas partes no suelen tener una relación contractual. Esto contrasta con la cadena de suministro de bienes físicos, en la que los fabricantes y distribuidores tienen contratos que pueden aprovecharse para agregar políticas o transferir obligaciones de cumplimiento. Sin embargo, en el modelo de suministro de FOSS, los operadores obtienen el software a través de diversas vías. Si bien el encargado del mantenimiento proporciona el software en formato fuente para su descarga pública, lo más habitual es que se distribuya a través de intermediarios que ofrecen paquetes instalables (por ejemplo, el "proyecto Debian") o productos y servicios. Más allá de los términos de la licencia de código abierto del encargado del mantenimiento, un operador rara vez tiene contrato con dicho intermediario. Solo una parte firma contratos con los encargados del mantenimiento. Cuando existe una relación contractual, suele ser para asistencia técnica, no para FOSS en sí.

3.2.3 El modelo de FOSS desvincula la financiación del uso

A diferencia de los bienes físicos, el software es mera información y no tiene un costo sustancial inherente por unidad adicional producida. La libertad de usar y compartir FOSS significa que las licencias otorgan derechos sin exigir un intercambio de dinero. Los usuarios, incluidos los operadores de infraestructura de Internet, pueden financiar el desarrollo y mantenimiento de FOSS si lo desean, pero la licencia no los obliga a ello, por lo que la financiación de los desarrolladores no está vinculada al uso de su software.

3.2.4 Por lo general, FOSS no tiene una única entidad jurídica responsable.

En el mundo de los bienes físicos, es bastante habitual suponer la existencia de una única entidad jurídica responsable, que, a su vez, puede ser objeto de una política o conllevar una carga de cumplimiento. A diferencia de los bienes físicos, la distribución de software a nivel mundial suele realizarse a un costo muy bajo o nulo a través de Internet. Esto permite a personas individuales o grupos de personas escribir y distribuir software sin necesidad de pagar y sin crear una entidad jurídica. El proyecto Debian[20] es un ejemplo destacado de proyecto de código abierto sin una entidad jurídica asociada. El software Debian se utiliza en campos como la

[20] Debian. "Nuestra filosofía: Por qué lo hacemos y cómo lo hacemos". https://www.debian.org/intro/philosophy.

energía nuclear, el transporte ferroviario, la automatización industrial y los equipos médicos. Aunque algunos proyectos de FOSS cuentan con una entidad jurídica que se encarga de su gestión, patrocinio o incluso empleo, para la mayoría no es así. Más adelante veremos que el DNS es inusual en este sentido, ya que cuenta con cuatro pequeñas organizaciones que se dedican profesionalmente al mantenimiento de FOSS.

3.3 Los sistemas propietarios dependen de FOSS

Las características de FOSS resultan ser relevantes para los sistemas que son propietarios (no FOSS). Esto se debe al hecho de que los sistemas propietarios modernos a menudo dependen de FOSS para funcionar. Las herramientas y bibliotecas de FOSS son omnipresentes en el desarrollo y la implementación de software propietario. Por ejemplo, la mayoría del software no se produce sin compiladores o entornos de tiempo de ejecución; el software no puede almacenar objetos o datos estructurados sin almacenes de objetos o bases de datos; el software no puede comunicarse con otros componentes sin un mecanismo para la transmisión de mensajes. Estas funciones de back-end suelen ser proporcionadas por FOSS.

En el caso específico del DNS, Cloudflare ofrece un ejemplo útil. Cloudflare opera un servicio de resolución del DNS público muy utilizado conocido como "1.1.1.1". El servicio se prestaba inicialmente con éxito utilizando Knot Resolver, que es un FOSS; sin embargo, posteriormente fue sustituido por un software propietario desarrollado internamente.[21] El software propietario que se ejecuta en el núcleo de 1.1.1.1 está escrito en Rust, un lenguaje de programación cuya especificación, implementación de referencia y compilador se proporciona como FOSS a través de una fundación sin fines de lucro.[22] Utiliza Tokio,[23] un tiempo de ejecución asíncrono que también es FOSS. Funciona con Linux, un sistema operativo FOSS, y está rodeado de una gran variedad de otros componentes de FOSS que proporcionan visibilidad y otras necesidades operativas.[24] El software propietario de Cloudflare detrás de 1.1.1.1 funciona a gran escala gracias a FOSS, y no a costa del mismo.

3.4 Fortalezas inherentes de FOSS en el ecosistema del DNS

El modelo de FOSS no es solo una construcción teórica; sus principios se traducen en beneficios tangibles que lo han convertido en el paradigma dominante para el software de infraestructura del DNS. Las libertades para estudiar, compartir y mejorar el software de forma colectiva crean un entorno que fomenta la transparencia, la flexibilidad y la innovación. No se trata de subproductos accidentales, sino más bien de fortalezas inherentes al modelo de FOSS que han demostrado ser especialmente adecuadas para las exigencias de la creación y del mantenimiento

[21] Wen, Anbang y Marek Vavruša. "Cómo utilizamos Rust y Wasm en el solucionador 1.1.1.1 de Cloudflare". Blog de Cloudflare, 28 de febrero de 2023. https://blog.cloudflare.com/big-pineapple-intro/.
[22] The Rust Foundation. "Acerca de nosotros: misión, liderazgo, junta directiva". https://rustfoundation.org/about/.
[23] Tokio. “Tutorial”, https://tokio.rs/tokio/tutorial.
[24] Graham-Cumming, John. “CloudFlare And Open-Source Software: A Two-Way Street.” [*CloudFlare y el software de código abierto*: *una calle de doble sentido*]. Blog de Cloudflare, 7 de octubre de 2013. https://blog.cloudflare.com/open source-two-way-street/.

de la infraestructura crítica de Internet. Las siguientes secciones detallan estas fortalezas específicas.

3.4.1 Transparencia y seguridad colaborativa

Las implementaciones del DNS de código abierto se benefician de la transparencia. La disponibilidad del código fuente para las implementaciones de FOSS ha permitido a una comunidad global de desarrolladores, investigadores y operadores identificar y abordar las vulnerabilidades, a menudo con mayor rapidez que en los sistemas propietarios. Han sido tema de estudio activo por parte de las comunidades académicas y de seguridad durante décadas,[25] lo que ha dado lugar a la notificación de vulnerabilidades tanto en el protocolo del DNS como en las implementaciones de código abierto.[26]

Si se identifican vulnerabilidades, los estrechos vínculos entre los tres grupos permiten abordar oportunamente cualquier problema grave y coordinar las divulgaciones y el lanzamiento de parches, lo que garantiza que los servidores críticos del DNS (como los servidores raíz) estén completamente protegidos antes de que la información se haga pública y que todos los demás servidores se actualicen sin demora.

En una encuesta realizada entre operadores de infraestructura del DNS (consultar el Apéndice C), los encuestados indicaron que valoraban la visibilidad de la transparencia de su cadena de suministro como una característica poderosa que les permite acelerar la corrección de vulnerabilidades en las dependencias de software del servicio del DNS que operan. Por ejemplo, ver las siguientes respuestas:[27]

> El código abierto expone RÁPIDAMENTE cualquier falla, ya sea relacionada con la seguridad o de otro tipo, y los parches se distribuyen mucho más rápido que en cualquier entidad comercial.
>
> Las grandes entidades comerciales como [omitido], [omitido] y [omitido] han publicado regularmente a lo largo de los años parches de seguridad mucho DESPUÉS de que se descubriera la vulnerabilidad.
>
> Siempre defendemos que el uso de FOSS beneficia a todos, tanto a los usuarios como a los consumidores de nuestros servicios. Les permite verificar que usamos componentes de software fiables. En los casos excepcionales en que se detecta un problema de

[25] Consultar, por ejemplo, el artículo de Paul Vixie, "DNS and BIND Security Issues," [*Problemas de seguridad de DNS y BIND*], en *Proceedings of the Fifth USENIX UNIX Security Symposium*, Salt Lake City, UT, 1995. https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/vixie.pdf.

[26] Para ilustrar el concepto de "tema de estudio activo", consultar, por ejemplo, el resumen de las conclusiones de 23 trabajos de investigación publicados en 2024 sobre la seguridad del DNS, presentado por Chaoyi Lu, "Resumen de los trabajos académicos sobre el DNS y la seguridad publicados en 2024" (presentación, ICANN82, Seattle, WA, 12 de marzo de 2025). https://static.sched.com/hosted_files/icann82/7b/1.1%20chaoyi-dnspapers2024-0304.pdf.

[27] Comité Asesor de Seguridad y Estabilidad de la ICANN, "Encuesta del SSAC de la ICANN sobre los impactos previstos de la regulación del código abierto en la infraestructura del DNS", comunicación personal, febrero de 2025.

seguridad en el software que utilizamos, se debate abiertamente y se soluciona a toda velocidad, algo muy diferente a lo que vemos con el software propietario.

Hay muchos ejemplos de software propietario con problemas de seguridad y un historial deficiente en cuanto a transparencia o correcciones. La comunidad de FOSS ha hecho un mejor trabajo que la mayoría de los proveedores en ambos aspectos.

El uso y la gestión del software de DNS FOSS es objeto de un debate activo y abierto entre los operadores en público. Cada uno de los principales sistemas de software del DNS tiene una lista de correo electrónico pública abierta para los usuarios[28] y una base de datos pública de errores o problemas accesible en todo el mundo.[29] La comunidad del DNS colabora en operaciones e investigación a través de la organización industrial del DNS, Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC).[30] Esta cultura de comunicación abierta contribuye a una concienciación más rápida y amplia de los problemas operativos, los errores de software, las incompatibilidades entre implementaciones y los errores de los operadores que afectan a otras partes del sistema.

3.4.2 Estabilidad y asistencia a largo plazo

En general, FOSS depende en gran medida del mantenimiento que realizan los voluntarios, generalmente a cargo de una sola persona. En el caso del DNS, cuatro organizaciones distintas (tres instituciones sin fines de lucro y una empresa comercial) de varios países y territorios de Norteamérica y Europa han desarrollado cuatro soluciones de código abierto principales.[31] Las cuatro se crearon en los primeros días de la adopción masiva de Internet y han logrado estabilidad en sus fuentes de ingresos y organización interna. Cada una de estas organizaciones lidera el desarrollo de su software escribiendo código nuevo y revisando y evaluando las contribuciones de código de comunidades activas distribuidas por todo el mundo. El compromiso a largo plazo de estas organizaciones patrocinadoras y el control técnico centralizado de los cambios en el software ayudan a mitigar las preocupaciones sobre la calidad, la seguridad y la fiabilidad que suelen surgir en los proyectos de FOSS desarrollados sin controles técnicos estrictos. La cultura de la comunidad técnica del DNS de código abierto es tal que un infiltrado necesitaría un esfuerzo sostenido durante mucho tiempo para construir las relaciones y la reputación necesarias para desempeñar un rol de confianza.

---

[28] Por ejemplo, consultar las listas de correo electrónico públicas de CZnic (https://lists.nic.cz/postorius/lists/knot-resolver-users.lists.nic.cz/), NLnet Labs (https://www.nlnetlabs.nl/support/mailing-lists/) y PowerDNS (https://mailman.powerdns.com/mailman/listinfo/).

[29] Por ejemplo, consultar el seguimiento de problemas para CoreDNS (https://github.com/coredns/coredns/issues) y BIND 9 (https://gitlab.isc.org/isc-projects/bind9/-/issues/).

