



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Seguridad en Soluciones DNS **Máster Universitario en Dirección TIC para la Defensa**

ALUMNO: Juan Félix Castela Mostazo

DIRECTORES: Norberto Fernández García
Carlos Zamorano Pinal

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Seguridad en Soluciones *DNS*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

UniversidadeVigo

RESUMEN

Una de las tecnologías fundamentales en el uso de Internet es el Sistema de Nombres de Dominio (DNS), se trata de una base de datos distribuida, cuya función principal consiste en traducir los nombres de dominio legibles por los humanos en las direcciones IP que utilizan los sistemas para enrutar el tráfico en redes.

La concepción inicial de Internet, donde los usuarios eran confiables, y el incremento exponencial de usuarios y dispositivos que se ha ido produciendo durante los años, hacen que el DNS haya ido sufriendo distintas evoluciones. Para resolver los problemas iniciales de Internet, el ingeniero Paul V. Mockapetris en 1983 propuso un Sistema de Nombres de Dominio

Debido a su importancia para el buen funcionamiento de Internet, le ha convertido en un objetivo fundamental para los ciberataques, entre las amenazas a las que se puede enfrentar, se pueden destacar:

- Ataques de Denegación de Servicio Distribuido (DDoS).
- Envenenamiento de Caché.
- Suplantación de Identidad (DNS spoofing).

El DNS posee una estructura jerárquica en forma de pirámide, que le permite manejar los millones de consultas diarias que se producen. Existiendo una variedad de distintos servidores, en función de la función que realizan dentro del ecosistema de Internet.

Para proteger el DNS se han ido implementando diferentes soluciones, llegando en esta última etapa al uso de la Inteligencia Artificial y Blockchain, para que las consultas se puedan realizar de una forma segura.

PALABRAS CLAVE

DNS, Servidor, Resolución, Seguridad, Integridad.

AGRADECIMIENTOS

A Verónica, que me ha cambiado la vida.

A la familia, que nunca falla.

A los que han estado ahí en esta etapa de mi vida.

A mis compañeros, lo mejor del Máster.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción y objetivos	5
1.1 Introducción.	5
1.1.1 Amenazas al DNS.....	5
1.1.2 Impacto de los fallos de Seguridad del DNS.	6
1.1.3 Seguridad de DNS en la actualidad.	6
1.2 Objetivos.	6
1.3 Estructura de la memoria.	6
2 Estado del arte	7
2.1 DNS.....	7
2.1.1 ¿Qué es un DNS?.....	7
2.1.2 Historia y Evolución del DNS.	7
2.1.3 Arquitectura del DNS.	10
2.2 Servidores DNS.....	12
2.2.1 Zonas. [24].....	12
2.2.2 Servidores Raíz (Root Servers).	12
2.2.3 Servidor Maestro o Primario.	14
2.2.4 Servidor Esclavo o Secundario.....	14
2.2.5 Servidor Caché.....	15
2.2.6 Servidor Renviador (Forwarder).....	15
2.2.7 Servidor sólo Autorizado (Authoritative Only).....	17
2.3 Dominios de Nivel Superior (TLD).	17
2.3.1 Dominio Secundario.	17
2.3.2 Registros DNS.	19
2.4 Funcionamiento del DNS.....	23
2.5 Amenazas y Vulnerabilidades en el DNS.	26
2.5.1 Amenazas.....	26
2.5.2 Vulnerabilidades.	35
2.5.3 Impacto de los Ataques DNS en Diversos Sectores.	37
3 Seguridad del DNS.....	45
3.1 Soluciones de Seguridad en DNS.	45
3.1.1 DNNSEC (Domain Name System Security Extensions).....	45

3.1.2 DNS sobre TLS (DoT).....	52
3.1.3 DNS sobre HTTPS (DoH).	56
3.1.4 Filtrado y Monitoreo de DNS.	67
3.1.5 Otras Soluciones de Seguridad.	74
4 Estudio de casos	87
4.1 Análisis de Incidentes Reales.....	87
4.1.1 Caso del Ataque DDoS a DYN (2016).....	87
4.1.2 Caso de Envenenamiento de Caché de Kaminsky (2008).	92
5 Análisis y propuestas de mejora.....	96
5.1 Propuestas de Mejora.	96
5.1.1 Setup de Referencia.	96
5.1.2 Análisis de Soluciones Existentes y sus Limitaciones.	97
6 Conclusiones y líneas futuras	100
6.1 Propuesta de Nuevas Estrategias.....	100
6.1.1 Integración de Inteligencia Artificial en la Seguridad DNS.	100
6.1.2 Uso de Blockchain para la protección del DNS.	102
6.1.3 Futuras Implementaciones DNS sobre HTTP (DoT).	104
6.1.4 Firewalls de Próxima Generación.....	105
7 Bibliografía.....	108

ÍNDICE DE FIGURAS

Figura 2-1. Gráfico de la línea temporal del DNS con los hitos clave desde 1969 hasta 2023. Gráfico creado con IA (ChatGPT).	10
Figura 2-2. Jerarquía del DNS. (Fuente: https://pandorafms.com/blog/es/monitorizacion-dns/).	11
Figura 2-3. Servidores Raíz DNS en el mundo. (Fuente: https://infotecnewsjr.blogspot.com).	13
Figura 2-4. Servidores DNS Maestros y Esclavos (Fuente: https://www.zeppelinlinux.es).	15
Figura 2-5. Servidores Autorizados y Cache (Fuente: https://www.zeppelinlinux.es).	16
Figura 2-6. Servidores Consulta Iterativa (Fuente: https://www.zeppelinlinux.es).	16
Figura 2-7. Servidores Consulta Recursiva (Fuente: https://www.zeppelinlinux.es).	17
Figura 2-8. Resolución de nombre de dominio (Fuente: https://www.zeppelinlinux.es).	24
Figura 2-9. Consulta a Servidor No Autorizado. (Fuente: https://www.zeppelinlinux.es).	25
Figura 2-10. Consulta a Servidor Renviador. (Fuente: https://www.zeppelinlinux.es).	25
Figura 2-11. Cifras ataques DNS en 2022. (Fuente: https://efficientip.com/).	27
Figura 2-12. Envenenamiento de Caché. (Fuente: https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning/).	27
Figura 2-13. Caché DNS Envenenada. (Fuente: https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning/).	28
Figura 2-14. Ataque DNS Spoofing. (Fuente: https://www.uv.mx/infosegura/general/noti_ataques-6/).	30
Figura 2-15. Ataque DDoS. (Fuente: https://www.akamai.com/es/glossary/what-is-a-dns-ddos-attack).	31
Figura 2-16. Funcionamiento Túnel DNS. (Fuente: https://www.akamai.com/es/glossary/what-is-dns-tunneling).	32
Figura 2-17. Secuestro de DNS. (Fuente: https://www.ionos.mx).	34
Figura 3-1. DNS sin usar DoH – DNS con DoH Habilitado. (Fuente: https://ccnadesdecero.es).	59
Figura 3-2. Comparación de Protocolos DNS. Gráfico creado con IA (ChatGPT).	67
Figura 4-1. Ataque a DYN. (Fuente: https://widefense.com).	88

ÍNDICE DE TABLAS

Tabla 2-1. Tabla Registros DNS.	18
Tabla 2-2. Tabla Registro A.	19
Tabla 2-3. Tabla Registro AAAA.	20
Tabla 2-4. Tabla Registro SOA.	22
Tabla 3-1. Comparativa de Proveedores.	65
Tabla 3-2. Comparativa DoH vs DoT.	67
Tabla 3-3. Comparativa <i>Firewall</i>	70
Tabla 3-4. Comparativa NIDS vs HIDS.....	73
Tabla 3-5. Comparación: <i>Firewall</i> vs. Integración IDS- <i>Firewall</i>	74
Tabla 6-1. Comparación Firewall Tradicionales vs NGFW.....	106

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción.

Una de las tecnologías fundamentales en el uso de Internet es el **Sistema de Nombres de Dominio** (DNS) [1], se trata de una base de datos distribuida, cuya función principal consiste en traducir los nombres de dominio legibles por los humanos en las direcciones IP que utilizan los sistemas para enrutar el tráfico en redes. Por ejemplo, www.google.com se traducirá en la dirección IP: 142.250.200.242. Es como una guía telefónica para la web, que permite el acceso a sitios web utilizando los nombres en vez de los números de las direcciones IP.

DNS fue introducido en 1983 [2], con la idea inicial de escalabilidad y eficiencia, pero sin tener en cuenta la seguridad, debido al auge de Internet y la evolución de los ciberataques, se han revelado muchas vulnerabilidades críticas en el protocolo, lo que ha supuesto muchos esfuerzos en mejorar la seguridad en soluciones DNS.

El DNS se considera fundamental en esta vida digital en la que vivimos, ya que es usado en múltiples aspectos [3], como:

1. **Navegación web:** Los usuarios acceden a los sitios web a través de los nombres de éstos, no utilizan las direcciones IP.
2. **Correo Electrónico:** Registros de DNS (como el MX, *Mail Exchange*) son fundamentales para el correcto enrutamiento del correo electrónico.
3. **Internet de las Cosas (IoT):** Los dispositivos conectados a la IoT interactúan continuamente con el DNS. Dependen de él para sus operaciones y actualizaciones, pero además, afecta al sistema de muchas maneras, por lo que es fundamental que se tengan en cuenta los efectos de la IoT en el DNS.
4. **Sistemas Empresariales:** Las redes corporativas y las tecnologías VPN (*Virtual Private Network*, Red Privada Virtual), también utilizan DNS para resolver los nombres internos.

1.1.1 Amenazas al DNS.

Como se trata de un intermediario en la infraestructura crítica de Internet, el DNS es un objetivo clave para los atacantes, entre las amenazas a las que se enfrenta podemos destacar [4]:

- **Ataques de Denegación de Servicio Distribuido (DDoS):** Cuyo objetivo es generar un ataque contra los servidores DNS para provocar un fallo que suponga una caída del servicio e interrumpir el acceso a los sitios web.

- **Envenenamiento de Caché:** Se basa en la introducción de información falsa en el caché de los servidores DNS, lo que hace que las consultas al mismo produzcan una respuesta incorrecta y envíen a los usuarios a sitios web equivocados.
- **Suplantación de Identidad (DNS spoofing):** Se alteran las entradas en un servidor DNS con el objetivo de redirigir a los usuarios a webs maliciosas donde el control lo tienen los atacantes.

1.1.2 Impacto de los fallos de Seguridad del DNS. [5]

Los fallos en la seguridad del DNS pueden suponer caídas significativas de los servicios y exponer datos sensibles a los atacantes, como muestran dos casos reales que se verán más adelante:

- **Ataques Denegación de Servicio Distribuido (DDoS) a DYN en 2016 [6]:** El ataque al proveedor DNS DYN en 2016, provocó una caída de servicios en plataformas como Twitter, Netflix y Spotify.
- **Envenenamiento de Caché de Kaminsky (2008) [5]:** En julio de 2008, el equipo de preparación para emergencias informáticas (US-CERT) de Estados Unidos anunció que el investigador Dan Kaminsky había descubierto un fallo fundamental en el protocolo del Sistema de nombres de dominio, que podría permitir a los atacantes realizar ataques de envenenamiento de caché en la mayoría de los servidores de nombres (solo djbdns, PowerDNS, MaraDNS y Unbound no eran vulnerables).

1.1.3 Seguridad de DNS en la actualidad.

Debido a la evolución de Internet, donde las redes cada vez son más complejas y los atacantes se encuentran en continua evolución para generar ataques más sofisticados, la seguridad en DNS se ha considerado fundamental en la integridad de los sistemas, por lo que organizaciones como ICANN [6] (*Internet Corporation for Assigned Names and Numbers*) y la IETF [7] (*Internet Engineering Task Force*) están trabajando para implementar estándares cada vez más seguros que puedan contener esas amenazas, como DNSSEC (*DNS Security Extensions*) o DNS sobre HTTPS (DoH), que veremos más adelante.

1.2 Objetivos.

La finalidad de este trabajo es demostrar la importancia del DNS en Internet y realizar un análisis técnico de la seguridad en soluciones DNS, viendo su evolución, amenazas, medidas adoptadas para garantizar la integridad del mismo, mostrando algunas nuevas estrategias basadas en el uso de la IA. Los objetivos específicos serán los siguientes:

- **Comprender la evolución del DNS:** Ver la evolución del DNS, desde su concepción hasta el estado actual.
- **Identificar Vulnerabilidades y Amenazas:** Realizar un análisis de los ataques más comunes y sus consecuencias.
- **Técnicas Emergentes:** Análisis de herramientas como DNSSEC, DoH, y DNS sobre TLS (DoT) y el impacto de éstas en la seguridad del DNS.
- **Buenas Prácticas para Soluciones Seguras:** Conjunto de buenas prácticas para administración y gestión del DNS.

2 ESTADO DEL ARTE

2.1 DNS.

2.1.1 ¿Qué es un DNS?

El **Sistema de Nombres de Dominio** (DNS) [1] es un sistema jerárquico y descentralizado que permite la traducción de los nombres de dominio de los sitios web, legibles por humanos, en direcciones IP, legibles para las máquinas, para que éstas puedan localizar y comunicarse con otros dispositivos.

El DNS es un intermediario entre los usuarios y la infraestructura de red, facilita a los usuarios el acceso a servicios en línea, ya que les permite a través del nombre del dominio llegar a los sitios web, en vez de tener que recordar las direcciones IP de cada uno de ellos.

Cada dispositivo en Internet posee una dirección IP, única y necesaria para poder encontrar la ubicación de ese dispositivo en la red. Cuando el usuario escribe un nombre de dominio en su navegador web (www.google.com) se debe traducir ese nombre a su dirección IP correspondiente (por ejemplo: 142.250.200.242), para que el ordenador la pueda entender y localizar el sitio web de www.google.com.

2.1.2 Historia y Evolución del DNS.

Desde la creación del DNS en 1983 [8], se ha convertido en un elemento esencial en la operatividad de Internet. Sus inicios fueron simplemente como traductor de nombres de dominios legibles por humanos a direcciones IP, pero la gran expansión de Internet ha hecho que vaya sufriendo una evolución constante.

Conforme el número de usuarios, dispositivos y servicios en línea han ido aumentando exponencialmente, el DNS [9] se ha tenido que enfrentar y superar distintos desafíos en diversas áreas:

- **Escalabilidad:** En sus inicios existían un número muy limitado de dominios, pero con la expansión de Internet han llegado a ser miles de millones, lo que ha requerido que la arquitectura del DNS haya tenido que optimizarse, con la implementación de servidores raíz distribuidos, balanceo de carga y *caching* [10], para mantener su rendimiento a nivel global.
- **Seguridad:** Como elemento fundamental en el funcionamiento de Internet, el DNS sufre continuos ataques y cada vez más sofisticados, lo que ha provocado que continuamente se vayan implementando medidas para mitigar estos ataques.
- **Privacidad:** La protección de la privacidad de los datos de usuarios ha provocado la preocupación sobre la vigilancia y la recopilación de datos, por lo que se han ido desarrollando diferentes protocolos para cifrar las consultas al DNS y proteger estos datos.

- **Adaptación tecnológica:** La evolución de Internet ha provocado el que DNS haya ido integrando nuevas tecnologías para mantenerse al día. Adaptación del protocolo IPv6, reemplazando al IPv4 (limitado espacio de direcciones Ip), así como la incorporación de dominios internacionalizados (IDNs), donde se permite el uso de caracteres no latinos en los nombres de dominio.
- **Crecimiento de servicios y aplicaciones:** DNS ya no solo se limita a la simple resolución de nombres, ahora juega un papel clave en servicios más avanzadas como balanceo de carga, distribución de contenido y enrutamiento inteligente de tráfico, capacidades que permiten la optimización de la experiencia del usuario y mejoran la eficiencia de las redes.

Gracias a esta evolución, el DNS sigue siendo un elemento esencial en la infraestructura de Internet y es capaz de responder a las necesidades cada vez más cambiantes en este entorno digital, convirtiéndose en un servicio crítico para la comunicación en línea.

A continuación, se hace un repaso histórico de los inicios de Internet y la evolución del DNS:

▪ **ARPANET y el Sistema HOSTS.TXT.**

En 1969 la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos (DARPA) creó la primera red de computadoras interconectadas ARPANET [11], que significaría el inicio de Internet. Para el intercambio de información entre los nodos era necesario un sistema capaz de identificar y localizar los equipos dentro de la red. Para resolver este problema, inicialmente se creó un fichero (HOSTS.TXT) [12], que consistía en un registro donde a cada dirección ip de cada nodo se le asignaba un nombre que era legible para los humanos. Fichero que era administrado y mantenido por el *Network Information Center* (NIC) [13], institución encargada de esta tarea. Pero a medida que ARPANET iba creciendo, surgieron una serie de necesidades que hicieron que la elección de este sistema no fuera lo suficientemente eficiente:

- **Dependencia centralizada:** Al ser gestionado únicamente por el NIC, esto suponía que cualquier cambio o actualización debía hacerse manualmente por esta institución. Además, como cada nodo debía descargarse las actualizaciones, dependían de la disponibilidad del NIC y de su capacidad para atender las peticiones de éstos.
- **Crecimiento exponencial:** Como la red ARPANET estaba compuesta por un número limitado de nodos, la solución del fichero HOSTS.TXT era eficiente, pero con el crecimiento exponencial de la red el tamaño del archivo comenzó a aumentar considerablemente, lo que complicó cada vez más su mantenimiento y también ralentizaba su distribución, ya que cada nodo debía de tener una copia actualizada.
- **Problemas en la asignación de nombres:** Como la asignación de nombres se debía hacer a mano, cada vez se estaba volviendo más compleja, lo que provocó errores en la asignación de nombres o duplicidad de los mismos.
- **Ineficiencia operativa:** Como todos los procesos se realizaban de manera manual y debido al incremento descomunal de equipos, estas operaciones requerían cada vez más tiempo y esfuerzo, lo que provocó que debía de idearse otro sistema más eficiente.

Todos estos problemas evidenciaron la necesidad de desarrollar un nuevo sistema que fuera más eficiente, descentralizado y escalable, capaz de gestionar los nombres en una red que crecía de esa manera. Por eso, en 1983 se desarrolló el **Sistema de Nombres de Dominio** (DNS) que introducía una nueva estructura jerárquica y distribuida, que resolvía los problemas anteriores de su antecesor el fichero HOSTS.TXT.

▪ **1983: La Propuesta de Paul Mockapertis.**

Una vez identificadas las carencias que suponía el uso del fichero HOSTS.TXT, en 1983 el ingeniero Paul V. Mockapertis [14] propuso el uso de un Sistema de Nombres de Dominio. En principio sus

especificaciones fueron publicadas en los **RFC 882** [15] y **883** [16], donde se introdujeron los conceptos fundamentales del sistema moderno de nombres de Internet.

Principales Características del DNS: [17]

1. **Jerarquía y Dominio Raíz:** La jerarquía del nuevo sistema tenía la forma de árbol invertido, donde la raíz (representada por un **.**) actúa como el nivel superior. A partir del nivel superior los nombres de dominio se van dividiendo en niveles organizados que incluyen:
 - a. Dominios de Nivel Superior (TLD, *Top Level Domain*, ejemplo: **.com**, **.org**).
 - b. Subdominios y Nombres Específicos (ejemplo: **mail.example.com**).
2. **Distribución Descentralizada:** Para eliminar uno de los errores de su antecesor, un único punto de distribución, los servidores DNS se fueron distribuyendo globalmente, gestionando cada uno de ellos diferentes partes del árbol de dominios.
3. **Resolución de Nombres:** Para realizar la traducción de nombres de dominios a direcciones ip se realizaban una serie de consultas:
 - a. **Recursivas:** Para resolver el nombre indicado por el cliente, el servidor DNS realiza múltiples consultas.
 - b. **Iterativas:** El servidor devuelve referencias para que el cliente continúe las consultas.

▪ **1984: Primeras Implementaciones.**

En 1984, la Universidad de Berkeley (California) desarrolló **BIND** (*Berkely Internet Name Domain*) [18] el primer software de servidor de DNS, ampliamente utilizado y aún sigue siendo un estándar en servidores DNS. Actualmente en su versión Bind9 [20], es utilizado ampliamente en Sistemas Operativos Linux y también en Unix.

▪ **1984 - 2000: Desarrollo y Estandarización.** [19]

En este período de tiempo y debido al gran crecimiento de Internet se fueron planteando nuevos retos como el aumento exponencial de las consultas DNS debido al aumento de usuarios y dispositivos y se introdujeron los subdominios para una mejor organización de los servicios (por ejemplo: *mail.example.com*).

Además se introdujeron los primeros TLD, que se dividían en dos clases:

- **Genéricos (gTLD):** Que se utilizan para clasificar las organizaciones en función de su propósito, como:
 - **.com:** Comercial.
 - **.org:** Organizaciones sin ánimo de lucro.
 - **.net:** Redes.
- **Códigos de País (ccTLD):** Utilizados para identificar a los países:
 - **.es:** España.
 - **.us:** Estados Unidos.
 - **.uk:** Reino Unido.

▪ **2000 - 2010: Desafíos de Seguridad y Escalabilidad.**

Con la expansión de Internet, la aparición de cada vez más dispositivos conectados a la red, el DNS se convirtió en un objetivo estratégico para los ciberataques, los más comunes son:

- **Envenenamiento de caché:** Redirigir a los usuarios a sitios maliciosos mediante la manipulación de las respuestas del DNS.
- **Suplantación (*Spoofing*):** Consiste en engañar a los usuarios falsificando las respuestas del DNS.
- **Ataques DDoS:** Provocar interrupciones del servicio mediante ataques de denegación de servicio a los servidores DNS.

Para garantizar la integridad del DNS en 2005 aparece DNSSEC (*Domain Name System Security Extensions*) que mediante la agregación de firmas digitales para la autenticación de respuestas, garantiza su integridad y previene de manipulaciones de terceros.

En 2010 la ICANN permite la aparición los nuevos TLDs personalizados que amplían considerablemente las posibilidades de los nombres de dominio, por ejemplo:

- .shop.
- .tech.

▪ 2010 - 2024: Avances Recientes.

En este período de tiempo se producen nuevos avances para ir adaptándose a los cambios en el uso de Internet:

- **Introducción de nombre de dominio internacionalizados (iDNS) [20]:** Que permiten el uso de caracteres de alfabetos no latinos (árabe, chino, cirílico) lo que mejora la accesibilidad global.
- **DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT) [21]:** Se utiliza el cifrado de las consultas mediante HTTPS o TLS, para mejorar la privacidad.
- **Adopción de IPv6:** Debido al agotamiento de direcciones IPv4, se adopta un nuevo protocolo IPv6 que utiliza direcciones de 128 bits, lo que requirió una serie de cambios en la infraestructura DNS para poder manejar direcciones más largas.

Como puede verse en la siguiente figura, el DNS ha ido evolucionando constantemente desde sus inicios en 1969.

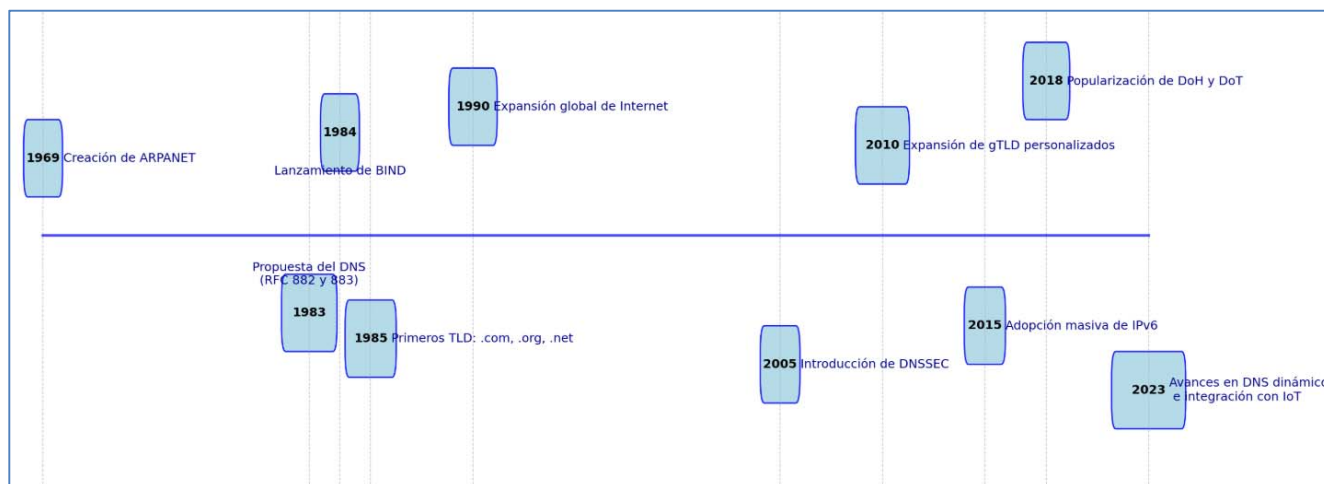


Figura 2-1. Gráfico de la línea temporal del DNS con los hitos clave desde 1969 hasta 2023. Gráfico creado con IA (ChatGPT).

2.1.3 Arquitectura del DNS.

Para asegurar una organización eficiente y escalable, el Sistema de Nombres de Dominio posee una estructura jerárquica que permite garantizar que sea capaz de manejar miles de millones de consultas diarias.

La **Jerarquía del DNS** [22] es la estructura central del Sistema de Nombres de Dominio, diseñado como un sistema distribuido y escalable que organiza los nombres de dominio en una pirámide jerárquica, como se puede observar en la figura 2-2, lo que le permite:

- Delegar responsabilidades.
- Facilitar la resolución de nombres.

- Soportar el crecimiento exponencial de Internet.

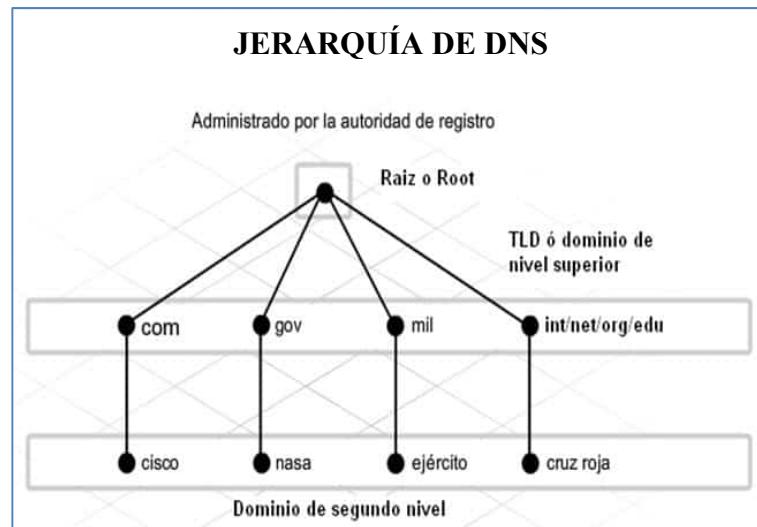


Figura 2-2. Jerarquía del DNS. (Fuente: <https://pandorafms.com/blog/es/monitorizacion-dns/>).

La estructura jerárquica del DNS organiza los nombres de dominio en niveles ascendentes, partiendo del host individual, hasta la raíz. Se asemeja a una estructura de árbol de forma invertida, donde cada uno de los niveles va delegando responsabilidades en el siguiente, manteniendo un diseño escalable y eficiente, que asegura la redundancia y confiabilidad, ya que la información se distribuya entre múltiples servidores globales, eliminando puntos únicos de fallo. Cada uno de los niveles tiene una función específica y debe contribuir a mantener la eficiencia del DNS y contribuir a la escalabilidad, esto permite que millones de dispositivos puedan interactuar en Internet.

▪ Jerarquía del DNS: Tipos de Servidores. [1]

Como ya se ha comentado, el DNS posee una estructura jerárquica y distribuida, para garantizar fundamentalmente la eficiencia, escalabilidad y redundancia. Cada componente dentro de esta jerarquía posee un rol claramente definido para mantener la operatividad del sistema:

- **Servidores Raíz (Root Server):** Capa superior jerárquica del DNS y son los encargados de dirigir las consultas hacia los servidores TLD. Existen 13 conjuntos de servidores raíz distribuidos globalmente mediante Anycast [25].
- **Servidores TLD (Top-Level Domain):** Encargados de la gestión de dominios de nivel superior y redirigen las consultas a los servidores autorizados de los dominios secundarios.
- **Servidores Autorizados:** Contienen la información definitiva para cada dominio, respondiendo a las consultas con datos precisos de cada dominio.
- **Servidores Recursivos (Resolvers):** Intermediarios del sistema, procesan las consultas y almacenan en caché las respuestas para futuras consultas, mejorando de esta manera la eficiencia del sistema.

▪ Jerarquía del DNS: Espacio de Nombres. [23]

- **Dominio Raíz (Root):** Nivel superior de la jerarquía se representa por un punto (.).
- **Dominios de Nivel Superior (TLDs):** Dominios de nivel superior (.com, .org) o los dominios de los códigos de país (.es).
- **Dominios Secundarios:** Incluyen los nombres personalizados dentro de un TLD (Ej: uvigo.es).
- **Subdominios:** Dentro de un dominio secundario se crean divisiones específicas (Ej: cud.uvigo.es).

2.2 Servidores DNS.

Los servidores de nombres de dominio son programas que se encargan de guardar información sobre nombres de dominio. Enlazan una dirección IP con un nombre de dominio, es decir, cada servidor DNS almacena una parte de la base de datos DNS.

2.2.1 Zonas. [24]

La zona es la parte del espacio de nombres de dominio que los servidores de nombres almacenan. Cuando un servidor DNS contiene una zona, se dice que es un **Servidor Autorizado** (*Authoritative*) para esa zona, pero los servidores que responden a preguntas de zonas que no contienen o no administran se dice que son **Servidores No Autorizados** (*non-authoritative*) [26].

Las zonas se almacenan en los servidores DNS en bases de datos o en ficheros de texto, en función del tipo de software que se haya utilizado para montar el servidor DNS, el formato de estos ficheros viene definido por la norma RFC 1035 [25]. Los ficheros o bases de datos de zona están formados por registros de recursos, que es donde se definen los tipos de datos en el DNS, cada uno de éstos contiene información sobre un objeto determinado. El servidor DNS utiliza estos registros de recurso para resolver las consultas que se le realizan.

Una zona no es lo mismo que un dominio, ya que el dominio es un subárbol del espacio de nombres de dominio y los datos asociados a los nombres de dominio pueden estar almacenados en una o varias zonas, que pueden estar distribuidas en uno o varios servidores DNS.

2.2.2 Servidores Raíz (Root Servers).

Parte fundamental de la arquitectura del Sistema de Nombres de Dominios, nivel más alto de la jerarquía y son el primer punto de contacto para la resolución de nombres. Su función principal es dirigir las consultas hacia los servidores de Nivel Superior (TLD), ya que los servidores raíz no almacenan información específica sobre nombres de dominio.

Función de los Servidores raíz:

- Responsables de proporcionar las referencias a los servidores TLD (.com, .org, .es, etc).
- Actúan como una guía telefónica, redirigiendo las consultas hacia el servidor adecuado para el TLD correspondiente. Lo que permite que el sistema sea escalable y no dependa de una sola identidad para la resolución de los nombres de dominio.
- Por ejemplo, cuando se realiza un consulta para el sitio web www.example.com, el servidor raíz recibe esta consulta y posteriormente la redirigirá al servidor TLD de .com.

Organización y Operación.

- **13 Conjuntos de Servidores Raíz:** Aunque realmente se trata de 13 identificadores principales (letras de la A la M) que representan diferentes operadores. Cada uno de los identificadores puede tener múltiples instancias distribuidas globalmente mediante la tecnología *Anycast*, en total se trata de más de 1.500 servidores distribuidos en diversos países y regiones.

El uso de esta tecnología permite que una única dirección ip se compartida por múltiples servidores distribuidos en distintas ubicaciones, lo que garantiza que las consultas las responda el servidor más cercano o el que esté menos congestionado, lo que mejora la eficiencia y resiliencia del sistema, reduciendo la latencia y mejorando la experiencia del usuario final.

Las instancias se encuentran distribuidas en las regiones principales: América del Norte, Europa, Asia-Pacífico, América Latina y África, lo que asegura que exista una cobertura a nivel global.

- **Independencia de operación:** Como cada conjunto de servidores es administrado por una organización independiente, tienen libertad para implementar políticas de seguridad, medidas de mitigación de ataques y actualizaciones de software y hardware. Esta estructura descentralizada

contribuye a que exista una estabilidad, evitando una concentración de poder, y seguridad en el conjunto del DNS.

Entre los operadores que administran los servidores del DNS, destacan:

Los 13 servidores DNS principales del mundo [27], situados en varios puntos del planeta, aunque mayoritariamente en Estados Unidos, como se puede observar en la figura 2-3.

Aproximadamente la mitad depende de organizaciones públicas estadounidenses.

- **Servidor A:** Network Solutions, Herndon, Virginia, USA.
- **Servidor B:** Instituto de Ciencias de la Información de la Universidad del Sur de California, USA.
- **Servidor C:** PSINet, Virginia, USA.
- **Servidor D:** Universidad de Maryland, USA.
- **Servidor E:** NASA, en Mountain View, California, USA.
- **Servidor F:** Internet Software Consortium, Palo Alto, California, USA.
- **Servidor G:** Agencia de Sistemas de Información de Defensa, California, USA.
- **Servidor H:** Laboratorio de Investigación del Ejército, Maryland, USA.
- **Servidor I:** NORDUnet, Estocolmo, Suecia.
- **Servidor J:** (TBD), Virginia, USA.
- **Servidor K:** RIPE-NCC, Londres, Inglaterra.
- **Servidor L:** (TBD), California, USA.
- **Servidor M:** Wide Project, Universidad de Tokyo, Japón.

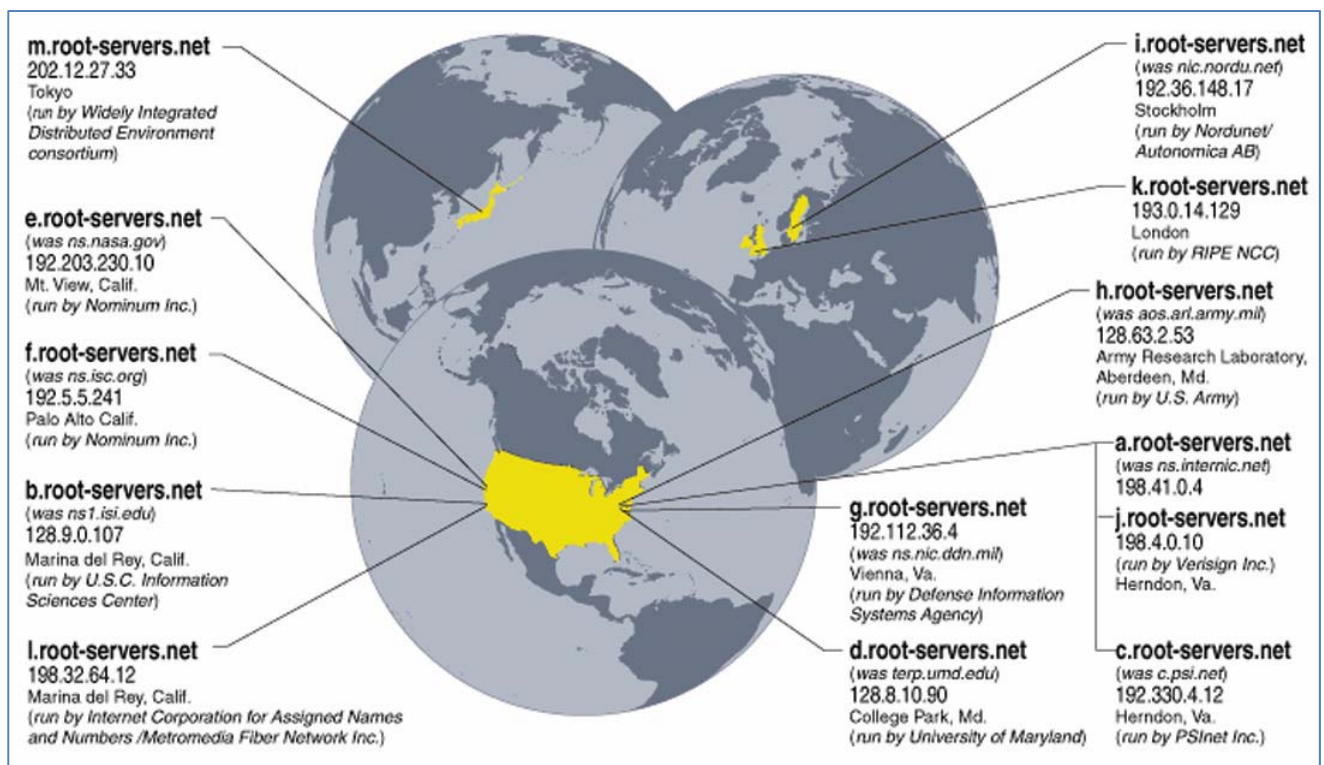


Figura 2-3. Servidores Raíz DNS en el mundo. (Fuente: <https://infotecnewsjr.blogspot.com>).

- **Resiliencia:** Con el uso de esta arquitectura distribuida y el uso de *Anycast* les proporciona una alta resiliencia frente a fallos y ataques, siendo el más común el de Denegación de Servicios Distribuido. Como las consultas se distribuyen entre la multitud de instancias que existen el sistema es capaz de asegurar la continuidad de su operación.

Importancia y rol de estos servidores en el DNS. [28]

- **Resolución de nombres:** Elemento fundamental en el proceso de resolución de nombres, son el primer eslabón en la cadena que traduce el nombre de un dominio en una dirección ip. Su correcta operación es clave para una eficaz navegación por Internet, ya que sin ellos los navegadores y otros servicios no serían capaces de localizar los recursos solicitados.
- **Escalabilidad:** Gracias a la distribución global de instancias y la implementación de *Anycast* el sistema es capaz de manejar miles de millones de consultas diarias y garantiza que el crecimiento exponencial de Internet no comprometa la eficiencia del DNS.
- **Redundancia:** La existencia de múltiples instancias para cada servidor raíz asegura que el sistema continúe funcionando en su conjunto en el caso de que varias de estas fallen, proporcionando una alta disponibilidad del sistema.

Ejemplo de Funcionamiento.

- **Consulta Inicial:** El usuario teclea en su navegador web: www.example.com.
- **Resolución en el Servidor Raíz:** Se realizan dos operaciones:
 - El servidor recursivo que el usuario tenga configurado en su equipo envía la consulta al servidor raíz más cercano.
 - El servidor raíz recibe la consulta, y proporciona la dirección del servidor TLD correspondiente, en este caso .com.

2.2.3 Servidor Maestro o Primario.

Servidor que define una o varias zonas de las que es autorizado. Posee unos archivos de zona que el administrador mantiene.

Cuando se realiza una consulta a este servidor pueden suceder dos cosas:

1. Si es un Servidor Autorizado, consulta a los ficheros de zona y responde a la pregunta.
2. Si es un Servidor No Autorizado, deberá preguntar a otros Servidores DNS o responder que no conoce la respuesta.

2.2.4 Servidor Esclavo o Secundario.

Servidor que define una o varias zonas de las que es autorizado, pero se diferencia del maestro en que los ficheros de zona los obtiene de otro servidor autorizado para la zona, que suele ser normalmente un servidor maestro, mediante un procedimiento que se denomina transferencia de zona. A diferencia de los archivos de zona del servidor maestro, los de este tipo de servidores son sólo de lectura, por lo que no se pueden administrar, la modificación de éstos se hace desde el servidor maestro. Su funcionamiento es igual que el del servidor maestro, como puede observarse en la figura 2-4.

Un servidor maestro puede ser maestro para una o varias zonas, pero a la vez también puede ser esclavo para otras. También, pueden existir varios servidores esclavos para una misma zona, debido a las siguientes razones:

- Balance de carga entre servidores DNS.
- Tolerancia a fallos.
- Reducción del tiempo de latencia.

Es aconsejable que servidores DNS para una misma zona estén repartidos en redes y localizaciones diferentes para poder seguir dando el servicio en caso de que un problema afecte a su ubicación.