[30] Centro de Investigación y Análisis de Operaciones para el DNS. “Introducción al DNS-OARC”, 3 de julio de 2008. https://www.dns-oarc.net/oarc/info.

[31] En orden alfabético; CZNIC, una asociación de proveedores de servicios de Internet (ISP) checos fundada en 1998; Internet Systems Consortium, Inc. (ISC), una corporación sin fines de lucro estadounidense creada en 1994 con el objetivo expreso de apoyar el software y los sistemas de código abierto para la infraestructura de Internet; NLnet Labs, una organización sin fines de lucro holandesa fundada en 1999 para desarrollar estándares abiertos y software de código abierto para DNS y enrutamiento entre dominios; y PowerDNS, una empresa holandesa fundada en 1999 para apoyar el desarrollo de software del DNS especializado para ISP.

3.4.3 Flexibilidad operativa a partir de la diversidad

La alta disponibilidad que se exige a los servicios del DNS implica la necesidad de contar con redundancias y evitar puntos únicos de falla. Para muchos operadores, esto incluye operar varias implementaciones independientes de DNS en software. Los operadores que subcontratan pueden seguir igualmente una estrategia de múltiples proveedores. Esto crea una demanda intrínseca de la existencia de varias soluciones, de modo que los operadores de servicios altamente fiables puedan ejecutar dos o más en paralelo y evitar depender de un único desarrollador de software o ser totalmente vulnerables a los problemas de un solo producto. La disponibilidad del software del DNS FOSS reduce las barreras para las organizaciones que desean operar su propia infraestructura, ya que proporciona una salida a la concentración y centralización del mercado.[32]

3.4.4 Promotor del crecimiento económico y la innovación

Se sabe que FOSS es un promotor del crecimiento.[33] [34] Como hemos visto, existen múltiples productos de código abierto disponibles de forma gratuita para cualquiera que necesite software de DNS, en cualquier parte del mundo. Los posibles usuarios son los proveedores de servicios de Internet, los registros y registradores de nombres de dominio y los usuarios de Internet. Las personas físicas, las organizaciones sin fines de lucro, las empresas emergentes y los expertos en la materia que no pudieran afrontar el costo de las licencias de software propietario podrían obtener el software que necesitan de Mi mayor preocupación, en la actualidad, es que utilizamos tantos componentes de código abierto en partes no críticas de nuestra infraestructura, para los que no tenemos contratos de asistencia técnica, que, en su conjunto, no podríamos costear las licencias incluso si estuvieran disponibles de forma gratuita. Como afirmó uno de los participantes en una encuesta a operadores del DNS (consultar el Apéndice C): "Mi mayor preocupación hoy en día es que utilizamos tantos componentes de código abierto en partes no

[32] Nottingham, Mark. “RFC 9518: Centralization, Decentralization, and Internet Standards” [*RFC 9518: Centralización, descentralización y estándares e Internet*]. Solicitud de Comentarios. Grupo de Trabajo en Ingeniería de Internet, 18 de diciembre de 2023. https://datatracker.ietf.org/doc/rfc9https://data.europa.eu/doi/10.2759/430161518/.

[33] "El análisis estima una relación costo-beneficio superior a 1:4 y prevé que un aumento del 10 % de las contribuciones a OSS generaría anualmente entre un 0,4 % y un 0,6 % adicional del PBI, así como más de 600 nuevas empresas de TIC en la UE. Los estudios de casos revelan que, al adquirir OSS en lugar de software propietario, el sector público podría reducir el costo total de propiedad, evitar la dependencia de un único proveedor y, por lo tanto, aumentar su autonomía digital. De la Comisión Europea. Dirección General de Redes de Comunicación, Contenidos y Tecnología. *The Impact of Open-Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy: Final Study Report. [El impacto del software y el hardware de código abierto en la independencia tecnológica, la competitividad y la innovación en la economía de la UE: Informe final del estudio]*. LU: Oficina de Publicaciones, 2021. https://data.europa.eu/doi/10.2759/430161.

[34] Wright, Nataliya Langburd, Frank Nagle y Shane Greenstein. “Open Source Software and Global Entrepreneurship” [*Software de código abierto y la iniciativa empresarial global*]. *Research Policy* 52, n.º 9 (2023): 104846. https://doi.org/10.1016/j.respol.2023.104846.

críticas de nuestra pila, para los que no tenemos contratos de asistencia técnica, que en total no podríamos afrontar las licencias, aunque estuvieran disponibles".[35]

La existencia de diversas soluciones de DNS FOSS tiene un efecto positivo en el desarrollo técnico y comercial del uso de Internet y de los programas y servicios en línea en general, tanto de código abierto como propietarios. Muchos sistemas propietarios y servicios alojados dependen en gran medida de componentes de código abierto para llevar adelante funciones críticas; muchas plataformas propietarias para servicios en la nube y en línea dependen de uno de los productos de DNS FOSS como componente.[36] Al mismo tiempo, gran parte de la infraestructura del DNS depende de bibliotecas criptográficas de FOSS como OpenSSL. Del mismo modo, Linux, un sistema operativo de código abierto, sirve de base para una parte importante de la infraestructura en la nube, los entornos de servidores y los dispositivos del Internet de las cosas (IoT). Este rol fundamental subraya la profunda influencia de FOSS en la innovación tecnológica. El software propietario suele incorporar estos marcos de FOSS al crear aplicaciones o funciones de código cerrado sobre ellos, lo que crea una relación simbiótica entre los dos modelos.[37]

3.4.5 Aporte a la autonomía digital

Dado que el uso de FOSS no suele requerir el pago de licencias ni compensaciones, la cantidad de capital necesaria para poner en marcha nuevas empresas digitales puede ser menor que si se utilizara software propietario. Además, la libertad para estudiar, modificar y redistribuir el código, que garantiza FOSS, permite el crecimiento del conocimiento y las habilidades locales, lo que da lugar a nuevos proyectos de investigación y de negocios. Las personalizaciones locales o los desarrollos posteriores no requieren ninguna autorización ni acuerdo por parte de los autores originales. Ningún servicio basado en FOSS puede ser bloqueado por titulares extranjeros de derechos de autor, ya que las licencias de FOSS no pueden revocarse; incluso en caso de conflictos comerciales y embargos, el código seguirá estando disponible.

3.5 Riesgos inherentes al modelo de FOSS

Si bien el modelo de FOSS ofrece importantes ventajas, sus características únicas también presentan una serie de riesgos distintos a los del software propietario tradicional. No se trata de defectos del modelo en sí, sino más bien de inconvenientes inherentes que deben comprenderse y gestionarse, especialmente cuando el software se utiliza en infraestructura crítica. El modelo económico, la naturaleza distribuida del desarrollo y la falta de relaciones contractuales

[35] Comité Asesor de Seguridad y Estabilidad de la ICANN, "Encuesta del SSAC de la ICANN sobre los impactos previstos de la regulación del código abierto en la infraestructura del DNS".
[36] Actualmente, no existe ninguna referencia independiente que respalde esta afirmación. Sin embargo, sobre la base de la investigación realizada colectivamente por los autores de este artículo, es posible afirmar con certeza que así es. Existen cuestiones de confidencialidad a la hora de revelar públicamente qué plataforma utiliza qué servicio, por lo que se trata de una afirmación bien fundada sin la documentación adecuada.
[37] Gortmaker, Jeff. "Open source software policy in industry equilibrium" [*Política de software de código abierto en el equilibrio industrial*]. Documento de trabajo, Tech. Rep, 2024. https://jeffgortmaker.com/files/Open_Source_Software_Policy_in_Industry_Equilibrium.pdf.

tradicionales tienen implicaciones para la sostenibilidad a largo plazo y la seguridad operativa. Las siguientes secciones describen estos riesgos inherentes en forma detallada.

3.5.1 Sostenibilidad financiera y agotamiento de los encargados del mantenimiento

Una de las principales amenazas para el DNS es el problema general de sostenibilidad financiera de FOSS. El modelo desvincula la financiación del uso (sección 3.2.3), lo que permite una adopción generalizada, pero también da lugar a la aparición de "oportunistas",[38] en cuyo caso todo el mundo podría depender de un software financiado por unos pocos.[39,40]

Como se señala en un informe del Grupo Asesor Técnico de Internet de Banda Ancha (BITAG):

> Existe una desconexión entre la compra de equipos de red con costosos contratos de asistencia técnica y la falta de financiación del software de código abierto del que, en muchos casos, dependen esos mismos equipos. Con frecuencia, el personal técnico de los operadores de red está dispuesto a apoyar el desarrollo, pero la estructura corporativa no se los permite, ya que este tipo de software no es algo que se pueda adquirir en forma de paquete con un contrato de asistencia técnica. Patrocinar el desarrollo de una función puede ser problemático, ya que los departamentos jurídicos suelen partir del supuesto de que el desarrollo de software da lugar a que el patrocinador sea el propietario [exclusivo] de la propiedad intelectual, lo cual es incompatible con el modelo de software libre y de código abierto.[41]

Si bien las cuatro principales implementaciones de DNS de código abierto son mantenidas por organizaciones que han logrado una estabilidad financiera y organizativa sostenida, todas ellas son organizaciones pequeñas. Cualquiera de ellas podría verse desestabilizada si su fuente de financiación se viera amenazada o si la normativa les impusiera cargas que superaran su capacidad para absorber los costos asociados. Si uno de los principales sistemas de código abierto recibiera un mantenimiento insuficiente o dejara de estar disponible por completo, el impacto en el DNS podría ser significativo.

Esto es especialmente cierto en el caso de las herramientas básicas que requieren un mantenimiento constante, pero que están desconectadas de los procesos empresariales

---

[38] Johnson, Justin Pappas. “Essays in Microeconomic Theory ” [*Ensayos sobre teoría microeconómic*a]. Disertación, Instituto Tecnológico de Massachusetts, 1999. http://hdl.handle.net/1721.1/9518.

[39] Kristoff, John, Alexander Band, Ondrej Filip y Jeff Osborn. *Panel: Panel OSS de sistemas centrales.* NANOG 84, 2022. https://www.youtube.com/watch?v=vWiW-3jMw7w.

[40] Por ejemplo, en un informe se destaca el desequilibrio entre el uso de software de enrutamiento esencial y las contribuciones financieras a su desarrollo: "Ilustramos la relevancia de este desequilibrio entre la financiación y el uso... con dos ejemplos. De las aproximadamente 2 000 instalaciones del software Routinator RP y las 1 400 redes que utilizan el software Krill delegated CA, menos de diez financian su desarrollo. La mayoría de los operadores dependen de la estabilidad, la continuidad y el desarrollo futuro del software, pero no contribuyen a ello". Grupo Asesor Técnico de Internet de Banda Ancha (BITAG), “Security of the Internet’s Routing Infrastructure ” [*Seguridad de la infraestructura de enrutamiento de Internet*], 2 de noviembre de 2022, 26. https://www.bitag.org/documents/BITAG_Routing_Security.pdf.

[41] Grupo de Trabajo Técnico BITAG, "Seguridad de la infraestructura de enrutamiento de Internet", 26.

principales de sus usuarios. Las cuatro implementaciones de DNS de código abierto más populares cuentan con el apoyo de equipos de desarrollo formados por no más de una docena de ingenieros, por lo que agregar requisitos al proyecto que pudieran requerir la dedicación de personal a tiempo completo, por ejemplo, supondría una carga considerable.

Los encargados del mantenimiento remunerados reciben financiación de diversas formas, algunas de las cuales pueden resultar inesperadas. Además de aceptar donaciones y ofrecer asistencia técnica privada, algunos proyectos ofrecen a los patrocinadores financieros acceso anticipado a correcciones de errores, asistencia para versiones obsoletas, desarrollo prioritario de funciones, acceso a paquetes pre compilados y servicios de seguridad adicionales.[42,43,44,45] Los organismos reguladores deben tener precaución a fin de no prohibir de manera involuntaria alguna de estas vías como posibles medios para que los encargados del mantenimiento de FOSS financien sus operaciones.

FOSS para DNS es excepcional en el sentido de que existen organizaciones de larga trayectoria que emplean a encargados del mantenimiento. Para su continuidad, el riesgo es la sostenibilidad *financiera*. Pero, en general, el riesgo es motivacional. La inmensa mayoría de FOSS es mantenido por una sola persona, en su tiempo libre.[46] Entre los ejemplos de software de DNS se incluye el software de DNS que suele incorporarse en los enrutadores pequeños y económicos que se utilizan en hogares y pequeñas empresas, Dnsmasq. En su mantenimiento participa principalmente un voluntario que, en su mayor parte, no recibe remuneración alguna.[47] Asimismo, una sola persona, en su tiempo libre, mantiene eficazmente varias bibliotecas de software avanzadas para la programación del DNS.[48] Otra implementación conocida del DNS, CoreDNS y la biblioteca subyacente Go DNS, cuentan con el apoyo de la comunidad y de un único encargado del mantenimiento que es voluntario (experto), respectivamente. Estos ejemplos ponen de relieve una característica definitoria del ecosistema del software: una pequeña organización o un único desarrollador pueden desempeñar un rol fundamental en la creación de software para una infraestructura digital mundial, sin tener que asumir el capital ni los gastos

[42] Por ejemplo, Internet Systems Consortium ofrece un servicio de notificación temprana de vulnerabilidades. Consultar Internet Systems Consortium, "Notificación temprana de vulnerabilidades (EVN)". https://www.isc.org/evn/.
[43] NLnet Labs ofrece, a través de su subsidiaria Open NetLabs, servicios de capacitación, consultoría, asistencia técnica y desarrollo de software. Consultar NLnet Labs, “Servicios de Open Netlabs - Consultoría” https://nlnetlabs.nl/services/consultancy/.
[44] PowerDNS ofrece una variedad de servicios y productos, entre los que se incluye PowerDNS Protect, un servicio de seguridad que incluye listas de bloqueo preventivas. Consultar “PowerDNS Protect”, https://www.powerdns.com/powerdns-protect.
[45] Para obtener una descripción general de los distintos tipos de modelos organizativos de código abierto, consultar “ Open Source Archetypes: A Framework For Purposeful Open Source” *[Arquetipos de código abierto*: *Un marco para el código abierto con propósito, Estrategias tecnológicas abiertas]*, Mozilla Corporation, 28 de octubre de 2019. https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf.
[46] Bressers, Josh. “Open Source Is One Person” [*El código abierto es una sola persona*]. Seguridad de código abierto, 28 de agosto de 2025. https://opensourcesecurity.io/2025/08-oss-one-person/.
[47] "Dnsmasq - Servicios de red para redes pequeñas". https://thekelleys.org.uk/dnsmasq/doc.html.
[48] Algunos ejemplos son *Net::DN*S para el lenguaje de programación Perl y *miekg/dns*, una biblioteca de DNS de Go utilizada en Kubernetes, Docker y la autoridad de certificación Let’s Encrypt. En la Tabla 7 se pueden encontrar más ejemplos de bibliotecas.

operativos que conlleva su funcionamiento. Para estos encargados del mantenimiento voluntarios que trabajan en solitario, a menos que este trabajo se convierta en su empleo principal a tiempo completo, el riesgo no es la sostenibilidad financiera, sino el agotamiento. Los reguladores deben tener precaución a la hora de imponer cargas adicionales que supongan un esfuerzo superior a la capacidad y la voluntad de los encargados del mantenimiento de invertir su tiempo libre en el mantenimiento de lo que, en esencia, son proyectos aficionados. Esta ha sido un área de estudio muy activa y los responsables de la formulación de políticas harían bien en tomar nota de las recomendaciones formuladas por los académicos.[49]

3.5.2 Riesgo de la cadena de suministro derivado de las dependencias compartidas

Una gran cantidad de software crítico, tanto FOSS como comercial, depende de algunos de los mismos componentes de FOSS. Un error grave en una biblioteca criptográfica de FOSS muy utilizada podría afectar todas las implementaciones DNS.[50] También hay otros componentes menos visibles que se reutilizan con frecuencia. Se trata de una debilidad potencial significativa, no solo en el DNS o en FOSS, sino en el software en general.[51] Los riesgos de sostenibilidad mencionados anteriormente en la sección 3.5.1 también se aplican a estos componentes compartidos, lo que agrava la amenaza.

Este riesgo se ve agravado por el hecho de que los colaboradores de FOSS con intenciones maliciosas pueden incorporar código malicioso en proyectos de código abierto o en sus componentes sin ser detectados. Pueden introducirse mediante la manipulación de los repositorios de paquetes o como contribuciones a proyectos. Es necesario estar atento a la hora de revisar y supervisar las dependencias del código para evitar que se incorpore código malicioso a los proyectos de software.

3.5.3 FOSS no incluye garantía ni asistencia técnica

El software de libre disposición es una opción atractiva, ya que se ofrece sin costo alguno y, por lo general, solo hay que descargar el paquete. Pero dado que no incluye garantía ni promesa de asistencia técnica, su uso también conlleva riesgos. Por defecto, no existe ningún contrato más allá del acuerdo de licencia de código abierto entre el proveedor del producto de FOSS y el usuario.[52] A menos que el usuario acuerde por su cuenta el mantenimiento con el encargado del

[49] Eghbal, Nadia. “Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure.” *[Caminos y puentes: El trabajo invisible detrás de nuestra infraestructura digital*]. Ford Foundation, 14 de julio de 2016. https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/.

[50] Al igual que el software de DNS, el desarrollo de software criptográfico es un trabajo especializado. Si bien existen algunos sistemas criptográficos de FOSS de larga duración, la diversidad y la calidad son un problema.

[51] Para consultar un ejemplo de un intento de hacer visibles las dependencias compartidas, consultar “Census III of Free and Open Source Software ”[*Censo III del software libre y de código abierto*], The Linux Foundation, diciembre de 2024: https://www.linuxfoundation.org/research/census-iii

[52] La existencia de relaciones contractuales entre los encargados del mantenimiento y los operadores es un error común, que se aborda en la sección 3.2.2.

mantenimiento u otras personas, no tendrá garantía alguna de mantenimiento activo ni asistencia técnica.

Si un producto tiene fallas de seguridad, ya sean introducidas accidentalmente, como en el caso del error Heartbleed de OpenSSL[53], o de forma maliciosa, como en el caso de la puerta trasera de xz Utils,[54] nadie está obligado a proporcionar soluciones. Si bien técnicamente cualquiera, incluido el usuario, puede obtener una copia del código fuente y corregir el problema manualmente, dicha "bifurcación" requiere una gran experiencia en ingeniería de software y recursos operativos, por lo que, en la mayoría de los casos, el usuario no tiene control efectivo sobre la disponibilidad de las correcciones. Este problema es especialmente grave en paquetes que, como OpenSSL y xz, se utilizan tan ampliamente que no hay sustitutos fácilmente disponibles. Los riesgos de la monocultura no se limitan al código abierto, pero esta puede ser una razón por la que esos riesgos generales sean aplicables a FOSS.

La disminución del interés por parte de la comunidad para proporcionar mantenimiento para FOSS podría convertirse en un incentivo para la entrada de organizaciones que ofrezcan mantenimiento bajo contrato. Sin embargo, los cambios en el código base realizados por estas organizaciones de apoyo normalmente se enviarían de vuelta al proyecto de FOSS para minimizar la carga que supone mantener un código base independiente. A su vez, esto permite que otros se beneficien de este mantenimiento sin tener que pagar por él. Esto conlleva un problema de oportunismo: cuando un proveedor de servicios utiliza FOSS, pero no contribuye a su mantenimiento, puede hacerlo a un costo menor que un competidor que sí lo hace, lo que le permite ofrecer precios más bajos.[55]

La falta de garantía o asistencia inherente puede mitigarse. Los operadores pueden capacitar y retener a los expertos de su plantilla, financiar o contratar a encargados del mantenimiento,[56] o celebrar contratos de asistencia técnica para acceder a los conocimientos de los encargados del mantenimiento o colaboradores expertos.[57] El informe de BITAG citado en la sección 3.5.1 ejemplifica los obstáculos organizacionales que impiden a los operadores hacerlo.

---

[53] "Heartbleed Bug," [*Error Heartbleed*], https://heartbleed.com/.
[54] Goodin, Dan. "What We Know about the xz Utils Backdoor That Almost Infected the World" [*Lo que sabemos sobre la puerta trasera xz Utils que casi infecta al mundo entero*]. Ars Technica, 1 de abril de 2024. https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/.
[55] Por ejemplo, una asociación empresarial alemana de desarrolladores de FOSS señaló esto como un problema en la adquisición pública de FOSS. Consultar el Grupo de Trabajo sobre Adquisiciones de la Open Source Business Alliance, «Criterios de selección para la adquisición sostenible de software de código abierto", Open Source Business Alliance, 11 de febrero de 2025. https://osb-alliance.de/publikationen/veroeffentlichungen/selection-criteria-for-the-sustainable-procurement-of-open source-software.
[56] Valsorda, Filippo. "I'm Now a Full-Time Professional Open Source Maintainer" [*Ahora soy un encargado profesional del mantenimiento de código abierto a tiempo completo*], 2 de febrero de 2023. https://words.filippo.io/full-time-maintainer/.
[57] Hay contratos de asistencia técnica disponibles para varios de los sistemas FOSS tratados en este informe.

3.5.4 Riesgos operativos en la implementación

La naturaleza distribuida de FOSS plantea retos operativos relacionados con la autenticidad del software, la aplicación de parches y la escasez de operadores cualificados.

Comprobación de la autenticidad del software

FOSS se distribuye libremente a través de Internet y, por lo tanto, podría ser objeto de secuestro o sustitución por código falsificado. Debido a este riesgo, FOSS es habitualmente firmado por el encargado del mantenimiento, utilizando métodos criptográficos sólidos. El usuario puede verificar estas firmas para garantizar la integridad del software. Todas las implementaciones de DNS FOSS más frecuentemente utilizadas en la infraestructura de Internet están firmadas. Sin embargo, es posible que los usuarios no comprueben estas firmas o que obtengan el software a través de intermediarios que no verifican ni mantienen la integridad del software.

Falta de información sobre las implementaciones y rapidez en la aplicación de parches

Existe un gran interés por parte de los investigadores en buscar vulnerabilidades en el software de DNS FOSS y un amplio historial de conclusiones y notificaciones de las mismas. Todos los principales proveedores de software de DNS siguen las mejores prácticas generalmente aceptadas para gestionar, corregir y divulgar las vulnerabilidades del software. Sin embargo, no hay una fuente confiable de información sobre si los usuarios actualizan su software a las versiones actuales y mejoradas, ni sobre la rapidez con la que lo hacen.