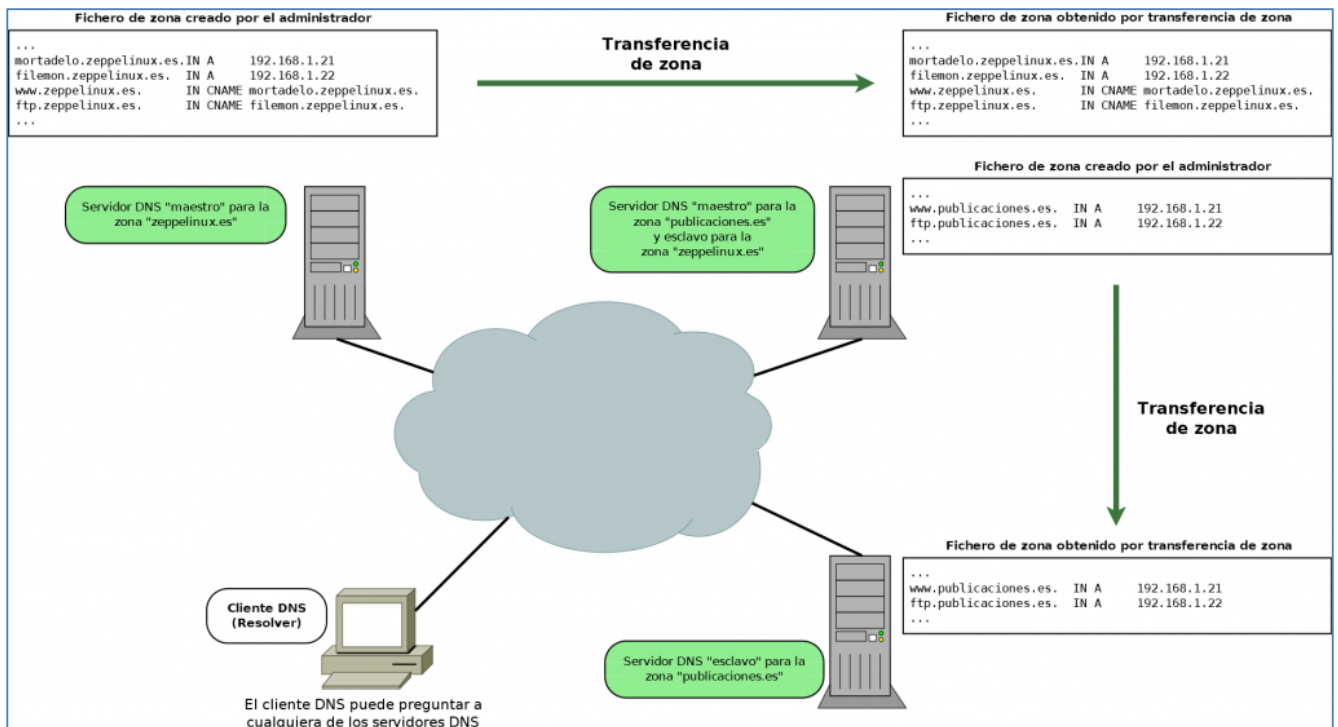


Figura 2-4. Servidores DNS Maestros y Esclavos (Fuente: <https://www.zeppelinix.es>).

2.2.5 Servidor Caché.

Servidores que se configuran para mejorar los tiempos de respuesta de las consultas, reducir la carga de los equipos y disminuir el tráfico de red, su funcionamiento se puede observar en la figura 2-5.

Si un servidor recibe una consulta sobre un dominio del que no es Autorizado, debe preguntar a otros servidores para resolverla. Si actúa como caché, esa información la guardará durante un tiempo para, en caso de ser consultado posteriormente, poder contestar sin necesidad de realizar de nuevo la consulta a otros servidores. Cada vez que es preguntado, este servidor lo primero que hace es comprobar si tiene esa información en su memoria caché. Un servidor DNS que es sólo caché (*cache only server*):

- No tiene autoridad sobre ninguna zona.
- Debe preguntar a otros servidores DNS a la hora de resolver las consultas que se realizan y guarda esas respuestas en su memoria cache.

2.2.1 Servidor Renviador (Forwarder).

Servidor DNS que es designado por otros servidores DNS para renviarle consultas. Se utilizan para minimizar las consultas y el tráfico de peticiones DNS desde una red hacia Internet. Permiten a los equipos locales utilizar su cache DNS para minimizar los tiempos de respuesta.

Existen dos formas de procesar las consultas:

1. **Consulta Iterativa:** El servidor DNS realiza la consulta a varios servidores DNS, pero empieza por servidores DNS Raíz, en la figura 2-6 se puede observar el funcionamiento de este tipo de consultas.
2. **Consulta Recursiva:** El servidor DNS renvía la consulta al renviador, para que sea éste el encargado de resolverla, en la figura 2-7 se puede observar el funcionamiento de este tipo de consultas.

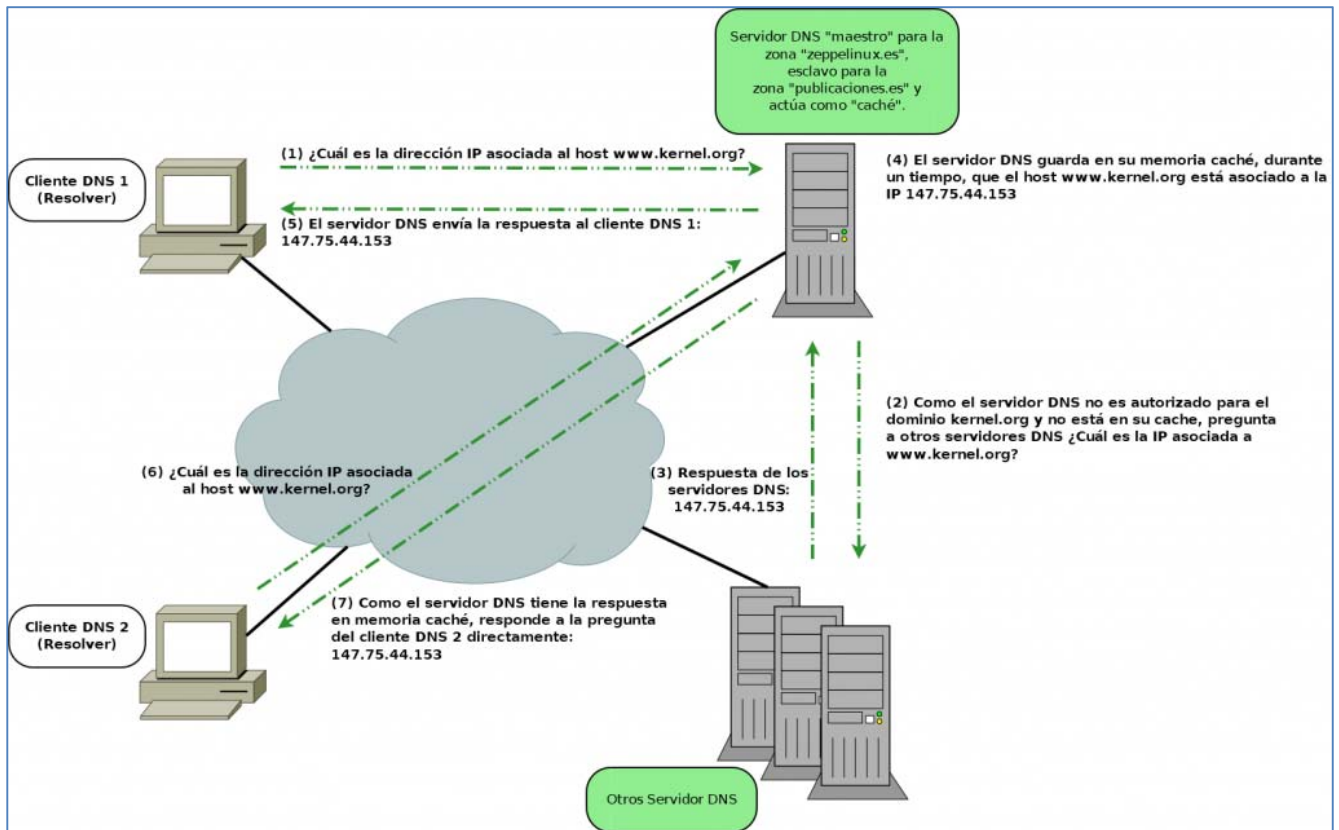


Figura 2-5. Servidores Autorizados y Cache (Fuente: <https://www.zeppelinlinux.es>).

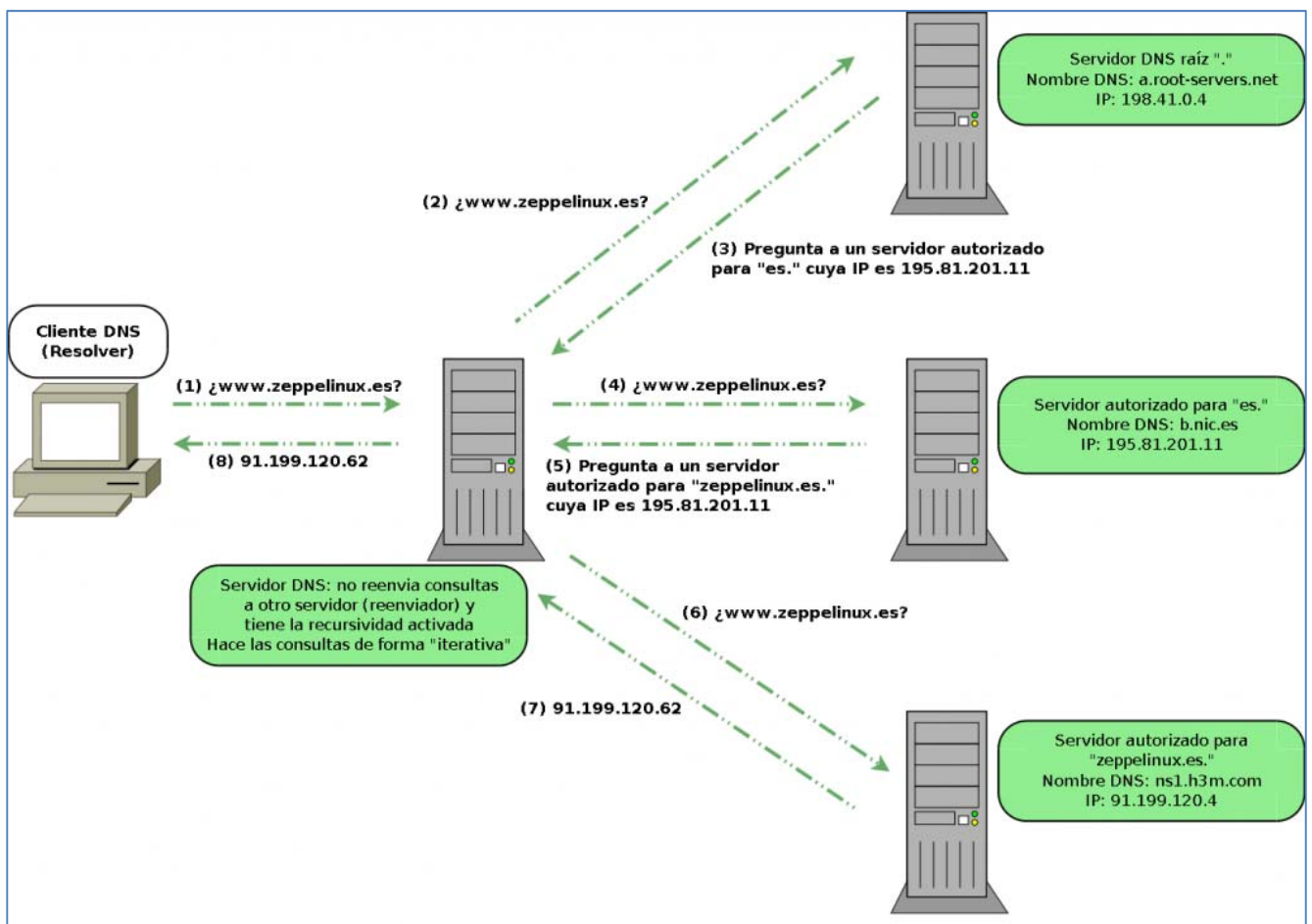


Figura 2-6. Servidores Consulta Iterativa (Fuente: <https://www.zeppelinlinux.es>).

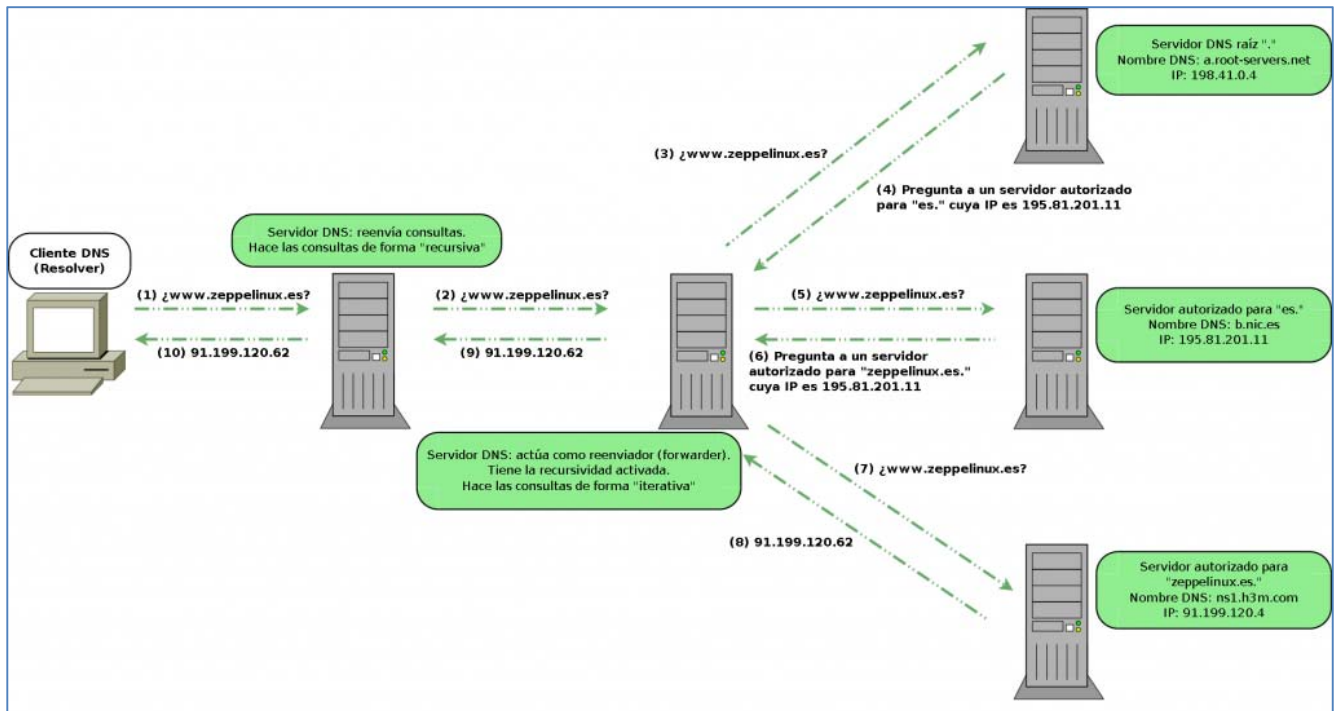


Figura 2-7. Servidores Consulta Recursiva (Fuente: <https://www.zeppelinix.es>).

2.2.2 Servidor sólo Autorizado (Authoritative Only).

Servidor que sólo responde a consultas relativas a sus zonas. Es un servidor que ni es Reenviador, ni Caché, ni tiene activada la recursividad.

2.3 Dominios de Nivel Superior (TLD). [32]

Un dominio de nivel superior o TLD (*Top Level Domain*) representa la primera para después de la zona raíz, dicho de otra manera, es todo lo que va detrás del punto final de un nombre de dominio. Por ejemplo, en el nombre de dominio "google.com", ".com" es el TLD.

2.3.1 Dominio Secundario.

Un dominio secundario es la porción del nombre de dominio que aparece antes del TLD cuando tecleamos la dirección de un sitio web. Por ejemplo, en www.google.es:

- **Google:** Dominio Secundario.
- **.es:** TLD, en este caso indica el código del país (España).

La gestión del dominio secundario la realiza su propietario, que tiene la capacidad para personalizar los registros del DNS, definir los subdominios que considere y controlar los servicios que tenga asociados.

Características del Dominio Secundario.

Componente esencial en la estructura del DNS, tiene las siguientes características:

1. **Identificación única:** Único dentro de su Dominio de Nivel Superior (TLD), lo que garantiza que cada dominio sea accesible y claramente identificable desde Internet. Por ejemplo, no pueden existir dos dominios **www.google.es** bajo el TLD **.es**.
2. **Gestión delegada:** Son los propietarios los responsables de la administración de los Dominios Secundarios. Cuando se registra un dominio, es el propietario el que tiene la capacidad para gestionar los registros DNS [31] [32] que tiene asociados ese dominio:
 - **Registro A:** Encargado de asociar el dominio a una determinada dirección IPv4.

- **Registro AAAA:** Asocia el dominio a una determinada dirección IPv6.
- **Registro MX:** Se definen los servidores de correo electrónico del dominio.
- **Registro CNAME:** Permite que diferentes nombres apunten al mismo dominio, ya que es capaz de darle distintos alias.
- **Registro TXT:** Ficheros de texto que contienen información del dominio que se utiliza para distintas funciones, como la verificación de la titularidad del dominio, prevención de correo basura, puntos de contacto.

Gracias al uso de este tipo de registros, los propietarios de los dominios pueden configurar el mismo en función de las necesidades específicas de los servicios que ofrecen, en la tabla siguiente figuran los registros DNS más comunes con la función que realizan y un ejemplo.

Tipo de Registro	Función	Ejemplo
A	Dirección IPv4	example.com -> 192.0.2.1
AAAA	Dirección IPv6	example.com -> 2001:db8::1
MX	Servidores de correo	mail.example.com
CNAME	Alias para otro dominio	www.example.com -> example.com
TXT	Información adicional (DKIM, DMARC, etc.)	v=spf1 include:_spf.example.com

Tabla 2-1. Tabla Registros DNS.

3. **Organización personalizada:** Para una mejor organización y segmentación las diferentes secciones o servicios de un sitio web, los dominios secundarios pueden subdividirse en subdominios. Por ejemplo:
 - mail.dominio.com: Subdominio dedicado a servicios de correo electrónico.
 - contacto.dominio.com: Sección del dominio donde figuran los datos de contacto.
 - info.dominio.com: Sección del dominio donde figura la información de este.

Gracias a esta estructura jerárquica se facilita la gestión y acceso a las diferentes secciones de un sitio web, haciendo más amigable la experiencia del usuario. Además, la administración interna del sitio también se hace más sencilla.

4. **Versatilidad:** El uso de dominios secundarios nos permite una amplia gama de propósitos:
 - **Sitios web:** Alojamiento de páginas web corporativas, personales, educativas, etc.
 - **Correos electrónicos:** Generación de cuentas de correo electrónico propias de cada dominio.
 - **Aplicaciones:** Despliegue de servicios web y aplicaciones asociadas al dominio.
 - **Servidores:** Asignación de nombres a servidores específicos dentro de la infraestructura del sitio web.

Esta versatilidad hace que cada dominio sea adaptado en función de las necesidades comerciales y tecnológicas de los servicios que se ofrecen.

5. **Seguridad y control:** El dominio secundario es el punto crítico donde se configuran las políticas de seguridad, como:
 - **DNNSEC (Domain Name System Security Extensions):** Extensión que se encarga de proteger la integridad de las respuestas del DNS.
 - **Registros TXT:** Como se ha comentado anteriormente, ficheros que contienen información del dominio.

6. **Escalabilidad:** A medida que la organización va ofreciendo más servicios a través del sitio web, se pueden ir agregando más subdominios.
7. **Coste-Eficiencia:** Gracias a la escalabilidad comentada anteriormente, se reducen costes de registro y gestión, y a partir del dominio principal, se pueden ir agregando más subdominios en función de las necesidades de la organización.

Retos Asociados a los Dominios Secundarios.

Aunque los dominios secundarios [33] ofrecen múltiples ventajas, también presentan una serie de inconvenientes relacionados con su gestión, seguridad y escalabilidad:

- **Complejidad en la gestión:** A medida que el dominio va creciendo y se van añadiendo más subdominios, la gestión de los servicios y de los registros DNS se va haciendo más compleja, lo que va a exigir un esfuerzo en la administración del sitio, sobre todo muy importante evitar los conflictos de subdominios o registros mal configurados.
- **Retos en la seguridad:** Los dominios secundarios y sus subdominios son objetivos muy atractivos para los atacantes que siempre buscan explotar las vulnerabilidades de los sitios o configuraciones incorrectas de los mismos.
- **Escalabilidad y rendimiento:** A medida que un dominio secundario va creciendo, van creciendo los subdominios y servicios, las consultas que se hacen al DNS se pueden ver afectadas ya que puede aumentar el tiempo de resolución de las mismas y los servidores mal dimensionados se pueden saturar.
- **Costes operativos:** Si el sitio va creciendo ofreciendo más servicios, creando más subdominios, también se incrementarán los costes asociados a la gestión y la seguridad del mismo, ya que se hará necesario la contratación de herramientas de gestión y la implementación de medidas de seguridad.

2.3.2 Registros DNS.

Los registros DNS son una parte fundamental en el DNS, esenciales para el buen funcionamiento del dominio ya que en función de los valores que tengan cada uno de ellos, permitirán la resolución de nombres de dominio, distribución de carga, administración de correo electrónico, seguridad y otros recursos esenciales para el funcionamiento del sitio web. A continuación, se muestra una relación de los registros más importantes:

▪ Registro A (*Address Record*).

Encargado de asociar el nombre de dominio con una dirección IPv4, lo que hace que los navegadores web y otros servicios sean capaces de localizar el servidor correspondiente. Se muestra un ejemplo en la Tabla 2-2.

example.com	Tipo de Registro	Valor	TTL
@	A	192.0.2.1	14400

Tabla 2-2. Tabla Registro A.

Donde:

@: Indica que se trata de un registro para el dominio raíz.

14400: TTL (Tiempo de vida) [34], indicado en segundos y por defecto para los registros A es de 14400 segundos.

▪ **Registro AAAA (IPv6 Address Record).**

Encargado de asociar el nombre de dominio con una dirección ip, igual que el registro A, pero con una dirección IPv6, permitiendo un espacio de direcciones mucho más extenso. Se muestra un ejemplo en la Tabla 2-3.

example.com	Tipo de Registro	Valor	TTL
@	AAAA	2001:0db8:85a3:0000: 0000:8a2e:0370:7334	14400

Tabla 2-3. Tabla Registro AAAA.

▪ **Registro MX (Mail Exchange Record).**

Registro de Intercambio de Correo, se encarga de dirigir al cliente de correo electrónico a un servidor de correo. Este registro indica cómo se deben enrutar los mensajes de correo electrónico de acuerdo con el protocolo simple de transferencia de correo (SMTP [35], protocolo estándar para todo correo electrónico.). En la tabla 2-4 se puede observar un ejemplo de este tipo de registros.

example.com	Tipo de registro	Prioridad	Valor	TTL
@	MX	10	mailhost1.example.com	45000
@	MX	20	mailhost2.example.com	45000

Tabla 2-4. Tabla Registro MX.

Donde:

Prioridad: Se prefiere el valor más bajo, en este caso, el servidor siempre intentará primero *mailhost1*, ya que tiene el valor más bajo.

▪ **Registro NS (Name Server).**

Servidor de Nombres, este registro indica qué servidor DNS es autorizado para un dominio. Estos registros indican a los clientes DNS dónde deberá ir a buscar la dirección IP de un determinado dominio. Puede ser que un dominio tenga varios registros de NS que puedan identificar servidores de dominios primarios y auxiliares de ese dominio. Si un registro NS no está bien configurado, los usuarios serán incapaces de cargar un sitio web o una aplicación. En la tabla 2-5 se puede observar un ejemplo de este tipo de registros:

example.com	Tipo de registro	Valor	TTL
@	NS	ns1.exampleserver.com	21600

Tabla 2-5. Tabla Registro NS.

▪ **Registro CNAME (Canonical Name Record).**

Este registro permite que un recurso pueda tener varios alias, lo que hace que múltiples nombres apunten a un mismo sitio, lo que hace más fácil la administración de dominios, ya que permite redirecciones y alias sin necesidad de tener varios registros A o AAAA. Todos los registros CNAME deben apuntar a un dominio, nunca a una dirección IP. El Registro CNAME solo apunta al cliente a la misma dirección IP que el dominio raíz. Una vez que el cliente llega a esa dirección IP, es el servidor web el que seguirá manejando la URL en ese sentido. Se muestra un ejemplo en la Tabla 2-6.

blog.example.com	Tipo de Registro	Valor	TTL
@	CNAME	es un alias de example.com	32600

Tabla 2-6. Tabla Registro CNAME.

Los Registros CNAME tienen unas restricciones en su uso, ya que los Registros MX y NS, no pueden apuntar a un registro CNAME, deben apuntar a un registro A o AAAA.

▪ **Registro TXT (*Text Record*).**

Registro que almacena información en formato .txt asociada a cada dominio, se utiliza para diversas configuraciones y verificaciones. Existen diversos tipos de registros:

- **DKIM (*DomainKeys Identified Mail*):** Correo Identificado con DomainKeys, se trata de un registro en el que se alojan las claves públicas asociadas a dominios específicos y se utilizan para firmar digitalmente los correos electrónicos, para garantizar que los correos electrónicos no sufren alteraciones.
- **DMARC (*Domain-based Message Authentication, Reporting and Conformance*):** Autenticación de mensajes, informes y conformidad basada en dominios, se utilizan para indicar a los servidores si deben poner un mensaje en cuarenta, rechazarlo o permitir su envío y también para enviar informes a direcciones de correo electrónico determinadas.
- **SPF (*Sender Policy Framework*):** Registro en el que se declaran qué dominios y equipos pueden o no enviar correos electrónicos en nombre de un dominio. Pueden contener dos partes: la lista de dominios autorizados y lista de remitentes prohibidos.

En 1993 la IETF (*Internet Engineering Task Force*) definió un formato específico para este tipo de registros. El atributo y el valor del mismo deben ir entre comillas y separados por un signo de igual, en la tabla 2-7 se pueden observar unos ejemplos de este tipo de registros:

host.widgets.com	Tipo de registro	Valor
@	TXT	"printer=lpr5"

sam.widgets.com	Tipo de registro	Valor
@	TXT	"favorite drink=orange juice"

Tabla 2-7. Tabla Registro TXT.

▪ **Registro PTR (*Pointer Record*).**

Registro de Puntero de DNS, que se encarga de proporcionar el nombre de dominio asociado a una dirección IP. Realiza la función contraria del Registro tipo A, que se encarga de proporcionar la dirección IP asociada a un nombre de dominio. Estos registros se utilizan en las búsquedas de DNS inverso, se trata de una consulta que comienza con la dirección ip y va a buscar el nombre de dominio. Los registros PTR se almacenan bajo la dirección IP invertida y con ".in-addr.arpa" añadido. Ejemplo de registro PTR: La dirección IP 192.0.2.255 se almacenaría en "**255.2.0.192.in-addr.arpa**".

Principales usos de los Registros PTR:

- **Antispam:** Algunos filtros antispam utilizan el DNS inverso para comprobar los nombres de dominio de los correos electrónicos y así confirman que esas direcciones IP son utilizadas por servidores de correo legítimos.
- **Registro:** Gracias a la búsqueda de DNS inverso se pueden convertir las direcciones IP en nombres de dominio más legibles.

▪ **Registro SOA (*Start of Authority*).**

Registro de Inicio de Autoridad, se encarga de almacenar toda la información que se considera importante sobre un dominio o sitio. Todos los DNS necesitan de este registro según lo establecido

por la IETF, importantes también para las transferencias de zona. En la tabla 2-8 se puede ver un ejemplo de un registro SOA.

Name	example.com
Tipo de registro	SOA
MNAME	ns.primaryserver.com
RNAME	admin.example.com
Serie	111111111
Actualizar	86400
RETRY	7200
EXPIRE	4000000
TTL	11200

Tabla 2-4. Tabla Registro SOA.

Donde:

MNAME: Nombre del Servidor de nombres primario de la zona.

RNAME: Dirección de correo electrónico del administrador. Destacar que aunque en este caso no figura la @ en la dirección de correo, los registros SOA sí que son capaces de identificar ese valor como la dirección de correo: admin@example.com.

Serie: Número de serie del registro. Suele tener formato de fecha (AAAAMMDDNN), siendo NN el número de revisión, que debe incrementarse cada vez se cambia el archivo de zona.

Actualizar: Tiempo en segundos que debe esperar un servidor DNS secundario antes de consultar el registros SOA del servidor DNS primario para comprobar si hay cambios.

RETRY: Tiempo en segundos que debe esperar un servidor para volver a pedir una actualización a un servidor de nombres de dominio primario que no responde.

EXPIRE: Tiempo en segundos que debe esperar un servidor secundario para obtener respuesta de un servidor primario antes de dejar de responder a las consultas de la zona.

TTL: Tiempo de Vida.

Ejemplo de un Registro DNS:

```
$TTL 86400
@ IN SOA ns1.ejemplo.com. admin.ejemplo.com. (
    2025010101 ; Número de serie
    7200      ; Refresco cada 2 horas
    3600      ; Reintento cada 1 hora
    1209600   ; Expiración a las 2 semanas
    3600 )    ; TTL mínimo de 1 hora
@ IN NS ns1.ejemplo.com.
@ IN NS ns2.ejemplo.com.
@ IN A 192.0.2.1
www IN CNAME ejemplo.com.
mail IN MX 10 mail.ejemplo.com.
```

Importancia de los Registros DNS.

Los Registros DNS son esenciales para el buen funcionamiento del Sistema de Nombres de Dominio, ya que deben asegurar que los servicios de Internet funcionan de una manera eficiente, segura y confiable.

- **Eficiencia:** Permiten a los usuarios acceder a los sitios y servicios de Internet de una manera ágil y sencilla gracias a la resolución rápida de los nombres de dominio.
- **Escalabilidad:** Debido al aumento considerable de usuarios y dispositivos en Internet, deben ser capaces de soportar gran cantidad de tráfico.
- **Flexibilidad:** Únicamente modificando el Registro DNS correspondiente, se puede cambiar la ubicación física de un servidor, sin que el usuario haya experimentado una pérdida de servicio.
- **Seguridad:** Gracias a los Registros TXT (SPF, DKIM, DMARC) se pueden implementar políticas de autenticación que previenen el *spam* y la suplantación de identidad.
- **Gestión de Correos Electrónicos:** Para garantizar la correcta entrega de correos electrónicos, se hace uso de los Registros MX, donde se definen los servidores de correo responsables de recibir los mensajes para un determinado dominio.

2.4 Funcionamiento del DNS.

Como se ha comentado anteriormente, el DNS es fundamental para el correcto funcionamiento de Internet, ya que se encarga de traducir los nombres de dominios legibles por humanos en direcciones IP legibles para las máquinas, a continuación se va a detallar el proceso de resolución de consultas por parte del DNS.

Un **cliente DNS** [36] se puede definir como un programa que realiza una pregunta a un servidor DNS y es capaz de interpretar las respuestas que éste le da. Para ello, existen una serie de librerías, que vienen en los Sistemas Operativos o se pueden instalar, que son las encargadas de realizar estas funciones. Cuando se realiza la consulta, las aplicaciones (clientes FTP, navegadores web, clientes de correo, etc.) invocan estas librerías para poder manejar los nombres de dominio. Para aumentar el rendimiento y minimizar el uso de la red, tanto los clientes como los servidores, almacenan esta información en la caché de respuestas, pudiendo acceder a ella más rápidamente.

Los clientes DNS pueden configurar la forma en que resuelven los nombres de dominio, ya que la mayoría de los sistemas operativos poseen una serie de ficheros de texto en los que pueden asociar las direcciones IP a nombres de dominio o de equipos, y configurar el cliente DNS de tal forma que sean estos ficheros los primeros que se consultan para hacer la resolución.

Cuando una aplicación quiere resolver un nombre, invoca al cliente DNS y habitualmente realiza el siguiente proceso:

1. La aplicación hace una consulta al cliente DNS para resolver el nombre de un dominio o de equipo.
2. Si se ha configurado para que la primera consulta se haga a la caché, se consulta ésta y si el nombre se encuentra ahí almacenado, se devuelve la respuesta a la consulta.
3. Si el nombre no se encuentra almacenado en la caché, se realizará la consulta al fichero *hosts* del equipo. En sistemas Windows éste se encuentra en: `%SYSTEMROOT%\system32\drivers\etc\hosts` y si se trata de Sistemas Unix/Linux se encuentra en: `/etc/hosts`. Si la respuesta se encuentra en este fichero, se devuelve a la aplicación.
4. Si aún no se ha proporcionado la respuesta a la aplicación, se eleva una consulta recursiva al servidor DNS que esté configurado y será éste el que devuelva la respuesta.

En la figura 2-10 se puede observar la resolución de un nombre de dominio.

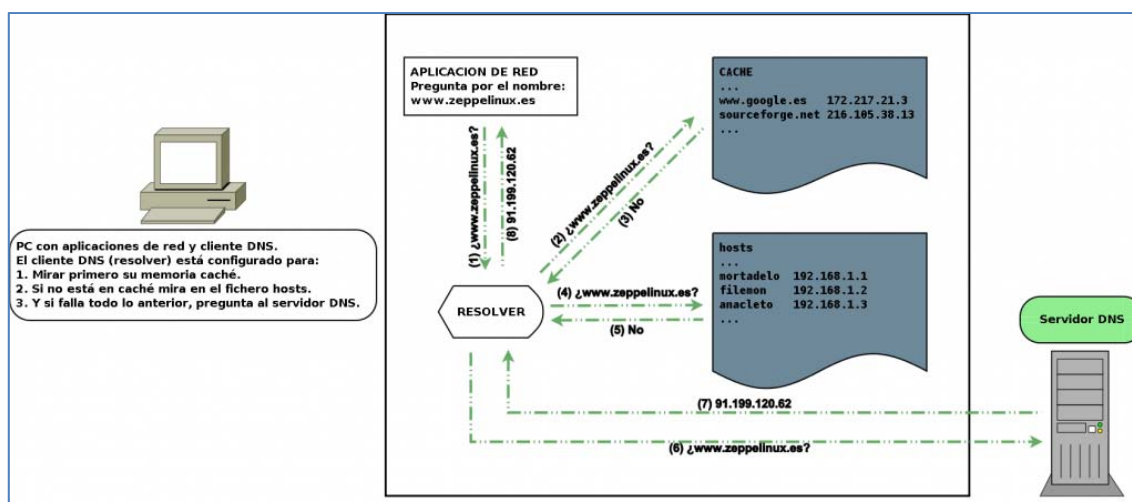


Figura 2-8. Resolución de nombre de dominio (Fuente: <https://www.zepellinux.es>).

Proceso de Resolución.

Para la resolución de los nombres de dominio, tanto los Clientes como los Servidores DNS realizan las consultas a otros Servidores DNS, estas consultas pueden ser recursivas o iterativas.

Consultas Recursivas.

Una consulta recursiva es cuando el servidor DNS da una respuesta completa o exacta. Existen tres tipos de respuesta:

1. **Positiva:** El servidor responde a la consulta que se le ha realizado. La respuesta contiene si el servidor es autorizado o no autorizado, pero no se puede saber si el servidor que ha respondido con autoridad es maestro o esclavo para el dominio por el que ha sido preguntado.
2. **Negativa:** El servidor no ha podido responder a la consulta que se le ha realizado, se produce lo que se llama una condición **NXDOMAIN**, se trata de un nombre de dominio que no existe, por lo que el DNS no es capaz de resolverlo.
3. **Error:** Se produce cuando por fallos en la red, caída del servidor, etc., no se puede preguntar a otros servidores DNS.

Una vez recibida la consulta y en función del tipo de servidor que la haya recibido: Autorizado (maestro o esclavo), Caché o Renviador se resolverá de una manera u otra.

Un ejemplo de resolución de DNS a un servidor no autorizado se puede ver en la figura 2-11.

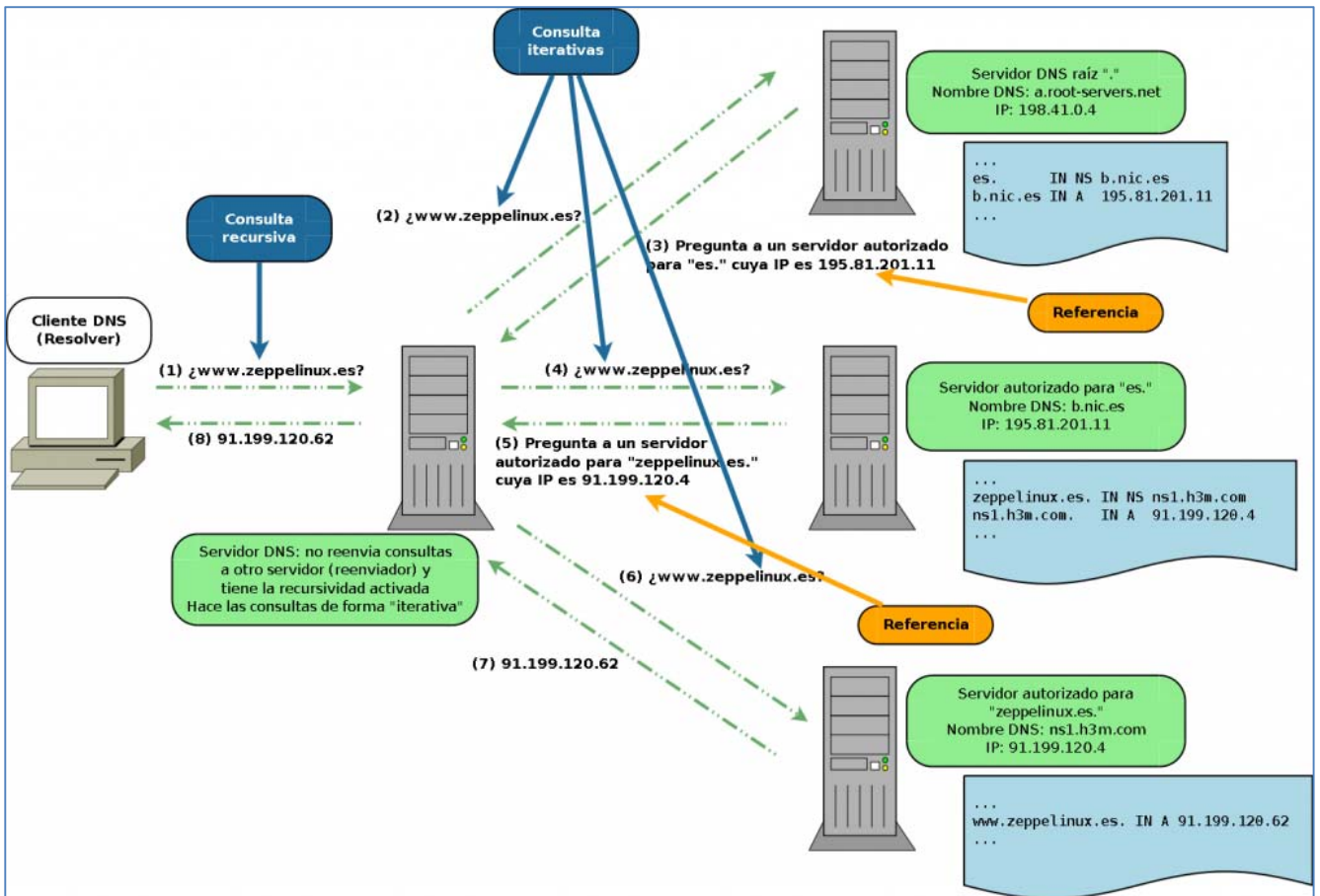
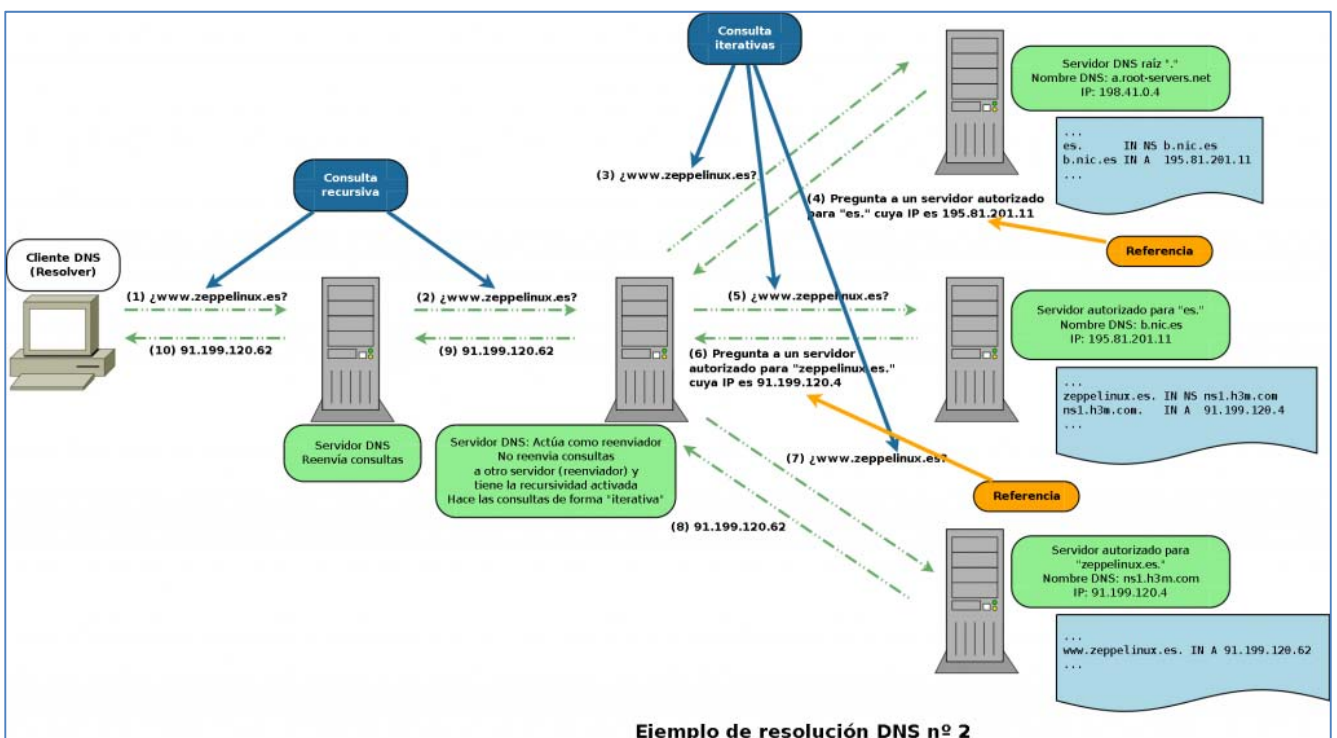


Figura 2-9. Consulta a Servidor No Autorizado. (Fuente: <https://www.zeppelinix.es>).

En la siguiente figura 2-12 se puede observar un ejemplo de resolución de DNS a un servidor configurado como Reenviador.