En el ámbito de FOSS en general, hay pocos datos con los que trabajar para evaluar este riesgo. El hecho de que los consumidores de software a menudo reciban el software a través de un tercero —un empaquetador de sistemas operativos o un entusiasta de FOSS que puede haber copiado y redistribuido el software— dificulta aún más el seguimiento de la implementación de las actualizaciones. Este riesgo podría abordarse mediante normativas que exijan algún tipo de notificación centralizada por parte de los operadores sobre cualquier software que sea crítico para sus operaciones de producción.

Subcontratación y escasez de personal cualificado

La complejidad que entraña el funcionamiento correcto de los sistemas FOSS supone un problema, ya que en algunas partes del mundo hay escasez de operadores cualificados. Esta combinación de criticidad y complejidad lleva a algunos responsables de la toma de decisiones a subcontratar los servicios en la nube, lo que puede debilitar la diversidad y la naturaleza distribuida del sistema, reduciendo potencialmente la resiliencia y la seguridad. Por ejemplo, si todos los habitantes de una región eligen un proveedor de servicios de correo electrónico gestionado conocido porque es más fácil que crear, operar y mantener sus propios servidores de correo electrónico, la disponibilidad del correo electrónico en toda la región estará determinada por la estabilidad de un único proveedor de servicios de correo electrónico.

También se está produciendo un cambio generacional en las empresas y los proveedores de servicios más pequeños, donde los empleados con menos experiencia se han vuelto dependientes de los servicios en la nube y están menos familiarizados con el funcionamiento de sus propios servicios de red. Varias organizaciones imparten cursos de capacitación para operadores (APNIC, NSRC, PCH) con el fin de desarrollar habilidades en materia de DNS y otras habilidades relacionadas con la administración de redes. En los proyectos de FOSS se intenta abordar este problema con paquetes pre compilados y funciones fáciles de usar, pero sigue siendo difícil competir con las alternativas de software como servicio.

4 Prevalencia de FOSS en el DNS y la infraestructura de registración de nombres de dominio

FOSS desempeña un rol crucial y dominante en las operaciones técnicas de los sistemas de nombres de dominio y registración de Internet. En las partes más críticas de esta infraestructura, FOSS es la norma y el software propietario es la excepción. La investigación de este informe establece que la infraestructura del DNS global y distribuida depende de FOSS. Al menos nueve de los doce operadores de RSS de Internet utilizan exclusivamente implementaciones de DNS FOSS. Del mismo modo, nueve de los diez mayores proveedores de servicios para TLD utilizan FOSS. En el ámbito de la registración de nombres de dominio, aunque muchos sistemas grandes son propietarios, la gran mayoría se basan en componentes de FOSS, y los principales proveedores de servicios de custodia de datos para registros y registradores también se basan en FOSS. Las siguientes secciones detallan la prevalencia de FOSS en cada componente de esta infraestructura crítica. La metodología se describe en el Apéndice B.

4.1 FOSS en la infraestructura de registración de nombres de dominio

La infraestructura de registración se refiere a los sistemas que facilitan la registración de nombres de dominio individuales y que hacen que los nombres de dominio registrados estén disponibles en el DNS público. Si bien no se dispone de datos explícitos sobre el alcance total del uso de FOSS, las pruebas muestran una profunda dependencia del mismo, tanto como sistemas completos como componentes fundamentales.

Varios operadores de registro mantienen una infraestructura de registración que es totalmente FOSS (Tabla 1). Por ejemplo, se sabe que la plataforma de registro FRED es utilizada por al menos 12 registros de ccTLD, y la plataforma Nomulus se utiliza para múltiples registros de gTLD.

Tabla 1: Sistemas FOSS utilizados para operaciones de registro

Sistema de software	Licencia de código abierto	Usado por
FRED	GPLv3	FRED es utilizado (al menos) por los ccTLD de Albania, Angola, Argentina, Bosnia y Herzegovina, Costa Rica, República Checa, Lesoto, Macao, Malaui, Macedonia del Norte, Paraguay y Tanzania.
Internet ee domain registry	MIT	ccTLD para Estonia (.ee).
Namingo	MIT	Namingo está diseñado para la próxima ronda del Programa de Nuevos gTLD de la ICANN de 2026.
Nomulus	Apache 2.0	Registros de gTLD de Google, incluidos .app, etc.

Tabla 2: Sistemas de registro basados en componentes de FOSS

Sistema de registro/Servicio backend	Ejemplos de componentes de código abierto en uso	Registro en uso por
Afnic	Servidor web, base de datos	20 TLD, incluido .fr
CIRA / SIDN / Hello Registry	Base de datos, servidor web, servidor de aplicaciones, informes, front end	6 ccTLD, 6 gTLD, incluidos .ca, .ie
CoCCA	Servidor web, servidor de aplicaciones, base de datos	56 ccTLD
CORE Association	Servidor web, base de datos, bibliotecas Java	1 ccTLD, 21 gTLD
GoDaddy Registry	Base de datos, servidores de aplicaciones, informes, supervisión, registro, pruebas, front end, DNS.	200+ TLD
Identity Digital	Base de datos	250 gTLD y ccTLD. incluidos los ccTLD .au, .me,.pr
Nominet	Base de datos, servidor de aplicaciones, análisis sintáctico, registro, pruebas, front end, servidor de nombres	85+ TLD, incluido .uk
TANGO Registry Services	Servidor web, base de datos, bibliotecas Java	8 gTLD
Tucows Registry	Base de datos, software de DNS y herramientas accesorias, servidores web y de correo electrónico, colas de mensajes,	222 “TLD", incluidos SLD administrados como TLD,

Sistema de registro/Servicio backend	Ejemplos de componentes de código abierto en uso	Registro en uso por
	orquestación y virtualización de infraestructuras, sistema operativo	incluidos .my y com.my
Verisign[58]	(no se proporciona ninguno)	.com, .net, .edu y otros TLD

[58] Verisign proporcionó la siguiente declaración para este informe: "Verisign utiliza su plataforma de resolución de DNS patentada Advanced Transaction Lookup and Analysis System (ATLAS). Verisign también utiliza una infraestructura de registración y resolución diseñada específicamente que emplea una colección diversa y seleccionada de componentes de software comercial y de código abierto para garantizar la redundancia.

Por el contrario, los registros y backends de registros más grandes suelen utilizar sistemas propietarios. Sin embargo, estos sistemas no suelen crearse desde cero, sino que a menudo se basan en extensiones e integraciones de componentes patentados y personalizados, como bases de datos y servidores web, que en su mayoría son FOSS (Tabla 2).

Esta dependencia en FOSS también se aplica a los servicios de custodia de datos, que almacenan de forma segura copias de los datos de registración de nombres de dominio. Los tres mayores proveedores de estos servicios, tanto para registros como para registradores, han construido sus sistemas, al menos parcialmente, sobre componentes de FOSS (Tabla 3).

Tabla 3: FOSS en agentes de custodia de datos

Agente de custodia de datos	Para Registros	Para Registradores	¿Incorpora FOSS en funciones clave?
Beilong Zedata (Beijing) Data Technology Co., Ltd	✓	✓	No
Centro de Información de Redes de Internet de China (CNNIC)	✓	✓	No
Centro de Información de Nombres Organizacionales de China (CONAC)	✓	✓	No
DENIC Services GmbH & Co. KG	✓	✓	Sí, parcialmente
Escrow4All	✓		Sí
Sociedad Anónima de Intercambio de Internet "MSK-IX"	✓	✓	Desconocido
NCC Group	✓		Sí, parcialmente
Centro de Información de Redes de Taiwán (TWNIC)	✓		No

La infraestructura del registrador no se midió ni fue objeto de encuestas a los fines de este informe. Consideramos probable que los registradores utilicen habitualmente extensiones e integraciones de componentes personalizadas y patentadas que en su mayoría son FOSS. Por ejemplo, algunos registradores utilizan el software de servidor web nginx o Apache para operar sus portales web para los registratarios. También utilizan soluciones FOSS para supervisar el software, analizar datos, gestionar códigos y otras necesidades.

4.2 FOSS en la infraestructura de publicación del DNS (servidores autoritativos)

La evidencia del dominio de FOSS es más clara en la infraestructura que publica información de dominios. En los niveles más altos de la jerarquía del DNS, la raíz y los TLD, FOSS es casi omnipresente.

El RSS es el nivel más alto de la jerarquía del DNS. De las 12 organizaciones independientes que operan los servidores raíz, al menos nueve utilizan exclusivamente implementaciones de DNS FOSS para responder a las consultas (Tabla 4).

Tabla 4: Uso de FOSS en el Sistema de Servidores Raíz

Identificador de servidor raíz	Software	de código abierto[59]
A, J	ATLAS (propietario) NSD	Parcialmente[60]
B	Knot BIND9	Sí[61,62]
C	BIND9	Sí
D	NSD	Sí
E	*desconocido* (FOSS), *interno* (propietario)[63]	Parcialmente[64]
F	BIND9, *interno* (propietario)[65]	Parcialmente
G	BIND9	Sí
H	NSD	Sí

[59] Willem Toorop et al., "RSSAC028 Implementation Study Report" [*Informe del estudio de implementación del documento RSSAC028*] (informe, NLnet Labs y Stichting Internet Domeinregistratie Nederland (SIDN), 27 de septiembre de 2023), 15. https://www.icann.org/en/system/files/files/rssac028-implementation-study-report-27sep23-en.pdf.

[60] Según la declaración de Verisign sobre las expectativas de servicio de RSSAC001v2 de los servidores raíz, "Verisign utiliza dos bases de código diferentes para el servicio raíz del DNS: (1) nuestra plataforma de resolución ATLAS patentada y de propiedad exclusiva, y (2) el software de código abierto NLnet Labs Name Server Daemon (NSD). Una, la otra o ambas implementaciones pueden estar en uso en un momento dado". https://a.root-servers.org/aroot-rssac001v2-expectations.pdf.

[61] "Servidor raíz del DNS de USC/ISI", https://b.root-servers.org/.

[62] "RSSAC023v2: History of the Root Server System" [*RSSAC023v2: Historia del Sistema de Servidores Raíz*]. Comité Asesor del Sistema de Servidores Raíz (RSSAC) de la ICANN, 17 de junio de 2020. https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf.

[63] Grant, Dani. "Delivering Dot" [*Prestando servicio al punto*] Blog de Cloudflare, 10 de septiembre de 2017. https://blog.cloudflare.com/f-root/.

[64] Bischof, Ralph. [64] Bischof, Ralph. ":E-Root Instance in San Francisco Servfails?" [*¿Fallo de la instancia :E del servidor raíz en San Francisco?*], 19 de junio de 2025. https://lists.dns-oarc.net/pipermail/dns-operations/2025-June/022899.html.

[65] Grant, "Delivering Dot" [*Prestando servicio al punto*].

Identificador de servidor raíz	Software	de código abierto[59]
I	*confidencial*	Sí[66]
K	BIND9 Knot NSD	Sí
L	Knot NSD	Sí
M	BIND9	Sí[67]

Si analizamos conjuntamente los ccTLD y los gTLD, observamos que nueve de los diez principales operadores que prestan servicios autoritativos para los registros de TLD utilizan FOSS para ello.[68]

Por debajo de la raíz y los TLD, existe una amplia gama de entidades, incluidos individuos, empresas, universidades y gobiernos que operan los servidores de nombres autoritativos. Si bien no se dispone de datos completos sobre este grupo tan diverso, se sabe que muchos de los sistemas de FOSS utilizados en la raíz y en los TLD son también las opciones más conocidas para estos operadores. Muchas de las organizaciones que ofrecen servicios secundarios del DNS son las mismas que prestan servicios de DNS autoritativos para los TLD. Las tablas 5 y 6 enumeran los sistemas FOSS y los productos comerciales adecuados para implementaciones autoritativas del DNS.

Los servidores de nombres autoritativos suelen integrarse con sistemas de aprovisionamiento para facilitar la actualización de la información de la zona e implementar la autorización y los controles adecuados sobre el mantenimiento de estos registros. Algunos de los sistemas de aprovisionamiento más populares son FOSS.[69]

Gran parte del contenido más visitado de Internet se aloja en unas pocas redes de contenido de gran tamaño, como YouTube, de Google, que utiliza un sistema de DNS propietario. Si bien varios grandes operadores de servicios autoritativos que operan el segundo nivel y los niveles inferiores de la jerarquía utilizan FOSS (por ejemplo, aquellos que también prestan servicio a las zonas raíz o TLD), no se cuenta con suficientes declaraciones públicas para realizar un estudio

[66] Compartido con permiso de Netnod en correspondencia con el SSAC con fecha del 13 de diciembre de 2024.
[67] "Servidor de DNS raíz M", https://m.root-servers.org/.
[68] Principales operadores por número de TLD a los que se prestan servicio. Consultar el Apéndice B para obtener una descripción de la metodología utilizada.
[69] Entre los sistemas más populares se encuentran VinylDNS (https://www.vinyldns.io/), gestionado por Comcast, y OctoDNS, gestionado por Amazon y Oracle. DNS Control es otro sistema de configuración conocido que gestiona el DNS tanto en sistemas autoalojados como en servicios en la nube, incluidos Cloudflare, el servicio Route53 de Amazon y Gandi, un registrador de lDNS y proveedor de alojamiento. DNS Control es otro sistema de configuración popular que gestiona el DNS tanto en sistemas autoalojados como en servicios en la nube, incluidos Cloudflare, el servicio Route53 de Amazon y Gandi, un registrador de lDNS y proveedor de alojamiento.

fiable y elaborar estadísticas sobre su uso de FOSS.[70] Consultar más información en las tablas que se presentan a continuación. Se trata de una laguna notable en la información disponible, ya que cuatro grandes proveedores pueden representar más de la mitad de las consultas de nombres autoritativos visibles en Internet.[71]

4.3 FOSS en la infraestructura de recuperación del DNS (resolutores)

La prevalencia de FOSS no se limita a la publicación de datos del DNS, sino que es igualmente significativa en la infraestructura que recupera esa información: el diverso ecosistema de resolutores del DNS. FOSS tiene una presencia significativa en todo el ecosistema de resolutores, desde redes locales hasta plataformas globales en la nube.

La mayoría de los usuarios reciben servicio de resolutores locales operados por sus ISP, empresas o instituciones educativas. En las investigaciones se ha estimado que el porcentaje total de usuarios que reciben servicio de los resolutores en la nube es inferior al 20 % en todo el mundo. El 80 % restante de los usuarios utiliza algún tipo de resolutor local.[72] Muchos de los sistemas de FOSS más comunes pueden utilizarse tanto para funciones autoritativas como de resolutor (Tabla 5).

Tabla 5: Sistemas de FOSS de uso común para aplicaciones de servidores del DNS

Sistema de software	Licencia de código abierto	Aplicación- Usuarios de ejemplo
BIND9	MPL 2.0	Autoritativos, Resolutores - CIRA, NIC.BR, Visionary Broadband
CoreDNS	Apache 2.0	Kubernetes, Autoritativo - Meta
dnsdist	GPL 2.0	Equilibrio de carga del DNS
Dnsmasq	GPL 2 o 3	Predominantemente resolutores: populares en sistemas integrados, como OpenWRT y puertas de enlace domésticas.
Knot DNS	GPL 3.0	Autoritativo - TLD .cz
Resolutor Knot	GPL 3.0	Resolutor - DNS4EU
NSD	BSD 3-Clause	Autoritativo - Rcode Zero
PowerDNS	GPL 2.0	Autoritativo- Rakuten

[70] Las mediciones fiables de la adopción de FOSS constituyen un problema difícil. Daniel Stenberg ofrece varias razones por las que esto es así en "What We Can't Measure" [*Lo que no podemos medir*], Daniel://Stenberg:// (blog), 5 de junio de 2025, https://daniel.haxx.se/blog/2025/06/05/what-we-cant-measure/.
[71] Huston, Geoff. "Looking at Centrality in the DNS" [*Análisis de la centralidad en el DNS*]. Blog de APNIC (blog), 22 de noviembre de 2022. https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/.
[72] Huston, "Looking at Centrality in the DNS" [*Análisis de la centralidad en el DNS*].

Recursor PowerDNS	GPL 2.0	Resolutor - British Telecom
Unbound	BSD 3-Clause	Resolutor - Quad9, Let's Encrypt
YADIFA	BSD 3-Clause	Autoritativo - TLD .eu

Si bien existen muchos productos comerciales para este mercado, la mayoría de ellos incorporan una o más soluciones de FOSS como componente del DNS central de su oferta (Tabla 6).

En la nube, las plataformas informáticas a hiperescala como Microsoft Azure, Google Cloud y AWS de Amazon operan importantes infraestructuras de resolutores para dar soporte a sus servicios. Al menos cuatro de los hiperescaladores más grandes confían en FOSS para la resolución de DNS,[73] mientras que otros han creado soluciones propietarias basadas en bibliotecas de DNS FOSS. (Tabla 7).

Por último, algunos usuarios finales configuran sus sistemas para eludir el resolutor provisto por su operador de red y, en su lugar, utilizan resolutores públicos abiertos. Mientras que dos de los servicios públicos más populares (8.8.8.8 de Google y 1.1.1.1 de Cloudflare) utilizan software propietario, otros resolutores públicos importantes, como Quad9 (9.9.9.9) y DNS4EU, se basan en FOSS. En el Apéndice B se ofrece más información al respecto.

[73] Vago por diseño basado en la confidencialidad.

Tabla 6: Ejemplos de servicios de DNS comerciales que incorporan FOSS

Fabricante	Producto	Solicitud	Incorpora FOSS
Akamai	Edge DNS	Resolutor híbrido en la nube y servicio autoritativo	No
Bluecat Networks	Integridad, Micetro	Autoritativo, resolutor	Sí
Cygna Labs	VitalQIP, DiamondIP	Autoritativo, resolutor	Sí
EfficientIP	SolidServer DDI	Autoritativo, resolutor, dispositivo y nube	Sí
F5	BIG-IP DNS	Resolutor	Sí
IBM	NS1 Connect	Servicio autoritativo basado en la nube	Desconocido
InfoBlox	Universal DDI & NIOS DDI	Autoritativo, resolutor, dispositivo y nube	Sí
Knipp	IronDNS	Autoritativo	Parcial.
Microsoft	Windows Server DNS	Autoritativo, resolutor, utilizado en redes empresariales, se integra con Active Directory.	No
	DNS de Azure	Servicio de resolutor en la nube	Sí
Netgate	pfSense	Resolutor	Sí
Oracle	OCI DNS	Servicio autoritativo en la nube	Sí
TCPWave	DDI Management	Dispositivo autoritativo	Sí

Tabla 7: Bibliotecas de FOSS utilizadas para aplicaciones de infraestructura del DNS

Sistema de software	Lenguaje de programación	Aplicación- Usuarios de ejemplo
c-ares	C	libcurl, curl, NodeJS
dnsjava	Java	Backends de registro (propietario)
dnspython	Python	Mailman, Samba, Ansible
domain	Rust	Cascade
miekg/dns	Ir	Let’s Encrypt, CoreDNS, Docker
ldns	C	Zonemaster, dnstap, servidores de nombres (propietario)
libunbound	C	Open vSwitch, libreswan, opendkim

Sistema de software	Lenguaje de programación	Aplicación- Usuarios de ejemplo
Net: DNS	Perl	Spamassassin, Mail::DMARC, Mail::DKIM, Mail:SPF

5 Casos prácticos actuales relacionados con la regulación de FOSS

En esta sección se evalúan varios casos contemporáneos de Estados Unidos, Reino Unido y la Unión Europea que ilustran cómo los responsables de la formulación de políticas están adaptando las regulaciones de ciberseguridad a las realidades únicas del ecosistema de FOSS. La Tabla 8 ofrece un resumen general de estos enfoques, que muestran una tendencia a eximir a los encargados del mantenimiento voluntarios de responsabilidad directa y que, a la vez, se centran en las responsabilidades de las entidades comerciales que integran o implementan FOSS. A continuación, se analiza cada caso en detalle.

Tabla 8: Resumen de los enfoques actuales sobre FOSS en el ámbito regulatorio

Sección	Enfoque clave	Regulación de ejemplo	Tratamiento de FOSS
5.1	Asignar responsabilidades	Estrategia de ciberseguridad de EE. UU. para 2023, Código del Reino Unido de 2025	Eximir a los encargados del mantenimiento de responsabilidad, centrarse en las entidades comerciales
5.2	Incentivar la colaboración	Reglamento de Ciberresiliencia de la UE	Incorporar la función opcional de "administrador" para incentivar el apoyo.
5.3	Evitar suposiciones de propiedad	Ley de implementación de la Directiva NIS 2 de la UE	Sin contratos = Sin proveedor directo, fomentar el apoyo
5.4	Evitar regímenes contradictorios	Directiva NIS 2 de la UE	Evitar superposiciones para elementos globales como servidores raíz

5.1 Asignar la responsabilidad a las partes interesadas con mayor capacidad de acción.

La Estrategia Nacional de Ciberseguridad de EE. UU. de 2023[74] buscaba trasladar la responsabilidad por los productos y servicios de software no seguros (objetivo estratégico 3.3).

[74] Presidente de EE. UU. “National Cybersecurity Strategy” [*Estrategia Nacional de Ciberseguridad]*. Washington, DC: La Casa Blanca, 1 de marzo de 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

En ella se formuló una visión de general en la que "las empresas que crean software deben tener libertad para innovar, pero también deben asumir su responsabilidad cuando incumplan el deber de diligencia respecto de los consumidores, las empresas o los proveedores de infraestructuras críticas". Desde el principio, la estrategia se centró en los encargados del mantenimiento de FOSS con un enfoque más diferenciado: "La responsabilidad debe recaer en las partes interesadas más capaces de tomar medidas para evitar resultados negativos, y no en los usuarios finales, que a menudo sufren las consecuencias de un software inseguro, ni en los desarrolladores de código abierto de un componente integrado en un producto comercial".

Del mismo modo, el Código de Prácticas de Seguridad de Software voluntario del Reino Unido de 2025[75] tiene como objetivo "ayudar a los proveedores de software y a sus clientes a reducir la probabilidad y el impacto de los ataques a la cadena de suministro de software y otros incidentes relacionados con la resiliencia del software". Se aplica igualmente a los proveedores de software comercial: "En el caso del software de código abierto, el desarrollador/encargado del mantenimiento no tiene ningún compromiso formal con su cadena de suministro posterior ni con el mantenimiento y la seguridad continuos de su código. Cualquier riesgo asociado al código abierto debe ser gestionado por los usuarios finales o los desarrolladores propietarios que utilicen código abierto en su software.