Ejemplo de resolución DNS nº 2

Figura 2-10. Consulta a Servidor Reenviador. (Fuente: <https://www.zeppelinix.es>).

Las consultas recursivas consumen muchos recursos de los servidores DNS, por lo que es habitual que los autorizados para alguna zona no respondan a ellas. Por ejemplo, los servidores DNS raíz y los autorizados para los dominios TLD no responden a este tipo de consultas.

Consultas Iterativas.

Una consulta iterativa es cuando el servidor DNS da una respuesta parcial. Existen cuatro tipos de respuesta:

1. **Positiva:** El servidor responde a la consulta que se le ha realizado y se indica si es autorizado o no.
2. **Negativa:** El servidor no ha podido responder a la consulta que se le ha realizado (NXDOMAIN).
3. **Indica Referencia:** El servidor responde indicando otros servidores a los que se puede preguntar.
4. **Error:** Se produce cuando se ha producido algún tipo de error.

2.5 Amenazas y Vulnerabilidades en el DNS.

El DNS está considerado un elemento fundamental para el buen funcionamiento de Internet, lo que lo convierte en un objetivo principal de ciberataques [37]. Desde sus inicios en 1983 y debido a su arquitectura abierta y jerárquica, la falta de mecanismos de seguridad en la concepción original, han hecho que este sistema sea vulnerable a múltiples amenazas y ciberataques.

La criticidad de este sistema para el buen funcionamiento de Internet hace que cualquier interrupción o manipulación indebida pueda tener un impacto muy significativo en la prestación de cualquier servicio, aplicaciones empresariales, correos electrónicos, plataformas de correo electrónico, etc.

Importancia del DNS en el ecosistema de internet. [38]

1. **Pilar de la conectividad:** Todas las operaciones que se hacen online, desde video llamadas a navegación web, dependen del buen funcionamiento del DNS para que se localicen los recursos correctos, por lo que el sistema se debe mantener estable para que todos los servicios funcionen correctamente.
2. **Dependencia universal:** Gobiernos, empresas y usuarios confían en el DNS para la mayoría de sus actividades digitales, por consiguiente, cualquier fallo o interrupción del sistema puede provocar graves pérdidas a nivel económico y social.
3. **Volumen y escalabilidad:** Debido a la inmensa cantidad de consultas que los miles de millones de dispositivos conectados a Internet realizan, el DNS es un bjetivo muy atractivo para los atacantes.
4. **Relación entre el DNS y la seguridad global:** El DNS juega un papel fundamental en la seguridad cibernética global, ya que multitud de herramientas y servicios de protección (Firewalls, IDS, IPS, etc.) dependen del DNS para identificar y bloquear actividades maliciosas. Un ataque al DNS puede tener un efecto cascada en la se pueden ver comprometidas otras capas de Internet.

2.5.1 Amenazas.

El DNS se diseñó en los años 80, cuando únicamente tenían acceso a Internet algunas agencias gubernamentales, científicos y el ejército. Debido a este uso tan restrictivo y la preocupación por la fiabilidad y la funcionalidad, no se tuvo en cuenta un factor tan importante como es la seguridad. Resultado de esto es que los servidores DNS siempre han sido vulnerables a una amplia gama de ataques.

Según el informe 2022 Global DNS Threat Report [39] de IDC, reveló los siguientes datos que se muestran en la figura 2-14:



Figura 2-11. Cifras ataques DNS en 2022. (Fuente: <https://efficientip.com/>).

A continuación se presentan las amenazas más comunes a las que se enfrenta el DNS.

Envenenamiento de Caché (*Cache Poisoning*). [40]

Se trata de un ataque por el cual los usuarios son redirigidos a un sitio web malicioso, creyendo que están accediendo al que ellos quieren. Los atacantes introducen información falsa en la caché del DNS y a la hora de hacer una consulta, devuelve una respuesta errónea, redirigiendo a los usuarios al sitio que los atacantes tienen bajo control.

Para envenenar la caché, los atacantes se hacen pasar por Servidores de nombres DNS, hacen una solicitud a un solucionador DNS y falsifican las respuestas cuando el solucionador de DNS realiza la consulta a un Servidor de nombres. Esto se hace posible porque los servidores DNS utilizan el protocolo UDP en vez de TCP y no se hace una verificación de la información DNS.

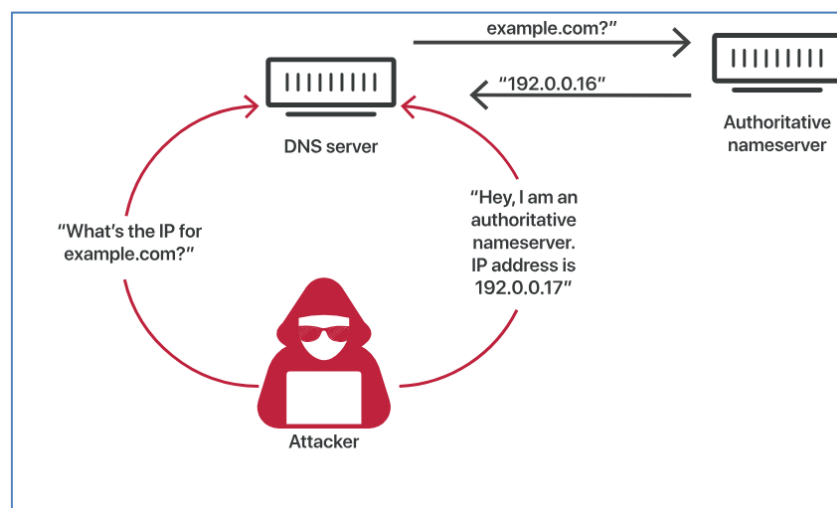


Figura 2-12. Envenenamiento de Caché. (Fuente: <https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning/>).

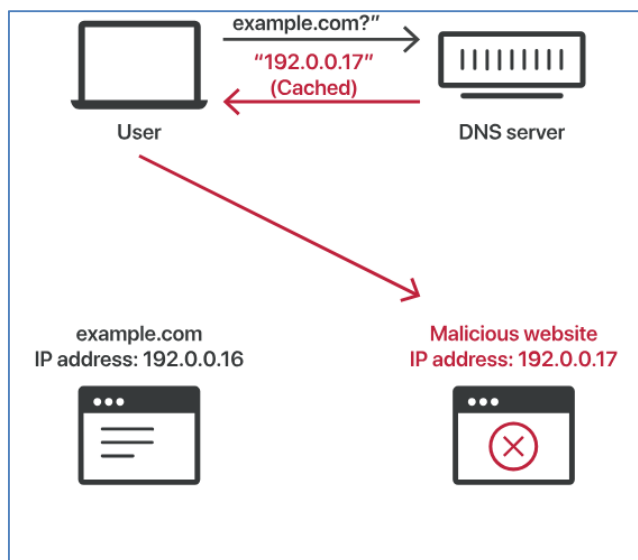


Figura 2-13. Caché DNS Envenenada. (Fuente: <https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning/>).

Como para la comunicación utilizan el protocolo UDP [41] (*User Datagram Protocol*), que no garantiza que la conexión esté abierta o de que el destinatario esté listo para la recepción del paquete, esto hace que UDP sea vulnerable a este tipo de ataque, ya que un atacante modificando los datos del encabezado del mensaje, puede enviarlo mediante UDP y que parezca que ha sido la respuesta de un servidor legítimo.

El solucionador DNS como cree que la respuesta proviene de un servidor legítimo, almacena esa información falsificada en su caché, ya que no puede verificar si esa información proviene de un servidor legítimo o no. Esto se debe a que el DNS se diseñó en los inicios de Internet, cuando solamente era usado por unas pocas entidades públicas y no se preveía que se pudiera difundir información falsa a través del DNS.

Pero este tipo de ataque no es tan sencillo, ya que las consultas que realiza el solucionador van a un servidor de nombres autorizado, por lo que los atacantes disponen de unas pocas milésimas de segundo para enviar la respuesta errónea, para devolverla antes de que llegue la auténtica.

Para realizar este ataque, los atacantes deben saber o adivinar una serie de cuestiones:

- Id de la solicitud.
- Servidor de nombres autorizado que resolverá la consulta.
- Consultas que no están almacenadas en la caché del solucionador, para que la consulta vaya al servidor de nombres autorizado.
- Puerto que el solucionador DNS está usando.

Es difícil detectar un envenenamiento de caché, por lo que es necesaria la implementación de herramientas de seguridad que sean capaces de detectar estos ataques. Sin embargo, hay unos signos reveladores de que se está produciendo este ataque, como pueden ser una caída inesperada del tráfico web o que se hayan producido cambios significativos en la actividad del DNS de un dominio.

Este tipo de ataques se puede evitar, siguiendo las siguientes prácticas de seguridad recomendadas:

- **Adopción de DNSSEC:** Con el uso de las extensiones de seguridad del DNS (DNSSEC) se pueden verificar los datos del DNS, ya que se utiliza la criptografía de clave pública para la verificación y autenticación de los datos.

- **Actualización y Aplicación de parches:** El software de DNS debe ser actualizado y parchado con regularidad ya que este va a reducir la posibilidad de que los atacantes puedan explotar alguna vulnerabilidad “zero-day” [42].
- **HTTPS para el tráfico del DNS:** DNS mediante HTTPS (DoH) hace que el tráfico sea cifrado, ya que las consultas se transfieren a través de una sesión cifrada de HTTPS, con lo que se ocultan las consultas DNS y se mantiene la privacidad.
- **Zero Trust en configuración de Servidores DNS:** Con la adopción de los principios de *Zero Trust* se requiere que todos los usuarios, dispositivos y aplicaciones se consideren comprometidos a menos que realicen una autenticación y validación continua.
- **Resolución de respuesta rápida del DNS:** Debido a que en este tipo de ataque se dispone de poco tiempo para inyectar la respuesta maliciosa, el DNS debe ser capaz de responder rápidamente para evitar este tipo de ataque.

Suplantación de DNS (DNS Spoofing). [43]

Con este tipo de ataque se alteran las respuestas en un servidor DNS para redirigir a la víctima a un sitio web que es controlado por el atacante. Este tipo de ataque se suele dar en entornos donde la víctima accede a Internet desde una Wi-Fi pública o también en situaciones donde el atacante puede alterar las tablas del ARP [43] (*Address Resolution Protocol*) y redirige a la víctima a un sitio web igual que el oficial, pero en el que el atacante tiene el control, siendo un lugar muy adecuado para realizar un ataque de *phishing* o instalación de algún *malware* en el dispositivo de la víctima.

Como se ha comentado anteriormente, las redes Wi-Fi públicas gratuitas son objetivos potenciales, ya que normalmente suelen estar mal configuradas o deficientemente protegidas, lo que da la oportunidad a los atacantes de ejecutar este tipo de ataque.

Si la víctima se conecta a una Wi-Fi pública, el atacante realiza los siguientes pasos:

1. El atacante se coloca entre la víctima y el Servidor DNS legítimo e intercepta las solicitudes de resolución de nombres de dominio, puede hacerlo mediante un ataque “*Man-in-the-middle*” [44] .
2. Ya con la comunicación interceptada, el atacante envía una respuesta falsa al usuario con una dirección IP falsa, redirigiendo al sitio web controlado por el atacante.
3. Como la víctima cree que se encuentra en un sitio web original, al realizar cualquier transacción le brinda la oportunidad al atacante de recopilar diversa información: contraseñas, información bancaria, datos de contacto, etc.

Existen algunos signos que pueden evidenciar que algo raro está ocurriendo y que el usuario puede estar siendo víctima de este tipo de ataque:

- Signos de que una página web, que se visita normalmente, presenta diseño, contenido o un comportamiento anómalo, puede tratarse de una mala copia.
- Alertas de seguridad del navegador, por las que nos indica que hay problemas con el certificado de seguridad o conexiones no seguras.
- Cambios en la configuración de las cuentas del usuario o accesos inusuales.

Para prevenir este tipo de ataques, se deben implementar unas medidas de seguridad como son las siguientes:

- **DNSSEC:** Como se comentó anteriormente, con el uso de las extensiones de Seguridad del DNS se añade una capa para autenticar las respuestas del DNS, garantizando que la información que recibe el usuario es legítima y no ha sido alterada.

- **Configuración segura del Servidor DNS:** Se debe realizar una configuración adecuada y mantenerlos continuamente actualizados.
- **Monitorización de la Red:** Para detectar posibles comportamientos anómalos que puedan indicar un intento de ataque.
- **Firewalls con inspección DNS:** Estos dispositivos analizan el tráfico DNS en busca de patrones o anomalías en el tráfico para impedir este tipo de ataques.
- **DNSCrypt:** Protocolo que cifra y autentica el tráfico DNS entre el usuario y los Servidores de Nombres.
- **Listas Blancas:** Confección de listas blancas de servidores confiables.

En España, en el año pasado algunas empresas se han visto implicadas en este tipo de ataques:

- **Tendam** [46], empresa dueña de diversas marcas como Women'secret, Springfield o Cortefiel, sufrió un ataque el pasado mes de octubre de 2024, por el cual se vieron expuestos los datos personales de sus clientes.
- **Alcampo** [47], cadena de supermercados, sufrió otro ataque el pasado mes de agosto de 2024, que requirió grandes medidas de contingencia para mantener sus servicios operativos.

En la figura 2-17 se puede observar el funcionamiento normal de un servidor DNS y cuando es víctima de ataque DNS Spoofing.



Figura 2-14. Ataque DNS Spoofing. (Fuente: https://www.uv.mx/infosegura/general/noti_ataques-6/).

Ataques de Denegación de Servicio (DoS y DDoS). [48]

Con estos ataques se trata de inundar un recurso con tráfico (DoS – Denegación de Servicio) o utilizando una red de equipos que se encarguen de realizar esa inundación (DDoS – Denegación de Servicio Distribuido), para intentar agotar los servicios del Servidor de Nombres de DNS, ya que le llegan una enorme cantidad de consultas que provoca el bloqueo o la limitación de velocidad del servidor DNS.

Según el modelo OSI (Modelo de Interconexión de Sistemas Abiertos), este tipo de ataques suelen ir dirigidos a las capas de Red (Capa 3), Transporte (Capa 4), Presentación (Capa 6) y Aplicación (Capa 7).

Existen diversos ataques de este tipo, pero se pueden clasificar en dos grandes grupos:

- **Ataque por inundación de DNS:** Con este tipo de ataques se intenta agotar los recursos de un servidor DNS mediante el envío de una multitud de consultas. Para este tipo de ataques se suelen utilizar botnets [49] distribuidos que se utilizan para ocultar el ataque usando diversos agentes de resolución recursivos, que son el origen del tráfico malicioso.

NXDOMAIN, conocido como Subdominio Pseudoaleatorio (PRSD), es una técnica de inundación del DNS mediante la cual los agentes maliciosos generan una enorme cantidad de solicitudes para dominios que no existen, con el fin de consumir los recursos del servidor de nombres autorizado mientras van agotando el grupo de caché de un agente de resolución recursiva. Si tiene éxito este ataque, va a aumentar los tiempos de resolución del DNS para consultas que son legítimas. Este tipo de ataques va dirigido a las capas 3 y 4, capas de la infraestructura.

- **Ataque por amplificación de DNS:** Este tipo de ataques no se dirige al servidor de nombres, sino que intenta consumir los recursos de otro equipo enviándole multitud de respuestas y solicitudes DNS que ese equipo no ha realizado. Similar a enviar una carta pero la dirección de contestación es la de equipo a atacar (objetivo). Todos estos mensajes van a llegar a un tercero, que no los esperaba, para intentar consumir los recursos del mismo. Los atacantes prefieren optar por explotar el DNS para este tipo de ataques, ya que como el protocolo usado es el UDP y se pueden enviar los mensajes a cualquier destino sin que haya una confirmación previa de que se esperan esos mensajes.

Se trata de ataques dirigidos a las capas de aplicación, capas 6 y 7. En la figura 2-18 se puede observar un ataque DDoS.

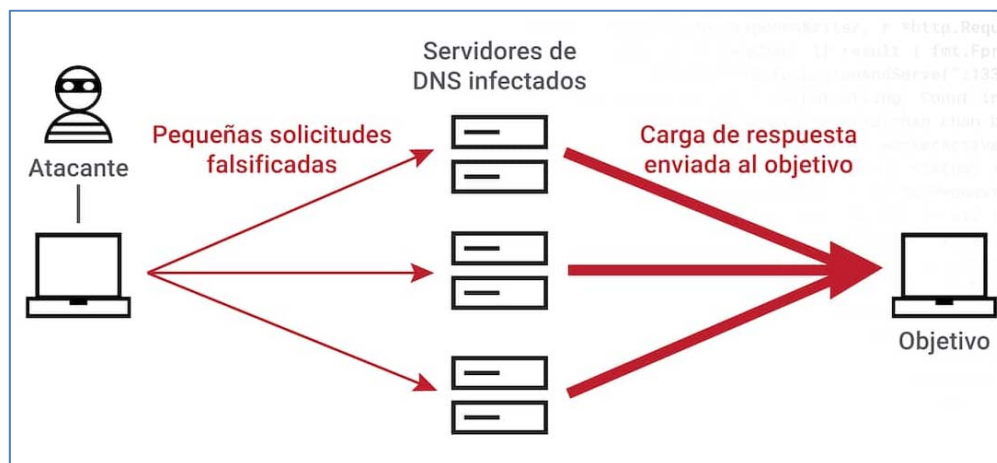


Figura 2-15. Ataque DDoS. (Fuente: <https://www.akamai.com/es/glossary/what-is-a-dns-ddos-attack>).

La detección y mitigación de este tipo de ataques no es sencilla sin que haya una interrupción del servicio a los usuarios, se pueden realizar una serie de recomendaciones que ayuden a mejorar la protección ante estos ataques:

- **Uso de red Anycast:** Con el uso de una red Anycast distribuida geográficamente se va a ampliar el área para absorber los ataques a gran escala.
- **Aumento de los TTL:** Con el aumento de los TTL de registro, se puede contribuir a la reducción de las consultas, tanto legítimas como ilegítimas, que llegan a los Servidores de Nombre Autentizados, y así se ahorrará ancho de banda del Servidor de Nombres.
- **Deshabilitar solicitudes ANY:** Si se deshabilitan del DNS las solicitudes ANY, que recupera todos los registros disponibles para un nombre de dominio, se va a evitar que los atacantes puedan realizar este tipo de consultas para realizar un ataque por amplificación.

- **Reducción de la superficie expuesta:** Si se minimiza la superficie expuesta al ataque se van a limitar las opciones de los atacantes y va a permitir centralizar todos los esfuerzos en proteger esa pequeña superficie. Esto se puede conseguir si colocamos esta superficie detrás de una Red de Distribución de Contenido [50] (CDN) o con el uso de Balanceadores de Carga, restringiendo el tráfico a partes críticas de nuestra infraestructura.
- **Uso de servicios de Mitigación:** Como por ejemplo <https://www.cloudflare.com/> [50] o <https://www.akamai.com/> [51].

Túneles DNS (DNS Tunneling). [52]

Este tipo de ataques comienza cuando un usuario descarga *malware* en un equipo o un atacante es capaz de explotar una vulnerabilidad e instalar algún tipo de software malicioso. La idea de los atacantes es querer tener el control del dispositivo para poder ejecutar comandos o exfiltración de datos, mediante la creación de un túnel intentando evitar las medidas de seguridad del perímetro de la red. Para este tipo de ataque el tráfico DNS es perfecto, ya que no suele controlarse por los sistemas de seguridad perimetrales, como los *firewalls*.

Este ataque funciona de la siguiente manera:

1. El atacante necesita crear y registrar un nombre de dominio y configurar un servidor de nombres autorizado que pueda controlar.
2. El *malware* del equipo infectado realiza alguna consulta al servidor DNS del atacante, este servidor le responde con paquetes de datos DNS que contienen comandos o datos que se ejecutarán en el equipo infectado.
3. De esta manera se establece una comunicación bidireccional entre los dos dispositivos y el atacante puede tener el control del equipo.

En la figura 2-19 se puede observar el funcionamiento del ataque túnel DNS.

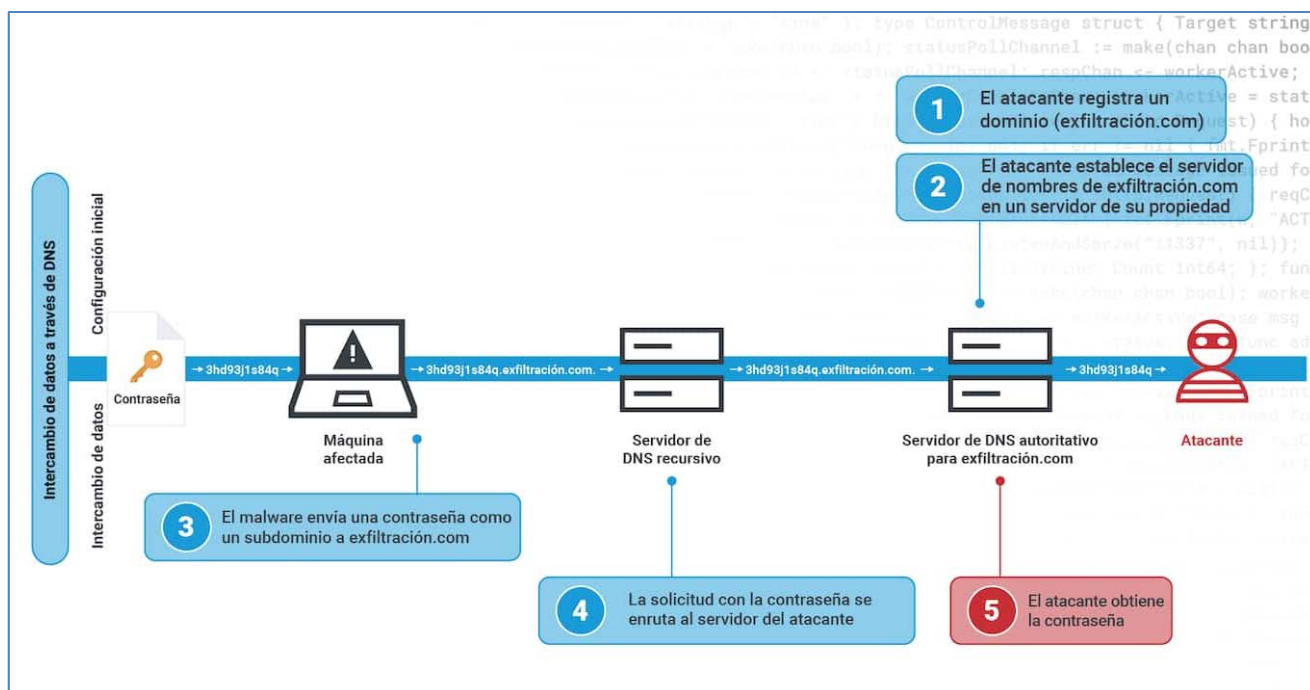


Figura 2-16. Funcionamiento Túnel DNS. (Fuente: <https://www.akamai.com/es/glossary/what-is-dns-tunneling>).

Con este tipo de ataque, al atacante podrá:

- **Instalación de *malware*:** Utilizando el túnel DNS pueden instalar *malware* en sistemas adicionales mediante movimiento lateral [53].
- **Recopilación de credenciales:** Una vez que se ha establecido la comunicación con el equipo infectado, el atacante tiene el control del equipo y podrá instalar cualquier software, como *keyloggers*, para recopilar credenciales del usuario y posteriormente hacer un uso fraudulento de ellas.
- **Explorar la Red:** Desde el equipo infectado, el atacante puede ser capaz de realizar un mapa de red y de esa manera identificar otros activos de gran valor a los que atacar.
- **Exfiltración de Datos:** Como la comunicación es bidireccional, desde el equipo infectado se puede enviar información mediante el túnel DNS que llegara al atacante.
- **Control del Equipo:** Como el atacante es capaz de tener el control del equipo infectado, lo puede utilizar para realizar otro tipo de ataques como DoS o DDoS.

Para evitar este tipo de ataques, se pueden seguir las siguientes prácticas recomendadas de seguridad:

- Cursos de concienciación para los usuarios, en los que se instruya sobre los peligros de ejecutar archivos sospechosos o abrir correos de remitentes no reconocidos.
- Uso de Antivirus y *Antimalware* para prevenir la infección de los equipos por ese *malware*, ya que esa infección es el primer paso para establecer el túnel DNS.
- Control del tráfico red, incluidas las solicitudes de DNS, mediante soluciones tecnológicas.
- Supervisión de los servicios que utilicen el túnel DNS, como antivirus para la recuperación de firmas, pero que pudieran utilizarse para otros motivos no legítimos.
- Utilización de soluciones avanzadas que permitan protegerse contra estas amenazas y mejorar la seguridad del DNS, para poder bloquear el *malware*, detener la exfiltración de datos y detectar contenido malicioso incrustado en el tráfico de DNS.

Secuestro de DNS (*DNS Hijacking*). [54]

Uno de los ataques más perjudicial para el DNS, también conocido como “Ataque de redireccionamiento DNS”, se produce cuando las consultas al DNS que realiza el equipo de la víctima son resueltas de manera incorrecta y redirigen al usuario a un sitio web malicioso. Este tipo de ataque requiere que se hagan cambios en la configuración del DNS, que normalmente se hace con la instalación de algún tipo de *malware* en el dispositivo de la víctima, lo que va a permitir al atacante tomar el control de sus enrutadores, interceptar las señales DNS o piratear las comunicaciones del DNS.

Mediante este tipo de ataque se puede llevar a cabo un ataque de *phishing*, si va dirigido a un usuario en particular, pero cuando va dirigido a empresas, especialmente de comercio electrónico, se les puede redireccionar a los clientes potenciales a una web maliciosa donde podrán obtener todos los datos usados en cualquier transacción comercial.

Este tipo de secuestro de DNS, algunas veces, es usado por Proveedores de Servicios de Internet (ISP) y algunos gobiernos, para tomar el control de las solicitudes DNS de sus usuarios. Los ISP utilizan este secuestro para recopilar información de sus propios usuarios, para cuando ellos visitan espacios de dominios desconocidos, y así poderles redirigir a éstos a su sitio web, donde tienen su propia publicidad, en vez de mostrarles una pantalla de error. En el caso de los Gobiernos, utilizan el secuestro para evitar que los ciudadanos visiten páginas que no están autorizadas por el mismo y así ejercen su censura y los redirigen a las que el Gobierno autoriza.

El secuestro de DNS, funciona de la siguiente manera:

Al escribir la dirección de un sitio web en el navegador, si la visitaste anteriormente posiblemente estará en la caché del navegador local y no será necesaria ninguna consulta al DNS, pero en caso

contrario, se ejecuta la consulta al servidor de nombres del DNS, que normalmente lo proporciona nuestro ISP. Este punto de la comunicación es el más vulnerable a los ataques, ya que no está cifrado, y cuando aprovechan los atacantes para interceptar la consulta y redirigir al usuario al sitio web malicioso. Hoy día, existen cuatro tipos de secuestro de DNS [58]:

1. **Secuestro Local:** El atacante instala un tipo de *malware*, generalmente un troyano, para atacar la configuración del DNS local. Una vez infectado el DNS, puede cambiar la configuración del mismo y así hacer que apunte a sus propios servidores DNS. De esta manera, todas las consultas que se realicen desde el navegador de la víctima, serán redirigidas hacia donde el atacante haya configurado.
2. **Secuestro del Enrutador:** Este suele ser el primer punto de ataques para los ciberdelincuentes. Debido fundamentalmente a que muchos de estos rúteres poseen contraseñas fáciles de adivinar o en otros casos, no han actualizado su *firmware* ante las vulnerabilidades que se han ido descubriendo. Al poder entrar en la configuración del rúter, pueden modificar el DNS preferido por el que ellos consideren, para tener el control de hacia dónde dirigir al usuario cuando realiza una solicitud al navegador.
3. **Secuestro Fraudulento:** Ataque muy complicado de realizar, ya que en este caso, los atacantes van a intentar secuestrar el servidor de nombres del ISP, cambian los registros DNS y así poder redirigir todas las consultas realizadas por los usuarios hacia sitios web maliciosos bajo su control. Al controlar directamente el servidor de nombres, los usuarios afectados son un gran número y es por esto que los ISP van protegiéndose de este tipo de ataques, por lo que este tipo de ataque es muy difícil de llevar a cabo.
4. **Ataques de Intermediario:** Ataques en los que el delincuente intercepta las comunicaciones entre el usuario y su DNS, aprovechando la falta de cifrado en muchas de estas solicitudes. Es cuando el atacante le devuelve al usuario una IP de destino diferente a la que le devolvería el verdadero DNS y así redirigirlo hacia el sitio web malicioso.

En la figurar 2-20 se puede ver gráficamente un ejemplo de ataque de secuestro de DNS.

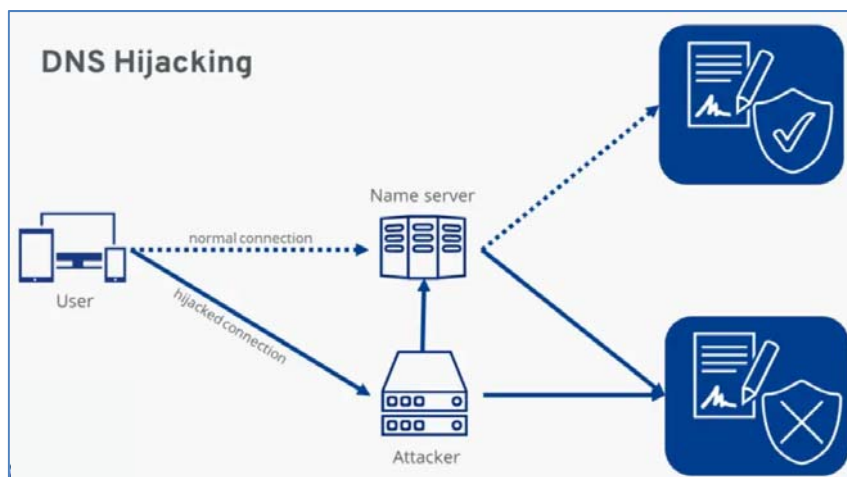


Figura 2-17. Secuestro de DNS. (Fuente: <https://www.ionos.mx>).

De manera sencilla existen diferentes formas de verificar si el DNS de un usuario ha sido pirateado.

- **Comando Ping [55]:** Se puede utilizar este comando para confirmar si una dirección IP existe. Se puede hacer la comprobación mediante una solicitud de ping a una dirección inexistente y si nuestro navegador sigue resolviendo, hay una alta posibilidad de que el DNS del usuario este comprometido.

- **Comprobar nuestro enrutador:** Se puede comprobar la configuración de nuestro enrutador desde la página de administración en línea y también existen servicios de comprobación de enrutadores que nos confirman si se está usando un servidor DNS autorizado.
- **Servicio WhoIsMyDNS.com:** [60] Servicio en línea que muestra los servidores DNS que está usando el usuario y la empresa propietaria. Como se ha comentado antes, lo normal es que el navegador del usuario use los servidores de su ISP, si al usar este servicio el usuario no reconoce los servidores DNS que está usando, es posible que su DNS haya sido secuestrado.

Independientemente del tipo de secuestro del que haya sido víctima el usuario, hay una serie de medidas que el usuario puede tener en cuenta para evitar este tipo de ataque y dar más seguridad a su DNS, como son, las siguientes:

- Evitar hacer click en enlaces que parezcan sospechosos o provengan de fuentes desconocidas. Hay que tener en cuenta que existen herramientas para acortar las URLs, con las que se puede ocultar el destino final del enlace. Una buena opción es, siempre que se ha confirmado que la dirección web es fiable, teclearla a mano, aunque sea necesario un poco más de tiempo.
- El uso de un antivirus de confianza es fundamental para conservar los dispositivos libres de infecciones y ataques. Este antivirus ayudará a localizar algún tipo de malware y a que nuestro dispositivo se mantenga actualizado.
- Cambiar los datos de acceso a nuestro enrutador también es una manera muy sencilla de evitar este tipo de ataques. Ya que la mayoría de los routers poseen los datos de acceso por defecto, es muy posible que éstos no sean todo lo seguros que se requiere, por lo que configurar una contraseña de acceso de administración robusta, es muy importante para protegerlos.
- El uso de una Red Privada Virtual (VPN) por la que va a ir todo nuestro tráfico web cifrado hacia un DNS, que emplea exclusivamente este tipo de solicitudes cifradas de extremo a extremo, protegiendo el equipo del usuario y sus servidores DNS.
- Se puede limitar el acceso a la configuración del DNS solo a los usuarios o personal que se considere y así evitar cualquier intento de acceso no autorizado.
- Habilitar el bloqueo de clientes, algunos registradores de DNS permiten el bloqueo de clientes, para evitar cualquier tipo de manipulación en los registros del DNS.
- Usar DNNSEC, para mantener la autenticidad de una búsqueda de DNS.

2.5.2 Vulnerabilidades.

Como el diseño original se enfocó fundamentalmente a la eficiencia y escalabilidad, sin tener en cuenta la parte de la seguridad, el DNS posee ciertas vulnerabilidades relacionadas con las características del protocolo y su arquitectura. Estas debilidades, sumadas con el rol crítico para el buen funcionamiento de Internet, hacen que el DNS sea un objetivo muy valioso para los atacantes. A continuación se van a detallar las áreas más significativas de vulnerabilidad [37] del DNS:

1. Falta de Autenticación y Validación.

El grupo de usuarios iniciales de Internet no requería de autenticación y validación ya que existía una confianza mutua entre los actores que intervenían, lo que provoca:

- **Respuestas DNS no verificadas:** Los clientes no validan la legitimidad de las respuestas que les llegan, lo que permite que muchas de ellas puedan ser manipuladas.

Impacto:

- **Suplantación de DNS:** Va a permitir a los atacantes redirigir a los usuarios a sitios web maliciosos donde pueden realizar ataques de *phishing* o robo de datos.
- **Envenenamiento de Caché:** Almacenamiento de respuestas falsas en la caché del *resolver*, para redirigir a los usuarios a sitios web maliciosos.

Mitigación:

Uso de DNSSEC para añadir firmas digitales a los registros DNS mediante las cuales se podrá verificar la autenticidad e integridad de las respuestas. Como cada registro DNS es firmado digitalmente con una clave privada, los *resolver* serán capaces de verificar estas firmas utilizando claves públicas que han sido distribuidas jerárquicamente desde la raíz hasta los dominios finales.

2. Dependencia de Caché.

El DNS usa la caché para mejorar su rendimiento, reduciendo las consultas redundantes y mejorando los tiempos de respuesta, pero, por otro lado, esto introduce una serie de riesgos, como pueden ser:

- **Manipulación de Caché:** Se produce cuando los atacantes son capaces de introducir datos falsos en la caché de un *resolver* y de esta manera generan respuestas erróneas a los usuarios que le realicen una consulta.
- **TTL Manipulado:** Se puede aumentar en Tiempo de Vida de los registros maliciosos, y de esta manera aumentar la duración del ataque.

Impacto:

- **Envenenamiento de Caché:** El atacante envía al usuario una respuesta falsa, anticipándose a la legítima del DNS, y el *resolver* almacena ésta en su caché, y así, todos los usuarios que realicen la misma consulta, serán redirigidos al sitio web malicioso.

Mitigación:

- **DNSSEC:** Con lo que se garantiza que los registros DNS no se alteran durante su transmisión.
- **Configuración de TTL Estricto:** Con la limitación de la duración de las entradas en la caché se minimizará el impacto de los datos que han sido manipulados.

3. Falta de Cifrado.

Como el tráfico que se genera entre el navegador web y el DNS va en texto plano, esto les da la oportunidad a las atacantes de interceptar esa comunicación, monitorearla y modificarla.

Impacto:

- **Monitoreo de Información:** Mediante el monitoreo de la información que va en texto plano los ISP o atacantes pueden recopilar toda la información y de esta manera recabar datos buscando información sensible y rastreando hábitos de navegación.
- **Ataques *Man-in-the-Middle* (MitM):** El atacante es capaz de interceptar la comunicación entre el usuario y el DNS, colocándose entre media de ambos, y de esta manera es capaz de alterar las consultas y las respuestas del DNS para poder redirigir a los usuarios a sitios web maliciosos.

Mitigación:

- **DNS sobre HTTPS (DoH):** Para dificultar la interceptación de las consultas, estas van cifradas utilizando HTTPS.

- **DNS sobre TLS (DoT):** De esta manera se asegura la privacidad y autenticidad cifrando el tráfico DNS mediante TLS.

4. Configuración Deficiente.

Si un servidor DNS no se encuentra correctamente configurado le va a dar la oportunidad a los atacantes de comprometer las redes y servicios.

Impacto:

- **Transferencias de Zonas Seguras:** Si los atacantes tienen la oportunidad de descargar bases de datos completas del DNS, van a tener acceso a información sensible, como por ejemplo, dirección IP internas.
- **Resolveres Abiertos:** Resolveres mal configurados pueden provocar ataques de amplificación.

Mitigación:

- **Restricción de Transferencia de Zona:** Se configuran los servidores de tal manera que sólo permitan transferencias a direcciones ip autorizadas.
- **Auditorías Periódicas:** Se realizan de forma regular para identificar y corregir posibles configuraciones deficientes.

2.5.3 Impacto de los Ataques DNS en Diversos Sectores.

Podemos decir que los ataques al DNS pueden tener un impacto devastador en sectores fundamentales, lo que puede afectar no sólo a la funcionalidad técnica, sino también a la seguridad nacional, estabilidad económica mundial y la confianza de los usuarios. A continuación se van enumerar una serie de sectores clave muy sensibles a los ciberataques.

Impacto de los Ataques DNS en Servicios Empresariales y Financieros.

El sector empresarial, particularmente el financiero [56], depende profundamente del DNS para garantizar la disponibilidad y seguridad de sus servicios. La banca en línea, el comercio electrónico y las plataformas empresariales son pilares fundamentales de la economía digital. El DNS actúa como el puente entre los usuarios y los sistemas de *backend* que sustentan estos servicios. Cualquier interrupción en el DNS puede tener efectos dominó que se extienden a lo largo de cadenas de suministro, transacciones financieras y mercados globales.

1. **Banca en Línea:** [57] Las plataformas bancarias mediante sus servicios *online*, necesitan al DNS para las distintas operaciones que deben realizar, como gestionar transacciones, acceder a datos de usuarios u operar sistemas de autenticación, en todos estos casos, un fallo en el DNS provocado por un ataque puede suponer la interrupción de los servicios y dejar a millones de usuarios sin poder acceder a sus cuentas.
2. **Comercio Electrónico:** En el *ecommerce* el DNS es fundamental, las tiendas *online* necesitan del DNS para que los clientes puedan visualizar su catálogo de productos, utilizar los sistemas de pago y gestionar el envío de los productos adquiridos. En determinadas fechas, ejemplo Black Friday, una interrupción en el servicio de estas tiendas puede suponer grandes pérdidas.
3. **Sistemas Empresariales:** Las empresas que utilizan plataformas de gestión empresarial, como SAP [58] o Salesforce [59], dependen del DNS para acceder a herramientas críticas. Un fallo en el DNS puede detener operaciones, desde la gestión de inventarios hasta la coordinación de proyectos globales.

Consecuencias Técnicas y Económicas.

1. Interrupciones Operativas.

Un ataque al DNS puede provocar una caída de servicios críticos durante horas o incluso días. Ataques de Denegación de Servicio Distribuido (DDoS) son muy comunes para este fin, con la intención de hacer caer el servicio.

Ejemplo Clave: Ataque DDoS a DYN (2016). [58]

En octubre de 2016, la botnet Mirai llevó a cabo uno de los ataques DDoS más grandes de la historia, dirigido al proveedor DNS DYN. Este ataque generó más de 1 Tbps de tráfico malicioso, afectando a gigantes como Twitter, Netflix, PayPal y Spotify. Durante varias horas, millones de usuarios en América del Norte y Europa no pudieron acceder a estos servicios. Este incidente subrayó cómo un ataque dirigido a un proveedor DNS puede tener un impacto global.

2. Daño Reputacional.

La confianza del cliente es el activo más valioso para las empresas, especialmente en sectores como el financiero y el comercio electrónico. Los clientes esperan acceso seguro y constante a servicios esenciales. Un ataque DNS que interrumpa operaciones o exponga datos sensibles puede erosionar esta confianza, lo que lleva a la pérdida de clientes y daños a largo plazo en la marca.

Efecto Competitivo: En este sector la seguridad es fundamental, por lo que las empresas que experimentan interrupciones frecuentes pueden perder clientes a favor de competidores percibidos como más seguros. En el sector financiero, una caída en la reputación puede afectar directamente la capacidad de una institución para atraer nuevos usuarios o mantener los actuales.

3. Pérdidas Económicas.

El coste de un ataque DNS no sólo afecta a una parte del negocio, incluyen pérdidas por interrupciones en las operaciones, gastos asociados con la mitigación del ataque y pérdidas indirectas por la disminución de la confianza del cliente.

- **Informe de IBM Security (2024) [61]:** Según este estudio, las grandes empresas pierden de media 4.88M \$ por cada ataque DNS exitoso, un 10% más que el pasado año. En el caso de empresas más pequeñas, aunque las cifras son menores, el impacto proporcional puede ser devastador.
- **Impacto a Largo Plazo:** Además de los costes inmediatos, los ataques DNS pueden generar desafíos financieros a largo plazo, como la disminución de la valoración de las acciones y mayores costes de ciberseguro.

Ejemplo Reales de ataques a DNS en sector empresarial/financiero.

Robo de Credenciales en Europa (2020). [62]

En 2020, un banco europeo fue víctima de un ataque de envenenamiento de caché, en el cual los atacantes redirigieron a los clientes a un sitio web fraudulento diseñado para imitar la plataforma oficial de banca en línea. Los clientes, confiando en la legitimidad del sitio, ingresaron sus credenciales de acceso y datos bancarios, que fueron capturados por los atacantes.