5.2 Incentivar la colaboración entre sectores para lograr un mantenimiento sostenible

La CRA de la UE[76] tiene como objetivo abordar el "bajo nivel de ciberseguridad de los productos con elementos digitales, que se refleja en vulnerabilidades generalizadas y en el suministro insuficiente e inconsistente de actualizaciones de seguridad para solucionarlas". Si bien exime de responsabilidad a los encargados del mantenimiento de FOSS que no monetizan FOSS, incentiva la colaboración entre industrias para el mantenimiento sostenible de FOSS mediante la introducción de un nuevo actor legal ("administrador de software de código abierto") que "proporciona apoyo de forma sostenida para el desarrollo" y garantiza "la viabilidad de esos productos". Los administradores son una función opcional, aún poco extendida, para las organizaciones con las que los encargados del mantenimiento de FOSS pueden optar por asociarse como medio para canalizar recursos de los fabricantes u operadores de infraestructuras esenciales que dependen de FOSS. Aunque la proporción de software libre que actualmente cuenta con el soporte de una organización similar a un administrador es muy reducida, la CRA podría incrementar esta práctica en el futuro, y es probable que se aplique a algunas de las organizaciones que mantienen software de DNS. Una última innovación en materia regulatoria es la futura opción de las "certificaciones de seguridad voluntarias", que dan lugar a la colaboración entre sectores en materia de verificación de antecedentes.

[75] "Código de prácticas de seguridad de software".
[76] Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo de 23 de octubre de 2024 relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia), 2024 DO (L 2024/2847) 1, https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

5.3 Evitar requisitos de seguridad de la cadena de suministro que presupongan el uso de software propietario

La Directiva NIS 2 de la UE tiene por objeto "mitigar las amenazas a los sistemas de redes y de información utilizados para prestar servicios esenciales en sectores clave".[77] Regula la infraestructura digital como un "sector de alta criticidad", asigna la responsabilidad de la gestión de la ciberseguridad y exige "medidas de gestión de riesgos", detalladas en una ley de implementación.[78] Entre ellos se incluyen "la seguridad de la cadena de suministro, incluidos los aspectos relacionados con la seguridad que afectan a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos". El Anexo que detalla estos requisitos se deriva de los controles de la norma ISO/IEC 27002:2022 y, contrariamente a la realidad de FOSS (consultar la sección 3.2.2), supone una cadena de obligaciones contractuales que llega hasta el desarrollador de software.

En su guía de implementación técnica para entidades reguladas,[79] la Agencia de la Unión Europea para la Ciberseguridad, ENISA, aclara el concepto de "prestador de servicios y proveedor directo" con respecto a FOSS: “En el caso del software libre y de código abierto (FOSS), las comunidades y los proyectos que desarrollan, mantienen y distribuyen software de forma abierta pueden no considerarse prestadores de servicios o proveedores directos cuando no exista una relación contractual entre la entidad pertinente y el proyecto de código abierto, más allá de la adhesión a una licencia de derechos de autor estandarizada, o cuando la relación contractual sea con un administrador de software de código abierto". En su lugar, recomienda "considerar la posibilidad de apoyar a las comunidades que desarrollan y mantienen FOSS e invertir en una relación mutuamente beneficiosa con ellas". Cuando resulte adecuado, esto podría suponer establecer una relación con el administrador de OSS pertinente que ‘proporcione asistencia de forma sostenida para el desarrollo y garantice la viabilidad de esos productos’.

Un informe de 2025 encargado por el Departamento de Ciencia, Innovación y Tecnología del Reino Unido analizó las prácticas de la industria en materia de código abierto y los riesgos de la cadena de suministro.[80] Entre otras cosas, el informe recomienda que las organizaciones "establezcan una política interna de OSS para gestionar la adopción de componentes de OSS" y "promuevan la participación activa con la comunidad de OSS para [...] garantizar componentes de OSS de alta calidad y un ecosistema de OSS sostenible". Por el contrario, una normativa en materia de seguridad de la cadena de suministro que no se adapte a FOSS impondría requisitos contractuales a los operadores con el fin de exigir la verificación de los antecedentes de los

[77] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, (Directiva NIS 2), 2022 DO (L 333) 80, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.
[78] Reglamento de Ejecución (UE) 2024/2690 de la Comisión del 22 de octubre de 2024, por el que se establecen las disposiciones de aplicación del Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, 2024 DO (L 2024/2690) 1, https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj.
[79] Agencia de la Unión Europea para la Ciberseguridad (ENISA), NIS2 Technical Implementation Guidance [*Guía para la implementación técnica de la NIS*2] (informe, Oficina de Publicaciones de la Unión Europea, 2025). https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.
[80] "Mejores prácticas de software de código abierto y gestión de riesgos en la cadena de suministro".

encargados del mantenimiento de FOSS, considerándolos "proveedores", aunque no se haya adquirido el FOSS. Una regulación tan poco pensada podría provocar que los profesionales de FOSS abandonaran sus proyectos, lo que dejaría a los proyectos con menos encargados del mantenimiento o con encargados del mantenimiento menos competentes, lo que a su vez provocaría un deterioro de la calidad. Esto va en contra del efecto deseado de la normativa sobre seguridad de la cadena de suministro.

5.4 Evitar normativas regionales contradictorias para las comunidades de FOSS en todo el mundo

La regulación directa del desarrollo de software y su uso en infraestructura crítica no es una práctica muy extendida. Dado que FOSS permite el desarrollo colaborativo a nivel mundial (sección 3.2.1), los futuros regímenes regulatorios deberían evitar crear requisitos superpuestos y mutuamente contradictorios que se diferencien en función de la ubicación física de los encargados del mantenimiento individuales.

La mencionada Directiva NIS 2 de la UE[81] veló por evitar una situación similar de superposición de regímenes con sus requisitos para los proveedores de servicios del DNS, al excluir los servidores de nombres raíz de su ámbito de aplicación, eludiendo así una situación en la que los operadores de servidores raíz estuvieran sujetos a regímenes regionales superpuestos y, en ocasiones, contradictorios.[82]

6 Conclusiones principales

Esta sección consolida el análisis central del informe en una serie de conclusiones que constituyen la base empírica de las pautas prácticas que se exponen a continuación.

Conclusión 1: FOSS es la base de la infraestructura crítica del DNS. A medida que los responsables de la formulación de políticas y los organismos reguladores de todo el mundo tratan de garantizar la seguridad de la cadena de suministro de software, es fundamental que sus esfuerzos se basen en una comprensión clara de cómo se construyen y mantienen realmente los sistemas más fundamentales de Internet. La investigación realizada para este informe establece que la infraestructura global del DNS actual depende en gran medida de FOSS. En las partes más críticas de esta infraestructura, FOSS es la norma y el software propietario es la excepción. Esto incluye el RSS, donde al menos nueve de los doce operadores utilizan exclusivamente implementaciones de DNS FOSS, y los TLD, donde nueve de los diez mayores proveedores de servicios utilizan FOSS.

[81] Directiva NIS 2.
[82] Se puede encontrar un resumen de los argumentos de Bert Hubert en “Dear EU: Please Don’t Ruin the Root” [*Estimada UE: Por favor no arruinen la raíz*], 10 de mayo de 2021, https://berthub.eu/articles/posts/dont-ruin-the-root/.

Conclusión 2: El modelo de desarrollo de FOSS es radicalmente diferente del software propietario. Mientras que el software propietario suele ser creado internamente por una sola organización, el modelo de FOSS es abierto y distribuido. Se basa en cuatro libertades esenciales que otorgan sus licencias: la libertad de usar, estudiar, compartir y modificar el software. Este marco fomenta un ecosistema único de encargados del mantenimiento, colaboradores y operadores que, por lo general, no se encuentran limitados por las relaciones contractuales que definen una cadena de suministro comercial tradicional.

Conclusión 3: FOSS no es inherentemente más o menos seguro que el software propietario; la seguridad depende del proceso y el mantenimiento, no de la visibilidad del código fuente. Las implicaciones de seguridad de este modelo abierto deben entenderse en el contexto de un debate que lleva décadas sin una respuesta clara. Como resumió el investigador en ingeniería de seguridad, Ross Anderson, en el caso de los sistemas grandes y complejos, la visibilidad del código fuente ayuda tanto a los atacantes como a los defensores por igual. A largo plazo, el hecho de que un sistema sea abierto o cerrado tiene poca relevancia para su seguridad. Ocultar el código fuente no proporciona seguridad adicional; en cambio, la seguridad de un sistema surge de la calidad de sus procesos de desarrollo, revisión y mantenimiento.

Conclusión 4: El ecosistema de DNS FOSS tiene fortalezas únicas que promueven la estabilidad y la resiliencia. Si bien la apertura en sí misma puede ser neutral, el proceso colaborativo que permite es especialmente eficaz para crear y mantener infraestructuras críticas de Internet. La transparencia inherente a FOSS permite a una comunidad global de desarrolladores, investigadores y operadores estudiar el código fuente y abordar las vulnerabilidades de forma colectiva, una práctica que a menudo da lugar a parches más rápidos que en los sistemas propietarios. Esto da lugar a ventajas inherentes, entre las que se incluyen una mayor seguridad colaborativa, resiliencia operativa gracias a la diversidad de software y una notable estabilidad proporcionada por el apoyo a largo plazo de organizaciones sin fines de lucro y comerciales dedicadas.

Conclusión 5: El modelo de FOSS conlleva riesgos inherentes que requieren un enfoque normativo personalizado, y no uno único para todos los casos. Las mismas características que proporcionan estas fortalezas también introducen un conjunto específico de riesgos que requieren un enfoque adaptado en cuanto a las políticas. Dado que el modelo de desarrollo de FOSS desvincula la financiación del uso, los proyectos pueden enfrentarse a retos relacionados con la sostenibilidad financiera y el agotamiento de los encargados del mantenimiento, en los que la infraestructura crítica puede depender de los esfuerzos voluntarios y sin financiación de unas pocas personas. Además, la reutilización generalizada de componentes de FOSS crea un riesgo de dependencias compartidas, en el que una vulnerabilidad en una sola biblioteca puede tener un impacto en cadena en todo el ecosistema. Estos problemas no pueden resolverse mediante regulaciones diseñadas para un mercado de software comercial y propietario.

Conclusión 6: La imposición de nuevas responsabilidades legales y financieras al desarrollo y la distribución de FOSS debe realizarse con precaución para evitar contaminar el entorno que propició el desarrollo de este elemento fundamental de la infraestructura de

Internet. La falta de una entidad jurídica única y responsable o de una cadena contractual convencional en los proyectos de FOSS hace que sea poco práctico y arriesgado aplicar los marcos de responsabilidad tradicionales. El modelo de desarrollo de FOSS depende de voluntarios individuales y de organizaciones pequeñas con fondos mínimos. Imponer cargas regulatorias pesadas a estos encargados del mantenimiento podría desalentar su participación, lo que podría frenar la innovación y provocar el abandono de software que es crucial para la infraestructura crítica de Internet.

Conclusión 7: FOSS es importante para permitir que ingresen nuevos proveedores al mercado de los servicios de Internet y ofrece oportunidades a los responsables de la formulación de políticas para fomentar el desarrollo de servicios locales y reducir la dependencia de los proveedores de servicios en la nube extranjeros. Más allá de su función técnica, FOSS es un facilitador del crecimiento económico, la autonomía digital y la competencia en el mercado. El modelo de desarrollo de FOSS reduce el costo de entrada en el mercado para las nuevas empresas al eliminar las tarifas de licencia de software. Esta accesibilidad fomenta la innovación y las habilidades locales, lo que proporciona a los responsables de la formulación de políticas una herramienta poderosa para crear un ecosistema digital más diverso y puede ayudar a reducir la dependencia de los servicios en la nube extranjeros.