- Impactos Directos:
 - o Robo de datos personales y financieros de miles de usuarios.
 - o Transferencias fraudulentas realizadas desde cuentas comprometidas.
- Impactos Indirectos:

- o Pérdida de confianza por parte de los clientes, lo que llevó a una disminución significativa del número de clientes del banco.
- o Costes asociados con la compensación a los clientes afectados y la implementación de medidas de seguridad adicionales.

Ataque DDoS a Proveedores de Servicios Bancarios (2021). [63]

Otro caso de ataque DNS fue a una empresa de servicios financieros con sede en Asia, objetivo de un ataque DDoS dirigido a sus servidores DNS. Durante más de 12 horas, los usuarios no pudieron acceder a las plataformas de banca móvil y en línea. Este ataque ocurrió durante un fin de semana clave de compras, lo que amplificó su impacto económico.

- Pérdidas Estimadas:
 - o Más de 3M \$ en transacciones no procesadas.
 - o Costes adicionales por la implementación de medidas de mitigación y recuperación.

El impacto de los ataques DNS en los servicios empresariales y financieros es profundo, afectando tanto la operatividad como la confianza de los clientes. A medida que la economía digital continúa creciendo, proteger la infraestructura DNS debe ser una prioridad para todas las empresas. Esto requiere inversiones en tecnologías avanzadas, como DNSSEC y redes *Anycast*, así como en la capacitación continua del personal para manejar incidentes de ciberseguridad.

Impacto de los Ataques DNS en Infraestructuras Críticas.

Las infraestructuras críticas constituyen los pilares fundamentales de las sociedades modernas, englobando sectores esenciales como la energía, la salud, el transporte y la logística. La creciente digitalización de estas infraestructuras ha mejorado significativamente su eficiencia, pero también ha incrementado su dependencia de tecnologías como el Sistema de Nombres de Dominio. Esto ha introducido nuevas vulnerabilidades, ya que el DNS se ha convertido en un objetivo estratégico para actores maliciosos que buscan interrumpir operaciones críticas, causar daño económico o socavar la seguridad nacional.

Un ataque al DNS en estos sectores puede tener efectos devastadores, no solo a nivel técnico y operativo, sino también en términos de impacto social y económico. Desde apagones masivos hasta la interrupción de servicios de emergencia, las consecuencias pueden ser catastróficas.

A continuación, se analiza cómo sectores específicos dependen del DNS y cómo un ataque [65] podría afectar su funcionamiento.

1. **Energía: Redes Eléctricas Inteligentes y Plantas de Energía:** Las redes eléctricas modernas, conocidas como redes inteligentes o *smart grids*, utilizan el DNS para coordinar el suministro de energía, monitorear el estado de los sistemas y responder a emergencias en tiempo real. Estas redes integran sensores IoT (Internet de las Cosas) y sistemas SCADA (*Supervisory Control and Data Acquisition*) que dependen de una comunicación continua.

Impacto de un Ataque DNS:

- Un ataque exitoso podría interrumpir la comunicación entre los componentes de la red, afectando la capacidad de distribuir energía de manera eficiente.
- Podría causar apagones en áreas urbanas densamente pobladas, afectando hogares, hospitales, negocios y sistemas de transporte.

- Ejemplo: En 2015, un ciberataque dirigido al sector energético de Ucrania [70] interrumpió el suministro eléctrico a más de 230,000 personas. Aunque no se trató específicamente de un ataque DNS, destacó la vulnerabilidad de las infraestructuras críticas a ciberataques.

2. **Salud: Atención Médica y Emergencias:** El sector de la salud depende cada vez más de sistemas conectados para gestionar registros médicos electrónicos, coordinar servicios de emergencia y operar dispositivos médicos. El DNS facilita la comunicación entre estos sistemas, permitiendo a los médicos y personal de apoyo acceder rápidamente a la información crítica.

Impacto de un Ataque DNS:

- Interrupción del acceso a registros médicos electrónicos, lo que puede retrasar diagnósticos y tratamientos.
- Fallos en la conectividad de dispositivos médicos esenciales, como ventiladores y monitores cardíacos.
- Descoordinación en servicios de emergencia, afectando la capacidad de respuesta en situaciones críticas.
- Ejemplo: En 2023, un hospital en California sufrió un ataque de *ransomware* que bloqueó el acceso a sistemas críticos, incluidos los servidores DNS, retrasando la atención a pacientes durante horas. [66].

3. **Transporte y Logística: Movilización Global y Cadena de Suministro:** El sector del transporte, que incluye aerolíneas, redes ferroviarias y sistemas de carga, depende del DNS para gestionar reservas, rastrear envíos y coordinar operaciones logísticas. En logística global, cualquier interrupción puede generar un efecto dominó, afectando a múltiples sectores y consumidores.

Impacto de un Ataque DNS:

- Retrasos significativos en vuelos y transporte terrestre debido a la imposibilidad de acceder a sistemas de reservas y seguimiento.
- Pérdidas económicas en empresas de logística debido a la interrupción de cadenas de suministro.
- Afectación a consumidores que dependen de servicios de entrega, especialmente en períodos de alta demanda como las fiestas.
- Ejemplo: El ataque NotPetya en 2017 [64], que se analiza más adelante, paralizó operaciones logísticas a nivel global, destacando la vulnerabilidad del sector al cibercrimen.

Ejemplo Reales.

Caso NotPetya (2017) [64].

El ataque NotPetya es uno de los ejemplos más significativos de cómo un ciberataque puede afectar infraestructuras críticas a nivel global. Aunque originalmente dirigido a Ucrania, este ataque de *ransomware* se propagó rápidamente a través de sistemas DNS y otros puntos vulnerables.

- Propagación:
 - o NotPetya explotó vulnerabilidades en el software utilizado por empresas ucranianas. Al propagarse, afectó a organizaciones multinacionales que compartían sistemas o se conectaban a servidores comprometidos.
 - o La falta de segmentación en las redes y configuraciones DNS inadecuadas facilitaron su rápida expansión.
- Impacto en el Sector de Logística:

- o Empresas como Maersk, una de las mayores compañías de transporte marítimo y logística del mundo, sufrieron interrupciones masivas en sus operaciones. Durante semanas, Maersk no pudo procesar envíos ni coordinar su cadena de suministro global, lo que resultó en pérdidas estimadas de 300M \$.
- Lecciones Aprendidas:
 - o La importancia de configurar adecuadamente los servidores DNS para evitar que actúen como vectores de propagación.
 - o La necesidad de contar con planes de contingencia robustos y sistemas de respaldo para minimizar el impacto de interrupciones.

Para proteger estas infraestructuras, es crucial adoptar un enfoque integral que combine tecnologías avanzadas, como DNSSEC y redes *Anycast*, con políticas de seguridad sólidas y capacitación continua. Garantizar la resiliencia del DNS no solo es una cuestión de seguridad técnica, sino también de estabilidad económica y social.

Impacto de los Ataques DNS en Usuarios Finales.

Los usuarios finales son los beneficiarios directos de los servicios proporcionados por Internet, y dependen en gran medida del Sistema de Nombres de Dominio para acceder a una amplia variedad de servicios esenciales. Desde el correo electrónico hasta las plataformas de redes sociales, educativas y de teletrabajo, el DNS permite una conectividad fluida y transparente. Sin embargo, esta dependencia también los expone a riesgos significativos en caso de que el DNS sea manipulado por actores maliciosos.

Los ataques al DNS, como el envenenamiento de caché, la suplantación (*spoofing*) y los túneles DNS, afectan directamente a la experiencia del usuario final, causando interrupciones en los servicios, comprometiendo la privacidad y, en muchos casos, facilitando el robo de datos sensibles. Estos ataques no solo tienen un impacto técnico, sino que también erosionan la confianza en los servicios en línea, dificultando la adopción de tecnologías digitales por parte de algunos segmentos de la población.

Consecuencias Directas.

Uno de los ataques más comunes y devastadores para los usuarios finales es el envenenamiento de caché, en el cual los atacantes manipulan los registros DNS almacenados en la caché de un servidor *resolver*. Esto permite que las consultas legítimas realizadas por los usuarios sean redirigidas a sitios maliciosos que imitan plataformas legítimas.

Impacto del Envenenamiento de Caché:

1. Distribución de Malware:
 - o Los sitios maliciosos pueden forzar la descarga de software malicioso en los dispositivos de los usuarios, comprometiendo su seguridad y privacidad. Este tipo de malware incluye troyanos, ransomware y spyware.
 - o Ejemplo [68]: En 2021, un ataque DNS en Europa redirigió a los usuarios de una plataforma gubernamental hacia un sitio que distribuía ransomware, paralizando los sistemas de miles de personas.
2. Robo de Datos Personales:
 - o Los atacantes utilizan sitios fraudulentos para capturar información sensible como nombres de usuario, contraseñas y datos bancarios. Este tipo de ataque es común en campañas de phishing.

- o Ejemplo [69]: En un ataque de phishing masivo en India en 2022, los atacantes utilizaron túneles DNS para redirigir a miles de usuarios a sitios que imitaban portales de banca en línea, resultando en el robo de millones de dólares.

3. Erosión de la Confianza del Usuario:

- o Los usuarios que caen víctimas de estos ataques a menudo pierden la confianza en las plataformas en línea, lo que puede afectar negativamente la adopción de servicios digitales.

Interrupción de Servicios:

Además de los ataques que redirigen a los usuarios a sitios maliciosos, las interrupciones en los servicios DNS pueden tener un impacto directo en la productividad y la experiencia del usuario.

1. Impactos Técnicos y Sociales:

- o Afectación de Servicios Esenciales:
 - Los usuarios enfrentan problemas para acceder a correos electrónicos, plataformas educativas y aplicaciones de teletrabajo, lo que interfiere con actividades diarias críticas.
- o Frustración del Usuario:
 - La incapacidad para acceder a servicios esenciales genera frustración, especialmente cuando se perciben retrasos en la resolución de problemas técnicos.

- ### 2. Ejemplo Relevante: Ataques DDoS al DNS [70]:
- En 2021, un ataque DDoS dirigido a un proveedor de DNS en América del Norte dejó sin acceso a servicios en línea a millones de usuarios durante casi 12 horas. Esto afectó especialmente a trabajadores remotos y estudiantes, quienes dependían de plataformas digitales para sus actividades diarias.

Impacto a Largo Plazo.

El impacto de los ataques al DNS en los usuarios finales va más allá de los daños inmediatos. Estos ataques tienen implicaciones a largo plazo que afectan la percepción de la seguridad en línea y la adopción de tecnologías digitales.

1. **Desconfianza en Servicios Digitales:** Los usuarios que han sido víctimas de ataques al DNS tienden a ser más cautelosos al usar servicios en línea, lo que puede ralentizar la transición hacia una sociedad digital.
2. **Efectos en la Economía Digital:** Los ataques al DNS no solo afectan a los usuarios finales, sino que también tienen un impacto negativo en las empresas, que enfrentan una disminución en la adopción de sus servicios y un aumento en los costes de seguridad.

Los ataques al DNS tienen un impacto profundo en los usuarios finales, afectando su acceso a servicios esenciales y comprometiendo su seguridad y privacidad. Casos como el ataque a Google en China en 2010 destacan la vulnerabilidad de esta tecnología y la importancia de implementar medidas de seguridad robustas. Proteger a los usuarios finales no solo es esencial para garantizar una experiencia en línea fluida, sino también para fomentar la confianza en el ecosistema digital global.

Impacto de los Ataques DNS en Gobiernos y Seguridad Nacional.

Los ataques dirigidos al DNS pueden desencadenar graves consecuencias, como la paralización de servicios públicos esenciales, la exposición de datos altamente confidenciales o incluso la desestabilización de la economía y la gobernabilidad de un país. En un entorno cada vez más interconectado y digitalizado, estas amenazas representan un desafío creciente para la seguridad nacional.

Interrupción de Servicios Gubernamentales. [72]

Los gobiernos dependen del DNS para una amplia gama de funciones, desde la comunicación interna hasta la prestación de servicios públicos. Un ataque al DNS puede interrumpir la capacidad de los sistemas gubernamentales [73] para operar de manera eficiente, afectando tanto a los ciudadanos como a las instituciones.

1. Impactos Directos:

- o **Interrupción de Operaciones:** Los ataques de denegación de servicio distribuido (DDoS) dirigidos a servidores DNS gubernamentales pueden hacer que los sistemas sean inaccesibles. Esto incluye portales de servicios públicos, sistemas de gestión de emergencias y plataformas de registro civil.
- o **Fallo en la Comunicación:** Los correos electrónicos, sistemas de videoconferencia y otras herramientas de comunicación interna también dependen del DNS. Una interrupción en estos sistemas puede dificultar la coordinación en situaciones críticas.

2. Ejemplo Práctico:

- o El ataque NotPetya en 2017, como ya se comentó anteriormente, que inundó varios sitios web de instituciones y empresas ucranianas, incluyendo bancos, ministerios, diarios y empresas de electricidad.

Compromiso de Datos Sensibles

Los servidores DNS no solo gestionan el tráfico de red, sino que también contienen información crítica sobre la infraestructura de un país. Un ataque exitoso puede comprometer datos confidenciales, incluidos registros ciudadanos, información fiscal y datos de inteligencia.

1. Riesgos Comunes:

- o **Exposición de datos ciudadanos:** Los registros de salud, impuestos y censo, almacenados en sistemas conectados, pueden ser vulnerables si los atacantes explotan el DNS para acceder a ellos.
- o **Información estratégica:** Los sistemas militares y de inteligencia, que dependen de redes conectadas, también están en riesgo de ser comprometidos a través de ataques al DNS.

2. **Impacto económico [74]:** Los gobiernos enfrentan costes significativos para mitigar estos ataques, además de posibles demandas por incumplimiento de las normativas de protección de datos.

Riesgo de Ciberespionaje.

El DNS es una herramienta clave para los actores maliciosos que buscan realizar actividades de espionaje. Los túneles DNS, en particular, son un método comúnmente utilizado para exfiltrar datos sensibles sin ser detectados.

Ejemplos Reales de ataques dirigidos al sector gubernamental.

Ataque a Estonia (2007). [75]

El ciberataque a Estonia en 2007 es uno de los ejemplos más significativos de cómo un ataque al DNS puede paralizar un país entero. Este ataque masivo, atribuido a actores rusos, fue dirigido a la infraestructura digital de Estonia tras una controversia política sobre la reubicación de un monumento.

1. **Detalles del ataque:**

- o Los atacantes llevaron a cabo múltiples ataques DDoS dirigidos a servidores DNS gubernamentales, bancos y medios de comunicación.
- o El tráfico malicioso sobrecargó los sistemas, dejando a los ciudadanos y al gobierno sin acceso a servicios en línea durante varios días.

2. **Impactos:**

- o **Interrupción de Servicios Públicos:** Los portales gubernamentales estuvieron inaccesibles, afectando la prestación de servicios básicos.
- o **Daño Reputacional:** Estonia, reconocida por su infraestructura digital avanzada, sufrió una pérdida de confianza en su resiliencia tecnológica.

3. **Lecciones Aprendidas:** Este ataque llevó a Estonia a desarrollar su estrategia de defensa cibernética, convirtiéndose en un líder mundial en ciberseguridad.

Ataques a Infraestructura en Medio Oriente (2019). [76]

En 2019, varias agencias gubernamentales en el Medio Oriente fueron blanco de ataques de suplantación DNS. Estos ataques redirigieron consultas legítimas hacia servidores maliciosos, utilizados para realizar actividades de espionaje.

1. **Detalles del ataque:**

- o Los atacantes modificaron los registros DNS para redirigir el tráfico de los sistemas gubernamentales hacia servidores controlados por ellos.
- o Esto permitió la interceptación de comunicaciones y la recopilación de datos confidenciales.

2. **Impactos:**

- o **Robo de Información Sensible:** Los atacantes accedieron a correos electrónicos, datos de ciudadanos y documentos internos.
- o **Compromiso Estratégico:** La información exfiltrada podría ser utilizada para influir en políticas regionales y operaciones militares.

3. **Respuesta Internacional:** Este incidente subrayó la necesidad de una cooperación internacional más fuerte para enfrentar las amenazas al DNS y proteger la seguridad nacional.

El impacto de los ataques al DNS en gobiernos y seguridad nacional es profundo y multifacético. Desde la interrupción de servicios esenciales hasta el robo de datos sensibles y el espionaje, estas amenazas representan un desafío significativo en el contexto de la ciberseguridad moderna. Los casos de Estonia y Medio Oriente destacan la gravedad de estas amenazas y la necesidad de implementar medidas preventivas robustas. A medida que los gobiernos dependen cada vez más del DNS, garantizar su resiliencia será esencial para proteger la estabilidad política, económica y social.

3 SEGURIDAD DEL DNS

3.1 Soluciones de Seguridad en DNS. [77]

El DNS está considerado un elemento fundamental para el buen funcionamiento de Internet, lo que le convierte en un objetivo principal de ciberataques. Desde sus inicios en 1983 y debido a su arquitectura abierta y jerárquica, la falta de mecanismos de seguridad en la concepción original, han hecho que este Sistema sea vulnerable a múltiples amenazas y ciberataques.

La criticidad de este sistema para el buen funcionamiento de Internet hace que cualquier interrupción o manipulación indebida pueda tener un impacto muy significativo en la prestación de cualquier servicio, aplicaciones empresariales, correos electrónicos, plataformas de comercio electrónico, etc.

En el contexto actual de ciberseguridad, donde los atacantes buscan constantemente nuevas formas de explotar las vulnerabilidades del sistema, la implementación de medidas de seguridad DNS efectivas no es solo una necesidad técnica, sino también una prioridad estratégica para las organizaciones de todos los tamaños. Estas medidas no solo buscan mitigar los riesgos existentes, sino también prevenir futuras amenazas, fortaleciendo así la confianza en la infraestructura de Internet.

Existen varias soluciones de seguridad para el Sistema de Nombres de Dominio diseñadas para proteger contra amenazas como envenenamiento de caché, ataques DDoS, secuestro de DNS, túneles de datos y más. Aquí te presento un desglose de las principales soluciones de seguridad DNS.

3.1.1 DNNSEC (*Domain Name System Security Extensions*).

DNNSEC [78] se trata de un conjunto de protocolos que añade una capa adicional de seguridad al Sistema de Nombres de Dominio. Su objetivo principal es proteger la información de los registros DNS que se transmiten a través de Internet. Asegura que los datos recibidos de un servidor DNS no han sido manipulados durante su transmisión, usando para ello firmas digitales y un sistema de clave pública. Lo que ayuda a prevenir ataques como el envenenamiento de caché y otros tipos de falsificación, garantizando que los usuarios lleguen al sitio web correcto y no a una réplica controlada por atacantes.

Para el buen funcionamiento de DNS, es necesario el uso de varios tipos de registros DNS específicos que van a permitir la validación de firmas, son los siguientes:

RRSIG (Firma del Registro de Recursos).

Pieza fundamental en el mecanismo de seguridad que proporciona DNSSEC. Su función principal es autenticar un conjunto de registros de recursos (RRset) mediante una firma digital generada por la clave privada del servidor autorizado de la zona.

Detalles Técnicos:

- Cada conjunto de registros en una zona DNS (RRset) tiene su correspondiente registro RRSIG.
- La firma RRSIG se genera utilizando un algoritmo criptográfico (por ejemplo, RSA/SHA-256 o ECDSA) y la clave privada asociada al servidor autorizado.
- Este registro contiene información adicional como:
 - o **Tipo cubierto:** Indica qué tipo de registro (A, MX, NS, etc.) está siendo autenticado.
 - o **Fecha de expiración y de inicio:** Especifica el período de validez de la firma, lo que ayuda a evitar el uso de firmas comprometidas o antiguas.
 - o **Identificador de clave:** Identifica la clave pública utilizada para verificar la firma.

Proceso de Verificación:

1. Cuando un cliente (resolver) realiza una consulta DNS, recibe tanto los registros solicitados como los correspondientes RRSIG.
2. El *resolver* utiliza la clave pública almacenada en el registro DNSKEY para validar la firma digital.
3. Si la validación es exitosa, el cliente puede confiar en que los datos no han sido alterados desde su origen.

Importancia: El registro RRSIG asegura la integridad y autenticidad de los datos DNS, protegiendo contra ataques como la suplantación de identidad y el envenenamiento de caché.

DNSKEY (Clave del Sistema de Nombres de Dominio).

El registro **DNSKEY** almacena la clave pública necesaria para verificar las firmas digitales generadas por los registros RRSIG.

Tipos de Claves:

1. Clave de Firma de Zona (ZSK):
 - o Utilizada para firmar los RRsets dentro de una zona.
 - o Su rotación es frecuente para minimizar el riesgo de compromiso.
2. Clave de Firma de Clave (KSK):
 - o Utilizada exclusivamente para firmar el registro DNSKEY que contiene la ZSK.
 - o Está vinculada a la zona superior a través de un registro DS, asegurando la cadena de confianza.

Campos Clave en DNSKEY:

- **Algoritmo criptográfico:** Define el método utilizado para firmar y verificar los datos (por ejemplo, RSA, ECDSA).
- **Flags:** Indican si la clave es una KSK o una ZSK.
- **Datos de clave pública:** Proporcionan los elementos necesarios para la verificación de las firmas RRSIG.

Importancia: El registro DNSKEY es esencial para el funcionamiento de DNSSEC, ya que proporciona el mecanismo para autenticar los registros en una zona y mantener la integridad de la información.

DS (Delegation Signer).

El registro **DS** actúa como el vínculo de confianza entre una zona padre y una zona hija en la jerarquía DNSSEC. Este registro contiene un *hash* de la clave pública KSK de la zona hija, almacenado en la zona padre.

Funcionamiento:

1. Cuando una zona hija se firma con DNSSEC, su KSK se representa mediante un *hash* en la zona padre como un registro DS.
2. Cuando un *resolver* verifica una firma DNSSEC, utiliza el registro DS en la zona padre para confirmar que la KSK en la zona hija es auténtica.

Campos en el Registro DS.

- **Clave de referencia:** Indica la clave específica en la zona hija.
- **Algoritmo:** Especifica el algoritmo utilizado para la generación del *hash*.
- **Digest type y Digest:** Determinan el método de *hash* (SHA-1, SHA-256) y el valor resultante del *hash*.

Importancia: El DS asegura la continuidad de la cadena de confianza desde la raíz hasta los dominios individuales, garantizando la autenticidad de cada zona.

NSEC y NSEC3.

Los registros **NSEC** y **NSEC3** están diseñados para manejar consultas sobre nombres de dominio inexistentes y evitar ciertos tipos de ataques.

NSEC: Enumeración Directa:

- Proporciona el siguiente nombre de dominio válido en orden alfabético dentro de la zona.
- Lista todos los tipos de registros disponibles para un nombre de dominio.
- **Limitación:** Permite a los atacantes enumerar todos los nombres de dominio en una zona, lo que puede ser una preocupación de privacidad.

NSEC3: Enumeración con Hash:

- Utiliza hashes criptográficos de los nombres de dominio para ocultar los nombres reales.
- Mejora la privacidad al prevenir la enumeración de zonas por parte de atacantes.
- Permite manejar de manera segura consultas negativas, como cuando un nombre de dominio no existe.

Ejemplos de Uso: Si un atacante intenta realizar una consulta para un nombre de dominio inexistente, NSEC o NSEC3 proporcionan una prueba criptográfica de la no existencia, evitando respuestas falsas.

CDNSKEY y CDS.

Los registros **CDNSKEY** y **CDS** simplifican la gestión de claves en entornos DNS dinámicos.

CDNSKEY:

- Similar a DNSKEY, pero se utiliza específicamente para informar a la zona padre sobre cambios en las claves públicas.

- Permite la actualización automática de las claves en configuraciones donde las zonas hijas experimentan cambios frecuentes.

CDS:

- Contiene un *hash* del CDNSKEY y solicita a la zona padre actualizar el registro DS correspondiente.
- Garantiza que la cadena de confianza permanezca intacta después de cambios en las claves.

Importancia: Estos registros son cruciales para mantener la integridad y la actualidad de las claves en configuraciones dinámicas, evitando interrupciones en la cadena de confianza.

Funcionamiento de DNNSEC.

1. Agrupación de Registro DNS en RRSets.

Con este primer paso se van organizar los registros DNS en los RRSets, que son un conjunto de registros de recursos. Este grupo de registros, comparten el mismo nombre y tipo, pero pueden contener diferentes datos. Agrupamiento crucial porque DNNSEC firma todo el conjunto como una sola unidad, no firma individualmente cada registro.

Con esta metodología se asegura que todos los registros que están relacionados se autenticuen juntos, con lo que se mantiene su integridad y autenticidad mientras transitan por Internet.

2. Firma de registros de recursos.

Ya agrupados los registros en RRSets, el siguiente paso es firmarlos digitalmente, a través de un registro especial RRSIG, que contiene la firma digital para el RRSets, y se genera utilizando una clave privada específica del servidor DNS. Componentes de un RRSIG:

- **Tipo cubierto:** Especifica el tipo de registros DNS que la firma cubre (por ejemplo, A, AAAA, TXT).
- **Algoritmo:** Denota el algoritmo criptográfico utilizado para generar la firma.
- **Periodo de validez:** Define cuánto tiempo es válida la firma.
- **Etiqueta de clave:** Identifica la clave que se utilizó para generar la firma.
- **Firma:** La propia firma criptográfica.

Con esta firma, cualquier alteración en el RRSets va a ser detectada, puesto que cualquier cambio haría que la firma no coincidiera al realizar la verificación con la clave pública correspondiente.

3. Claves de Firma de Zona (ZSK).

Utilizadas para firmar los RRSets. La ZSK es parte de un par de claves, que incluye la clave privada que se mantiene segura y una clave pública que es la que va a distribuirse a través de un registro DNSKEY. Con esta clave pública, cada vez que cualquiera reciba un RRSets firmado, puede verificar la firma y de esta manera se asegura que los datos no han sido alterados.

Sistema fundamental, porque con él se verifican la autenticidad de los datos sin necesidad de tener que acceder directamente a la clave privada.

4. Claves de Firma de Clave (KSK).

Un nivel más alto, la KSK se va a utilizar para la firma del registro DNSKEY, que contiene la clave pública de la KSK. Con esto se añade una capa adicional de seguridad, y se asegura también la autenticidad de la clave pública de la ZSK.

Igualmente que la ZSK, la KSK posee una clave privada, utilizada para la firma, y una pública que es la que se distribuye para la verificación.

5. Registros de Firmante de Delegación (DS).

Elemento fundamental, ya que contiene un *hash* criptográfico de la clave pública de la KSK y se almacena en la zona DNS padre. De esta forma, se proporciona un método para que la zona padre, sea capaz de autenticar la clave utilizada por la zona hija, de esta manera se mantiene la Cadena de Confianza desde la raíz del DNS hasta el dominio final.

6. NSEC y NSEC3.

Registros encargados de abordar el problema de la **denegación explícita de existencia**. Cuando se realiza una consulta por un nombre de dominio que no existe, DNSSEC debe responder de manera que se pueda verificar que la respuesta es legítima.

Estos dos registros listan el siguiente nombre de dominio válido en la zona, permitiendo a los clientes DNS verificar que ese nombre no existe, sin que se revelen todos los nombres de la zona.

7. Cadena de Confianza.

Con la Cadena de Confianza se asegura que todos los registros DNSKEY y DS se validan en un proceso continuo, desde el dominio del nivel superior hasta el último dominio.

Modos de Funcionamiento de DNNSEC.

El funcionamiento de DNNSEC es diferente, en función de la forma en que haya sido implementado:

- **Firma sin Conexión de Zonas Estáticas.**

Modo muy útil para zonas DNS que raramente se actualizan o cambian, ya que las claves privadas necesarias para firmar los registros DNS se encuentran aisladas en un sistema que no tienen conexión a Internet. De esta manera el riesgo de que sean robadas o comprometidas por ataques cibernéticos es mínimo. La firma de la zona se hace en un entorno seguro, y posteriormente los datos firmados se transfieren a los Servidores DNS autorizados que tienen conexión a Internet.

Este modo es ideal para organizaciones que realizan las actualizaciones de una forma planificada y no tienen que realizar cambios con mucha frecuencia.

- **Firma Online Centralizada.**

La firma de los datos se hace en un entorno controlado y seguro. Suele hacerse en servidores dedicados que aunque poseen conexión a Internet, se encuentran fuertemente protegidos y su acceso es restringido. Estos servidores son los encargados de realizar la firma de todos los datos de la zona, y una vez firmados se distribuyen a los Servidores DNS autorizados encargados de responder a las consultas de los usuarios.

Con este modo la actualización de los datos DNS se efectúa de una forma más rápida y flexible comparada con el modo anterior y es más adecuado para entornos en los que las actualizaciones de los registros se deben hacer de una manera más dinámica y frecuente.

- **Firma Sobre la Marcha.**

Este modo se diferencia de los dos anteriores en que la firma de los registros DNS se hace en tiempo real por los Servidores DNS autorizados en el momento en el que se hacen las consultas. De esta manera se ofrece la máxima flexibilidad y se minimizan los tiempos de espera para la actualización de los datos de la zona DNS.

Por contra, presenta una serie de riesgos de seguridad, ya que las claves privadas deben almacenarse en servidores que están directamente conectados a Internet, lo que provoca que éstas estén expuestas a un mayor riesgo de ataque cibernético. Y además, la carga computacional de los servidores puede aumentar, ya que con cada consulta se podría tener que realizar una operación de firma.

3.1.1.1 Ventajas y desventajas del uso de DNNSEC. [83]

Ventajas del Uso de DNSSEC:

1. **Garantía de Autenticidad.**

Uno de los beneficios clave de DNSSEC es su capacidad para autenticar las respuestas DNS, asegurando que provengan de fuentes legítimas. Este nivel de autenticidad se logra mediante la firma digital de registros DNS, que los *resolver* pueden verificar utilizando claves públicas.

Importancia de la autenticidad:

- Protege a los usuarios finales contra redirecciones maliciosas a sitios web fraudulentos.
- Incrementa la confianza en servicios críticos como la banca en línea, las plataformas de comercio electrónico y las redes gubernamentales.

2. **Protección de la Integridad de los Datos.**

DNSSEC asegura que los datos DNS no hayan sido modificados o manipulados durante su transmisión. Este beneficio es fundamental en un entorno donde los ataques a la integridad de los datos son cada vez más comunes.

Se logra mediante firmas digitales asociadas a los registros DNS, cualquier alteración en los datos invalida la firma, alertando a los *resolveres* de la manipulación.

3. **Prevención de Ataques:** DNSSEC aborda específicamente algunas de las amenazas más peligrosas que afectan al DNS:

- **Envenenamiento de caché:** Este ataque manipula las respuestas DNS almacenadas en caché, redirigiendo a los usuarios a destinos maliciosos. Con DNSSEC, las respuestas en caché deben ser validadas, eliminando esta vulnerabilidad.
- **Ataques de suplantación de identidad:** Los atacantes que intenten falsificar respuestas DNS se enfrentarán a la barrera de las firmas digitales, que no pueden ser reproducidas sin la clave privada correspondiente.
- **Amenazas avanzadas:** Aunque DNSSEC no cifra las consultas DNS, complementa tecnologías como DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT), que protegen la privacidad de las consultas.

4. **Fomento de la Confianza en Internet:** La implementación de DNSSEC fortalece la infraestructura global de Internet al introducir una cadena de confianza:

- **Cadena jerárquica:** Desde la raíz del DNS hasta los dominios individuales, cada zona valida la autenticidad de la zona siguiente mediante registros DNSKEY y DS.
- **Repercusión global:** A medida que más dominios adoptan DNSSEC, se construye un ecosistema más seguro y confiable, beneficiando tanto a las empresas como a los usuarios finales.

5. **Cumplimiento Normativo:** En algunos sectores, la implementación de DNSSEC es más que una recomendación; es un requisito legal o normativo:

- **Regulaciones en la Unión Europea y los Estados Unidos:** Actores como la banca, la salud y las infraestructuras críticas están obligados a implementar medidas de ciberseguridad robustas, donde DNSSEC desempeña un papel esencial.
- **Mejora en auditorías:** DNSSEC proporciona un marco para demostrar la autenticidad e integridad de los datos, simplificando el cumplimiento de estándares como el RGPD o las normativas del NIST.

Desventajas del Uso de DNSSEC:

1. Complejidad Técnica.

La implementación y gestión de DNSSEC no es trivial y requiere conocimientos avanzados:

- **Gestión de claves criptográficas:**
 - Las claves privadas deben ser generadas y almacenadas de manera segura, lo que a menudo requiere el uso de hardware especializado como módulos de seguridad de hardware (HSM).
 - La rotación de claves (ZSK y KSK) introduce complejidades adicionales, ya que debe realizarse de manera sincronizada para evitar interrupciones.
- Errores en la configuración:
 - Una configuración incorrecta puede invalidar toda la zona DNS, causando fallos en la resolución de nombres.

2. Impacto en el Rendimiento.

La inclusión de firmas digitales y registros adicionales aumenta el tamaño de las respuestas DNS:

- **Problemas asociados:**
 - Respuestas más grandes pueden causar fragmentación de paquetes, especialmente en redes que no soportan bien el protocolo EDNS (*Extension Mechanisms for DNS*) [84].
 - La fragmentación aumenta la latencia y puede ser explotada por atacantes mediante ataques de fragmentación DNS.
- **Soluciones parciales:**
 - El uso de DNS sobre TCP mitiga estos problemas, aunque introduce una sobrecarga adicional en el tráfico.

3. Costes de Implementación: DNSSEC implica una inversión significativa en términos de infraestructura y capacitación:

- **Infraestructura:**
 - Actualización de servidores DNS para soportar DNSSEC.
 - Implementación de sistemas de monitoreo y auditoría para garantizar el correcto funcionamiento.
- **Formación:**
 - Los administradores de sistemas necesitan capacitación específica para gestionar DNSSEC y mitigar sus desafíos.

4. Adopción Limitada: A pesar de los esfuerzos por promover DNSSEC, su adopción sigue siendo desigual:

- **Dominios sin soporte:** Muchas organizaciones, especialmente las pequeñas y medianas empresas, no han adoptado DNSSEC debido a su complejidad o costes.
- **Compatibilidad:** Algunos *resolver* y sistemas antiguos no manejan adecuadamente DNSSEC, lo que puede causar fallos en la resolución o ineficiencias.

DNSSEC representa un paso crucial hacia una Internet más segura, ofreciendo autenticidad, integridad y resistencia contra amenazas específicas del DNS. Sin embargo, su adopción no está exenta de desafíos. La complejidad técnica, el coste inicial y los problemas de compatibilidad son obstáculos que requieren una planificación cuidadosa y un compromiso a largo plazo.

A pesar de estas limitaciones, los beneficios de DNSSEC, como la autenticidad de los datos y la protección contra ataques, son invaluable en un mundo cada vez más digitalizado. La combinación de DNSSEC con tecnologías complementarias, como DoH y DoT, puede crear un ecosistema más robusto

y confiable. A medida que Internet sigue evolucionando, DNSSEC desempeñará un papel clave en garantizar la seguridad y la confianza en la infraestructura digital global.

3.1.2 DNS sobre TLS (DoT).

DNS sobre TLS (DoT) [79] es un protocolo avanzado diseñado para asegurar las consultas del Sistema de Nombres de Dominio mediante el cifrado del tráfico utilizando Transport Layer Security (TLS). Este protocolo fue estandarizado por la Internet Engineering Task Force (IETF) en el RFC 7858 [80], publicado en 2016. La implementación de DoT responde a la necesidad de proteger la privacidad y seguridad de los usuarios, especialmente en un ecosistema digital donde las amenazas cibernéticas están en constante evolución.

En el modelo DNS tradicional, las consultas se transmiten en texto plano, lo que las hace vulnerables a ataques como la interceptación, manipulación y espionaje. Esto expone información sensible sobre los hábitos de navegación de los usuarios y los hace susceptibles a ataques como el “DNS spoofing” o “DNS hijacking”. DoT surge como una solución eficaz para mitigar estas vulnerabilidades al cifrar las consultas DNS desde el origen hasta el destino, asegurando que estas no sean visibles ni manipulables por terceros.

Además, DoT complementa otros protocolos de seguridad, como DNSSEC, que valida la autenticidad de las respuestas DNS. La combinación de DoT y DNSSEC crea un ecosistema robusto que garantiza tanto la privacidad como la integridad de las consultas DNS. Este enfoque es especialmente crítico en redes públicas, donde los usuarios enfrentan un mayor riesgo de ataques de intermediarios.

Con el aumento de la adopción de dispositivos IoT, la protección del tráfico DNS se vuelve aún más esencial. Muchos dispositivos IoT no cuentan con configuraciones de seguridad avanzadas, lo que los hace vulnerables a ataques. Al implementar DoT, las organizaciones y los usuarios finales pueden asegurar que las consultas DNS realizadas por estos dispositivos sean protegidas contra posibles amenazas.

En resumen, DNS sobre TLS no solo mejora la privacidad y seguridad del tráfico DNS, sino que también establece un estándar para futuras implementaciones de seguridad en Internet. Su capacidad para integrar autenticidad, confidencialidad y resistencia a ataques lo convierte en una herramienta clave para construir un ecosistema digital más seguro.

Adopción y Expansión.

Desde su estandarización, DoT ha sido adoptado por grandes proveedores de DNS como Google, Cloudflare [83] y Quad9 [84], y se ha integrado en sistemas operativos modernos como Android y herramientas avanzadas como Unbound [114] y Knot Resolver [87]. A medida que crece la conciencia sobre la privacidad en línea, DoT se posiciona como un estándar fundamental para proteger las consultas DNS en un ecosistema digital en constante evolución.

Funcionamiento DNS sobre TLS. [81]

DoT establece un canal cifrado entre el cliente y el servidor DNS a través del puerto 853, dedicado exclusivamente para este protocolo. Esto garantiza que el tráfico DNS esté separado del tráfico web regular y que las consultas y respuestas permanezcan inaccesibles para posibles interceptores. A continuación, se detalla su funcionamiento en profundidad.

Componentes Principales:

1. Cliente DNS:

- o El cliente DNS puede ser un navegador, una aplicación móvil, un sistema operativo o cualquier dispositivo que necesite resolver nombres de dominio.

- o Antes de enviar consultas DNS, el cliente encapsula las consultas estándar en un formato compatible con TLS.
- o El cliente establece una conexión con un servidor DNS configurado para admitir TLS en el puerto 853, asegurando que el tráfico sea cifrado.
- o Los clientes avanzados pueden mantener conexiones persistentes para reducir la latencia en consultas múltiples.

2. Servidor DNS:

- o Responde a las consultas DNS después de descifrarlas y procesarlas.
- o Está configurado para operar en el puerto 853, con soporte para conexiones TLS.
- o Verifica la integridad de las consultas y responde con datos precisos, protegidos contra manipulaciones.
- o Utiliza certificados TLS válidos para autenticar la conexión con el cliente.

Flujo de Trabajo.

1. Inicio de la Conexión.

- El cliente inicia una conexión TCP al puerto 853 del servidor DNS.
- A continuación, se realiza la negociación del protocolo TLS (*Handshake TLS*). Durante esta fase, se autentican las identidades tanto del cliente como del servidor mediante certificados digitales.
 - o **Autenticación del Servidor:** El servidor presenta su certificado TLS al cliente para demostrar su identidad y garantizar que las consultas se dirigen a un servidor legítimo.
 - o **Establecimiento de una Clave de Sesión:** Se genera una clave de sesión única para cifrar todas las comunicaciones posteriores entre el cliente y el servidor.
- Una vez completada la negociación TLS, se establece un canal seguro de extremo a extremo.

2. Envío de Consultas.

- Las consultas DNS estándar, codificadas en formato *wireformat* (formato binario nativo de las consultas DNS), se encapsulan dentro de la conexión TLS.
- El cliente utiliza la conexión segura para enviar múltiples consultas DNS reutilizando el mismo canal TLS. Esto reduce la latencia y mejora la eficiencia del canal.

3. Procesamiento y Respuesta.

- El servidor descifra las consultas recibidas a través del canal seguro y las procesa en su *resolver* DNS.
- Una vez que el servidor obtiene la respuesta de la consulta (por ejemplo, la dirección IP asociada a “google.es”), ésta se cifra nuevamente utilizando la clave de sesión y se envía de regreso al cliente.
- El cliente descifra la respuesta y la utiliza para completar la solicitud original

Beneficios Técnicos.

1. Privacidad Garantizada:

- o Al operar en un puerto dedicado (853), el tráfico DNS cifrado es más fácil de identificar y aislar, permitiendo a las redes corporativas administrar mejor las políticas de seguridad.
- o Reduce el riesgo de monitoreo o manipulación por parte de intermediarios maliciosos o curiosos.

2. Eficiencia en Redes Complejas:

- o Soporta multiplexación, lo que permite enviar múltiples consultas y recibir respuestas dentro de una misma conexión TLS. Esto optimiza el uso del canal, reduciendo la latencia y minimizando el consumo de recursos.
 - o El canal persistente elimina la necesidad de renegociar TLS para cada consulta, acelerando significativamente el tiempo de resolución.
3. Autenticación Mejorada:
- o Los certificados TLS verifican que las comunicaciones se realicen con servidores confiables, eliminando la posibilidad de ataques de intermediarios (MITM).
 - o El uso de claves únicas para cada sesión mejora la seguridad, garantizando que las comunicaciones sean privadas incluso si otras conexiones están comprometidas.

Ventajas de DNS sobre TLS.