7 Pautas aplicables a los responsables de la formulación de políticas

Esta sección se funda en las conclusiones del informe para proporcionar pautas directas y aplicables a los responsables de la formulación de políticas. El objetivo es permitir el desarrollo de una normativa eficaz y no perjudicial que refuerce, en lugar de que socave, el ecosistema de FOSS, que es fundamental para el funcionamiento seguro y estable de Internet.

Pauta 1: Reconocer el rol fundamental de FOSS. Este informe establece el hecho de que la infraestructura global del DNS depende de FOSS. En las partes más críticas de esta infraestructura, FOSS es la norma y el software propietario es la excepción. Por lo tanto, los responsables de la formulación de políticas deben reconocer explícitamente en cualquier legislación o normativa pertinente que FOSS sustenta la infraestructura crítica de Internet y que su uso es una fortaleza que debe preservarse. Este reconocimiento debe servir de base para la regulación desde la etapa inicial de diseño, con el fin de evitar daños involuntarios al ecosistema.

Pauta 2: Consultar a la comunidad de FOSS. El modelo de desarrollo de FOSS es abierto, distribuido y fundamentalmente diferente al del software propietario. Se trata de un ecosistema de encargados del mantenimiento, colaboradores y operadores que, por lo general, no están sujetos a las relaciones contractuales que definen una cadena de suministro comercial tradicional. Es esencial que participen todos los sectores del ecosistema de FOSS (incluidas empresas, organizaciones sin fines de lucro, encargados del mantenimiento individuales e instituciones comunitarias) a lo largo de todo el proceso de desarrollo de políticas. Esto garantiza que las

normativas se basen en sus realidades operativas y evita daños no deseados al ecosistema de FOSS y, en consecuencia, a la infraestructura crítica de Internet.

Pauta 3: Aprovechar los casos más recientes en materia de regulación de FOSS. Como se detalla en la sección 5, las recientes iniciativas regulatorias ya han comenzado a abordar las características únicas de FOSS, sin dejar de avanzar en los objetivos esenciales en materia de políticas. Estos casos proporcionan un marco valioso para desarrollar nuevas políticas que se adapten a las características únicas del ecosistema de FOSS. La aplicación de estas lecciones significa diseñar políticas y regulaciones que:

- Asignen la responsabilidad a las partes interesadas más capaces de actuar. El deber de cuidado recae sobre las entidades que implementan software en productos comerciales o infraestructura crítica, no sobre los desarrolladores voluntarios de FOSS que crean los componentes.
- Incentiven la colaboración entre industrias en materia de mantenimiento sostenible. La viabilidad de los productos de FOSS críticos puede garantizarse mediante el apoyo de modelos jurídicos innovadores, como el "administrador de software de código abierto", que canaliza los recursos de la industria.
- Eviten los requisitos de seguridad de la cadena de suministro que presuponen un modelo de software propietario. Se debe recordar que, en FOSS, a menudo no existe una relación contractual directa entre el encargado del mantenimiento y el operador más allá de la propia licencia de código abierto.
- Eviten crear regímenes regionales contradictorios para las comunidades globales de FOSS. En la normativa se deben evitar las obligaciones superpuestas y contradictorias para los proyectos globales de FOSS, a fin de impedir la fragmentación del desarrollo y el menoscabo de la seguridad.

Pauta 4: Incentivar la sostenibilidad de FOSS. El modelo de FOSS desvincula la financiación del uso, lo que se sabe que genera problemas de sostenibilidad financiera y agotamiento de los encargados del mantenimiento. La infraestructura crítica puede depender de pequeñas organizaciones o de los esfuerzos voluntarios y sin financiación de unas pocas personas. Para mitigar este riesgo, se alienta a los responsables de la formulación de políticas a crear políticas favorables que fomenten los aportes de los sectores público y privado a proyectos críticos de FOSS como una forma de inversión en un bien público compartido.

Pauta 5: Abordar los riesgos sistémicos de manera colectiva. La reutilización generalizada de componentes de FOSS crea un riesgo de dependencias compartidas, en el que una vulnerabilidad en una sola biblioteca puede tener un impacto en cadena en todo el ecosistema, tanto en productos de FOSS como de software propietario. Dado que se trata de un riesgo sistémico inherente a todo el desarrollo de software moderno, las políticas deberían fomentar y financiar soluciones colaborativas para todo el ecosistema, como la mejora de las herramientas de seguridad y la investigación independiente, en lugar de hacer recaer toda la carga sobre los encargados del mantenimiento voluntarios individuales.

8 Reconocimientos, divulgaciones de interés y abstenciones

En pos de la transparencia, estas secciones brindan al lector información sobre aspectos del proceso del SSAC. La sección Reconocimientos enumera los miembros del SSAC, los expertos externos y el personal de la ICANN que redactaron conjuntamente o contribuyeron directamente en este documento específico o quienes brindaron revisiones. La sección Divulgaciones de interés apunta a las biografías de todos los miembros del SSAC, que manifiestan intereses que pueden representar un conflicto, ya sea real, presunto o potencial, con la participación de un miembro en la elaboración de este informe. La sección Abstenciones identifica a los miembros individuales que se han abstenido de participar en el debate del tema con el que se relaciona este informe. A excepción de los miembros mencionados en la sección Abstenciones, este documento tiene la aprobación consensuada de todos los miembros del SSAC.

8.1 Reconocimientos

El Comité desea expresar su agradecimiento a los siguientes miembros del SSAC, invitados y personal de la ICANN por su tiempo, aportes y revisión en la elaboración de este informe.

Miembros del SSAC
Joe Abley
Maarten Aertsen (copresidente del grupo de trabajo)
Gautam Akiwate
Tim April
Nabil Benamar
KC Claffy
Hadia Elminiawi
Ondrej Filip (miembro del SSAC hasta el 31 de diciembre de 2024)
James Galvin
Robert Guerra
Russ Housley
Matthias Hudobnik
Geoff Huston
Layal Jebran
Merike Kaeo (miembro del SSAC hasta el 31 de diciembre de 2024)
Andrei Kolesnikov
Warren “Ace” Kumari
Barry Leiba (copresidente del grupo de trabajo)
John Levine
Russ Mundy
Ram Mohan
Matt Thomas
Peter Thomassen
Tara Whalen
Suzanne Woolf
Jiankang Yao

Invitados
Vittorio Bertola
Merike Kaeo (invitada después del 1 de enero de 2025)
Vicky Risk
Raffaele Sommese

Personal de la ICANN
John Emery (editor)
Daniel Gluck
Gustavo Lozano Ibarra
Michael Puckett
Carlos Reyes
Danielle Rutherford (editora, autora colaboradora)
Kathy Schnitt
Steve Sheng (miembro del personal de apoyo del SSAC hasta el 30 de noviembre de 2024)

8.2 Divulgaciones de interés

La información biográfica de los miembros del SSAC y sus divulgaciones de Interés al momento de la publicación está disponible en: https://www.icann.org/en/ssac/members/archive/16-05-2025.

8.3 Abstenciones

No hubo ninguna abstención.

Apéndice A: Glosario y acrónimos

A.1 Glosario de términos

Servidor autoritativo: Servidor que contiene los registros del DNS oficiales y definitivos de un nombre de dominio en particular. Proporciona las respuestas finales a las consultas al DNS para ese dominio.

Colaborador: Persona u organización que ofrece mejoras a un proyecto de FOSS, por ejemplo, enviando código, documentación o informes de errores.

Custodia de datos: Almacenamiento de una copia de los datos de registración de nombres de dominio en un tercero acreditado por la ICANN para su custodia.

Nombre de dominio: Nombre único y legible por el ser humano (por ejemplo, icann.org) que identifica una dirección específica en Internet y constituye la base de las URL.

Sistema de Nombres de Dominio (DNS): El sistema global y descentralizado que actúa como la "libreta de direcciones de Internet", traduciendo los nombres de dominio legibles por el ser humano a las direcciones IP numéricas necesarias para localizar servicios y dispositivos informáticos.

Protocolo de aprovisionamiento extensible (EPP): Protocolo técnico estandarizado utilizado para automatizar las transacciones entre los registros y registradores de nombres de dominio, tales como registraciones, renovaciones y transferencias.

Bifurcación: Un nuevo proyecto de software independiente que se inicia tomando una copia del código fuente de un proyecto de FOSS existente.

Software libre y de código abierto (FOSS): Software con una licencia que otorga a los usuarios cuatro libertades esenciales: usar, estudiar, compartir y modificar el software. Esto define un modelo de desarrollo colaborativo, no solo software gratuito.

Dirección de protocolo de Internet (IP): Etiqueta numérica única asignada a cada dispositivo conectado a una red informática que utiliza el Protocolo de Internet para comunicarse.

Nombre de dominio internacionalizado (IDN): Nombre de dominio en el que una o más de sus etiquetas contienen caracteres que no son letras, dígitos o guiones ASCII.

Encargado del mantenimiento: Persona o grupo responsable de la dirección general y control de calidad de un proyecto de FOSS. Tiene la autoridad para aceptar o rechazar contribuciones a la versión oficial del software.

Operador: Persona física u organización que implementa y utiliza software para ejecutar un servicio. En el contexto del DNS, un operador es una entidad que ejecuta componentes de la infraestructura del DNS, como servidores autoritativos o resolutores.

Publicación (en el DNS): Proceso técnico de hacer que los registros del DNS de un dominio estén disponibles en servidores autoritativos para que otros usuarios de Internet puedan encontrar el nombre de dominio.

Resolutor recursivo (o resolutor): Servidor, a menudo operado por un proveedor de servicios de Internet (ISP), que actúa en nombre del dispositivo de un usuario para encontrar la dirección IP correcta para un nombre de dominio solicitado.

Registración (en el DNS): El proceso administrativo de reservar un nombre de dominio único agregándolo a la base de datos maestra autoritativa (el registro) para un dominio de alto nivel específico.

Registratario: Persona física u organización que registra y posee los derechos sobre un nombre de dominio específico.

Registrador: Organización abierta al público que actúa como minorista de nombres de dominio, gestionando la reserva de dominios en nombre de los registratarios.

Registro: Base de datos maestra y autoritativa de todos los nombres de dominio registrados dentro de un dominio de alto nivel específico (por ejemplo, el registro .org). La organización que mantiene esta base de datos es el operador del registro.

Sistema de servidores raíz (RSS): Conjunto de servidores situados en el nivel más alto de la jerarquía del DNS que se encargan de dirigir las consultas a los servidores de dominio de alto nivel correctos.

Dominio de alto nivel (TLD): Segmento de un nombre de dominio situado a la derecha del punto final, como .com, .org o .uk.

Localizador uniforme de recursos (URL): La dirección completa utilizada para encontrar un recurso específico en Internet, que normalmente incluye un protocolo (por ejemplo, https), un nombre de dominio y una ruta específica (por ejemplo, https://www.icann.org/resources).

A.2 Abreviaturas utilizadas en este informe

ccTLD: Dominio de alto nivel con código de país
DNS: Sistema de nombres de dominio
EPP: Protocolo de aprovisionamiento extensible
FOSS: Software libre y de código abierto
gTLD: Dominio genérico de alto nivel
IP: Protocolo de Internet

ISP: Proveedor de servicios de Internet
RSS: Sistema de servidores raíz
SSAC: Comité Asesor de Seguridad y Estabilidad
TLD: Dominio de alto nivel
URL: Localizador uniforme de recursos
IDN: Nombre de dominio internacionalizado

Apéndice B: Metodología y conclusiones de la investigación sobre la prevalencia de FOSS

Este apéndice ofrece un resumen exhaustivo e independiente de la investigación original del informe. Detalla tanto la metodología utilizada para obtener los resultados sobre la prevalencia del software libre y de código abierto (FOSS) como las propias conclusiones, que se presentan en la sección 4 de este informe.