1. **Mejora de la privacidad en línea:** Al cifrar las consultas DNS, DoT impide que terceros no autorizados, como proveedores de servicios de Internet (ISP) o atacantes, intercepten y analicen las solicitudes de navegación, protegiendo así la información sobre los sitios web que los usuarios visitan.
2. **Protección contra ataques de intermediarios (*Man-in-the-Middle*):** El cifrado TLS asegura que las comunicaciones entre el cliente y el servidor DNS no puedan ser manipuladas o falsificadas, previniendo ataques como el envenenamiento de caché DNS o la suplantación de identidad.
3. **Integridad de los datos:** DoT garantiza que las respuestas DNS no sean alteradas durante la transmisión, asegurando que los usuarios reciban información auténtica y precisa sobre las direcciones IP asociadas a los dominios que consultan.
4. **Resiliencia contra la censura y el bloqueo:** Al utilizar un puerto específico (TCP/853), DoT facilita la identificación y gestión del tráfico DNS cifrado, pudiendo bloquear puertos para evitar que sea usado.
5. **Compatibilidad con infraestructuras existentes:** La implementación de DoT es relativamente sencilla y puede integrarse en sistemas y redes actuales sin requerir cambios significativos, lo que facilita su adopción para mejorar la seguridad de las comunicaciones DNS.

Consideraciones adicionales:

- **Latencia:** Aunque DoT introduce una ligera sobrecarga debido al establecimiento de conexiones TLS, en la mayoría de los casos, esta latencia adicional es imperceptible para el usuario final.
- **Soporte y adopción:** No todos los servidores DNS públicos soportan DoT. Sin embargo, proveedores como Cloudflare, Google y Quad9 ya ofrecen este servicio, y su adopción está en crecimiento.

Desafíos y Limitaciones de DNS sobre TLS.

1. Sobrecarga Computacional.

- **Impacto en dispositivos con recursos limitados:** El proceso de cifrado TLS requiere mayor capacidad de procesamiento y memoria comparado con las consultas DNS estándar no cifradas. Esto puede afectar especialmente a dispositivos de bajo consumo como enrutadores domésticos, dispositivos IoT (Internet de las Cosas), y equipos antiguos. En un entorno con múltiples dispositivos solicitando datos al servidor DNS, el tiempo de establecimiento de la conexión TLS puede aumentar ligeramente la latencia y consumir más energía, lo que es crítico en redes con gran cantidad de dispositivos IoT.
- **Mitigación:** Se recomienda implementar hardware más eficiente o usar técnicas de optimización, como el reuso de conexiones TLS persistentes, que minimizan los costes asociados con el establecimiento de múltiples sesiones cifradas.

2. Requiere Configuración Manual.

- **Compatibilidad limitada en aplicaciones y navegadores:** Aunque DoT es ampliamente soportado en servidores DNS y sistemas operativos como Android (a partir de la versión 9), no tiene una integración nativa en la mayoría de los navegadores web. Esto significa que las aplicaciones y navegadores no usan DoT automáticamente, lo que obliga a configuraciones adicionales.
- **Implicación para los usuarios:** Los usuarios finales deben tener conocimientos técnicos para configurar clientes DoT en sus dispositivos o confiar en herramientas específicas como aplicaciones de terceros. Esto limita la adopción en audiencias menos técnicas. A diferencia con DoH que está integrado en navegadores modernos como Google Chrome, Firefox y Microsoft Edge, haciéndolo más accesible.
- **Mitigación:** La industria está avanzando hacia sistemas operativos y aplicaciones con soporte automático para DoT, lo que facilitará la configuración y el uso sin intervención del usuario.

3. Interferencia en Redes Restringidas.

- **Restricción del tráfico en el puerto 853:** DoT utiliza un puerto TCP/853 dedicado, que es fácilmente identificable. En redes empresariales o públicas con políticas de tráfico estrictas, este puerto puede ser bloqueado, limitando la funcionalidad de DoT. Por ejemplo en países con censura en línea, las autoridades pueden monitorear y bloquear el tráfico en el puerto 853, dificultando el uso de DoT para garantizar privacidad en estas redes. DoH tiene una ventaja en este aspecto, ya que utiliza el puerto HTTPS (443), comúnmente permitido en redes restringidas.
- **Mitigación:** En algunos casos, se pueden usar técnicas como el encapsulamiento de DoT dentro de VPNs o el reconfiguramiento para operar en puertos no estándar, aunque esto puede introducir desafíos adicionales.

4. Confianza en los Servidores DNS.

- **Dependencia de proveedores de DNS confiables:** Aunque DoT cifra las consultas DNS, no protege contra la recopilación de datos por parte del servidor DNS mismo. Los proveedores de DNS que ofrecen DoT aún pueden registrar, analizar y almacenar consultas DNS, lo que representa un riesgo para la privacidad si no son confiables. Así por ejemplo si un servidor DoT pertenece a un proveedor que comparte datos con terceros o carece de políticas claras de privacidad, los usuarios no están completamente protegidos.
- **Necesidad de transparencia:** Los usuarios deben evaluar las políticas de privacidad de los proveedores de DNS antes de confiar en ellos. Algunos proveedores como Cloudflare y Quad9 tienen políticas públicas de no registro (*no-logging*), lo que los hace opciones más seguras.
- **Mitigación:** Implementar soluciones como el cifrado extremo a extremo o el uso de sistemas descentralizados de resolución DNS (por ejemplo, DNSCrypt o servicios basados en *blockchain*) puede reducir el riesgo de recopilación de datos.

Implementaciones Destacadas.

Proovedores Compatibles: Los principales proveedores de DNS han implementado soporte para DoT con características únicas, lo que los hace atractivos para diferentes casos de uso:

- **Google Public DNS** [82]: Google Public DNS es uno de los *resolver* más utilizados a nivel mundial, ofreciendo soporte para DoT con una infraestructura altamente optimizada para garantizar alta disponibilidad, baja latencia y tolerancia a fallos.
- **Cloudflare (1.1.1.1)** [83]: Cloudflare ofrece un servicio DNS orientado a la privacidad, con políticas estrictas de no registro (no-logging) y un fuerte enfoque en la velocidad.
- **Quad9** [84]: Este proveedor combina la privacidad de DoT con una capa adicional de seguridad al bloquear automáticamente dominios maliciosos y sospechosos en tiempo real.

Soporte en Sistemas Operativos y Aplicaciones:

- **Android 9+**: Desde Android 9, Google introdujo soporte nativo para DoT en las configuraciones de DNS privadas. Los usuarios pueden habilitar DoT a nivel del sistema, asegurando que todas las consultas DNS sean cifradas.
- **Unbound (Código Abierto)**: Unbound es un resolver DNS de código abierto desarrollado por NLnet Labs. Es ampliamente utilizado para configurar DoT en servidores y es conocido por su flexibilidad y alto desempeño.
- **Knot Resolver (Código Abierto)**: Knot Resolver, desarrollado por CZ.NIC, es otro resolver DNS de código abierto que incluye soporte nativo para DoT y está diseñado para configuraciones personalizadas avanzadas.

3.1.3 DNS sobre HTTPS (DoH). [85]

DNS sobre HTTPS (DoH) es un protocolo que encapsula las consultas del Sistema de Nombres de Dominio en solicitudes HTTPS, utilizando el puerto 443. Este enfoque introduce cifrado en el nivel de transporte, protegiendo las consultas DNS contra interceptaciones y manipulaciones. DoH está diseñado para mejorar la privacidad y la seguridad de los usuarios, especialmente en un entorno donde las amenazas a la privacidad en línea están en constante evolución. Su adopción masiva ha sido impulsada por la necesidad de garantizar comunicaciones seguras y confiables en un ecosistema digital cada vez más complejo.

Origen del Protocolo DoH.

El desarrollo de DoH tiene sus raíces en los crecientes problemas de privacidad y seguridad asociados con las consultas DNS tradicionales. Estas consultas, que operan en texto plano, han sido durante mucho tiempo un objetivo para atacantes interesados en interceptar y manipular tráfico de red. En respuesta, la IETF estandarizó DoH en 2018 con la publicación del RFC 8484 [86], como parte de un esfuerzo global para abordar estas vulnerabilidades.

Objetivos del Diseño DoH.

1. **Confidencialidad**: La confidencialidad es uno de los pilares fundamentales del diseño de DoH. Este protocolo garantiza que las consultas DNS no puedan ser monitoreadas o interceptadas por terceros no autorizados, incluidos los proveedores de servicios de Internet (ISP) y actores malintencionados. Esto se logra mediante el cifrado de extremo a extremo proporcionado por HTTPS, que asegura que las consultas y respuestas DNS estén protegidas en todo su recorrido desde el cliente hasta el servidor DoH.
 - o **Protección contra vigilancia masiva**: DoH impide que las consultas DNS sean utilizadas como una fuente de datos para perfiles de navegación.
 - o **Evita ataques de espionaje**: Al cifrar las consultas, se protege la privacidad incluso en redes públicas o no confiables, como Wi-Fi en cafeterías o aeropuertos.

2. **Integridad:** La integridad asegura que las respuestas DNS no sean manipuladas durante el tránsito. Esto es crucial para evitar ataques como el “*DNS spoofing*”, donde un atacante puede redirigir a los usuarios a sitios maliciosos al alterar las respuestas DNS. DoH utiliza los mecanismos de integridad inherentes a TLS, como la verificación de certificados y la autenticación del servidor, para garantizar que los datos no sean modificados o interceptados.
 - o **Protección contra ataques de intermediarios:** El protocolo bloquea intentos de manipulación de consultas o respuestas.
 - o **Validación de origen:** Asegura que las respuestas DNS provienen de un servidor legítimo.
3. **Interoperabilidad:** La interoperabilidad fue un objetivo clave para facilitar la adopción de DoH. Al basarse en HTTPS, DoH puede integrarse sin problemas con la infraestructura existente de Internet, como navegadores, aplicaciones y sistemas operativos. Esto reduce las barreras de entrada tanto para proveedores como para usuarios finales.
 - o **Aprovechamiento de HTTPS:** DoH utiliza el puerto 443, ampliamente adoptado y generalmente permitido en redes empresariales y residenciales.
 - o **Compatibilidad con CDN:** Al integrarse con redes de distribución de contenido (CDN), DoH puede proporcionar respuestas DNS rápidas y fiables.
 - o **Despliegue sencillo:** Los desarrolladores y administradores pueden implementar DoH sin necesidad de realizar cambios significativos en sus infraestructuras existentes.

Funcionamiento del Protocolo DoH.

Arquitectura.

DoH opera enviando consultas DNS dentro del protocolo HTTPS, utilizando las capacidades de cifrado de TLS para garantizar la seguridad de las comunicaciones. La arquitectura de DoH está diseñada para integrarse sin problemas con la infraestructura existente de la web, lo que facilita su adopción y despliegue en aplicaciones modernas. La estructura general de una consulta DoH incluye:

1. **Encabezados HTTPS:**
 - o Proporcionan la información necesaria para establecer y mantener la conexión HTTPS. Incluyen detalles como la versión del protocolo HTTP, el método de solicitud (GET o POST) y metadatos relacionados con la autenticación y el cifrado.
 - o A través del encabezado *Content-Type*, se especifica que el contenido incluye datos de consulta DNS.
2. **Cuerpo de la consulta:**
 - o Contiene las consultas DNS codificadas, ya sea en formato JSON para aplicaciones más legibles o en formato *wireformat*, que es el estándar binario utilizado por los protocolos DNS tradicionales.
 - o El cuerpo también puede incluir parámetros adicionales que mejoren la interoperabilidad con sistemas avanzados, como etiquetas para rastreo de consultas.
3. **Puerto 443:**
 - o Es el puerto estándar para HTTPS, lo que permite que el tráfico DoH se mezcle con el tráfico HTTPS regular.
 - o Este uso hace que el tráfico DoH sea más difícil de identificar y bloquear, especialmente en redes que intentan censurar o restringir ciertas actividades en línea.

Flujo de Trabajo de una Consulta DoH.

1. Generación de la consulta:

- o El cliente, como un navegador web, una aplicación móvil o un sistema operativo, genera una consulta DNS para resolver un nombre de dominio.
- o La consulta incluye información como el nombre de dominio solicitado y el tipo de registro DNS (por ejemplo, A, AAAA, MX).
- o Esta consulta se codifica en uno de los dos formatos soportados por DoH: JSON o Wireformat.
- o La generación de la consulta también puede incluir parámetros adicionales, como identificadores de sesión o datos específicos para resolver conflictos en redes complejas.

2. Encapsulamiento en HTTPS:

- o La consulta codificada se encapsula en una solicitud HTTPS, utilizando los métodos GET o POST:

1. GET:

1. Los datos de la consulta se incluyen en la URL como una cadena de consulta.
2. Este método es más adecuado para consultas pequeñas debido a las limitaciones de longitud de la URL.

2. POST:

1. Los datos se colocan en el cuerpo de la solicitud HTTP, lo que permite manejar consultas más grandes.
2. Este método ofrece mayor privacidad, ya que los datos de la consulta no son visibles en los registros del servidor o intermediarios.

- o La solicitud HTTPS también incluye encabezados específicos, como *Content-Type: application/dns-message*, que indica al servidor que la solicitud contiene datos DNS.

3. Resolución de la consulta:

- o Al recibir la solicitud HTTPS, el servidor DoH realiza varias tareas:

1. Descifrado y validación:

1. Descifra la solicitud utilizando TLS y valida que provenga de un cliente autorizado.
2. Esto incluye la verificación de certificados y autenticación mutua si está habilitada.

2. Extracción de la consulta DNS:

Extrae los datos DNS del cuerpo o la URL de la solicitud, dependiendo del método utilizado.

- o La consulta DNS se reenvía a un resolver DNS tradicional, que puede ser un resolver recursivo o un servidor autorizado.

4. Respuesta del servidor:

- o El servidor DNS tradicional genera una respuesta basada en la consulta recibida:

1. Esto puede incluir registros A para direcciones IPv4, registros AAAA para IPv6 o registros específicos como CNAME o MX.

- o El servidor DoH encapsula la respuesta en un mensaje HTTPS:

1. La respuesta se codifica en el mismo formato (*wireformat* o JSON) utilizado en la consulta original.
 2. El servidor añade metadatos de seguridad y compresión para optimizar el envío.
- o La respuesta HTTPS se envía de vuelta al cliente a través de la conexión TLS existente, asegurando que los datos no puedan ser interceptados o modificados en tránsito.

En la figura siguiente se puede observar la diferencia de que el DNS emplee DOH o no:

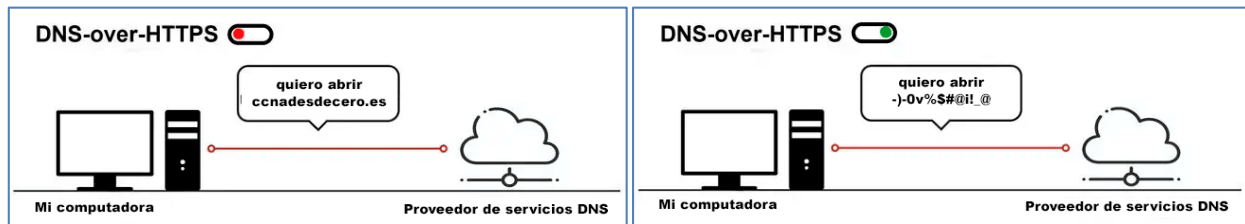


Figura 3-1. DNS sin usar DoH – DNS con DoH Habilitado. (Fuente: <https://ccnadesdecero.es>).

Características Adicionales de la Arquitectura.

1. Compatibilidad con HTTP/2 y HTTP/3:

- Las versiones modernas de HTTP, como HTTP/2 y HTTP/3, introducen características que mejoran significativamente el rendimiento y la latencia. DoH puede aprovechar estas tecnologías para ofrecer un servicio más eficiente:
 - o **Multiplexación de solicitudes:** HTTP/2 permite que múltiples consultas DNS sean enviadas simultáneamente a través de una sola conexión, reduciendo el tiempo de espera y mejorando la eficiencia.
 - o **Reducción de la latencia:** HTTP/3, basado en el protocolo QUIC (Quick UDP Internet Connections) [95], elimina los tiempos de espera asociados con retransmisiones de TCP, lo que mejora aún más el rendimiento de las consultas DoH.
 - o **Compresión de encabezados:** HTTP/2 incluye técnicas de compresión que minimizan el tamaño de los encabezados de las solicitudes, optimizando el uso del ancho de banda.

2. Resiliencia ante restricciones de red:

- Al utilizar el puerto 443, DoH logra evitar bloqueos específicos de DNS implementados en redes que intentan restringir o censurar el acceso a ciertos dominios.
 - o **Dificultad para la censura:** Debido a que el tráfico DoH se mezcla con el tráfico HTTPS normal, los sistemas de filtrado no pueden distinguir fácilmente entre solicitudes web y consultas DNS cifradas.
 - o **Soporte para redes complejas:** En entornos empresariales o residenciales con restricciones de red, DoH mantiene la conectividad sin requerir configuraciones adicionales por parte del usuario.
 - o **Reducción de vulnerabilidades:** La resiliencia de DoH contra intentos de interceptación lo convierte en una herramienta clave para proteger la privacidad en redes públicas o no confiables.

3. Optimización de recursos:

- DoH optimiza la utilización de recursos al permitir la reutilización de conexiones HTTPS existentes para procesar múltiples consultas DNS. Esto reduce la carga en la red y mejora la velocidad de resolución:

- o **Menor sobrecarga de conexión:** Al reutilizar conexiones abiertas, DoH evita los costes de tiempo y recursos asociados con el establecimiento de nuevas conexiones TLS para cada consulta.
- o **Consolidación de tráfico:** La agrupación de consultas DNS dentro de solicitudes HTTPS minimiza el número de paquetes enviados, mejorando el rendimiento general de la red.

Beneficios Técnicos.

1. Cifrado extremo a extremo:

- o DoH utiliza TLS para cifrar todas las consultas DNS, lo que garantiza que los datos estén protegidos desde el cliente hasta el servidor DoH.
- o Esto elimina la posibilidad de que atacantes intercepten y analicen las consultas DNS mientras están en tránsito.
- o El cifrado TLS también previene ataques como el “*eavesdropping*”, donde los atacantes monitorean silenciosamente las comunicaciones sin alterar los datos.
- o Además, este cifrado extremo a extremo asegura que las respuestas DNS no sean visibles ni manipulables por intermediarios, como redes Wi-Fi públicas o proxies no seguros.

2. Privacidad mejorada:

- o Al proteger las consultas DNS, DoH impide que proveedores de servicios de Internet y otras entidades puedan rastrear las actividades de navegación de los usuarios.
- o Esto es especialmente relevante en países donde el monitoreo del tráfico DNS se utiliza para restringir o vigilar el acceso a contenidos en línea.
- o DoH oculta las consultas DNS dentro del tráfico HTTPS normal, lo que dificulta la creación de perfiles de usuario basados en solicitudes DNS.
- o También protege contra prácticas invasivas de marketing, donde los datos DNS pueden ser explotados para dirigir anuncios personalizados o vender información de navegación.

3. Evasión de censura:

- o Al utilizar el puerto 443, compartido con el tráfico HTTPS, DoH dificulta que los mecanismos de censura detecten y bloqueen consultas DNS específicas.
- o Este beneficio es crucial en redes donde se implementan restricciones estrictas de acceso a ciertos dominios o servicios.
- o Al camuflar el tráfico DNS como tráfico web normal, DoH permite a los usuarios acceder a contenido bloqueado sin necesidad de herramientas adicionales como VPN.
- o Además, la resiliencia ante bloqueos hace que DoH sea una solución ideal en entornos corporativos o educativos donde las políticas de filtrado pueden ser excesivamente restrictivas.

4. Integridad de los datos:

- o DoH garantiza que las respuestas DNS no puedan ser manipuladas durante su tránsito entre el servidor DoH y el cliente.
- o Utilizando TLS, el protocolo incluye mecanismos de verificación que aseguran que las respuestas provienen de un servidor autorizado y no han sido alteradas.
- o Esto protege contra ataques de “*DNS spoofing*” y “*DNS cache poisoning*”, donde los atacantes intentan redirigir a los usuarios a sitios maliciosos mediante la modificación de respuestas DNS.
- o También mejora la confianza en la resolución DNS al asegurar que los datos son precisos y coinciden con las solicitudes originales del cliente.

Ventajas de DNS sobre HTTP.

1. Seguridad mejorada:

- o DoH protege contra ataques comunes al DNS, como el “*DNS spoofing*” y “*man-in-the-middle*”. Al cifrar las consultas y respuestas DNS, garantiza que los datos no puedan ser interceptados ni modificados durante su tránsito.
- o También reduce el riesgo de ataques de “*DNS cache poisoning*”, donde los atacantes inyectan respuestas falsas en el caché DNS para redirigir a los usuarios a sitios maliciosos.
- o Además, DoH añade una capa adicional de seguridad al dificultar la manipulación del tráfico DNS en redes públicas o no seguras.

2. Privacidad del usuario:

- o DoH encripta las consultas DNS, impidiendo que proveedores de servicios de Internet, intermediarios y actores maliciosos puedan monitorear el tráfico DNS para rastrear hábitos de navegación.
- o Es especialmente útil en países o entornos donde el monitoreo del tráfico DNS se utiliza para censura o vigilancia.
- o Protege a los usuarios de la explotación comercial de sus datos de navegación por parte de terceros.

3. Interoperabilidad:

- o DoH aprovecha la infraestructura existente de HTTPS, lo que facilita su adopción en aplicaciones modernas sin necesidad de desarrollar tecnologías adicionales.
- o Gracias a su compatibilidad con el protocolo HTTPS, puede integrarse fácilmente con navegadores, sistemas operativos y aplicaciones móviles.
- o Permite a los desarrolladores implementar DoH sin realizar cambios significativos en la infraestructura existente.

4. Desempeño constante:

- o Al integrarse con redes de distribución de contenido (CDN), DoH mantiene tiempos de respuesta bajos y consistentes, incluso en redes con alta latencia o congestionadas.
- o Las CDN optimizan el enrutamiento y el almacenamiento en caché, mejorando la velocidad de resolución DNS en regiones geográficamente dispersas.

5. Compatibilidad amplia:

- o DoH cuenta con soporte en navegadores líderes como Mozilla Firefox, Google Chrome y Microsoft Edge, así como en sistemas operativos modernos como Windows 10 y 11.
- o Este soporte generalizado facilita la adopción por parte de los usuarios finales y organizaciones.

Desafíos y Limitaciones de DNS sobre HTTP.

1. Sobrecarga de red:

- o El cifrado adicional introduce una sobrecarga computacional que puede aumentar la latencia de las consultas DNS, especialmente en redes con recursos limitados.
- o Aunque HTTP/2 y HTTP/3 mejoran la eficiencia al permitir múltiples consultas en una sola conexión, el impacto en redes lentas sigue siendo significativo.

Soluciones:

- **Optimización de protocolos:** Implementar HTTP/3 (basado en QUIC) para reducir los tiempos de retransmisión y mejorar la eficiencia en redes de alta latencia.
- **Uso de CDN y caché local:** Integrar redes de distribución de contenido (CDN) y aprovechar cachés DNS locales para minimizar la dependencia de conexiones recurrentes al servidor DoH.
- **Balanceo de carga:** Distribuir las consultas entre múltiples servidores DoH para reducir la presión en servidores individuales y optimizar tiempos de respuesta.
- **Compresión de datos:** Utilizar técnicas avanzadas de compresión, como la compresión de encabezados de HTTP/2, para minimizar el tamaño de las solicitudes y respuestas.

2. Confianza en el servidor DNS:

- o A pesar del cifrado, los servidores DoH aún pueden registrar y analizar las consultas DNS de los usuarios.
- o La elección de proveedores confiables, como Cloudflare o Quad9, es crucial para mitigar riesgos asociados con la privacidad.
- o Este desafío plantea la necesidad de estándares más estrictos sobre la gestión de datos por parte de los proveedores de DoH.

Soluciones:

- **Elegir proveedores confiables:** Optar por proveedores como Quad9 o Cloudflare, que han establecido políticas claras de privacidad y no retención de datos.
- **Uso de resolvers DoH autogestionados:** Configurar servidores DoH propios dentro de la red organizacional para mantener un control total sobre las consultas y evitar el almacenamiento externo.
- **Adopción de estándares de privacidad:** Implementar protocolos como Oblivious DoH (ODOH), que separan las identidades del cliente y las consultas para garantizar mayor anonimato.
- **Auditorías independientes:** Promover auditorías regulares de proveedores de DoH para verificar el cumplimiento de políticas de privacidad.

3. Conflictos en entornos corporativos:

- o En redes corporativas o educativas, donde el filtrado de contenido basado en DNS es común, DoH puede interferir al camuflar las consultas DNS dentro del tráfico HTTPS.
- o Esto dificulta la implementación de políticas de seguridad como el bloqueo de sitios maliciosos o inapropiados.
- o Para abordar este desafío, las organizaciones pueden adoptar soluciones híbridas que combinen DoH con mecanismos de control a nivel de red.

Soluciones:

- **Adopción de soluciones híbridas:** Integrar DoH con DNSSEC para garantizar autenticidad y control, sin comprometer la privacidad.
- **Resolver corporativos:** Implementar servidores DoH internos que cumplan con las políticas de seguridad específicas de la organización.
- **Monitorización del tráfico HTTPS:** Usar herramientas de inspección HTTPS (con TLS *terminators*) para identificar y gestionar el tráfico DoH, sin comprometer las políticas de seguridad.
- **Políticas de confianza:** Establecer listas blancas para dominios específicos y restringir el acceso a *resolver* externos que no cumplan con las políticas organizativas.

4. Complejidad de implementación:

- o La integración de DoH con sistemas heredados puede requerir actualizaciones significativas en la infraestructura existente, incluyendo resolvers DNS y configuraciones de red.
- o La configuración inicial puede ser técnica y compleja, especialmente para organizaciones con recursos limitados.

Soluciones:

- **Automatización de la configuración:** Implementar herramientas de automatización como Ansible o *scripts* de configuración para simplificar el despliegue de DoH en entornos existentes.
- **Infraestructura híbrida:** Mantener un enfoque gradual combinando sistemas DNS tradicionales y DoH durante el proceso de migración.
- **Capacitación técnica:** Proporcionar formación específica al personal técnico sobre la implementación y gestión de DoH.
- **Soporte de proveedores:** Colaborar con proveedores de DoH que ofrezcan soluciones preconfiguradas o soporte técnico personalizado.

5. Dependencia del proveedor:

- o La centralización en un número reducido de proveedores de DoH, como Google y Cloudflare, genera preocupaciones sobre la monopolización del tráfico DNS y la privacidad del usuario.
- o Esto también plantea el riesgo de que una interrupción en un proveedor afecte a un gran número de usuarios y servicios.
- o La diversificación de proveedores y el desarrollo de soluciones descentralizadas son esenciales para mitigar estos riesgos.

Soluciones:

- **Diversificación de proveedores:** Configurar múltiples resolvers DoH en las preferencias del cliente para distribuir la carga y evitar la dependencia de un único proveedor.
- **Promoción de alternativas descentralizadas:** Apoyar proyectos como NextDNS y resolver proyectos comunitarios que prioricen la transparencia.
- **Implementación de resolvers privados:** Desplegar servidores DoH propios dentro de redes empresariales o domésticas, eliminando la dependencia externa.
- **Participación en iniciativas de gobernanza:** Colaborar con organismos como la IETF) para fomentar estándares que promuevan la descentralización y la competencia justa.

Implementaciones Destacadas.

Proveedores Compatibles: Los principales proveedores de DNS han implementado soporte para DoH con características únicas, lo que los hace atractivos para diferentes casos de uso:

- **Cloudflare.**

Características:

- Baja latencia gracias a su extensa red global de servidores distribuidos.
- Compromiso con la privacidad: No guarda registros de las consultas por más de 24 horas.
- Protección contra ataques DDoS integrando DoH con su infraestructura resistente a ataques.

Soluciones:

- **Para empresas y usuarios individuales:** Cloudflare es ideal para quienes buscan un resolver rápido con una política clara de privacidad.
- **Implementación:** Configurar Cloudflare como el resolver principal en sistemas operativos o aplicaciones para aprovechar su baja latencia.
- **Integración:** Cloudflare también es compatible con Oblivious DoH (ODoH), lo que permite mayor anonimato al separar las consultas DNS de la identidad del cliente.
- **Google Public DNS.**

Características:

- Amplia adopción gracias a la robusta infraestructura de Google.
- Resolución rápida con una red global de puntos de presencia (PoP).
- Garantiza alta disponibilidad y estabilidad.

Soluciones:

- **Para entornos de alta demanda:** Google Public DNS es ideal para empresas que requieren resolución DNS rápida y confiable.
- **Seguridad:** Configurar DNSSEC en conjunto con Google Public DNS para garantizar autenticidad en las respuestas.
- **Uso práctico:** Integrar con aplicaciones móviles y dispositivos IoT para garantizar resolución eficiente incluso en redes limitadas.

Consideraciones:

- Evaluar cuidadosamente las políticas de privacidad de Google, ya que pueden recopilar metadatos asociados con las consultas DNS.
- **Quad9: Servicio enfocado en seguridad.**

Características:

- Bloquea automáticamente dominios maliciosos basándose en datos de amenazas en tiempo real.
- Sin fines de lucro, con un fuerte enfoque en la privacidad del usuario.
- Compatible con DNSSEC para validar la autenticidad de las respuestas.

Soluciones:

- **Para organizaciones que priorizan la seguridad:** Quad9 es ideal para proteger redes contra *phishing*, *malware* y otras amenazas cibernéticas.
- **Configuración personalizada:** Integrar Quad9 en rúteres empresariales para filtrar tráfico malicioso antes de que alcance los dispositivos finales.
- **Educación:** Ideal para redes escolares y comunitarias donde la protección contra sitios web dañinos es esencial.
- **NextDNS [87]: Servicio con configuraciones avanzadas.**

Características:

- Permite configuraciones personalizadas, como listas negras/blancas de dominios y perfiles de usuarios.
- Monitoreo detallado del tráfico DNS con opciones de generación de informes.
- Compatible con DoH, DoT y DNSSEC.

Soluciones:

- **Para usuarios avanzados:** NextDNS es ideal para quienes desean un control granular sobre sus consultas DNS y monitoreo en tiempo real.
- **Control parental:** Configurar NextDNS en entornos familiares para filtrar contenido inapropiado y monitorizar actividades de navegación.
- **Protección adicional:** Utilizar NextDNS en combinación con aplicaciones de seguridad para crear un ecosistema robusto contra amenazas.
- **OpenDNS [88]: Solución empresarial avanzada.**

Características:

- Capacidades avanzadas de filtrado de contenido y análisis de amenazas.
- Integración con plataformas empresariales para políticas de seguridad personalizadas.
- Ofrece servicios de protección específicos contra *malware* y *phishing*.

Soluciones:

- **Para empresas:** OpenDNS es ideal para redes corporativas que necesitan controlar el acceso a dominios específicos y proteger contra amenazas cibernéticas.
- **Políticas escalables:** Implementar políticas basadas en usuarios o departamentos para personalizar el acceso y la seguridad.
- **Monitoreo:** Aprovechar las capacidades de análisis para identificar patrones sospechosos y prevenir ataques.

En la siguiente tabla se muestra una comparativa entre los distintos proveedores:

Proveedor	Enfoque Principal	Ventaja Destacada	Mejor Uso
Cloudflare	Privacidad y rapidez	Baja latencia	Usuarios individuales y empresas pequeñas
Google DNS	Infraestructura global	Alta disponibilidad	Resolución rápida en alta demanda
Quad9	Seguridad	Filtrado de amenazas	Redes escolares, comunitarias y empresariales
NextDNS	Configuración avanzada	Monitoreo detallado	Control parental y usuarios avanzados
OpenDNS	Empresas	Capacidades de filtrado	Redes corporativas

Tabla 3-1. Comparativa de Proveedores.

El impacto global de DNS sobre TLS se ha visto amplificado gracias a la colaboración entre proveedores líderes, proyectos de código abierto y sistemas operativos populares. Aunque enfrenta desafíos como la necesidad de configuraciones manuales y limitaciones en redes restringidas, su capacidad para proteger la privacidad y la integridad de las consultas DNS lo posiciona como un estándar emergente en seguridad de Internet.

El futuro de DoH está lleno de oportunidades y desafíos. Las implementaciones emergentes como ECH (*Encrypted Client Hello*) [98], la adopción masiva, la compatibilidad con IPv6, están sentando las bases para un ecosistema DNS más seguro, privado y eficiente. Con el tiempo, estas mejoras garantizarán que DoH no solo sea una herramienta esencial para la privacidad en línea, sino también un estándar universalmente aceptado.

En la tabla siguiente se muestra una comparativa entre DoH y DoT.

Aspecto	DNS sobre HTTPS (DoH)	DNS sobre TLS (DoT)
Puertos utilizados	Usa el puerto 443, compartido con el tráfico HTTPS estándar, lo que dificulta su identificación y bloqueo.	Usa el puerto 853, un puerto dedicado para tráfico DNS cifrado, lo que facilita su identificación y manejo en redes administradas.
Transporte	Encapsula las consultas DNS en solicitudes HTTPS, utilizando el protocolo HTTP/2 o HTTP/3 para optimizar la transmisión.	Transmite consultas DNS sobre una conexión cifrada mediante TLS sobre TCP.
Velocidad y latencia	Generalmente más rápido en redes modernas debido a las optimizaciones de HTTP/2 y HTTP/3.	Puede ser ligeramente más lento en redes con alta latencia, ya que utiliza solo TCP sin las optimizaciones de QUIC.
Compatibilidad con redes	Es menos susceptible a bloqueos en redes restringidas, ya que utiliza el mismo puerto que HTTPS.	Puede ser bloqueado en redes que restringen el puerto 853, especialmente en entornos con censura estricta.
Privacidad	Ofrece un alto nivel de privacidad al combinarse con HTTPS, pero puede mezclarse con tráfico web, lo que dificulta su gestión.	Proporciona privacidad mediante cifrado TLS, con tráfico fácilmente distinguible, útil para redes administradas.
Facilidad de implementación	Integrado en navegadores como Firefox, Chrome y Edge, lo que facilita su adopción por usuarios finales.	Necesita configuración adicional en dispositivos y aplicaciones, aunque está soportado de manera nativa en Android 9+ y superiores.
Gestión en redes corporativas	Es más difícil de gestionar debido a su mezcla con tráfico HTTPS general, lo que complica su diferenciación en análisis de red.	Más fácil de gestionar en entornos empresariales debido a su puerto dedicado y características específicas.
Seguridad	Ofrece seguridad robusta mediante HTTPS, pero depende de la	Seguridad igualmente fuerte gracias al cifrado TLS, con menor superficie de ataque por usar un puerto dedicado.

Aspecto	DNS sobre HTTPS (DoH)	DNS sobre TLS (DoT)
	implementación correcta por parte de los servidores DNS.	
Uso recomendado	Ideal para usuarios finales que buscan privacidad y resistencia a bloqueos en redes restringidas.	Preferido en entornos corporativos o administrados, donde se necesita visibilidad y control del tráfico DNS cifrado.

Tabla 3-2. Comparativa DoH vs DoT.

La figura 3-4 muestra una comparación visual entre los protocolos DNS estándar, DoT y DoH, destacando factores como puertos utilizados, facilidad de adopción, y vulnerabilidades típicas.

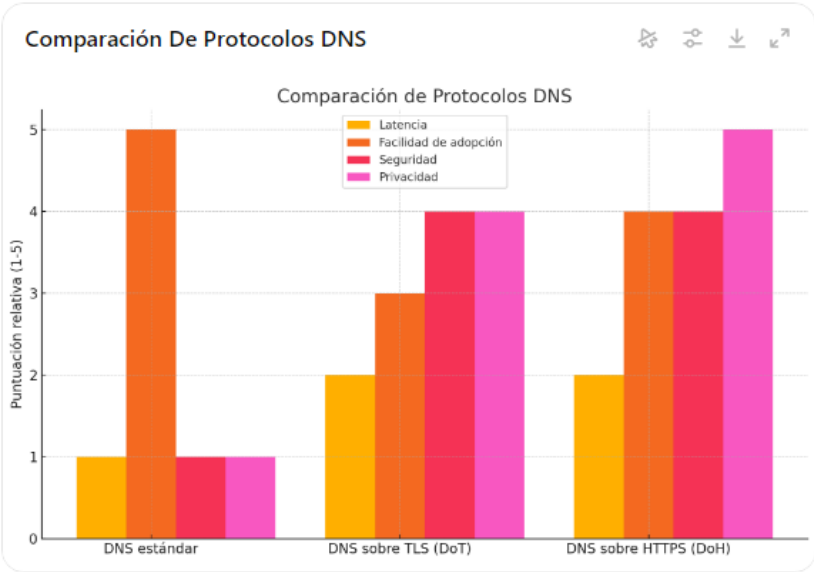


Figura 3-2. Comparación de Protocolos DNS. Gráfico creado con IA (ChatGPT).

3.1.4 Filtrado y Monitoreo de DNS. [89]

El filtrado de DNS es una práctica esencial para mitigar riesgos y garantizar la productividad en redes corporativas. Actúa como una capa defensiva para proteger contra actividades maliciosas y mantener el control del acceso a contenidos inapropiados.

- **Funcionamiento del filtrado de DNS:**
 - Se basa principalmente en listas negras (*blacklists*), donde se catalogan dominios asociados a actividades maliciosas, como distribución de malware, phishing o contenido inapropiado.
 - Los servidores DNS equipados con filtrado rechazan las solicitudes de resolución hacia estos dominios, bloqueando así el acceso.
 - Alternativamente, las listas blancas (*whitelists*) garantizan que solo se permita el acceso a dominios autorizados.
- **Beneficios clave:**
 - **Protección contra amenazas:** Evita que los usuarios accedan a sitios web peligrosos que podrían comprometer la red o sus dispositivos.

- **Control de contenido:** Las organizaciones pueden implementar políticas para restringir el acceso a categorías de contenido como juegos, redes sociales o sitios no relacionados con el trabajo.
- **Mejora del rendimiento:** Al bloquear dominios no autorizados, se reduce el tráfico innecesario y el consumo de ancho de banda, mejorando la eficiencia general de la red.

3.1.4.1 *Firewalls*.

Los *firewalls* [90] son dispositivos o software que actúan como la primera línea de defensa en la infraestructura de red. Su propósito es controlar el tráfico de entrada y salida de una red según un conjunto de reglas de seguridad predefinidas, con el objetivo de proteger contra accesos no autorizados y amenazas externas.

1. **Rol central en la seguridad de la red:** Los *firewalls* analizan y filtran paquetes de datos según criterios como dirección IP, protocolo, puertos, o contenido. Esto los convierte en un componente esencial para prevenir accesos no autorizados, ataques de *malware*, y la exfiltración de datos.
2. **Evolución del concepto:** Desde su aparición en la década de 1980, los *firewalls* han evolucionado significativamente, pasando de simples filtros de paquetes a soluciones avanzadas como ***firewalls de próxima generación (NGFW)***, que incluyen capacidades de inspección profunda de paquetes y detección de amenazas basadas en inteligencia artificial.

Tipos Principales de *Firewalls*.

1. *Firewall* de Filtrado de Paquetes:

Características principales:

- Analizan cada paquete de datos de forma individual, evaluando parámetros como la dirección IP de origen y destino, puertos, y el protocolo utilizado.
- Las reglas de filtrado se basan en estos parámetros básicos.

Ventajas:

- **Velocidad y simplicidad:** Debido a su diseño simple, los *firewalls* de filtrado de paquetes ofrecen un alto rendimiento con mínima latencia.
- **Coste:** Son una solución económica y ampliamente disponible.

Desventajas:

- **Falta de contexto:** No consideran el estado de la conexión ni el contenido del paquete, lo que los hace vulnerables a ataques más sofisticados como suplantación de IP o tráfico fragmentado.
- **Limitaciones en seguridad:** Carecen de la capacidad de inspeccionar datos cifrados o identificar amenazas avanzadas.

Aplicación práctica: Adecuados para entornos simples donde las amenazas son mínimas o donde se requiere un control básico del tráfico.

2. *Firewall* de Inspección con Estado (*Stateful*).

Características principales:

- Supervisan y mantienen información sobre el estado de las conexiones activas, como puertos utilizados y secuencia de paquetes, permitiendo decisiones más informadas.

- Permiten o bloquean tráfico según el contexto de la conexión, no solo basado en reglas estáticas.

Ventajas:

- **Mejor seguridad:** Al considerar el estado de las conexiones, estos *firewalls* son más efectivos contra ataques como falsificación de paquetes (*spoofing*).
- **Versatilidad:** Ideales para redes modernas con necesidades de monitoreo continuo.

Desventajas:

- **Mayor consumo de recursos:** La supervisión de conexiones activas puede aumentar la carga en el hardware, especialmente en redes de alta capacidad.
- **Latencia moderada:** Aunque no significativa, la inspección con estado puede introducir ligeras demoras.

Aplicación práctica: Utilizados ampliamente en redes corporativas, donde la seguridad y la capacidad de manejar múltiples conexiones simultáneamente son críticas.

3. Firewall de Aplicación (Proxy).

Características principales:

- Funcionan como intermediarios entre el cliente y el servidor, inspeccionando y procesando todo el tráfico en el nivel de aplicación.
- Interpretan y analizan el contenido completo de las comunicaciones, como solicitudes HTTP o consultas DNS.

Ventajas:

- **Control granular:** Permiten establecer reglas detalladas basadas en el contenido, lo que mejora la protección contra ataques dirigidos a aplicaciones específicas.
- **Seguridad avanzada:** Al analizar el contenido de los datos, son efectivos contra *malware* y amenazas ocultas en el tráfico legítimo.

Desventajas:

- **Latencia elevada:** La inspección exhaustiva del contenido introduce demoras significativas.
- **Requieren mayor potencia de hardware:** Su funcionamiento intensivo en recursos puede ser un desafío para redes de alta capacidad.

Aplicación práctica: Usados en entornos críticos como redes gubernamentales, financieras o de salud, donde la seguridad del contenido es primordial.

En la siguiente tabla se muestra una pequeña comparativa entre los diferentes tipos de *Firewall*:

Tipo de <i>Firewall</i>	Ventajas	Desventajas	Aplicación Ideal
Filtrado de Paquetes	Rápido y económico	Vulnerable a ataques avanzados	Redes simples con bajo riesgo
Inspección con Estado	Seguro y versátil	Mayor carga de hardware	Redes corporativas y de alta demanda
Proxy (Aplicación)	Control granular y seguridad avanzada	Latencia elevada y alto costo	Redes críticas con datos sensibles

Tabla 3-3. Comparativa Firewall.

Los *firewalls* son una solución flexible y robusta para proteger las redes contra amenazas cibernéticas. La elección del tipo de firewall depende de factores como el tamaño de la red, la sensibilidad de los datos y los requisitos de rendimiento. Aunque los *firewalls* de filtrado de paquetes son una solución básica, los de inspección con estado y los de aplicación ofrecen niveles más altos de seguridad para entornos con necesidades avanzadas.

Funciones Clave de los *Firewalls*.

- **Filtrado de Tráfico:** Los *firewalls* permiten aplicar políticas de seguridad para bloquear tráfico no autorizado hacia o desde direcciones IP específicas, dominios sospechosos o protocolos particulares. El filtrado de tráfico es esencial para prevenir ataques de reconocimiento (*scanning*), conexiones a servidores de comando y control (C&C), y el acceso a contenido inapropiado en entornos corporativos.
- **Prevención de Intrusiones:** Los *firewalls* modernos integran sistemas de prevención de intrusos (IPS) que detectan patrones maliciosos y bloquean automáticamente intentos de acceso no autorizado antes de que comprometan la red. Un *firewall* puede identificar y bloquear un ataque de fuerza bruta o una explotación de vulnerabilidades como *SQL injection*. La capacidad de prevenir intrusiones protege la infraestructura contra amenazas avanzadas persistentes (APT) y minimiza el impacto de incidentes de seguridad.
- **Registro y Monitoreo:** Los *firewalls* generan registros detallados de eventos relacionados con el tráfico de red, incluyendo intentos bloqueados, conexiones activas y posibles anomalías. Con lo que facilitan la auditoría de seguridad y el cumplimiento normativo y ayudan a identificar patrones de comportamiento malicioso a través del análisis forense posterior a incidentes. Por ejemplo, un análisis de registros podría revelar intentos repetidos de acceso no autorizado desde una misma dirección IP, permitiendo ajustar las políticas de bloqueo.

Consideraciones para su Implementación.

La implementación de un firewall debe adaptarse a las necesidades específicas de la organización, teniendo en cuenta varios factores clave:

1. Requisitos de la Red:

- **Volumen de tráfico:** La capacidad del *firewall* debe ser suficiente para manejar el volumen de tráfico sin introducir latencia significativa.
- **Sensibilidad de los datos:** Las redes que procesan información crítica o sensible, como datos financieros o médicos, requieren *firewalls* con funcionalidades avanzadas, como inspección profunda de paquetes (DPI) y análisis de tráfico cifrado.

2. Funcionalidades Adicionales:

- **Sistemas de detección y prevención de intrusos (IDPS):** Combinar capacidades de *firewall* con detección y prevención de intrusos mejora significativamente la protección contra amenazas internas y externas.
- **Filtrado de contenido:** Permite a las organizaciones restringir el acceso a categorías de contenido no deseadas, como redes sociales o contenido explícito.
- **Prevención de pérdida de datos (DLP):** Protege contra la exfiltración de datos sensibles al monitorear y controlar la transferencia de información fuera de la red.

3.1.4.2 Sistemas de Detección de Intrusos (IDS).

Los Sistemas de Detección de Intrusos (*Intrusion Detection Systems*, IDS) [91] son herramientas fundamentales en la seguridad de redes que complementan a los firewalls al proporcionar capacidades de monitoreo y análisis en tiempo real. Estos sistemas detectan actividades sospechosas dentro de la red y generan alertas para prevenir incidentes de seguridad, ofreciendo una capa adicional de protección frente a amenazas tanto internas como externas.

Tipos Principales de IDS.

1. IDS Basados en NIDS:

Los **IDS Basados en Red (NIDS)** [92] son sistemas diseñados para supervisar el tráfico de red en tiempo real. Colocados estratégicamente en puntos clave de la red, analizan el flujo de datos en busca de patrones maliciosos, anomalías y posibles amenazas. Los NIDS son una herramienta esencial para proteger infraestructuras críticas que manejan grandes volúmenes de tráfico, ofreciendo detección temprana de ataques y una capa de protección proactiva.

Descripción de los NIDS: Los NIDS monitorean el tráfico de red en puntos estratégicos como:

- **Servidores DNS:** Supervisan consultas para detectar intentos de envenenamiento de caché, *tunneling* DNS o accesos maliciosos.
- **Pasarelas de red:** Identifican intentos de intrusión desde redes externas.
- **Subredes críticas:** Aseguran la integridad del tráfico dentro de segmentos sensibles de la red.

Funcionamiento técnico:

- Los NIDS analizan paquetes en tránsito utilizando métodos como la comparación con firmas de amenazas conocidas, heurísticas y aprendizaje automático para identificar anomalías o comportamientos sospechosos.
- Trabajan principalmente en modo pasivo, lo que significa que no interfieren directamente con el tráfico, pero generan alertas cuando detectan incidentes.

Ventajas de los NIDS:

- **Protección de infraestructuras críticas:** Los NIDS son ideales para entornos que manejan grandes volúmenes de tráfico, como centros de datos, redes empresariales y servidores DNS. Proporcionan un monitoreo constante que detecta actividades maliciosas en etapas iniciales.
- **Detección temprana de ataques dirigidos a la red:** Identifican amenazas antes de que estas comprometan los sistemas internos. Ejemplos de ataques detectados incluyen:

- **Intentos de envenenamiento de caché DNS:** Alteración maliciosa de las respuestas DNS para redirigir a usuarios a sitios falsificados.
- **Ataques de denegación de servicio (DoS):** Aumento repentino de solicitudes para agotar los recursos de la red o del servidor.
- **Cobertura amplia:** Al monitorear todo el tráfico que atraviesa un punto de la red, los NIDS tienen una visibilidad completa, lo que permite identificar amenazas distribuidas o múltiples vectores de ataque simultáneamente.
- **Adaptabilidad:** Los sistemas NIDS modernos utilizan inteligencia artificial y aprendizaje automático para detectar nuevas variantes de amenazas basadas en patrones anómalos en el tráfico.

2. IDS Basados en *Host* (HIDS):

Los **Sistemas de Detección de Intrusos Basados en *Host* (HIDS)** [93] son herramientas diseñadas para monitorear la actividad en dispositivos individuales, como servidores, estaciones de trabajo y *endpoints* críticos. Operan directamente en el sistema operativo, proporcionando una protección detallada frente a ataques internos y actividades maliciosas en un nivel granular.

Descripción de los HIDS:

Funcionamiento técnico: Los HIDS supervisan eventos específicos en un equipo, tales como:

- Intentos de acceso no autorizado.
- Modificaciones en archivos críticos del sistema.
- Instalación de software no autorizado.
- Cambios en configuraciones de seguridad o privilegios de usuarios.
- **Monitoreo continuo:** Los HIDS recopilan registros detallados de eventos locales, utilizando algoritmos para identificar patrones de comportamiento malicioso o anomalías. También realizan correlaciones entre eventos para detectar intentos de ataque avanzados.
- **Ubicación e implementación:** Cada HIDS se instala en dispositivos individuales, lo que les permite detectar amenazas que pueden pasar desapercibidas para los sistemas de detección basados en red (NIDS).

Ventajas de los HIDS:

- **Detección de ataques internos o actividades maliciosas:** Los HIDS son especialmente efectivos para identificar ataques provenientes del interior de la organización, como empleados descontentos que intentan manipular o exfiltrar información sensible. También son útiles para detectar *malware* que se ejecuta localmente en un *host*, incluso si este *malware* evade la detección en la red.
- **Monitoreo granular a nivel de host:** Proporcionan un control exhaustivo sobre eventos locales en el sistema, lo que permite una protección personalizada y adaptada a la criticidad del dispositivo. Pueden ser configurados para monitorear únicamente procesos y archivos clave, minimizando el impacto en el rendimiento del sistema.
- **Capacidades de análisis forense:** Los registros generados por los HIDS son una fuente valiosa para investigaciones post-incidente, ya que ofrecen un historial completo de actividades realizadas en el equipo.
- **Compatibilidad con políticas de cumplimiento:** Los HIDS facilitan el cumplimiento de normativas como PCI-DSS, GDPR y HIPAA, al asegurar la protección de los datos sensibles y generar reportes de auditoría.

En la siguiente tabla se muestra una comparación entre los NIDS y HIDS.

Aspecto	NIDS	HIDS (<i>Host-based IDS</i>)
Cobertura	Monitorea el tráfico en toda la red.	Supervisa actividades en dispositivos individuales.
Ubicación	Se instala en puntos clave como servidores DNS o pasarelas.	Se implementa en servidores y endpoints específicos.
Ejemplo de detección	Identificación de un ataque DoS dirigido al servidor DNS.	Detección de intentos de acceso no autorizado en un servidor de archivos.
Ventaja principal	Proporciona una visión amplia del tráfico para identificar amenazas distribuidas.	Ofrece protección detallada y granular en dispositivos críticos.

Tabla 3-4. Comparativa NIDS vs HIDS.

3.1.4.3 Sistemas de Detección de Intrusos (IDS) y *Firewalls*.

La **integración entre Sistemas de Detección de Intrusos (IDS) y *firewalls*** [94] es una estrategia clave en la ciberseguridad moderna [95]. Esta combinación permite ofrecer un enfoque de defensa en profundidad al unir las capacidades de bloqueo de tráfico del *firewall* con la habilidad del IDS para detectar y analizar actividades maliciosas más complejas [96].

1. Descripción de la Integración.

- **Función de los *Firewalls*:** Los *firewalls* actúan como la primera línea de defensa, filtrando el tráfico basado en reglas predefinidas (como bloquear direcciones IP sospechosas o restringir ciertos puertos).
- **Función de los IDS:** Los IDS complementan a los *firewalls* al analizar el tráfico que ha pasado por las reglas del *firewall*, detectando patrones maliciosos complejos, anomalías o ataques dirigidos que no pueden ser bloqueados únicamente por las políticas estáticas del *firewall*.
- **Mecanismo de integración:**
 - Cuando el IDS detecta un comportamiento sospechoso (como un aumento inusual de tráfico en un puerto específico o la comunicación con un servidor de comando y control), genera una alerta.
 - Esta alerta puede ser utilizada para modificar dinámicamente las reglas del *firewall* y bloquear el tráfico sospechoso en tiempo real.

2. Ventajas de la Integración.

1. **Capacidad de respuesta mejorada:** Al combinar el análisis detallado de los IDS con las capacidades de bloqueo de los *firewalls*, las organizaciones pueden mitigar rápidamente amenazas avanzadas como ataques persistentes avanzados (APT) y exfiltración de datos. Por ejemplo si un IDS detecta una comunicación maliciosa que intenta eludir las políticas de seguridad, puede notificar al *firewall* para bloquear la IP en tiempo real.
2. **Alertas en tiempo real y ajuste dinámico:** Los IDS generan alertas que pueden ser utilizadas por los *firewalls* para ajustar dinámicamente las políticas, asegurando que las redes estén protegidas frente a ataques en evolución. Por ejemplo un ataque de denegación de servicio (DoS), el IDS puede identificar el origen del tráfico malicioso y comunicarlo al *firewall* para bloquear automáticamente ese origen.

3. **Defensa en profundidad:** La integración crea múltiples capas de protección, dificultando que los atacantes exploten vulnerabilidades o eludan las medidas de seguridad. Esto incluye la protección contra ataques internos y externos, así como amenazas emergentes.

3. Consideraciones para la Implementación.

1. **Compatibilidad de herramientas:** Es esencial garantizar que el IDS y el *firewall* sean compatibles y puedan comunicarse eficazmente mediante protocolos como Syslog, SNMP o APIs específicas.
2. **Balance entre rendimiento y seguridad:** La integración puede aumentar la carga en ambos sistemas, especialmente si el IDS genera un gran número de alertas. Es crucial establecer umbrales y filtros para evitar falsas alarmas.
3. **Capacitación del equipo de seguridad:** El personal debe ser capacitado para interpretar las alertas generadas por el IDS y ajustar las políticas del *firewall* según sea necesario.

En la siguiente table se muestra una comparativa entre los *Firewall* tradicionales y los integrados con un IDS.

Aspecto	Solo Firewall	Integración IDS-Firewall
Cobertura de amenazas	Bloquea amenazas conocidas mediante reglas predefinidas.	Detecta y responde a amenazas avanzadas, incluso si no están predefinidas.
Respuesta a ataques	Estática; requiere intervención manual para ajustes.	Dinámica; ajusta las políticas del firewall automáticamente en tiempo real.
Visibilidad de la red	Limitada al tráfico que coincide con las reglas.	Análisis profundo de tráfico y comportamiento, proporcionando mayor visibilidad.
Capacidad de escalamiento	Limitada frente a ataques complejos.	Escalable; identifica y responde a múltiples vectores de ataque simultáneamente.

Tabla 3-5. Comparación: *Firewall* vs. Integración IDS-*Firewall*.

La integración entre IDS y *firewalls* es una práctica esencial en la ciberseguridad moderna, ya que combina la capacidad de los *firewalls* para bloquear tráfico con la inteligencia de los IDS para detectar patrones maliciosos avanzados. Este enfoque sinérgico permite a las organizaciones mitigar rápidamente ataques en evolución, ajustar dinámicamente las políticas de seguridad y fortalecer la defensa en profundidad.

3.1.5 Otras Soluciones de Seguridad.

La protección del Sistema de Nombres de Dominio es esencial para garantizar la disponibilidad, integridad y privacidad de los servicios en línea. Implementar medidas de seguridad que no requieran modificar los protocolos DNS permite una protección inmediata y efectiva. A continuación, se describen soluciones prácticas, rápidas y ampliamente utilizadas.

3.1.5.1 Filtrado DNS.

El filtrado DNS [97] es una técnica de ciberseguridad que consiste en bloquear consultas DNS relacionadas con dominios maliciosos o sospechosos. Este sistema actúa como una primera línea de defensa para prevenir amenazas como malware, phishing y botnets. El filtrado se basa en el uso de listas negras, también conocidas como “blacklists”, que contienen dominios asociados con actividades maliciosas. Estas listas pueden ser mantenidas por proveedores de servicios DNS, organizaciones de ciberseguridad o comunidades de código abierto.

El objetivo principal del filtrado DNS es proteger a los usuarios y sistemas de interactuar con dominios malintencionados al detener las consultas DNS antes de que puedan resolverse en direcciones IP. Esto asegura que los dispositivos conectados no establezcan comunicación con servidores que representen un riesgo de seguridad.

Funcionamiento.

El filtrado DNS opera interceptando las solicitudes que realizan los dispositivos al Sistema de Nombres de Dominio. Cada vez que un dispositivo intenta acceder a un dominio (por ejemplo, www.ejemplo.com), realiza una consulta al resolver DNS configurado. Si el dominio está en una lista negra, el resolver DNS bloquea la solicitud, devolviendo un mensaje de error o redirigiendo al usuario a una página de advertencia.

1. **Resolveres DNS configurados con listas negras:** Los *resolver* están configurados para consultar bases de datos que contienen listas de dominios maliciosos. Estas listas pueden incluir dominios asociados con:
 - o Distribución de *malware*.
 - o Campañas de *phishing*.
 - o Control y comando de *botnets*.
 - o Contenidos inapropiados o riesgosos.
2. **Listas negras dinámicas:** Las listas negras son actualizadas continuamente por los proveedores de servicios de filtrado DNS. Las actualizaciones se basan en análisis automatizados, inteligencia de amenazas y reportes de usuarios o investigadores de ciberseguridad.
3. **Bloqueo o redirección:** Cuando un dominio sospechoso es detectado, el sistema puede:
 - o Bloquear la conexión devolviendo una respuesta negativa al cliente.
 - o Redirigir al usuario a una página de advertencia o a una dirección IP segura, explicando el motivo del bloqueo.

Ejemplos de Implementación.

1. **Cisco Umbrella [98]:** Cisco Umbrella es uno de los servicios más conocidos de filtrado DNS. Ofrece protección contra amenazas en tiempo real, utilizando inteligencia de amenazas para identificar dominios maliciosos antes de que puedan ser explotados. Este servicio está diseñado para empresas y permite políticas de control de acceso basadas en la ubicación o el tipo de dispositivo.
2. **Quad9:** Quad9 es un servicio de resolución DNS gratuito que integra filtrado de dominios maliciosos utilizando fuentes de inteligencia de múltiples organizaciones. Además, protege la privacidad del usuario al no registrar las direcciones IP de las consultas realizadas.
3. **Google Safe Browsing [99] y OpenDNS:** Google Safe Browsing utiliza datos de inteligencia para proteger a los usuarios de dominios asociados con ataques de phishing y distribución de malware. OpenDNS, ahora parte de Cisco, proporciona servicios de resolución DNS seguros y configurables.

4. **Pi-hole [100]:** Pi-hole es una herramienta de código abierto que actúa como un filtro DNS local. Está diseñado para bloquear anuncios y rastreadores, pero también puede configurarse para filtrar dominios maliciosos mediante listas negras personalizadas.

Ventajas.

1. **No requiere cambios en el protocolo:** El filtrado DNS opera utilizando los estándares existentes del sistema DNS, lo que facilita su adopción sin necesidad de modificar la infraestructura de red subyacente.
2. **Fácil implementación:** Configurar un *resolver* para utilizar listas negras o servicios de filtrado es un proceso sencillo. Solo requiere actualizar las configuraciones DNS en los dispositivos o enrutadores.
3. **Eficiencia en la protección:** El filtrado DNS bloquea las amenazas en su etapa inicial, antes de que los usuarios puedan interactuar con dominios peligrosos, reduciendo el riesgo de infección y compromisos en la red.
4. **Coste accesible:** Muchos servicios de filtrado DNS, como Quad9, ofrecen opciones gratuitas o de bajo costo, lo que los hace accesibles para empresas pequeñas y usuarios domésticos.

Retos y Desafíos.

A pesar de sus ventajas, el filtrado DNS tiene algunas limitaciones:

- **Falsos positivos:** Algunos dominios legítimos pueden ser bloqueados erróneamente debido a listas negras inexactas.
- **Dependencia de listas negras:** La efectividad del filtrado depende de la actualización constante y la precisión de las listas.
- **Protección limitada:** El filtrado DNS no protege contra ataques que no utilicen nombres de dominio, como aquellos que operan directamente con direcciones IP.

3.1.5.2 Implementación de Anycast DNS.

El modelo Anycast DNS [101] es una tecnología ampliamente utilizada para mejorar la distribución y eficiencia de las consultas DNS a nivel global. Anycast asigna una única dirección IP a múltiples servidores distribuidos en diferentes ubicaciones geográficas. Esto permite que una consulta DNS sea respondida por el servidor más cercano al origen de la solicitud, reduciendo la latencia y optimizando los tiempos de respuesta.

En un entorno Anycast, los servidores que comparten la misma dirección IP están diseñados para responder a solicitudes DNS de forma autónoma, permitiendo una distribución dinámica de la carga de trabajo. Esta tecnología es especialmente valiosa para mitigar los efectos de ataques de denegación de servicio distribuido (DDoS), mejorar la disponibilidad del sistema y garantizar una experiencia de usuario más rápida y segura.

Funcionamiento.

La implementación de Anycast en un sistema DNS requiere la configuración de múltiples servidores con la misma dirección IP pública y el uso de protocolos avanzados de enrutamiento, como el Border Gateway Protocol (BGP). A continuación, se detalla el funcionamiento de esta tecnología:

1. **Dirección única, múltiples servidores:** En un modelo Anycast, una única dirección IP está asociada a varios servidores DNS distribuidos estratégicamente en diversas ubicaciones geográficas. Cada servidor actúa como una réplica de los demás, almacenando información idéntica para responder a las consultas DNS.

2. **Selección del servidor más cercano:** Cuando un usuario realiza una consulta DNS, los rúteres BGP analizan las rutas disponibles y redirigen la solicitud al servidor más cercano desde el punto de vista de la red. La proximidad no se mide necesariamente en términos geográficos, sino en función del menor número de saltos de red, asegurando tiempos de respuesta más rápidos.
3. **Distribución del tráfico:** Al dispersar las consultas DNS entre varios servidores, Anycast equilibra la carga de trabajo, optimizando la utilización de los recursos y evitando la saturación de un único servidor. En caso de que uno de los servidores falle o quede inaccesible, las consultas se redirigen automáticamente al siguiente servidor disponible.
4. **Resiliencia frente a fallos:** Si un servidor deja de estar operativo, el sistema Anycast lo elimina automáticamente de las rutas activas. Esto asegura que las consultas continúen siendo atendidas por otros servidores en funcionamiento, garantizando la disponibilidad del servicio.

Beneficios de Anycast.

1. **Resiliencia frente a ataques DDoS:** Una de las principales ventajas de Anycast es su capacidad para mitigar los ataques de denegación de servicio distribuido. Al dispersar el tráfico malicioso entre múltiples servidores, se reduce el impacto en cualquier servidor individual, evitando que el sistema colapse. Esto dificulta que un atacante concentre su esfuerzo en un único objetivo.
2. **Mejora de los tiempos de respuesta:** Gracias a la redirección de consultas al servidor más cercano, los usuarios experimentan tiempos de respuesta más rápidos. Esto es especialmente importante en servicios críticos como plataformas de comercio electrónico, aplicaciones financieras y servicios en tiempo real.
3. **Alta disponibilidad:** La redundancia inherente al sistema Anycast asegura que las consultas sean atendidas incluso si uno o más servidores fallan. Esto hace que el sistema sea más fiable y resistente a interrupciones.
4. **Eficiencia en la distribución del tráfico:** Al equilibrar la carga de trabajo entre múltiples servidores, Anycast mejora la eficiencia operativa, evitando la saturación de recursos y permitiendo una escalabilidad más efectiva.
5. **Optimización del rendimiento global:** Los usuarios finales disfrutan de una experiencia más rápida y consistente, independientemente de su ubicación, lo que mejora la percepción del servicio.

Desafíos y Consideraciones.

1. **Configuración compleja:** Implementar Anycast requiere conocimientos avanzados de enrutamiento y redes, así como una infraestructura bien diseñada para garantizar su efectividad.
2. **Costes asociados:** Mantener una red Anycast global puede ser costoso, especialmente para pequeñas empresas o proyectos con presupuestos limitados.
3. **Enrutamiento ineficiente en casos específicos:** En situaciones excepcionales, las rutas de red podrían llevar a que una consulta se desvíe a un servidor más lejano, lo que podría afectar el tiempo de respuesta.

3.1.5.3 Monitorización y Análisis de Tráfico DNS.

La monitorización y el análisis del tráfico DNS [102] es una estrategia esencial en ciberseguridad, diseñada para identificar patrones anómalos o comportamientos sospechosos que puedan indicar la presencia de amenazas o actividades maliciosas. Dado que el Sistema de Nombres de Dominio es una infraestructura crítica para el funcionamiento de Internet, los atacantes a menudo lo utilizan como un vector para realizar actividades ilícitas como exfiltración de datos, ataques de denegación de servicio distribuido y comunicación con servidores de comando y control (C&C).

Este proceso implica la supervisión en tiempo real de las consultas DNS generadas dentro de una red, así como el análisis histórico para detectar tendencias o patrones que puedan ser indicativos de ataques en curso o preparativos para futuros compromisos. La monitorización permite no solo identificar problemas existentes, sino también predecir y prevenir posibles amenazas antes de que puedan causar un daño significativo.

Funcionamiento.

El proceso de monitorización y análisis del tráfico DNS puede dividirse en varias etapas:

1. **Captura del tráfico DNS:** Los paquetes de datos que contienen consultas y respuestas DNS son capturados mediante herramientas de análisis de red, como Zeek (anteriormente conocido como Bro) o Wireshark. Estos paquetes son luego procesados para extraer información relevante, como el dominio solicitado, la dirección IP del cliente, y los servidores DNS involucrados.
2. **Análisis en tiempo real:** Las consultas DNS se analizan mientras son generadas, comparándolas con listas negras de dominios maliciosos, patrones de actividad sospechosa o configuraciones predeterminadas. Por ejemplo, un alto número de solicitudes a dominios desconocidos puede ser un signo de actividad de *malware*.
3. **Establecimiento de *baselines*:** Se crea un perfil normalizado del comportamiento del tráfico DNS en la red. Esto incluye datos sobre el volumen promedio de consultas, los dominios más visitados y los tiempos habituales de actividad. Los desvíos significativos de este perfil pueden ser indicativos de amenazas.
4. **Detección de anomalías:** Los datos capturados se procesan mediante técnicas de análisis avanzado, como aprendizaje automático o algoritmos heurísticos, para identificar comportamientos inusuales que puedan ser indicativos de actividades maliciosas.
5. **Generación de alertas y reportes:** Cuando se detectan anomalías, el sistema genera alertas que son enviadas a los administradores de seguridad. Los reportes detallados permiten tomar medidas correctivas rápidas y fundamentadas.

Ventajas.

1. **Detección temprana de amenazas:** La supervisión del tráfico DNS en tiempo real permite identificar actividades maliciosas antes de que puedan comprometer los sistemas. Por ejemplo, detectar un volumen inusualmente alto de consultas hacia dominios sospechosos puede indicar un ataque en progreso.
2. **Prevención de exfiltración de datos:** Los atacantes suelen utilizar el DNS como canal para filtrar información confidencial desde una red comprometida hacia el exterior. La monitorización activa puede identificar este tipo de actividad al detectar consultas DNS inusuales, como aquellas que contienen datos codificados en la consulta.
3. **Identificación de comunicación con servidores C&C:** Muchas *botnets* y *malware* se comunican con sus servidores de comando y control utilizando el DNS. Analizar el tráfico puede revelar consultas repetitivas hacia dominios asociados con actividades maliciosas, permitiendo a los administradores interrumpir la comunicación entre el *malware* y sus controladores.
4. **Optimización del rendimiento de la red:** Más allá de la seguridad, el análisis del tráfico DNS ayuda a mejorar el rendimiento de la red al identificar cuellos de botella, mal uso de recursos o configuraciones incorrectas.
5. **Cumplimiento normativo:** Algunas normativas de ciberseguridad, como el GDPR en Europa o el CCPA en Estados Unidos, requieren que las organizaciones tengan controles para proteger los datos de los usuarios. La monitorización DNS puede ayudar a cumplir con estos requisitos al detectar posibles fugas de información.

Herramientas de Monitorización y Análisis de DNS.

1. **Zeek (Bro)** [103]: Zeek es una plataforma de análisis de tráfico de red altamente escalable y flexible. Aunque inicialmente fue desarrollada como una herramienta de detección de intrusos, su capacidad para analizar protocolos como DNS lo convierte en una opción ideal para la supervisión y el análisis del tráfico DNS. Zeek permite identificar patrones de comportamiento anómalos y genera registros detallados que los administradores pueden usar para investigaciones posteriores.
2. **Splunk** [104]: Splunk es una solución comercial ampliamente utilizada para el análisis y visualización de datos de eventos en tiempo real. Con Splunk, las organizaciones pueden centralizar y analizar registros DNS, identificar consultas anómalas y correlacionarlas con otros eventos de seguridad. Además, Splunk ofrece herramientas de aprendizaje automático para automatizar la detección de amenazas.
3. **Wireshark** [105]: Aunque no está diseñado específicamente para DNS, Wireshark es una herramienta poderosa para capturar y analizar paquetes de red. Permite a los administradores inspeccionar consultas DNS específicas, identificar patrones sospechosos y realizar análisis forenses detallados.
4. **DNS Query Analytics (DQAnal)** [106]: Esta herramienta está diseñada específicamente para el análisis detallado del tráfico DNS, ayudando a identificar consultas relacionadas con exfiltración de datos, bots o malware.
5. **OpenDNS Umbrella** [107]: Una solución basada en la nube que combina filtrado DNS y análisis en tiempo real. OpenDNS ofrece un enfoque preventivo, bloqueando dominios maliciosos antes de que puedan ser accedidos, y proporciona informes detallados sobre el tráfico DNS.

Retos y Desafíos.

1. **Volumen de datos:** En redes grandes, el volumen de tráfico DNS puede ser enorme, lo que dificulta el análisis en tiempo real. Las herramientas deben ser lo suficientemente robustas para manejar estos volúmenes sin comprometer el rendimiento.
2. **Falsos positivos:** Es posible que algunas consultas legítimas sean clasificadas erróneamente como sospechosas, lo que puede generar interrupciones innecesarias en el servicio.
3. **Complejidad en la configuración:** Configurar y mantener una solución efectiva de monitorización DNS requiere experiencia técnica avanzada y recursos dedicados.
4. **Evolución de las amenazas:** Los atacantes están constantemente desarrollando técnicas más sofisticadas para evadir la detección, lo que obliga a las herramientas de análisis a evolucionar continuamente.

3.1.5.4 Resolver DNS Privados y Confiables.

Los *resolver* DNS privados y confiables [108] son servicios diseñados para proporcionar una resolución de nombres de dominio segura y eficiente, incorporando características avanzadas de ciberseguridad. Estos *resolver* actúan como intermediarios entre los dispositivos de los usuarios y los servidores DNS autorizados, traduciendo nombres de dominio en direcciones IP legibles por máquinas.

Lo que distingue a los *resolver* privados y confiables es su capacidad para implementar medidas de seguridad adicionales, como el bloqueo de dominios maliciosos basados en inteligencia de amenazas, protección contra ataques de envenenamiento de caché DNS y la adopción de protocolos modernos como DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT). Además, estos *resolver* suelen garantizar la privacidad de los usuarios mediante políticas estrictas de no registro, evitando que las consultas DNS sean almacenadas o compartidas con terceros.

En un contexto donde las amenazas cibernéticas evolucionan rápidamente, los *resolver* DNS confiables se han convertido en una herramienta esencial para proteger tanto a individuos como a organizaciones frente a ataques dirigidos al sistema DNS.

Funcionamiento.

El proceso de resolución de nombres a través de estos *resolver* sigue los pasos básicos del sistema DNS, pero incorpora medidas de seguridad avanzadas:

1. **Recepción de la consulta DNS:** Cuando un usuario realiza una solicitud para acceder a un dominio, esta es enviada al *resolver* DNS configurado en su dispositivo o red. Los *resolver* confiables, como Google Public DNS o Quad9, interceptan esta consulta.
2. **Análisis de seguridad:** Antes de resolver la consulta, el *resolver* analiza el dominio solicitado, comparándolo con bases de datos de inteligencia de amenazas actualizadas. Si el dominio es identificado como malicioso (por ejemplo, relacionado con *phishing*, *malware* o *botnets*), la consulta es bloqueada, y el usuario puede ser redirigido a una página de advertencia.
3. **Resolución segura:** Si el dominio es legítimo, el *resolver* lo traduce a una dirección IP consultando los servidores DNS autorizados y devuelve la respuesta al dispositivo del usuario. Este proceso incluye medidas para prevenir el envenenamiento de caché, asegurando que las respuestas no hayan sido manipuladas.
4. **Privacidad de las consultas:** Para proteger la privacidad del usuario, muchos *resolver* privados utilizan protocolos cifrados como DNS sobre HTTPS (DoH) o DNS sobre TLS (DoT). Estos protocolos encriptan las consultas DNS, impidiendo que terceros puedan interceptar o registrar el tráfico.

Ventajas.

1. **Bloqueo de dominios maliciosos:** Los *resolver* DNS confiables utilizan bases de datos de inteligencia de amenazas actualizadas para bloquear el acceso a dominios asociados con actividades maliciosas, como distribución de *malware*, *phishing* o servidores de comando y control (C&C). Esto reduce significativamente el riesgo de compromisos.
2. **Protección contra ataques de envenenamiento de caché DNS:** Los ataques de envenenamiento de caché buscan manipular las respuestas DNS para redirigir a los usuarios hacia sitios web fraudulentos. Los *resolver* confiables mitigan este riesgo mediante la validación de las respuestas DNS y el uso de características como la aleatorización de puertos de origen.
3. **Privacidad del usuario:** Servicios como Quad9 y Cloudflare garantizan que las consultas DNS no sean registradas ni compartidas con terceros, protegiendo así la privacidad del usuario y evitando que sus hábitos de navegación sean utilizados con fines comerciales.
4. **Velocidad y eficiencia:** Los *resolveres* privados y confiables suelen contar con infraestructuras optimizadas y distribuidas geográficamente, lo que reduce la latencia y mejora los tiempos de resolución DNS.
5. **Compatibilidad con tecnologías modernas:** El soporte para protocolos como DoH y DoT garantiza que las consultas DNS estén protegidas contra la interceptación, incluso en redes inseguras como Wi-Fi públicas.
6. **Fácil implementación:** Configurar un *resolver* confiable es un proceso sencillo que solo requiere actualizar las configuraciones DNS en el dispositivo o enrutador.

Retos y Desafíos.

1. **Dependencia de terceros:** Aunque los *resolveres* confiables ofrecen muchas ventajas, el uso de servicios de terceros implica confiar en sus políticas de privacidad y prácticas de seguridad.
2. **Falsos positivos:** En ocasiones, los dominios legítimos pueden ser bloqueados erróneamente debido a listas negras mal gestionadas, lo que puede afectar la productividad de los usuarios.
3. **Requerimientos de configuración:** Para aprovechar plenamente los beneficios de los *resolveres* confiables, los administradores de red deben asegurarse de que los dispositivos y enrutadores estén configurados correctamente.

3.1.5.5 Configuración Segura de Servidores DNS.

La configuración segura de los servidores DNS, tanto autorizados como *resolver*, es un componente fundamental en la ciberseguridad de las infraestructuras de red. Esta práctica implica la aplicación de ajustes y medidas específicas que buscan minimizar vulnerabilidades explotables por atacantes, como el envenenamiento de caché, ataques de denegación de servicio o accesos no autorizados.

Medidas de Configuración Segura.

1. **Deshabilitar la Recursividad en Servidores Autorizados [109]:** Los servidores DNS autorizados, responsables de responder consultas específicas sobre dominios que controlan, no necesitan resolver otras consultas fuera de su ámbito. Dejar la recursividad habilitada en estos servidores puede abrir una puerta a ataques, como el envenenamiento de caché y el abuso para amplificar ataques DDoS.
 - o **Cómo implementarlo:** Configurar el servidor DNS para que solo responda a consultas relacionadas con los dominios que gestiona y rechace solicitudes de resolución recursiva. Por ejemplo:
 - En servidores BIND, la opción `recursion no;` en el archivo de configuración deshabilita esta funcionalidad.
 - o **Beneficios:**
 - Reduce la superficie de ataque al limitar las funcionalidades del servidor.
 - Previene el abuso de servidores autorizados en ataques de amplificación.
2. **Configurar Restricciones Basadas en IP para Clientes Autorizados [110]:** Restringir el acceso a servidores DNS recursivos solo a clientes confiables es una medida clave para evitar el uso indebido. Esto incluye configurar listas blancas de direcciones IP que tengan permiso para enviar consultas.
 - o **Cómo implementarlo:** Utilizar reglas de acceso para permitir consultas solo desde direcciones IP específicas, como redes internas o socios confiables. Por ejemplo:
 - En BIND, la directiva `allow-query` permite definir qué direcciones IP pueden realizar consultas.
 - o **Beneficios:**
 - Protege contra abusos de resolución DNS desde redes externas.
 - Minimiza el riesgo de que el servidor sea utilizado en ataques distribuidos.
3. **Implementar Tiempos de Vida (TTL) Ajustados [111]:** Los valores de TTL determinan cuánto tiempo las respuestas DNS permanecen almacenadas en la caché de *resolver*. Configurar TTLs más cortos puede ayudar a mitigar el impacto de ataques de envenenamiento de caché al reducir el tiempo en que las entradas alteradas pueden afectar a los usuarios.
 - o **Cómo implementarlo:** Ajustar los valores de TTL para dominios críticos según el equilibrio entre seguridad y rendimiento. Un TTL de entre 5 y 15 minutos es una práctica común para dominios sensibles.
 - o **Beneficios:**
 - Limita la duración de datos potencialmente corruptos en caché.
 - Permite actualizaciones rápidas en caso de cambios en los registros DNS.
4. **Habilitar DNSSEC:** DNSSEC es una extensión que añade firmas digitales a las respuestas DNS para autenticar su origen y garantizar que no hayan sido manipuladas en tránsito. Implementar DNSSEC en servidores autorizados es una medida esencial para proteger contra el envenenamiento de caché.

- o **Cómo implementarlo:** Configurar las claves criptográficas necesarias y firmar digitalmente los registros DNS. Esto se puede lograr utilizando herramientas integradas en servidores como BIND o NSD.
 - o **Beneficios:**
 - Asegura la integridad y autenticidad de las respuestas DNS.
 - Proporciona protección robusta contra ataques de *spoofing*.
5. **Monitoreo y Registro Activo:** Habilitar el registro detallado de actividades en los servidores DNS permite identificar patrones anómalos o intentos de explotación en tiempo real.
- o **Cómo implementarlo:** Configurar niveles avanzados de registro (*logging*) en servidores DNS como BIND para capturar información sobre consultas, respuestas y posibles errores.
 - o **Beneficios:**
 - Facilita la detección temprana de ataques.
 - Proporciona datos para análisis forense en caso de incidentes.

Ventajas.

1. **Mejora Inmediata de la Seguridad Operativa:** Las configuraciones seguras ofrecen una protección efectiva sin necesidad de modificar protocolos o implementar tecnologías completamente nuevas. Esto permite a las organizaciones responder rápidamente a las amenazas.
2. **Reducción de la Superficie de Ataque:** Limitar las funcionalidades no esenciales de los servidores DNS y aplicar restricciones basadas en IP reduce las oportunidades para que los atacantes exploten las vulnerabilidades.
3. **Prevención de Abusos en Ataques Distribuidos:** Configurar límites y controles adecuados asegura que los servidores DNS no puedan ser utilizados como herramientas en ataques DDoS de amplificación.
4. **Mitigación de Amenazas Conocidas:** Prácticas como la desactivación de la recursividad y la implementación de DNSSEC ayudan a prevenir amenazas bien documentadas, como el envenenamiento de caché y ataques de suplantación.
5. **Cumplimiento Normativo:** Muchas normativas de ciberseguridad, como el GDPR y el CCPA, exigen la protección adecuada de las infraestructuras críticas. Las configuraciones seguras ayudan a las organizaciones a cumplir con estos requisitos.

Caso de Éxito: Caso de Google Public DNS.

Google Public DNS es un ejemplo destacado de un resolver DNS configurado de manera segura. Este servicio ha implementado técnicas avanzadas, como:

- **DNSSEC:** Garantizando la autenticidad de las respuestas DNS.
- **Políticas de acceso:** Permitiendo consultas solo desde redes confiables.
- **Mitigación contra DDoS:** Usando redes Anycast para dispersar el tráfico malicioso.

Estas medidas han convertido a Google Public DNS en un estándar de referencia para resolvers seguros.

3.1.5.6 Actualización y Mantenimiento Regular del Software DNS.

El software que impulsa los servidores DNS, como cualquier otra tecnología, requiere actualizaciones y mantenimiento regular para garantizar su seguridad, estabilidad y eficiencia. Mantener el software actualizado es una medida fundamental para proteger los servidores DNS de vulnerabilidades conocidas que puedan ser explotadas por atacantes. Además, las actualizaciones suelen incluir mejoras en el rendimiento, nuevas características y soluciones a problemas detectados en versiones anteriores.

Actualizar regularmente el software [112] de los servidores DNS no solo protege contra amenazas externas, sino que también asegura que el sistema se mantenga alineado con los estándares de la industria y las mejores prácticas en ciberseguridad.

Importancia de la Actualización Regular.

1. **Protección contra Vulnerabilidades Conocidas:** Los atacantes suelen aprovechar vulnerabilidades conocidas en el software DNS para ejecutar ataques. Los proveedores de software, como ISC (para BIND) o Microsoft (para Microsoft DNS Server), publican parches para abordar estas vulnerabilidades. No aplicar estas actualizaciones deja a los servidores expuestos a riesgos evitables.
2. **Cumplimiento de Normativas de Seguridad:** Muchas regulaciones, como el Reglamento General de Protección de Datos (GDPR) [122] en Europa o el estándar PCI DSS [123] para datos de tarjetas de pago, exigen que las organizaciones mantengan su software actualizado como parte de las medidas de seguridad obligatorias.
3. **Compatibilidad con Nuevos Protocolos:** Las actualizaciones también incluyen soporte para nuevos protocolos o estándares, como DNS over HTTPS (DoH) o DNS over TLS (DoT), que mejoran la privacidad y seguridad del DNS.
4. **Optimización del Rendimiento:** Los proveedores de software frecuentemente implementan mejoras en el rendimiento en las nuevas versiones, lo que permite que los servidores DNS procesen las consultas más rápido y con mayor eficiencia.
5. **Reducción de Riesgos Operativos:** Las actualizaciones también corrigen errores o *bugs* en el software que podrían causar interrupciones o inestabilidad en el servicio DNS.

Mantenimiento Regular del Software DNS.

El mantenimiento no se limita únicamente a las actualizaciones; también implica prácticas regulares para garantizar que el servidor funcione de manera óptima:

1. **Auditorías de Seguridad Periódicas:** Realizar evaluaciones regulares para identificar configuraciones incorrectas o vulnerabilidades en el software DNS.
2. **Monitoreo Continuo:** Implementar sistemas de monitoreo para detectar actividades anómalas o fallos en el servidor DNS en tiempo real.
3. **Pruebas de Compatibilidad:** Antes de implementar actualizaciones en un entorno de producción, es esencial realizar pruebas en un entorno controlado para garantizar que las nuevas versiones sean compatibles con la infraestructura existente.
4. **Documentación y Capacitación:** Mantener un registro actualizado de todas las actualizaciones aplicadas y capacitar al personal de TIC en las mejores prácticas para la gestión de servidores DNS.