B.1 Enfoque general y desafíos

Determinar con certeza qué software utilizan los operadores en la práctica es todo un desafío. Si bien se introdujeron ciertos registros del Sistema de Nombres de Dominio (DNS) (por ejemplo, version.bind, authors.bind, id.server) para ayudar a los usuarios finales a identificar la versión del servidor del DNS con el que se están comunicando, estos registros no se han adoptado de forma generalizada debido a los posibles riesgos de seguridad y a la necesidad de realizar una configuración manual. En la bibliografía se han analizado otros métodos, entre ellos, el análisis pasivo y las mediciones activas. Sin embargo, estos enfoques suelen tener un alcance limitado - algunos solo pueden identificar infraestructuras recursivas - y se enfrentan a desafíos de escalabilidad.

Por estas razones, el enfoque adoptado en este informe se centra en evaluar a los grandes operadores del DNS en función de su cuota de mercado, lo que permite confirmar directamente un uso significativo de software de código abierto.

B.2 Infraestructura de registración de nombres de dominio

B.2.1 Metodología

Para evaluar el uso de FOSS en la infraestructura de registración, el Comité Asesor de Seguridad y Estabilidad (SSAC) realizó una encuesta entre los grandes registros y proveedores de backend de registros. Para evaluar el uso de FOSS en los servicios de custodia de datos, se realizó una encuesta a los agentes de custodia de datos (DEA) aprobados por la ICANN que figuran en el sitio web de la ICANN, y el foco estaba puesto en el software utilizado para los componentes clave del servicio (transferencia de datos, verificación de firmas, verificación de depósitos e interacción con la API de las Interfaces de Informes de Registración (RRI)).

B.2.2 Conclusiones

La infraestructura de registración se refiere a los sistemas que facilitan la registración de nombres de dominio individuales y los ponen a disposición en el DNS público. Si bien no se dispone de datos explícitos sobre el alcance total del uso de FOSS, las pruebas muestran una

profunda dependencia del mismo, tanto como sistemas completos como componentes fundamentales.

Varios operadores de registro, especialmente en el ámbito de los dominios de alto nivel con código de país (ccTLD), mantienen una infraestructura de registración que es totalmente FOSS (Tabla 1, Tabla 2). Por ejemplo, se sabe que la plataforma de registro FRED es utilizada por al menos 12 registros de ccTLD, y la plataforma Nomulus se utiliza para diversos TLD genéricos (gTLD).

Por el contrario, los registros y proveedores de servicios backend de registros más grandes suelen utilizar sistemas propietarios. Sin embargo, estos sistemas no suelen crearse desde cero, sino que son extensiones e integraciones de componentes patentados y personalizados, como bases de datos y servidores web, que en su mayoría son FOSS.

Esta dependencia en FOSS se extiende a los servicios de custodia de datos (Tabla 3), que almacenan de forma segura copias de los datos de registración de nombres de dominio. Los mayores proveedores de estos servicios, tanto para registros como para registradores, han construido sus sistemas, al menos parcialmente, sobre componentes de FOSS.

B.3 Infraestructura del DNS

B.3.1 Metodología

Análisis de los servidores autoritativos: Para investigar el uso de FOSS en la infraestructura de TLD, se utilizó el siguiente procedimiento:

1. La zona raíz se obtuvo de la IANA y los TLD se vincularon a las direcciones IP (Protocolo de Internet) de sus servidores de nombres.
2. Se realizó un análisis independiente de los ccTLD teniendo en cuenta tanto los TLD de dos letras como sus equivalentes etiqueta-A (Punycode) (para tener en cuenta los ccTLD con nombres de dominio internacionalizados (IDN)).
3. Se utilizó la biblioteca ip2asn de Python para asignar estas direcciones IP a sus respectivos Números del Sistema Autónomo (ASN) y nombres de ASN (operadores).
4. La cuota de mercado se calculó como el número de TLD alojados por un operador determinado dividido por el número total de TLD (teniendo en cuenta que varios operadores pueden alojar un mismo TLD simultáneamente).
5. Se identificaron los 25 principales operadores y se verificó manualmente su uso de software de código abierto para los servidores de nombres autoritativos.

Análisis de los resolutores: No existen estudios fiables sobre la base instalada total de resolutores. Para este informe, el análisis se centró en enumerar los principales operadores y tipos de implementaciones (por ejemplo, locales, en la nube, públicas) y en investigar si

utilizaban software FOSS o propietario sobre la base de declaraciones públicas y conocimientos directos.

B.3.2 Conclusiones

Servidores autoritativos: La evidencia del dominio de FOSS es más clara en la infraestructura que publica información de dominios. En los niveles más altos de la jerarquía del DNS, la raíz y los TLD, FOSS es casi omnipresente. El sistema de servidores raíz (RSS) se encuentra en la cúspide del DNS. De las 12 organizaciones independientes que operan los servidores raíz, al menos nueve utilizan exclusivamente implementaciones de DNS FOSS para responder a las consultas (Tabla 4).

Este patrón continúa en el siguiente nivel de la jerarquía con los servidores de nombres de TLD (Tabla 5). La investigación realizada para este informe reveló que nueve de los diez principales operadores que prestan servicios de DNS autoritativos para registros de TLD utilizan de FOSS para ello. Además, 20 de los 25 principales operadores que prestan este servicio para los ccTLD utilizan software DNS FOSS, que presta servicio a un total de 234 ccTLD únicos.

Resolutores: La prevalencia de FOSS no se limita a la publicación de datos del DNS, sino que es igualmente significativa en la infraestructura que recupera esa información: el diverso ecosistema de resolutores del DNS.

La mayoría de los usuarios reciben servicio de resolutores locales operados por sus proveedores de servicios de Internet (ISP), empresas o instituciones educativas. Si bien existen muchos productos comerciales para este mercado, la mayoría de ellos incorporan una o más soluciones FOSS como componente del DNS central de su oferta.

En la nube, las plataformas informáticas a hiperescala como Microsoft Azure, Google Cloud y Servicios Web de Amazon operan importantes infraestructuras de resolutores para dar soporte a sus servicios. Al menos cuatro de los hiperescaladores más grandes confían en FOSS para la resolución del DNS, mientras que otros han creado soluciones propietarias basadas en bibliotecas de DNS FOSS.

Apéndice C: Encuesta sobre las perspectivas de los operadores del DNS respecto a FOSS y la regulación del software

El Comité Asesor de Seguridad y Estabilidad (SSAC) realizó una encuesta informal en línea sobre los impactos previstos de la regulación del código abierto en la infraestructura del Sistema de Nombres de Dominio (DNS) con el fin de recopilar información para este informe. Se utilizó la herramienta EUSurvey para proteger la privacidad y el anonimato de los encuestados.[83] Se solicitaron respuestas a la comunidad técnica del DNS en varias listas de correo electrónico, entre ellas: las listas de correo electrónico técnico y jurídico del Consejo de Registros de Dominios Nacionales de Alto Nivel de Europa (CENTR), los grupos de trabajo sobre DNS y código abierto de Réseaux IP Européens Network Coordination Centre (RIPE NCC) y las listas de correo electrónico de usuarios de varios sistemas de software de DNS de código abierto. La encuesta también se presentó en la reunión del Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC) celebrada en febrero.

El objetivo principal de la encuesta era averiguar si los operadores técnicos del DNS conocen las iniciativas normativas y preguntarles qué efectos prevén que pueda tener la regulación del software libre y de código abierto (FOSS). La encuesta estuvo abierta durante el mes de febrero de 2025. Se recibieron 98 respuestas que abarcaban una muestra representativa de funciones en la infraestructura del DNS.

En primer lugar, se preguntó a los encuestados sobre su participación en el DNS. 96 de los 98 encuestados informaron participar en la infraestructura del DNS, y 64 encuestados también informaron tener participación en la registración de nombres de dominio. Veinticuatro encuestados incluyeron "desarrollador/proveedor de software" como una de sus funciones, pero ninguno de ellos respondía únicamente como desarrollador de software. (No se preguntó si el software era de código abierto o cerrado).

Los encuestados eran usuarios de código abierto y estaban bastante al tanto de la normativa. Casi todos los encuestados afirmaron utilizar código abierto (93 %). Aproximadamente un tercio (33 %) también declaró utilizar software propietario. El treinta por ciento de los encuestados también asesora a otros sobre la implementación y el funcionamiento de FOSS. Este grupo tenía un alto nivel de conocimiento de las iniciativas normativas actuales. Se proporcionó una lista de iniciativas normativas y se preguntó: "¿Cuáles de estas iniciativas normativas se conocen? (Marcar todas las conocidas)". Setenta y siete encuestados (aproximadamente el 77 %) indicaron que conocían una o más. Más del 40 % de los encuestados conocía el Reglamento de Ciberresiliencia de la UE, la Ley de Ciberseguridad y la Directiva NIS2. El treinta por ciento de los encuestados también indicó que estaba familiarizado con una o más de las iniciativas del Gobierno de los Estados Unidos, incluidas las Órdenes Ejecutivas 14028 y 14144, el programa Secure Software Development Attestation (*Certificación de desarrollo de software seguro*) o la

[83] "EUSurvey – About." [*Sobre EUSurvey*] https://ec.europa.eu/eusurvey/home/about.

marca CyberTrust para dispositivos del Internet de las cosas (IoT). Otras regulaciones mencionadas por los encuestados fueron la Ley Australiana de Seguridad de Infraestructura Crítica (SOCI), el Reglamento General de Protección de Datos (GDPR), la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y las autorizaciones del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) de Estados Unidos y Canadá.

Se consultó "¿Qué preocupaciones específicas se tienen sobre el impacto de la regulación del software en su organización?", con opciones tanto positivas como negativas. Todos los encuestados pudieron responder a esta pregunta, incluidos aquellos que no indicaron estar familiarizados con ninguna de las normativas específicas que mencionamos.

- El 72 % de los encuestados consideraba que era bastante probable que algunos proyectos de código abierto se abandonaran o dejaran de estar disponibles
- El 66 % pensaba que el cumplimiento normativo aumentaría el costo del software para ellos
- El 49 % estaba preocupado por la posibilidad de que algunos proyectos de código abierto de los que dependen pudieran pasar a utilizar licencias propietarias
- El 29 % pensaba que la regulación impediría a su organización publicar software como código abierto
- El 21 % anticipó que mejorará la seguridad del código abierto que utilizan
- El 7 % prevé que la regulación reducirá la carga que supone para sus organizaciones evaluar la seguridad y la calidad del software.

Si bien se solicitaron específicamente comentarios sobre los impactos positivos y las oportunidades, en un intento por mantener una posición equilibrada, los encuestados se mostraron en su mayoría pesimistas.

C.1 Comentarios libres (inquietudes específicas)

La encuesta invitaba a realizar comentarios de forma abierta sobre inquietudes específicas relativas al impacto de la regulación del software, además de preguntar sobre las oportunidades o los impactos positivos previstos.

Las inquietudes más citadas fueron las siguientes:

- Mayores costos de cumplimiento
- Implementación más lenta del software
- Posible abandono de algunos proyectos de código abierto debido a las cargas normativas
- Mayor complejidad en el cumplimiento normativo para los usuarios de software de código abierto