Ventajas de Mantener el Software DNS Actualizado.

1. **Protección Contra Amenazas Evolutivas:** A medida que las amenazas cibernéticas evolucionan, los proveedores de software responden con actualizaciones que mitigan riesgos conocidos. Aplicar estos parches asegura que los servidores estén protegidos contra los vectores de ataque más recientes.

2. **Conformidad con Estándares de Seguridad:** Las actualizaciones mantienen los servidores alineados con los estándares de la industria, como DNSSEC, DoH y DoT, que refuerzan la seguridad y privacidad en las comunicaciones DNS.
3. **Reducción de Costes por Incidentes:** Resolver problemas de seguridad después de un ataque puede ser costoso. La actualización regular del software reduce significativamente el riesgo de incidentes, minimizando costes asociados con interrupciones, recuperación y daño reputacional.
4. **Mejoras en la Eficiencia Operativa:** Los servidores actualizados suelen ser más rápidos y estables, lo que beneficia tanto a los usuarios finales como a los administradores de sistemas.
5. **Preparación para el Futuro:** Los avances tecnológicos, como IPv6, requieren servidores DNS que estén equipados para manejar estas transiciones. Las actualizaciones aseguran que los servidores estén listos para estos cambios.

Ejemplo: Actualización de Servidores DNS.

1. **BIND (*Berkeley Internet Name Domain*)** [113]: Uno de los servidores DNS más utilizados a nivel mundial. La *Internet Systems Consortium* (ISC), responsable de su desarrollo, publica actualizaciones periódicas para corregir vulnerabilidades y mejorar su funcionalidad. Por ejemplo, la versión más reciente incluye soporte mejorado para DNSSEC y medidas contra ataques de amplificación.
2. **Unbound** [114]: Este servidor DNS de código abierto es conocido por su rendimiento y seguridad. Las actualizaciones de Unbound suelen incluir mejoras en la validación de DNSSEC, soporte para DoH y DoT, y parches de seguridad para abordar vulnerabilidades descubiertas.
3. **Microsoft DNS Server** [115]: Incluido en las plataformas de Windows Server, Microsoft DNS Server recibe actualizaciones regulares como parte del ciclo de parches de Windows. Estas actualizaciones a menudo corrigen vulnerabilidades críticas y mejoran la compatibilidad con servicios en la nube.

Desafíos y Consideraciones.

1. **Interrupciones Temporales:** La aplicación de actualizaciones puede requerir reinicios del servidor, lo que podría interrumpir temporalmente el servicio si no se planifica adecuadamente.
2. **Compatibilidad con Infraestructuras Existentes:** Algunas actualizaciones podrían no ser compatibles con configuraciones o software heredados, lo que podría requerir ajustes adicionales.
3. **Falta de Automatización:** En entornos grandes, actualizar manualmente múltiples servidores DNS puede ser una tarea compleja y propensa a errores.
4. **Falsos Sentimientos de Seguridad:** Aunque las actualizaciones son esenciales, no reemplazan otras medidas de seguridad, como la configuración adecuada del servidor y el monitoreo continuo.

3.1.5.7 Importancia de la Concienciación en Seguridad DNS.

La educación y concienciación de los usuarios en seguridad DNS [116] es un componente crítico para proteger las infraestructuras digitales de organizaciones y empresas. Aunque las tecnologías avanzadas como *firewalls*, *resolver* confiables y medidas de mitigación de ataques son esenciales, los usuarios siguen siendo el eslabón más vulnerable en la cadena de seguridad. Los errores humanos, como la falta de atención a señales de advertencia o la interacción inadvertida con sitios web maliciosos, son responsables de una gran proporción de los incidentes de ciberseguridad.

En el contexto del DNS, la concienciación implica entrenar a los usuarios para reconocer consultas sospechosas, identificar patrones de comportamiento malintencionados y comprender los riesgos asociados con interacciones inseguras. Esto incluye no solo al personal técnico, sino también a empleados de todos los niveles, ya que los atacantes a menudo dirigen sus esfuerzos hacia individuos con acceso limitado al conocimiento técnico pero con privilegios de acceso significativos.

La concienciación debe abarcar conceptos clave, como el papel del DNS en la red, cómo los atacantes pueden explotarlo (por ejemplo, a través del *phishing* o el envenenamiento de caché), y cómo las prácticas seguras pueden reducir estos riesgos. También debe incluir formación específica para personal técnico, como la configuración segura de *resolver* y la implementación de políticas DNS robustas.

Importancia de la Concienciación en Seguridad DNS. [117]

1. **El Factor Humano en la Seguridad:** Los usuarios son a menudo el objetivo principal de los ciberataques. La ingeniería social y las técnicas como el *phishing* dependen de la falta de conocimiento o atención de los individuos. Educar a los usuarios para reconocer señales de advertencia, como direcciones URL sospechosas o correos electrónicos que solicitan información confidencial, reduce significativamente el riesgo de ataques exitosos.
2. **Reducción de Riesgos Asociados a Errores Humanos:** Los errores humanos, como la mala configuración de *resolver* DNS, la falta de actualización del software o el uso de prácticas inseguras, pueden comprometer la seguridad del sistema. La educación y capacitación ayudan a minimizar estos errores al promover buenas prácticas.
3. **Fortalecimiento de la Seguridad Organizacional:** Cuando los empleados están capacitados para identificar y responder a actividades sospechosas, la organización en su conjunto se beneficia de una defensa más sólida contra amenazas cibernéticas.
4. **Cumplimiento Normativo:** Muchas regulaciones de ciberseguridad, como el GDPR y el CCPA, exigen que las organizaciones eduquen a sus empleados en prácticas seguras. Implementar programas de concienciación ayuda a cumplir con estos requisitos legales.

Metodologías de Educación y Concienciación.

1. **Talleres y Seminarios para Personal Técnico:** La formación del personal técnico debe incluir conceptos avanzados sobre la seguridad DNS. Los talleres pueden cubrir temas como:
 - o Configuración segura de *resolver*, incluyendo la deshabilitación de recursividad en servidores autorizados y la implementación de DNSSEC.
 - o Gestión y monitorización de consultas DNS para detectar actividades anómalas.
 - o Respuesta a incidentes relacionados con ataques de DNS, como el envenenamiento de caché o los ataques DDoS.
2. **Capacitación General para Todos los Empleados:** La formación general debe enfocarse en enseñar a los empleados a identificar comportamientos sospechosos y comprender la importancia del DNS en la seguridad general. Ejemplos de temas incluyen:
 - o Cómo identificar correos electrónicos o enlaces sospechosos que puedan redirigir a dominios maliciosos.
 - o Importancia de reportar actividades sospechosas al equipo de TIC.
3. **Simulaciones de Ataques:** Las simulaciones son una forma efectiva de entrenar a los usuarios para que reconozcan ataques en un entorno controlado. Por ejemplo, una simulación de *phishing* puede ayudar a los empleados a identificar señales de advertencia en correos electrónicos maliciosos.

4. **Políticas de Seguridad Claras y Accesibles:** Las políticas de seguridad deben ser comunicadas de manera efectiva para que todos los empleados comprendan su papel en la protección de la infraestructura DNS. Esto incluye directrices sobre el uso seguro de redes y la gestión de accesos.
5. **Plataformas de Aprendizaje en Línea:** Las herramientas de aprendizaje en línea permiten a los empleados acceder a materiales educativos en su propio tiempo. Estas plataformas pueden incluir videos, cuestionarios interactivos y escenarios prácticos relacionados con la seguridad DNS.

Beneficios de la Educación y la Concienciación.

1. **Reducción del Riesgo Global:** Una fuerza laboral educada es menos propensa a caer en ataques de *phishing* o comprometer la infraestructura DNS debido a errores de configuración o falta de conocimiento.
2. **Mejora de la Respuesta a Incidentes:** Los empleados capacitados pueden reconocer y reportar actividades sospechosas de manera más efectiva, lo que permite a los equipos de seguridad responder más rápido.
3. **Aumento de la Resiliencia Organizacional:** Al crear una cultura de seguridad, la organización puede enfrentar amenazas cibernéticas con mayor confianza y preparación.
4. **Cumplimiento de Estándares de Seguridad:** Los programas de educación y concienciación ayudan a las empresas a cumplir con normativas y estándares de ciberseguridad, evitando sanciones legales.
5. **Mejoras en la Colaboración Interdepartamental:** Los programas de concienciación fomentan una mejor comunicación entre los departamentos técnicos y no técnicos, lo que fortalece la seguridad general de la organización.

Ejemplo de Implementación.

Una organización puede diseñar un programa integral de educación y concienciación de la siguiente manera:

1. **Evaluación Inicial:** Realizar una encuesta o prueba para evaluar el nivel de conocimiento de los empleados sobre seguridad DNS.
2. **Desarrollo de Materiales Personalizados:** Crear módulos educativos adaptados a diferentes niveles de conocimiento técnico dentro de la organización.
3. **Sesiones Prácticas:** Organizar talleres regulares para personal técnico sobre configuraciones seguras de DNS y sesiones informativas para empleados generales sobre cómo evitar amenazas relacionadas con el DNS.
4. **Monitoreo y Evaluación:** Implementar un sistema de monitoreo para rastrear la efectividad del programa y realizar ajustes según sea necesario.

4 ESTUDIO DE CASOS

4.1 Análisis de Incidentes Reales.

4.1.1 Caso del Ataque DDoS a DYN (2016).

El ataque de denegación de servicio distribuido (DDoS) que tuvo como objetivo a DYN en el año 2016 se destacó como uno de los eventos más significativos y perturbadores en la historia de Internet. DYN, una compañía especializada en servicios de DNS (Sistema de Nombres de Dominio), juega un papel esencial en la operación global de la red. Durante este ataque, los servidores de DYN fueron inundados por una gran cantidad de tráfico malicioso, lo que resultó en la interrupción de servicios y plataformas ampliamente utilizadas, como Twitter, Reddit y Netflix.

Este evento expuso de manera clara las vulnerabilidades inherentes a la infraestructura de Internet, subrayando la necesidad de adoptar medidas de seguridad robustas para proteger estos sistemas críticos. Asimismo, este ataque evidenció cómo los ciberdelincuentes pueden emplear *botnets*, es decir, redes de dispositivos comprometidos, para ejecutar ataques DDoS de gran envergadura. Como consecuencia, se incrementó la preocupación en torno a la seguridad de los dispositivos conectados al Internet de las Cosas, destacando la urgencia de implementar protocolos de seguridad más rigurosos.

El análisis del ataque DDoS a DYN ocurrido en 2016 proporciona una valiosa comprensión sobre las tácticas utilizadas por los atacantes, las brechas que explotaron y las estrategias más efectivas para mitigar tales ataques. Este conocimiento es crucial para que las organizaciones fortalezcan sus defensas frente a futuras amenazas de este tipo, promoviendo así un ecosistema digital más seguro y resiliente.

4.1.1.1 Descripción del ataque DDoS a DYN de 2016. [118]

Objetivos del ataque.

El ataque DDoS que tuvo como blanco a DYN en 2016 [119] se ha catalogado como uno de los más notorios y significativos en la historia de Internet. Este ciberataque afectó a una amplia variedad de sitios web y servicios en línea. Su principal propósito fue desestabilizar las operaciones de DYN, una empresa especializada en servicios de DNS.

El impacto de este ataque se extendió más allá de la empresa, ocasionando una interrupción masiva en la conectividad de Internet. Esto afectó considerablemente a compañías y usuarios en todo el mundo. Los atacantes dirigieron su esfuerzo principalmente hacia aquellos sitios web y servicios que dependían de los servidores DNS de DYN para garantizar su funcionamiento.

Más allá de la interrupción de los servicios en línea, el objetivo final de los atacantes era generar daños económicos sustanciales y deteriorar la reputación de las empresas afectadas. Al limitar el acceso a sus plataformas y servicios, los agresores pretendían provocar una disminución de ingresos y minar la confianza que los usuarios tenían en estas organizaciones, exacerbando el impacto negativo a largo plazo.

En la figura siguiente se puede observar como este ataque afectó a un número muy elevado de países.

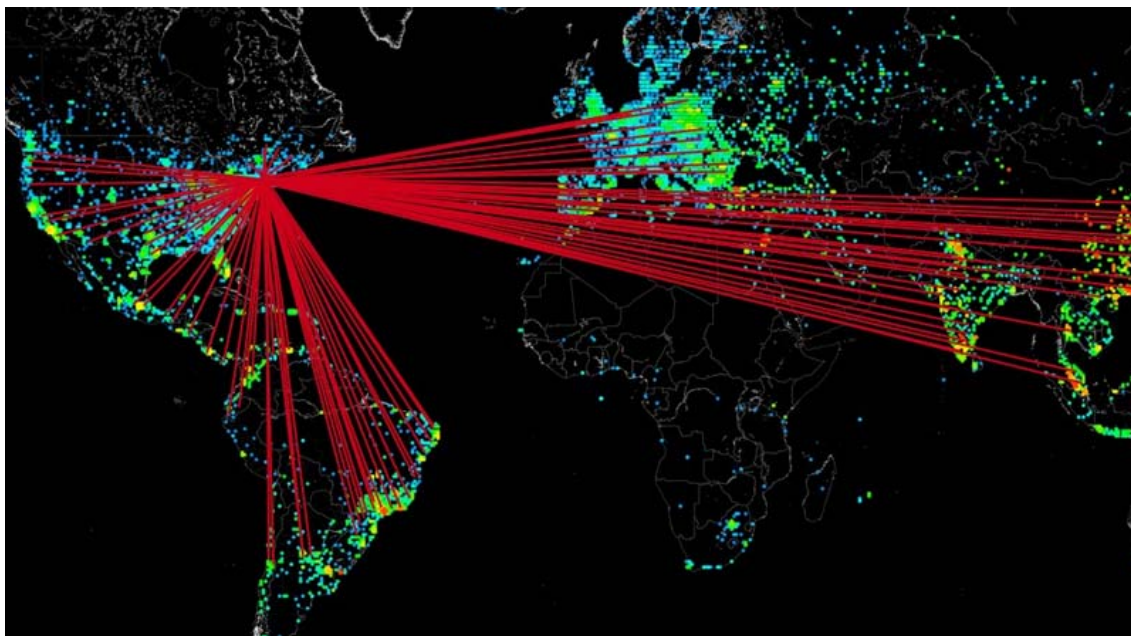


Figura 4-1. Ataque a DYN. (Fuente: <https://wodefense.com>).

Modus operandi del ataque.

El ataque DDoS que afectó a DYN en 2016 se llevó a cabo utilizando una técnica conocida como “amplificación de DNS”. Los atacantes emplearon una red de dispositivos comprometidos, botnets, para generar y enviar una cantidad masiva de solicitudes de DNS fraudulentas hacia los servidores de DYN.

Estas solicitudes, aunque parecían originarse desde direcciones IP auténticas, eran en realidad creadas por los dispositivos infectados que formaban parte de la botnet. La gran cantidad de peticiones falsas generadas por los atacantes provocaba que los servidores DNS de DYN se saturaran, sobrecargándolos y causando una interrupción en el servicio.

La técnica de amplificación de DNS permitió a los atacantes incrementar considerablemente el impacto del ataque, ya que cada solicitud falsa podía desencadenar múltiples respuestas desde los servidores DNS. Esto hizo que el ataque resultara especialmente potente y complicado de neutralizar.

Infraestructura utilizada.

Para ejecutar el ataque DDoS contra DYN, los atacantes desplegaron una infraestructura avanzada que incluía una red de dispositivos comprometidos junto con servidores de comando y control (C&C). Estos servidores se encargaban de gestionar y coordinar las acciones de los dispositivos infectados, además de enviarles las instrucciones necesarias para llevar a cabo el ataque.

La botnet empleada en el ataque estaba conformada por diversos dispositivos comprometidos, que iban desde computadoras personales hasta dispositivos del Internet de las Cosas. Estos equipos habían sido previamente infectados por los atacantes y eran utilizados como “peones” en el ataque. Asimismo,

los atacantes implementaron métodos de ocultamiento y enmascaramiento de su identidad, como el uso de direcciones IP falsificadas y el acceso a través de redes anónimas, para dificultar su localización y seguimiento.

Técnicas empleadas.

En el ataque DDoS contra DYN en 2016, los atacantes emplearon una variedad de estrategias para lograr su objetivo de interrumpir los servicios proporcionados por este proveedor de DNS. Entre las técnicas utilizadas se destacan:

- **Inundación de tráfico:** Los atacantes saturaron los servidores de DYN con un volumen masivo de tráfico, lo que generó una sobrecarga que impedía a los servidores atender las solicitudes legítimas de los usuarios. Este enfoque, conocido como ataque de denegación de servicio distribuido (DDoS), se llevó a cabo mediante una red de dispositivos comprometidos que enviaban el tráfico malicioso.
- **Amplificación del ataque:** Aprovechando vulnerabilidades presentes en algunos servicios de Internet, como servidores NTP (*Network Time Protocol*) y servidores DNS abiertos, los atacantes incrementaron significativamente la cantidad de tráfico dirigido a los servidores de DYN. Esta técnica multiplicaba el impacto del ataque al amplificar las solicitudes maliciosas enviadas.
- **Reflexión del ataque:** Los atacantes utilizaron servidores intermediarios, conocidos como servidores de reflexión, para redirigir el tráfico malicioso hacia los servidores de DYN. De esta forma, lograron ocultar su identidad al no comunicarse directamente con los servidores objetivo, dificultando su detección y bloqueo.

La combinación de estas estrategias permitió a los atacantes generar un volumen de tráfico tan descomunal que los servidores de DYN quedaron completamente abrumados, haciendo que sus servicios resultaran inaccesibles para los usuarios legítimos. El propósito principal del ataque era desestabilizar las operaciones de DYN y causar un impacto significativo en la infraestructura de Internet.

De acuerdo con DYN, el ataque se llevó a cabo mediante la infección de aproximadamente 100,000 dispositivos comprometidos, muchos de ellos hackeados con un *malware* especializado que afecta cámaras y DVR. La empresa señaló inicialmente que parte del ataque involucraba el *malware* Mirai; sin embargo, más tarde confirmó en su blog que todo el ataque provenía de *botnets* basadas en Mirai, convirtiendo a este *malware* en la principal herramienta de la ofensiva. Además, la organización destacó que el ataque podría haberse evitado, ya que muchos de los dispositivos comprometidos presentaban fallas de seguridad que facilitaron su explotación por parte de los hackers.

El hecho de que el ataque involucrara a 100,000 dispositivos sugiere que los hackers podrían haber lanzado una ofensiva DDoS aún más devastadora. Según Ofer Gayer [129], investigador de seguridad en Imperva, esto podría haber sido solo una advertencia: *“Tal vez los atacantes sabían que este nivel de ataque era suficiente y decidieron no utilizar todo su arsenal. Muchas veces, estos ataques buscan extorsionar, pero el objetivo del ataque del viernes pasado fue DYN, un proveedor clave de infraestructura de Internet, lo que logró ralentizar el acceso a más de una docena de sitios importantes”*.

4.1.1.2 Consecuencias del ataque DDoS a DYN de 2016.

Esta interrupción en los servicios fue particularmente grave para las empresas y organizaciones que dependían de DYN para operar sus sitios web y plataformas en línea de forma estable. Esto provocó una pérdida significativa de productividad y afectó negativamente la experiencia de los usuarios. Además, muchas compañías se vieron obligadas a destinar recursos importantes para mitigar los efectos del ataque y reforzar sus medidas de seguridad para prevenir futuros incidentes.

El ataque DDoS a DYN en 2016 resaltó la necesidad crítica de implementar medidas de seguridad robustas para proteger la disponibilidad de servicios en línea. Las organizaciones deben estar preparadas

para enfrentar este tipo de amenazas y adoptar estrategias proactivas que aseguren la continuidad de sus operaciones en caso de interrupciones similares.

Pérdidas económicas.

El ataque DDoS contra DYN en 2016 también tuvo un impacto económico considerable. Según diversos informes, se calcula que las empresas afectadas sufrieron pérdidas millonarias, tanto directas como indirectas.

Estas pérdidas fueron provocadas por varios factores. En primer lugar, la interrupción de los servicios ocasionó una reducción significativa en el tráfico de usuarios, lo que derivó en una caída de los ingresos provenientes de publicidad y transacciones en línea. Asimismo, muchas organizaciones se vieron obligadas a invertir en soluciones para mitigar el ataque y reforzar sus medidas de seguridad, lo que representó gastos adicionales.

Además de los costes inmediatos, el ataque también afectó la confianza de los usuarios y la reputación de las empresas implicadas. Esto podría traducirse en una disminución de la clientela y pérdidas económicas a largo plazo.

4.1.1.3 Análisis forense del ataque DDoS a DYN de 2016.

El ataque masivo DDoS dirigido contra DYN en 2016 se convirtió en uno de los ciberataques más destacados en la historia. Este incidente involucró una serie de ataques DDoS a los servidores DNS de DYN, que provocaron interrupciones en servicios populares como Twitter, Spotify y Reddit. Este evento subrayó la importancia de comprender cómo se estructuran y ejecutan los ciberataques.

Recopilación de evidencias.

Un paso clave para investigar un ataque DDoS es la recopilación de evidencias que permitan determinar su naturaleza y alcance. Durante el ataque a DYN, los equipos de seguridad de la empresa se enfocaron en reunir y analizar registros de tráfico de red, datos de los servidores y otra información relevante. Este proceso resulta esencial para entender cómo se ejecutó el ataque y establecer medidas de prevención para futuros incidentes.

Además de recopilar datos internos, DYN colaboró con proveedores de servicios de Internet y otras entidades afectadas para obtener una visión más amplia del ataque. Esta colaboración permitió identificar patrones, características y el alcance general del incidente.

Con todas las evidencias reunidas, los investigadores analizaron los datos para determinar el origen del ataque, las técnicas empleadas y las posibles motivaciones detrás del mismo. Este análisis exhaustivo es crucial para diseñar estrategias de defensa y mitigación contra futuros ataques DDoS.

Identificación de los culpables.

En la investigación del ataque a DYN se utilizaron diversas técnicas forenses para identificar a los responsables. Estas incluyeron el análisis de registros de tráfico de red, el rastreo de direcciones IP sospechosas y la cooperación con agencias de seguridad y cuerpos policiales especializados en delitos cibernéticos.

A medida que la investigación avanzaba, se descubrió que el ataque se realizó mediante una *botnet* compuesta por miles de dispositivos comprometidos. Los expertos lograron rastrear esta red de dispositivos infectados hasta los atacantes y finalmente identificar a los responsables.

4.1.1.4 Mirai Mortal. [120]

Las botnets Mirai empleadas en el ataque contra DYN “eran botnets “independientes y distintas” de aquellas utilizadas para perpetrar los ataques DDoS contra el blog de Brian Krebs [131] y el proveedor francés de servicios de Internet y alojamiento OVH”.

“A comienzos de ese mes, ‘Anna_Senpai’ [132], el hacker responsable de manejar la gran botnet Mirai usada en el ataque a Krebs, hizo público el código fuente de Mirai en línea. Desde entonces, otros piratas informáticos han utilizado este malware para crear sus propias botnets y llevar a cabo ataques DDoS”, señalaron.

El malware Mirai puede eliminarse fácilmente de los dispositivos infectados, que suelen ser enrutadores, cámaras DVR o WebIP, servidores Linux y dispositivos de Internet de las Cosas que ejecutan Busybox. Reiniciar los dispositivos es suficiente para limpiar el malware, pero si sus propietarios no toman medidas para protegerlos, pueden volver a infectarse en cuestión de minutos.

Lamentablemente, algunos de estos dispositivos no pueden ser adecuadamente asegurados debido a contraseñas predeterminadas incrustadas y a la falta de actualizaciones proporcionadas por los fabricantes. Por ahora, no existe una solución definitiva para este problema, aunque se han propuesto alternativas, incluida la idea de “hackear de vuelta” para recuperar el control de los dispositivos comprometidos. A medida que crece el número de dispositivos IoT infectados, es probable que esta opción sea considerada más seriamente.

Colaboración con agencias de seguridad.

En un ataque de gran magnitud como el DDoS contra DYN, la cooperación con agencias de seguridad y cuerpos policiales especializados resulta esencial. Durante la investigación, DYN colaboró estrechamente con entidades como el FBI y el Departamento de Seguridad Nacional de los Estados Unidos, compartiendo información, coordinando esfuerzos y trabajando en la persecución legal de los responsables.

Esta colaboración permitió a DYN acceder a recursos adicionales, incluyendo expertos en delitos cibernéticos y herramientas avanzadas de análisis forense. Este apoyo fue clave para acelerar el proceso de investigación y garantizar que se tomaran medidas adecuadas para prevenir futuros ataques similares.

El ataque DDoS a DYN en 2016 marcó un antes y un después en la historia de la ciberseguridad. A través de la recopilación de evidencias, la identificación de los responsables y la cooperación con agencias de seguridad, se lograron esclarecer los detalles de este ataque masivo. Estos esfuerzos no solo ayudaron a DYN, sino también a la comunidad de ciberseguridad, aportando importantes aprendizajes sobre la necesidad de preparación y trabajo conjunto para combatir ciberataques de gran escala.

4.1.1.5 Lecciones Aprendidas.

Avances en la detección y mitigación de ataques DDoS.

Uno de los principales retos de los ataques DDoS radica en su capacidad para abrumar una red mediante un volumen masivo de tráfico falso, lo que puede saturar recursos y afectar el desempeño de los servicios en línea. Tras el ataque DDoS a DYN en 2016, se han implementado mejoras significativas en los métodos de detección y mitigación de este tipo de amenazas.

Las herramientas de detección y mitigación de ataques DDoS han evolucionado notablemente, incorporando algoritmos avanzados diseñados para identificar patrones de tráfico inusual y diferenciar entre tráfico legítimo y malintencionado. Estas soluciones utilizan técnicas como el análisis de comportamiento, la inspección detallada de paquetes y la inteligencia artificial para detectar y contrarrestar los ataques DDoS con mayor eficacia.

También se ha fortalecido la capacidad de respuesta frente a estos incidentes, reduciendo el tiempo necesario para su detección y mitigación. Empresas y proveedores de servicios han adoptado sistemas de monitoreo en tiempo real que permiten identificar ataques rápidamente y responder de manera oportuna. Adicionalmente, se han establecido protocolos de respuesta y colaboración con las autoridades pertinentes para actuar de manera coordinada y eficaz frente a un ataque DDoS.

Reforzamiento de la infraestructura de red.

Otra enseñanza importante derivada del ataque a DYN en 2016 ha sido la necesidad de mejorar la infraestructura de red para resistir ataques de esta naturaleza. Las empresas y proveedores de servicios han realizado inversiones significativas para fortalecer sus sistemas, incorporando medidas adicionales de seguridad contra ataques DDoS.

Entre las estrategias adoptadas destaca la implementación de sistemas de balanceo de carga y distribución de tráfico, que redirigen el tráfico malicioso y garantizan la continuidad de los servicios en línea. Estos sistemas distribuyen el tráfico entre varios servidores, dificultando que un ataque DDoS logre saturar un único servidor o centro de datos.

Asimismo, se ha impulsado la adopción de protocolos de seguridad más avanzados, como el Protocolo de Internet versión 6 (IPv6), que proporciona una mayor capacidad de direccionamiento y mayor resistencia a los ataques DDoS. También se han mejorado los sistemas de enrutamiento y filtrado para bloquear el tráfico malicioso antes de que alcance las redes internas.

Conclusión.

El ataque DDoS dirigido contra DYN en 2016 fue un evento sin precedentes que evidenció las debilidades en la infraestructura que sostiene Internet. A través de un análisis detallado del incidente, hemos logrado comprender tanto su complejidad como el impacto que tuvo sobre la disponibilidad de servicios en línea.

Las repercusiones de este ciberataque fueron significativas, afectando a importantes empresas y a usuarios a nivel mundial. No obstante, este suceso también dejó valiosas enseñanzas. Es esencial que las organizaciones fortalezcan sus medidas de seguridad y adopten estrategias efectivas para mitigar ataques DDoS, protegiendo así sus sistemas y asegurando la continuidad de sus operaciones.

En un mundo cada vez más conectado, los ciberataques constituyen una amenaza permanente. Tanto las empresas como los usuarios individuales deben asumir la responsabilidad de implementar medidas proactivas para protegerse. La colaboración entre los diferentes sectores, la adopción de prácticas de seguridad más sólidas y la sensibilización acerca de los riesgos son elementos fundamentales para prevenir futuros ataques y preservar la estabilidad y seguridad de Internet.

4.1.2 Caso de Envenenamiento de Caché de Kaminsky (2008). [121]

A finales de 2007, mientras trabajaba en la optimización de rutas para servidores web, Dan Kaminsky identificó una vulnerabilidad crítica en el protocolo DNS. Al experimentar con registros de recursos y la caché DNS, descubrió que era posible insertar información falsa en la caché de los servidores DNS utilizando respuestas fraudulentas. En febrero de 2008, Kaminsky confirmó la gravedad de esta vulnerabilidad al lograr, mediante una implementación en lenguaje C, inyectar datos falsos en menos de 10 segundos.

Consciente del impacto potencial de este hallazgo, Kaminsky contactó a Paul Vixie, del Internet Systems Consortium (ISC). Este primer contacto derivó en la creación de un equipo de trabajo que incluyó a empresas clave como Microsoft, Cisco y Yahoo. El 31 de marzo de 2008, este grupo se reunió en las instalaciones de Microsoft para desarrollar una solución conjunta que mitigara la vulnerabilidad antes de hacerla pública.

Este incidente puso de manifiesto la importancia de reforzar la seguridad en el protocolo DNS y promovió la adopción de medidas como la aleatorización de puertos de origen y la implementación de DNSSEC para garantizar la autenticidad e integridad de las respuestas DNS.

4.1.2.1 Gestión Coordinada de la Solución.

En marzo de 2008, un grupo de 16 especialistas en seguridad informática se reunió en las oficinas de Microsoft con el objetivo de abordar la vulnerabilidad crítica en el Sistema de Nombres de Dominio (DNS) identificada por Dan Kaminsky. Este equipo contó con la participación de representantes de empresas destacadas como Microsoft, Cisco y Yahoo, quienes colaboraron para analizar el impacto de la vulnerabilidad y desarrollar una solución eficaz.

La estrategia implementada consistió en diseñar parches de seguridad que aumentaran la aleatoriedad en las consultas DNS, dificultando así los intentos de envenenamiento de caché. Se planificó una distribución simultánea de estas actualizaciones en todos los sistemas afectados, con el fin de garantizar una protección uniforme para la infraestructura de Internet. Durante este proceso, la confidencialidad fue clave para evitar que información sensible cayera en manos de atacantes antes de que se aplicaran las soluciones.

El 8 de julio de 2008, se lanzó una actualización de seguridad diseñada para abordar las vulnerabilidades en DNS que permitían la suplantación de identidad. Este esfuerzo fue parte de una estrategia coordinada destinada a mitigar los riesgos asociados con la vulnerabilidad descubierta.

Esta gestión discreta y coordinada logró neutralizar de manera eficaz una amenaza que pudo haber tenido un impacto significativo en la seguridad de Internet. La cooperación entre organizaciones y expertos en seguridad estableció un importante precedente para la respuesta a vulnerabilidades críticas en infraestructuras digitales.

4.1.2.2 Anuncio Público.

El 8 de julio de 2008, se realizó un anuncio coordinado para informar sobre una vulnerabilidad crítica en el Sistema de Nombres de Dominio, descubierta por Dan Kaminsky. Este esfuerzo incluyó la colaboración de diversas empresas y organizaciones, con el objetivo de mitigar los riesgos antes de que la información fuera divulgada públicamente.

En la conferencia Black Hat de agosto de 2008, Kaminsky ofreció una presentación detallada sobre la vulnerabilidad, destacando la gravedad del problema y las acciones tomadas para reducir su impacto.

Este evento representó un hito en la coordinación de la seguridad en Internet, subrayando la importancia de la colaboración entre investigadores, empresas y organizaciones para enfrentar vulnerabilidades críticas en infraestructuras fundamentales.

4.1.2.3 Divulgación y Reacciones.

En julio de 2008, ocurrieron una serie de eventos clave relacionados con la divulgación de una vulnerabilidad crítica en el Sistema de Nombres de Dominio (DNS).

Especulaciones sobre la Vulnerabilidad.

El 21 de julio de 2008, Thomas Dullien, conocido en la comunidad de seguridad como Halvar Flake, publicó en su blog una hipótesis sobre la naturaleza de la vulnerabilidad DNS descubierta por Dan Kaminsky. En su análisis, Dullien planteó que la vulnerabilidad permitía a los atacantes generar respuestas falsas, facilitando ataques de envenenamiento de caché DNS. Aunque inicialmente describió su análisis como una conjetura, su evaluación fue precisa y reflejaba la seriedad del problema.

Divulgación Accidental por Matasano Security.

Ese mismo día, un empleado de Matasano Security compartió en el blog de la empresa detalles técnicos específicos sobre la vulnerabilidad DNS. Aunque la publicación fue retirada rápidamente, la información ya había sido replicada en otros sitios, lo que resultó en una difusión masiva e incontrolada. Esta divulgación prematura generó controversia en la comunidad de seguridad, ya que Kaminsky había solicitado mantener los detalles en reserva para permitir que los administradores de sistemas aplicaran las actualizaciones necesarias.

Reacciones en la Comunidad de Seguridad.

A pesar de los esfuerzos de Kaminsky por mantener el control sobre la situación y coordinar una respuesta efectiva, la divulgación de detalles técnicos provocó un desorden en la comunidad de seguridad. La proliferación de opiniones encontradas y recomendaciones contradictorias complicó la respuesta al problema. Mientras algunos expertos sugirieron esperar antes de actualizar los sistemas para comprender completamente la vulnerabilidad, otros insistieron en la necesidad de una acción inmediata para prevenir posibles ataques. La falta de información clara y la rápida propagación de los detalles técnicos dificultaron una respuesta unificada.

Relevancia de la Coordinación en la Divulgación de Vulnerabilidades.

Este incidente subrayó la importancia de una gestión adecuada y coordinada en la divulgación de vulnerabilidades críticas. Las filtraciones prematuras pueden entorpecer los esfuerzos de mitigación y aumentar la probabilidad de explotación por parte de atacantes. La comunidad de seguridad reconoció la necesidad de establecer protocolos más rigurosos para la divulgación de vulnerabilidades, buscando un equilibrio entre la transparencia y la protección de la infraestructura digital.

4.1.2.4 Soluciones Propuestas y Retos.

El envenenamiento de caché DNS es un método malicioso que inserta información incorrecta en la caché de un servidor DNS, redirigiendo a los usuarios hacia sitios web fraudulentos sin que lo perciban. Este tipo de ataque facilita actividades como el *phishing*, la propagación de *malware* y el robo de datos confidenciales.

Acciones Implementadas para Reducir el Riesgo de Envenenamiento de Caché DNS:

1. **Aleatorización de Puertos de Origen:** Esta medida implica emplear puertos de origen aleatorios en las solicitudes DNS, lo que dificulta que un atacante pueda predecir los parámetros necesarios para falsificar respuestas legítimas. Esta técnica incrementa la complejidad de las comunicaciones DNS, disminuyendo la probabilidad de que los ataques sean exitosos.
2. **Adopción de DNSSEC:** DNSSEC añade una capa adicional de seguridad al DNS mediante el uso de firmas digitales para autenticar tanto la integridad como la procedencia legítima de las respuestas DNS. Esto garantiza que los datos no han sido manipulados ni provienen de fuentes no confiables, bloqueando ataques de envenenamiento de caché.

Debates y Opiniones Críticas:

- **Rol de Dan Kaminsky:** Dan Kaminsky, quien identificó la vulnerabilidad en el protocolo DNS en 2008, abogó activamente por implementar soluciones como DNSSEC. Sin embargo, su papel prominente generó escepticismo en ciertos sectores, donde se cuestionó tanto la magnitud del problema como las soluciones propuestas.

- **Propuestas Alternativas:** También se discutieron opciones alternativas, como mantener los registros DNS válidos hasta su expiración. Aunque esto podría mejorar la seguridad, podría comprometer la flexibilidad del sistema DNS, lo que suscitó debates sobre cómo equilibrar funcionalidad y seguridad en este entorno.

Reflexiones Finales.

Dan Kaminsky, destacado especialista en ciberseguridad, subrayó la relevancia de gestionar la seguridad en Internet de manera global, advirtiendo que podrían existir vulnerabilidades similares a las del DNS en otros protocolos esenciales, como BGP, SNMPv3 o SSL.

Este caso destacó la importancia de contar con organismos especializados, como los Equipos de Respuesta a Emergencias Informáticas (CERT), que tienen la misión de coordinar respuestas ante vulnerabilidades críticas. Los CERT desempeñan un rol clave en proteger la integridad, confidencialidad y disponibilidad de la información en los entornos digitales, funcionando como puntos de coordinación y reacción frente a amenazas cibernéticas.

En España, el Instituto Nacional de Ciberseguridad (INCIBE) [134] cumple una función crucial en la protección de infraestructuras críticas y la gestión de incidentes de ciberseguridad. En 2023, el INCIBE atendió más de 83,500 incidentes, de los cuales 58,000 afectaron a ciudadanos y 22,000 a empresas. Los sectores financieros, de transporte y de energía fueron los más impactados, representando el 25%, 25% y 22% de los casos, respectivamente. Además, se registraron más de 26,200 incidentes relacionados con malware, incluidos 621 ataques de ransomware.

La colaboración entre los sectores público y privado resulta esencial para reforzar la ciberseguridad a nivel nacional e internacional. La creación y coordinación de los CERT se ha convertido en una herramienta imprescindible para garantizar la seguridad tanto a nivel nacional como global.

5 ANÁLISIS Y PROPUESTAS DE MEJORA

5.1 Propuestas de Mejora.

A continuación se presenta un SETUP recomendado de referencia de seguridad en el DNS que contempla todos los mecanismos existentes que considera se deben aplicar como protección inicial de un DNS, al menos debería contener:

5.1.1 Setup de Referencia.

Un entorno seguro de DNS debe incluir configuraciones avanzadas que fortalezcan cada aspecto de la resolución y transmisión de datos:

1. Protección criptográfica: DNSSEC.

- **Objetivo:** Garantizar la autenticidad e integridad de las respuestas DNS.
- **Detalles:**
 - o Configuración jerárquica de claves criptográficas, incluyendo ZSK y KSK.
 - o Validación mediante registros DNSKEY, RRSIG y DS.
 - o Implementación en todas las zonas DNS críticas para crear una cadena de confianza desde la raíz hasta los dominios finales.
- **Impacto:** Evita ataques como el envenenamiento de caché y la suplantación de identidad, asegurando que las respuestas DNS no hayan sido manipuladas en tránsito.

2. Cifrado de consultas: DoH y DoT.

- **DNS sobre HTTPS (DoH):**
 - o Permite el cifrado de consultas DNS utilizando HTTPS, protegiendo la privacidad del usuario contra observadores no autorizados.
 - o Compatible con navegadores modernos como Chrome y Firefox.
- **DNS sobre TLS (DoT):**
 - o Proporciona cifrado similar pero a nivel de transporte, optimizado para servidores DNS.
- **Ventaja combinada:** Mitigan ataques de intermediarios (MITM) y previenen el rastreo de consultas DNS.

3. Mitigación de DDoS.

- **Redes Anycast:**

- o Distribuyen el tráfico DNS entre múltiples instancias globales, mejorando la resistencia frente a ataques masivos.
- **Sistemas avanzados de monitoreo:**
 - o Soluciones como Arbor Networks [135] detectan y mitigan patrones de tráfico anómalo en tiempo real.
- **Limitación:** Aunque robustas, las soluciones DDoS pueden ser costosas para pequeñas organizaciones.

4. Control de transferencias de zona.

- **Protocolo TSIG (*Transaction Signatures*):**
 - o Autentica transferencias entre servidores DNS utilizando claves compartidas.
- **Listas de control de acceso (ACL):**
 - o Restringen las transferencias a servidores autorizados, previniendo la filtración de datos sensibles.

5. Monitoreo y auditoría en tiempo real.

- **Inteligencia artificial para análisis predictivo:**
 - o Identifica patrones que podrían anticipar ataques, como intentos de envenenamiento de caché.

5.1.2 Análisis de Soluciones Existentes y sus Limitaciones.

En el ámbito de la seguridad del Sistema de Nombres de Dominio (, se han desarrollado diversas soluciones para abordar las amenazas que afectan su funcionamiento y la privacidad de los usuarios. Aunque estas soluciones han demostrado ser efectivas en gran medida, no son infalibles y presentan limitaciones que deben considerarse. Este análisis profundiza en las principales soluciones existentes, y limitaciones, así como en los desafíos que enfrentan.

1. DNSSEC.

Ventaja:

DNSSEC es una extensión diseñada para garantizar la autenticidad e integridad de las respuestas DNS mediante el uso de firmas digitales. Estas firmas aseguran que las respuestas provengan de una fuente legítima y que no hayan sido manipuladas en tránsito. DNSSEC protege contra ataques como el envenenamiento de caché, que busca redirigir a los usuarios hacia dominios maliciosos.

Limitación:

- **Exposición de la privacidad:** Aunque DNSSEC asegura la integridad de las respuestas, no cifra las consultas ni las respuestas DNS. Esto significa que terceros pueden interceptar y monitorear las consultas DNS para analizar los patrones de navegación de los usuarios, comprometiendo su privacidad.
- **Adopción limitada:** A pesar de sus beneficios, la implementación de DNSSEC no está universalmente adoptada. Muchas organizaciones, proveedores de servicios de Internet y servidores DNS aún no han habilitado esta tecnología debido a la complejidad técnica y los costes asociados.
- **Sobrecarga operativa:** La gestión de las claves criptográficas necesarias para DNSSEC puede ser compleja, especialmente en organizaciones con infraestructuras DNS amplias.

2. DoH (DNS over HTTPS) y DoT (DNS over TLS).

Ventaja:

DoH y DoT son protocolos diseñados para proteger la confidencialidad de las consultas DNS mediante el cifrado. Estas tecnologías impiden que terceros intercepten o manipulen las solicitudes DNS, protegiendo la privacidad del usuario, especialmente en redes públicas o inseguras.

Limitación:

- **Incremento en la latencia:** El cifrado y la necesidad de establecer conexiones HTTPS o TLS introducen un retraso adicional en la resolución de nombres de dominio. Aunque esta latencia es mínima en redes modernas, puede ser significativa en aplicaciones sensibles al tiempo.
- **Mayor capacidad de procesamiento:** El cifrado requiere recursos computacionales adicionales, tanto en el lado del cliente como en el del servidor. Esto puede representar un desafío para dispositivos con capacidades limitadas, como dispositivos IoT, y para servidores DNS que manejan grandes volúmenes de tráfico.
- **Fragmentación de la seguridad:** La implementación de DoH puede dificultar la supervisión del tráfico DNS por parte de las organizaciones, ya que las consultas cifradas son más difíciles de monitorear y filtrar en comparación con las consultas tradicionales.
- **Compatibilidad y adopción:** Aunque el soporte para DoH y DoT está aumentando, no todos los servidores DNS y aplicaciones son compatibles con estos protocolos, lo que limita su efectividad.

3. Mitigación de DDoS.

Ventaja:

Las estrategias de mitigación de ataques de denegación de servicio distribuido (DDoS) están diseñadas para garantizar la disponibilidad del DNS incluso durante ataques masivos. Estas soluciones incluyen el uso de redes Anycast, servicios especializados como Cloudflare, y herramientas avanzadas de análisis y filtrado de tráfico.

Limitación:

- **Costes elevados:** Implementar soluciones de mitigación de DDoS puede ser costoso, especialmente para pequeñas y medianas organizaciones que carecen de recursos financieros significativos. Esto las deja vulnerables a ataques dirigidos.
- **Ataques dirigidos a dispositivos IoT:** La creciente proliferación de dispositivos IoT comprometidos ha ampliado la superficie de ataque. Muchas soluciones de mitigación actuales no pueden prevenir completamente el tráfico malicioso generado por estas redes de dispositivos infectados, que son utilizadas como parte de *botnets* para lanzar ataques.
- **Dependencia de terceros:** Muchas organizaciones dependen de proveedores externos para la mitigación de DDoS, lo que puede generar riesgos adicionales relacionados con la confianza, la privacidad y la disponibilidad del servicio.

4. Monitoreo y Análisis del Tráfico DNS.

Ventaja:

El monitoreo en tiempo real y el análisis del tráfico DNS permiten identificar y mitigar amenazas de manera proactiva. Estas herramientas pueden detectar actividades anómalas, como consultas hacia dominios maliciosos o intentos de exfiltración de datos a través de canales DNS.

Limitación:

- **Falsos positivos:** Los sistemas de monitoreo pueden generar alertas basadas en comportamientos que no necesariamente representan una amenaza, lo que puede llevar a una sobrecarga de trabajo para los equipos de seguridad.
- **Requiere personal capacitado:** Interpretar los datos generados por herramientas de monitoreo DNS requiere experiencia y habilidades especializadas. Las organizaciones que carecen de personal capacitado pueden tener dificultades para aprovechar al máximo estas herramientas.
- **Complejidad operativa:** Implementar y mantener un sistema de monitoreo efectivo puede ser técnicamente complejo y demandar recursos significativos, tanto en términos de tiempo como de costes.

5. Otras Limitaciones Generales.

- **Fragmentación de Soluciones:** Las soluciones actuales suelen abordar aspectos específicos de la seguridad DNS (como la privacidad o la disponibilidad), pero no ofrecen una protección integral. La combinación de múltiples soluciones puede ser costosa y difícil de gestionar.
- **Velocidad de Evolución de las Amenazas:** Los atacantes continúan desarrollando técnicas más sofisticadas para evadir las defensas existentes. Las soluciones de seguridad deben actualizarse constantemente para mantenerse al día con estas amenazas en evolución.
- **Falta de Estándares Globales:** Aunque existen iniciativas para mejorar la seguridad DNS, la falta de estándares globales unificados dificulta la implementación de soluciones consistentes a nivel mundial.

Conclusión.

Las soluciones actuales para mejorar la seguridad y privacidad del DNS han logrado avances significativos, pero presentan limitaciones que deben ser abordadas para garantizar una protección más completa. Mientras que DNSSEC asegura la integridad de las respuestas y DoH/DoT protegen la confidencialidad de las consultas, ambos enfrentan desafíos relacionados con la adopción, la latencia y la capacidad de procesamiento. Por su parte, las estrategias de mitigación de DDoS y las herramientas de monitoreo en tiempo real ofrecen soluciones efectivas, pero a menudo requieren recursos significativos y personal especializado.

En el futuro, será fundamental desarrollar tecnologías integrales que combinen la protección de la privacidad, la disponibilidad y la integridad del DNS, al tiempo que se abordan las limitaciones actuales. Esto incluirá inversiones en investigación, la creación de estándares globales y la adopción de enfoques colaborativos entre organizaciones, gobiernos y la comunidad técnica.

6 CONCLUSIONES Y LÍNEAS FUTURAS

6.1 Propuesta de Nuevas Estrategias.

En este apartado se van a comentar nuevas estrategias para mejorar la seguridad del DNS, se van a considerar dos propuestas: el uso de la Inteligencia Artificial y *Blockchain*.

6.1.1 Integración de Inteligencia Artificial en la Seguridad DNS.

En un panorama digital donde las amenazas cibernéticas evolucionan rápidamente, las redes son cada vez más complejas y el volumen de tráfico DNS crece exponencialmente, la integración de la Inteligencia Artificial (IA) con la infraestructura DNS representa un cambio revolucionario. Este avance no solo aborda las amenazas de seguridad con mayor eficacia, sino que también optimiza el rendimiento de las redes, introduciendo un nivel de automatización, predicción y defensa proactiva sin precedentes.

A continuación, se amplía y contextualiza cómo la IA está transformando el DNS, abordando tanto sus aplicaciones actuales como los desafíos y perspectivas a futuro.

El Rol Transformador de la IA en el DNS.

La Inteligencia Artificial se distingue por su capacidad para procesar y analizar grandes volúmenes de datos en tiempo real. Cuando se aplica al DNS, la IA permite identificar patrones y anomalías en el tráfico que serían imposibles de detectar mediante métodos tradicionales. Esto hace que la IA sea una herramienta indispensable para abordar las crecientes amenazas cibernéticas y optimizar la gestión de infraestructuras DNS.

1. Automatización en la Detección y Respuesta a Amenazas.

La IA permite automatizar procesos complejos de detección y respuesta, mejorando significativamente la velocidad y precisión con la que las amenazas son identificadas y neutralizadas.

- **Análisis en tiempo real:** Los sistemas basados en IA supervisan el tráfico DNS en tiempo real, identificando patrones sospechosos, como consultas repetitivas a dominios maliciosos, túneles DNS utilizados para exfiltración de datos y algoritmos de generación de dominios (DGA) asociados con *malware*.

- **Acción inmediata:** Al detectar una amenaza, la IA puede tomar medidas automáticamente, como bloquear consultas a dominios sospechosos, aislar dispositivos comprometidos o ajustar configuraciones para mitigar riesgos.
- **Ventajas frente a técnicas tradicionales:** Mientras que los métodos convencionales dependen de listas negras estáticas y reglas predefinidas, la IA utiliza algoritmos de aprendizaje automático para adaptarse y responder a nuevas amenazas de manera dinámica.

2. Predicción Proactiva de Amenazas.

La capacidad predictiva de la IA supera el enfoque reactivo tradicional, permitiendo anticiparse a las amenazas antes de que se materialicen.

- **Modelos predictivos:** Mediante el análisis de datos históricos y tendencias, los algoritmos de IA identifican señales tempranas de posibles ataques, como aumentos anómalos en las consultas DNS que podrían indicar un ataque DDoS inminente.
- **Prevención de ataques:** Por ejemplo, si un patrón de tráfico sugiere la preparación de un ataque de *phishing*, la IA puede alertar a los administradores o bloquear proactivamente los dominios involucrados.
- **Ventaja competitiva:** La predicción de amenazas permite a las organizaciones mantenerse un paso adelante de los atacantes, reduciendo los tiempos de respuesta y el impacto de los incidentes.

3. Filtrado de Contenido Basado en DNS Mejorado.

El filtrado de contenido es una función esencial para proteger a los usuarios de dominios maliciosos, y la IA lleva esta capacidad a un nivel superior.

- **Análisis dinámico:** En lugar de depender exclusivamente de listas negras estáticas, los sistemas impulsados por IA evalúan en tiempo real características como la antigüedad del dominio, la reputación de la dirección IP y el comportamiento del servidor.
- **Defensa contra técnicas evasivas:** La IA detecta y bloquea tácticas avanzadas como el “*fast-flux*”, donde los atacantes cambian rápidamente las direcciones IP asociadas a un dominio para evadir la detección.
- **Personalización y flexibilidad:** Las soluciones basadas en IA pueden adaptarse a las necesidades específicas de las organizaciones, permitiendo políticas de filtrado personalizadas que consideren factores contextuales y de comportamiento.

4. Optimización del Rendimiento de la Red.

La IA no solo mejora la seguridad, sino que también puede optimizar el rendimiento del DNS, lo que resulta en una mejor experiencia para los usuarios finales.

- **Balanceo de carga dinámico:** Analizando patrones de tráfico, la IA puede redirigir las consultas hacia los servidores más rápidos y menos congestionados, evitando cuellos de botella durante picos de tráfico.
- **Optimización de caché:** La IA ajusta dinámicamente los tiempos de vida (TTL) de las entradas en caché, asegurando una resolución más rápida de consultas recurrentes sin comprometer la frescura de los datos.
- **Reducción de la latencia:** Identificando rutas óptimas para el tráfico DNS, la IA mejora la velocidad de las consultas, lo que es especialmente beneficioso para aplicaciones sensibles al tiempo.

5. Reducción de Falsos Positivos.

Uno de los desafíos en la detección de amenazas es diferenciar entre actividades legítimas y sospechosas. La IA aborda este problema mediante:

- **Análisis contextual avanzado:** Considerando factores como el comportamiento histórico del usuario, la hora del día y los patrones de tráfico, la IA reduce significativamente los falsos positivos.
- **Aprendizaje continuo:** Los sistemas basados en IA se actualizan constantemente con nuevos datos, mejorando su precisión y adaptándose a los cambios en el entorno de amenazas.

Desafíos en la Integración de IA con el DNS.

Aunque las aplicaciones de la IA en el DNS son prometedoras, también enfrentan desafíos que deben ser superados:

1. **Entradas Adversariales:** Los atacantes pueden manipular los datos de entrada para engañar a los modelos de IA, lo que subraya la necesidad de entrenar los sistemas con conjuntos de datos robustos y diversos.
2. **Transparencia y Explicabilidad:** En ciberseguridad, es crucial entender cómo y por qué un sistema basado en IA toma ciertas decisiones. La falta de explicabilidad puede dificultar la confianza en estas soluciones.
3. **Requerimientos Computacionales:** Los algoritmos de IA, especialmente en tiempo real, requieren una infraestructura tecnológica avanzada, lo que puede ser un obstáculo para organizaciones con recursos limitados.
4. **Costes de Implementación:** Integrar IA en la seguridad DNS puede ser costoso, especialmente en términos de desarrollo, mantenimiento y capacitación del personal.

Perspectivas Futuras.

La integración de la IA con el DNS seguirá evolucionando, impulsada por avances en tecnología y una mayor necesidad de seguridad. Algunas tendencias emergentes incluyen:

- **IA Federada:** Modelos que permiten la colaboración entre diferentes organizaciones sin compartir datos sensibles, mejorando la seguridad global.
- **IA Explicable (XAI):** Herramientas que ofrecen mayor transparencia en las decisiones de la IA, aumentando la confianza de los usuarios en estos sistemas.
- **Integración con Blockchain:** Combinar la IA con tecnologías como *blockchain* podría fortalecer aún más la seguridad y la trazabilidad en la gestión del DNS.

6.1.2 Uso de Blockchain para la protección del DNS.

La creciente dependencia del Sistema de Nombres de Dominio para el funcionamiento de Internet ha puesto de manifiesto sus vulnerabilidades inherentes. La implementación de la tecnología *blockchain* ofrece una solución innovadora para reforzar la seguridad del DNS, proporcionando una infraestructura descentralizada, transparente e inmutable que aborda problemas críticos como la manipulación de datos, la falta de confianza y la resiliencia frente a ataques.

Implementación de Blockchain en la Seguridad DNS.

La tecnología *blockchain* introduce un cambio paradigmático en la forma en que se protege el DNS, permitiendo a las organizaciones mitigar riesgos asociados con sistemas centralizados. Su arquitectura distribuida elimina puntos únicos de fallo, mejora la autenticidad de los datos y proporciona un registro inmutable de todas las transacciones relacionadas con el DNS.

Eliminación de Puntos Únicos de Fallo.

Blockchain descentraliza la infraestructura DNS al distribuir la información de los nombres de dominio a través de una red de nodos. Este diseño asegura que ningún nodo único pueda comprometer la funcionalidad completa del sistema. Este modo de distribuir la información presenta las siguientes ventajas:

- **Aumento de la Disponibilidad:** Al replicar datos en múltiples nodos, el sistema garantiza que incluso si un nodo es atacado o comprometido, otros nodos puedan continuar proporcionando el servicio.
- **Mejora de la Resiliencia:** La descentralización hace que los ataques a gran escala sean menos efectivos, ya que la información está dispersa en la red.

Verificación de Cambios.

Una de las principales ventajas de *blockchain* es su capacidad para registrar todas las modificaciones realizadas en un sistema, lo que mejora la transparencia y evita manipulaciones no autorizadas. Cada cambio en los registros DNS se registra como una transacción en *blockchain*, lo que garantiza que todos los datos sean transparentes y rastreables.

- Aplicaciones:
 - **Auditorías de Seguridad:** *Blockchain* permite mantener un historial completo de todas las modificaciones realizadas en los registros DNS, facilitando auditorías rápidas y eficaces.
 - **Protección contra Manipulación:** La inmutabilidad de *blockchain* asegura que los cambios realizados sin consenso sean detectados y rechazados por la red.
- Impacto:
 - Incrementa la confianza en la autenticidad de los registros DNS, asegurando que los usuarios finales sean dirigidos a los destinos correctos.
 - Reduce el riesgo de ciberataques, como el **envenenamiento de caché**, al garantizar que todos los datos sean legítimos y no manipulados.

Proyectos Actuales.

La aplicación de *blockchain* al DNS ha dado lugar a proyectos innovadores que están transformando la gestión de nombres de dominio:

- **Handshake:** [136] Rediseña el DNS mediante *blockchain*, eliminando dependencias de registros centralizados.
- **Ethereum Name Service (ENS):** [137] Esta plataforma asigna nombres legibles a direcciones Ethereum y otros recursos mediante *blockchain*, reduciendo errores y aumentando la seguridad

Desafíos en la Implementación.

Aunque la tecnología *blockchain* ofrece numerosos beneficios, también presenta desafíos significativos:

1. **Escalabilidad:** Las redes *blockchain* actuales enfrentan dificultades para manejar el volumen masivo de consultas DNS globales. Estas limitaciones de rendimiento afectan su viabilidad para aplicaciones a gran escala.
2. **Interoperabilidad:** Integrar *blockchain* con sistemas DNS tradicionales requiere resolver problemas técnicos complejos para garantizar una transición fluida.
3. **Coste:** La implementación de sistemas basados en *blockchain* puede ser costosa, especialmente para pequeñas organizaciones, debido a la necesidad de infraestructura avanzada y personal capacitado.

6.1.3 Futuras Implementaciones DNS sobre HTTP (DoT).

1. Integración con HTTP/3.

- **Adopción de técnicas de HTTP/3:** HTTP/3, basado en el protocolo QUIC, ofrece ventajas significativas en términos de velocidad y eficiencia, especialmente en redes con alta latencia. Aunque DoT actualmente utiliza el puerto 853 bajo TCP, adaptar su arquitectura para aprovechar QUIC podría reducir los tiempos de establecimiento de conexiones y mejorar la resiliencia en condiciones adversas.
- **Ventajas esperadas:**
 - Establecimiento más rápido de conexiones gracias al protocolo sincrónico de QUIC.
 - Mejora en la recuperación de paquetes perdidos debido a la transmisión independiente de flujos.
- **Estado actual:** Investigaciones académicas y pruebas piloto están evaluando la factibilidad de integrar DoT con QUIC para beneficiar su desempeño en redes globales.

2. Automatización de Configuraciones.

- **Simplificación de la adopción:** Una de las barreras clave para la adopción de DoT es la necesidad de configuraciones manuales por parte de los usuarios o administradores de red. Herramientas avanzadas de automatización podrían facilitar este proceso, reduciendo la complejidad y el tiempo necesario para implementar DoT en entornos personales y empresariales.
- **Desarrollos en curso:**
 - *Scripts* personalizados que detectan automáticamente servidores DoT compatibles y ajustan las configuraciones del sistema operativo.
 - Integración con administradores de configuración como Ansible o Terraform para despliegues a gran escala.

3. Despliegue en Infraestructuras Empresariales.

- **Integración con herramientas de seguridad corporativa:** La integración de DoT con soluciones empresariales como *firewalls*, *proxies* y VPN puede proporcionar una capa adicional de seguridad en redes corporativas, asegurando la privacidad y la integridad de las consultas DNS.
- **Desarrollos en curso:**
 - Algunos fabricantes de *firewalls* como Palo Alto Networks [138] y Fortinet [139] ya han comenzado a implementar soporte para DoT en sus soluciones empresariales.

4. Adopción Masiva.

- **Expansión del soporte nativo:** A medida que más sistemas operativos y aplicaciones nativas soporten DoT, se espera que el protocolo se convierta en un estándar global para la privacidad en DNS.
 - **Progresos actuales:**
 - o Android 12 y posteriores ya incluyen configuraciones avanzadas de DNS privadas que soportan DoT.
 - o Distribuciones de Linux como Ubuntu y Fedora están incluyendo Unbound como opción predeterminada para consultas DNS cifradas.
 - o Navegadores web como Firefox y Chrome han expresado interés en añadir compatibilidad con DoT, complementando su soporte para DNS sobre HTTPS (DoH).
 - **Impacto esperado:** La facilidad de configuración en dispositivos personales y redes domésticas aumentará significativamente la adopción de DoT entre usuarios no técnicos.

6.1.4 Firewalls de Próxima Generación.

Los *firewalls* de próxima generación (Next-Generation Firewalls, NGFW) han transformado la forma en que se protege la infraestructura de red al integrar capacidades tradicionales con tecnologías avanzadas. Estas herramientas no solo controlan el tráfico basado en reglas, sino que también identifican y mitigan amenazas modernas utilizando inspección profunda de paquetes, inteligencia artificial y bases de datos en tiempo real.

Estos NGFW, nos ofrecen una serie de funcionalidades, que refuerzan más el gran valor que tienen los *Firewall* en la defensa del DNS:

1. Inspección Profunda de Paquetes (DPI): La Inspección Profunda de Paquetes (*Deep Packet Inspection, DPI*) permite analizar el contenido completo de los paquetes de datos, desde la capa de aplicación hasta el núcleo de la carga útil. Esto incluye el tráfico cifrado, como HTTPS, lo que hace posible identificar amenazas que antes podían ocultarse, lo que nos proporciona las siguientes ventajas:

- Detectar *malware*, *spyware* o *exploits* que puedan estar incrustados en las comunicaciones cifradas.
- Ofrece una visión granular del tráfico, lo que facilita la segmentación de la red y la aplicación de políticas específicas.

Pero también tiene un inconveniente, ya que la inspección de tráfico cifrado puede generar una carga adicional en los recursos del *firewall*, afectando el rendimiento si no se implementa adecuadamente.

2. Prevención de Amenazas Avanzadas: Los NGFW integran bases de datos de inteligencia en tiempo real que recopilan información sobre dominios, direcciones IP y patrones de tráfico asociados con amenazas cibernéticas. Esto permite identificar y bloquear ataques antes de que puedan afectar la red. Tienen las siguientes características principales:

- **Actualización constante:** Las bases de datos se actualizan continuamente para incluir nuevos indicadores de compromiso (IOC).
- **Análisis en tiempo real:** Los NGFW evalúan el tráfico contra estas bases de datos para bloquear automáticamente amenazas conocidas.

Las ventajas que ofrece este tipo de acciones son las siguientes:

1. Reducción de los tiempos de respuesta ante nuevas amenazas.
2. Mitigación proactiva de ataques como *ransomware* y *phishing* dirigido.

3. Integración con Inteligencia Artificial (IA): La inclusión de inteligencia artificial en los NGFW permite identificar patrones maliciosos, predecir amenazas y adaptar las políticas de seguridad de manera automática. Tienen las siguientes características principales:

- **Aprendizaje automático (*Machine Learning*):** Gracias al Machine Learning las máquinas serán capaces de acceder a las bases de datos y se actualizarán continuamente en busca de nuevos indicadores de compromiso (IOC).
- **Automatización:** Ajustes dinámicos en las políticas de seguridad basados en el análisis continuo del tráfico de red.

Las ventajas que ofrece este tipo de acciones son las siguientes:

1. Mejora la detección de amenazas persistentes avanzadas (APT).
2. Reduce la dependencia de la intervención humana, acelerando las respuestas a incidentes.

Pero también se enfrentan a los siguientes retos:

1. Los algoritmos de IA necesitan entrenamiento continuo para adaptarse a las nuevas técnicas de evasión empleadas por los atacantes.
2. La implementación de IA puede aumentar los costes iniciales de los NGFW.

En la siguiente tabla se presenta una comparación detallada entre los **Firewalls de Próxima Generación (NGFW)** y los **Firewalls Tradicionales** en distintos aspectos.

Aspecto	<i>Firewalls Tradicionales</i>	<i>Firewalls de Próxima Generación (NGFW)</i>
Funcionalidad principal	Filtrado de paquetes basado en reglas para direcciones IP, puertos y protocolos.	Funciones avanzadas como filtrado a nivel de aplicación, prevención de intrusos e inspección profunda de paquetes (DPI).
Detección de amenazas	Básica; depende de reglas y firmas estáticas.	Incluye detección avanzada de amenazas con inteligencia en tiempo real y análisis de comportamientos.
Inspección del tráfico	Inspecciona únicamente los encabezados de los paquetes; no examina el contenido.	Inspecciona paquetes completos, incluido el contenido (<i>payload</i>), incluso en tráfico cifrado (por ejemplo, HTTPS).
Conciencia de aplicaciones	Limitada; no puede diferenciar el tráfico según aplicaciones o servicios.	Identifica y controla el tráfico a nivel de aplicaciones.
Integración con inteligencia de amenazas	No integrado con fuentes externas de inteligencia de amenazas.	Integrado con fuentes de inteligencia de amenazas para bloquear dominios, IPs y comportamientos maliciosos de forma proactiva.
Prevención de intrusos	Ausente o requiere sistemas adicionales.	Incluye sistemas de prevención de intrusos (IPS) para detectar y bloquear actividad maliciosa.
Escalabilidad	Adecuado para redes pequeñas con necesidades básicas de seguridad.	Diseñado para redes modernas y complejas que requieren escalabilidad y controles granulares.
Conciencia de usuarios y dispositivos	Limitada o inexistente.	Rastrean y controlan el tráfico basado en identidades de usuarios, roles y tipos de dispositivos.
Compatibilidad con la nube e IoT	No diseñado para entornos modernos de nube o IoT.	Optimizado para infraestructuras basadas en la nube y centradas en IoT con políticas avanzadas y análisis.
Impacto en el rendimiento	Mínimo; se enfoca en filtrado básico.	Puede introducir latencia debido a funciones avanzadas como DPI, mitigado por hardware de alto rendimiento.
Costo	Costes iniciales más bajos.	Costes más altos debido a sus características avanzadas y capacidades de rendimiento.

Tabla 6-1. Comparación Firewall Tradicionales vs NGFW.

Conclusión.

La integración de la Inteligencia Artificial con el DNS marca el inicio de una era de redes más inteligentes, seguras y eficientes. Al automatizar procesos, anticipar amenazas y optimizar el rendimiento, la IA no solo responde a los desafíos actuales, sino que también establece las bases para un entorno digital más robusto y preparado para el futuro. Aunque aún enfrenta desafíos, el desarrollo continuo de esta tecnología promete transformar radicalmente la seguridad y la gestión del DNS.

La implementación de *blockchain* en la seguridad del DNS representa una evolución significativa hacia un Internet más seguro y confiable. Al eliminar puntos únicos de fallo, garantizar la inmutabilidad de los datos y proporcionar transparencia, esta tecnología aborda muchas de las limitaciones del sistema DNS tradicional. Sin embargo, para lograr una adopción generalizada, es necesario superar desafíos relacionados con la escalabilidad y la interoperabilidad. La continua investigación y desarrollo en este campo será crucial para maximizar su potencial y garantizar una infraestructura de Internet más resiliente

7 BIBLIOGRAFÍA

- [1] CLOUDFARE: <https://www.cloudflare.com/es-es/learning/dns/what-is-dns/>.
- [2] E. Vieito: <https://dinahosting.com/blog/historia-del-sistema-dns/#:~:text=Aunque%20realmente%2C%20la%20historia%20del,de%20entonces%20era%20bastante%20limitado.>
- [3] INFORMATECDIGITAL,: https://informatecdigital.com/internet/dns-definicion-tipos-y-caracteristicas/?utm_source=chatgpt.com.
- [4] CLOUDFARE: <https://www.cloudflare.com/es-es/learning/dns/dns-security/>.
- [5] G. V. Álvarez: https://www.cs.upc.edu/~gabriel/files/DNS_Kaminsky.pdf.
- [6] CYBERPROTEGIDOS: <https://cyberprotegidos.info/amenazas-y-ataques/anatomia-ciberataque-desentranando-notorio-ataque-ddos-dyn-2016/>.
- [7] ICANN: <https://www.icann.org/es>.
- [8] IETF, «<https://www.ietf.org>,»
- [9] REVISTACOMPLETA: https://revistacompleta.com/evolucion-y-seguridad-del-dns/?utm_source=chatgpt.com.
- [10] ADMINISTRADOR DE SISTEMAS:
https://administraciondesistemas.com/dns/?utm_source=chatgpt.com.
- [11] AZION: <https://www.azion.com/es/learning/cdn/que-es-caching/>.
- [12] WIKIPEDIA: https://en.wikipedia.org/wiki/Hosts_%28file%29?.
- [13] IONOS: <https://www.ionos.es/digitalguide/servidores/configuracion/archivo-hosts/>.
- [14] NIC: <https://nic.com/>.
- [15] WIKIPEDIA: https://es.wikipedia.org/wiki/Paul_Mockapetris?.
- [16] P. Mockapetris, «RFC»: <https://www.rfc-editor.org/rfc/pdf/rfc882.txt.pdf>.

- [17] P. Mockapetris «RFC»: <https://www.rfc-editor.org/rfc/pdf/rfc883.txt.pdf>.
- [18] B. Vargas: https://www.byronvargas.com/web/cual-es-la-funcion-de-los-dns/?utm_source=chatgpt.com.
- [19] ISC: <https://www.isc.org/bindhistory/>.
- [20] Internet System Consortium: <https://www.isc.org/bind/>.
- [21] J. González: <https://cotidianidades.online/cuando-aparecio-el-internet-por-primera-vez-historia-y-evolucion/>.
- [22] S. Hussain: https://www.icann.org/es/blogs/details/hello-world-enabling-internationalized-domain-names-idns-16-6-2021-es?utm_source=chatgpt.com.
- [23] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/dns-over-tls/>.
- [24] PANDORAFMS: <https://pandorafms.com/blog/es/monitorizacion-dns/>.
- [25] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/access-management/what-is-dns-filtering/>.
- [26] J. Carlos: <https://www.zeppelinlinux.es/espacio-de-nombres-de-dominio-domain-name-space>.
- [27] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/glossary/dns-zone/>.
- [28] J. Carlos: <https://www.zeppelinlinux.es/servidores-de-nombres-sus-tipos-y-zonas/>.
- [29] P. Mockapetris «RFC»: <https://www.rfc-es.org/rfc/rfc1034-es.txt>.
- [30] E. Romero: <https://infotecnewsjr.blogspot.com/2017/03/sabe-ud-que-son-y-donde-se-encuentran.html>.
- [31] X. S. Martin: https://aodatacloud.es/blog/conceptos-sistema-de-nombres-de-dominio-dns/?utm_source=chatgpt.com.
- [32] WIKIPEDIA: https://es.wikipedia.org/wiki/Dominio_de_nivel_superior.
- [33] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/dns-records/>.
- [34] ADMINISTRACIONDESISTEMAS.COM: <https://administraciondesistemas.com/tipos-de-registros-dns-una-guia-detallada/>.
- [35] M. Chica: <https://www.cdmon.com/es/blog/subdominios>.
- [36] F. G. d. Zúñiga: <https://www.arsys.es/blog/que-es-el-ttl-y-para-que-sirve>.
- [37] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/email-security/what-is-smtp/>.
- [38] J. Carlos: <https://www.zeppelinlinux.es/clientes-dns-proceso-de-resolucion-cache-ttl-y-rekursividad/>.
- [39] Y. Tarada: <https://powerdmarc.com/es/dns-vulnerabilities/>.
- [40] R. Oliveira: <https://hospedagemdesit.es/o-que-e-dns/>.
- [41] R. Fouchereau, 2022 Global DNS Threat Repor, European Security, IDC, 2022.
- [42] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning/>.

- [43] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/ddos/glossary/user-datagram-protocol-udp/>.
- [44] INCIBE: <https://www.incibe.es/ciudadania/blog/que-es-una-vulnerabilidad-zero-day>.
- [45] IONOS: <https://www.ionos.es/digitalguide/servidores/seguridad/dns-spoofing/>
- [46] J. Jiménez: <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-arp/>.
- [47] D. C. Barbosa: <https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/>.
- [48] P. d. Toro: <https://www.newtral.es/ciberataque-tendam/20241009/#:~:text=El%20pasado%205%20de%20octubre%2C%20el%20Grupo%20TENDAM,de%20los%20miembros%20de%20su%20club%20de%20fidelizaci%C3%B3n..>
- [49] INCIBE: <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-alcampo>.
- [50] AKAMAI: <https://www.akamai.com/es/glossary/what-is-a-dns-ddos-attack>.
- [51] KASPERSKY: <https://latam.kaspersky.com/resource-center/threats/botnet-attacks?srsId=AfmBOooIemuRP0aVD5dhX-kDPUhxWfgDEnv06k5Z5o5VAXtrvxphozO>.
- [52] WIKIPEDIA: https://es.wikipedia.org/wiki/Red_de_distribuci%C3%B3n_de_contenidos.
- [53] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/ddos/ddos-mitigation/>.
- [54] AKAMAI: <https://www.akamai.com/es/products/prolexic-solutions>.
- [55] AKAMAI: <https://www.akamai.com/es/glossary/what-is-dns-tunneling>.
- [56] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/security/glossary/what-is-lateral-movement/>.
- [57] E. E. d. IONOS: <https://www.ionos.mx/digitalguide/servidores/seguridad/que-es-el-dns-hijacking/>.
- [58] KASPERSKY: <https://www.kaspersky.es/resource-center/definitions/what-is-dns-hijacking>.
- [59] AXARNET: <https://axarnet.es/blog/ping-ip-windows-macos-linux>.
- [60] WHOISMYDNS: <https://whoismydns.com/>.
- [61] ITDIGITAL: <https://www.itdigitalsecurity.es/actualidad/2020/10/el-sector-financiero-el-mas-perjudicado-por-los-ataques-dns>.
- [62] M. L. Domínguez: <https://cybersecuritynews.es/impacto-de-los-ataques-dns-en-las-organizaciones-perdidas-financieras-y-dano-reputacional>.
- [63] SAP: <https://www.sap.com/spain/about/what-is-sap.html>.
- [64] SALESFORCE: <https://www.salesforce.com/es/products/what-is-salesforce/>.
- [65] K. Daniels: <https://widefense.com/blog/el-ataque-ddos-mas-grande-registrado-que-afecto-a-grandes-companias>.

- [66] IBM, «Cost of a Data Breach Report 2024,» IBM, 20224. IBM, 2024.
<https://www.ibm.com/reports/data-breach>.
- [67] A. Warburton: <https://www.welivesecurity.com/la-es/2020/11/20/analisis-sad-dns-vulnerabilidad-permite-envenenamiento-cache-dns/>.
- [68] S. Winterfeld: https://www.akamai.com/es/blog/security-research/attack-trends-in-financial-services?utm_source=chatgpt.com.
- [69] S. González: <https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/>.
- [70] M. Molist: https://www.elconfidencial.com/tecnologia/2016-01-21/amenazas-en-la-oscuridad-como-los-hackers-pueden-provocar-un-apagon-en-tu-ciudad_1138837/.
- [71] NIVEL 4: <https://blog.nivel4.com/ransomware/ciberataque-paraliza-una-serie-de-hospitales-en-los-estados-unidos>.
- [72] WIKIPEDIA: https://es.wikipedia.org/wiki/Ciberataques_en_Ucrania_de_2017.
- [73] COMPUTERWORLD: <https://www.computerworld.es/article/2122202/europa-fue-victima-de-uno-de-cada-cinco-ataques-de-ransomware-en-2021.html>.
- [74] TIMES OF INDIA: <https://timesofindia.indiatimes.com/gadgets-news/50-government-websites-hacked-8-data-breaches-in-2022-says-it-minister-ashwini-vaishnaw/articleshow/97602572.cms>.
- [75] SECURE LIST: <https://securelist.lat/ddos-attacks-in-q4-2021/96226/>.
- [76] TICPYMES: <https://www.ticpymes.es/tecnologia/los-ataques-dns-castigan-a-la-administracion-publica/>.
- [77] HAYCANAL: <https://haycanal.com/web/noticias/13922/los-ataques-al-dns-suponen-a-la-administracion-publica-mas-de-6-millones-de-euros-al-ano>.
- [78] M. L. Domínguez: <https://cybersecuritynews.es/impacto-de-los-ataques-dns-en-las-organizaciones-perdidas-financieras-y-dano-reputacional/>.
- [79] WIKIPEDIA: https://es.wikipedia.org/wiki/Ciberataques_en_Estonia_de_2007.
- [80] IT DIGITAL SECURITY: <https://www.itdigitalsecurity.es/endpoint/2019/03/una-oleada-de-ataques-dns-afecta-a-entidades-de-todo-el-mundo>.
- [81] H. Holm: <https://www.digicert.com/es/blog/how-to-troubleshoot-dns-issues-for-security-and-performance>.
- [82] M. Beucher: <https://ciberseguridadtips.com/dnssec/>.
- [83] CIBERSEGURIDAD: <https://ciberseguridad.com/guias/dnssec/>.
- [84] C. Clavero: <https://www.adslzone.net/2019/02/01/edns-dns-velocidad-seguridad/>.
- [85] DEVELOPERS GOOGLE: <https://developers.google.com/speed/public-dns/docs/dns-over-tls>.
- [86] L. Z. J. H. Z. Hu, Specification for DNS over Transport Layer Security (TLS, Internet Engineering Task Force (IETF) , 2016.

- [87] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/what-is-1.1.1.1/>.
- [88] QUAD9: <https://quad9.net/es/>.
- [89] A. Soto: <https://www.lynksthings.com/posts/sysadmin/unbound/>.
- [90] KNOT RESOLVER: <https://www.knot-resolver.cz/>.
- [91] I. P. S. (INCIBE): <https://www.incibe.es/incibe-cert/blog/protege-tus-peticiones-dns-dns-over-tls>.
- [92] GOOGLE PPUBLIC DNS: <https://developers.google.com/speed/public-dns?hl=es-419>.
- [93] CCNADESDECERO: <https://ccnadesdecero.es/dns-over-https-que-es/>.
- [94] P. Hoffman: <https://www.rfc-editor.org/rfc/pdf/rfc8484.txt.pdf>.
- [95] Equipo editorial de IONOS: <https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/quic-protocolo-de-transporte-de-internet-basado-en-udp/>.
- [96] NEXTDNS: <https://nextdns.io/>.
- [97] OPENDNS: <https://www.opendns.com/>.
- [98] S. d. Luz: <https://www.redeszone.net/tutoriales/seguridad/que-es-ech-caracteristicas-activacion/>.
- [99] CLOUDFLARE: https://www.cloudflare.com/es-es/learning/access-management/what-is-dns-filtering/?utm_source=chatgpt.com.
- [100] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/>.
- [101] IBM: <https://www.ibm.com/es-es/topics/intrusion-detection-system>.
- [102] L. A. A. Durán: <https://ciberseguridadhoy.es/tipos-de-sistemas-de-deteccion-de-intrusiones-ids-y-sus-funciones/>.
- [103] VPN UNLIMITED: <https://www.vpnunlimited.com/es/help/cybersecurity/host-based-ids>.
- [104] L. R. Iturralde, «Integración de un sistema de detección de intrusos y un escáner de vulnerabilidades para la detección efectiva de ataques informáticos,» *Serie Científica de la Universidad de las Ciencias Informáticas*, p. 18, 2016.
- [105] CALCULADORAIP: <https://calculadoraip.org/ccna-cybersecurity-operations-cyber-ops/ids-ips-y-siem/>.
- [106] CHECKPOINT: <https://www.checkpoint.com/lp/quantum-force-intrusion-prevention-system>.
- [107] CISCO: <https://umbrella.cisco.com/info/cisco-umbrella-dns-security-demo>.
- [108] GOOGLE: <https://safebrowsing.google.com/>.
- [109] Pi-hole: <https://pi-hole.net/>.
- [110] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/what-is-anycast-dns/>.
- [111] XITORING: <https://xitoring.com/es/blog/what-is-dns-monitoring/>.
- [112] E. Figueras: <https://emiliofigueras.github.io/herramienta/Zeek-1/>.

- [113] WIKIPEDIA: <https://es.wikipedia.org/wiki/Splunk>.
- [114] WIRESHARK: <https://www.wireshark.org/>.
- [115] Manage Engine: <https://www.manageengine.com/dns-dhcp-ipam/help/domain-query-analytics-in-ddi-central.html>.
- [116] CISCO: <https://umbrella.cisco.com/opendns-cisco-umbrella>.
- [117] B. Vargas: <https://www.byronvargas.com/web/que-es-un-dns-privado-y-publico/>
- [118] L. Subiabre: <https://luissubiabre.wordpress.com/2014/04/29/deshabilitar-recursividad-dns/>.
- [119] SALESFORCE: <https://help.salesforce.com/s/articleView?id=000386441&type=1>.
- [120] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/cdn/glossary/time-to-live-ttl/>.
- [121] B. Vargas: <https://www.byronvargas.com/web/el-dns-se-actualiza-automaticamente>.
- [122] *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO*, 2016.
- [123] PCI Security Standards Council, *PCI DSS*, PCI Security Standards Council, 2018.
- [124] WIKIPEDIA: <https://en.wikipedia.org/wiki/BIND>.
- [125] MICROSOFT: <https://learn.microsoft.com/es-es/windows-server/networking/dns/quickstart-install-configure-dns-server?tabs=powershell>.
- [126] KASPERSKY: <https://www.kaspersky.es/resource-center/definitions/what-is-security-awareness-training>.
- [127] J. M. Ochoa: <https://www.alhambrait.com/blog/concienciacion-en-ciberseguridad-por-que-es-importante/>.
- [128] WIKIPEDIA: https://es.wikipedia.org/wiki/Ciberataque_a_Dyn_de_octubre_de_2016.
- [129] Computerworld España: <https://www.computerworld.es/article/2128806/el-ataque-ddos-de-dyn-fue-causado-por-100-000-dispositivos-infectados.html>.
- [130] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/ddos/glossary/mirai-botnet/>.
- [131] J. Condliffe: <https://www.technologyreview.es/s/6722/el-investigador-que-se-volvio-detective-para-descubrir-al-hacker-que-le-infecto>.
- [132] O. Buxton: <https://www.avast.com/es-es/c-mirai>.
- [133] G. A. Verdejo, «La vulnerabilidad del sistema de nombres,» 2008.
- [134] INCIBE: <https://www.incibe.es/>.
- [135] NETSCOUT: <https://www.netscout.com/arbor..>
- [136] Linkedin: <https://es.linkedin.com/pulse/dns-basado-en-blockchain-francisco-torrecillas-gilabert..>
- [137] Wiki LEMON: <https://wiki.lemon.me/ethereum/ethereum-name-service-ens-que-es/>.
- [138] PALO ALTO NETWORKS: <https://www.paloaltonetworks.es/network-security/advanced-dns-security>.

[139] FORTINET: <https://www.fortinet.com/lat>.

[140] CLOUDFLARE: <https://www.cloudflare.com/es-es/learning/dns/top-level-domain/>.

[141] O. Espinosa: <https://www.redeszone.net/tutoriales/internet/dominios-tld/>.

[142] WIKIPEDIA: https://en.wikipedia.org/wiki/Operation_Aurora.

* NOTA: Para la búsqueda, identificación y recomendación de fuentes y sitios relevantes donde encontrar información de apoyo para la realización del trabajo se ha contado con el apoyo de la herramienta de inteligencia artificial: OpenAI (2024), ChatGPT 4o.