Linux:

Vamos a instalar el servidor BIND9 en la versión 9.19 , este es un servidor exclusivo de Linux y es suficientemente flexible, por otra parte, este goza de ser servidor DNS estándar y tener una documentación bastante amplia. Esta versión de BIND es multiplataforma en Ubuntu 20.04, pero no lo son las que la siguen, por lo tanto, añadiremos un repositorio con paquetes actualizados de la siguiente manera:

```
sudo add-apt-repository ppa:isc/bind-dev
sudo apt update
sudo apt install bind9
```

En caso de que BIND9 u otros servidores DNS fallasen en Ubuntu, deberíamos cambiar en la configuración, las IPs desde donde escuchan. No puede estar en 0.0.0.0, porqué intentará habitar el mismo espacio que *systemd-resolved,* por esa razón habrá que cambiarlo para que escuche en 127.0.0.1 y 10.0.109.X.
Para especificar la zona 2daw.iesmariaenriques.es el archivo de configuración */etc/bind/named.conf.local* se hace de la siguiente manera:

```
zone “2daw.iesmariaenriques.es” {
        type master;
        File “etc/bind/2daw.iesmariaenriquez.es.zone”
}
```

Luego copiamos una de las plantillas de registro DNS como */etc/bind/db.local*
Después de hacer los cambios se debe recargar el servicio *named*, para esto haremos:

```
sudo service named restart
```

Esta fila tiene como función ser .2daw y fila1.2daw. Es el servidor autoritativo.

MULTIPLATAFORMA:

El servidor BIND9 es el servidor que usamos para construir el dominio y zona fila2.2daw….
Para instalar BIND requerimos de actualizar nuestros paquetes locales e instalar el software mediante el manejador de paquetes APT, además incluimos la documentación de algunas utilidades comunes:

```
sudo apt-get update
sudo apt-get install bind9 bind9utils bin9-doc
```

Ahora ya podemos empezar a configurar el servidor. Para que BIND actúe como servidor DNS de almacenamiento caché, obligará al servidor a buscar recursivamente respuestas de otros servidores DNS cuando un cliente emita una consulta. Esto es porque está consultando cada servidor DNS relacionado por turno hasta que encuentre la respuesta completa.

Nos movemos a los archivos de configuración de enlaces:

```
cd /etc/bind
```

Para un servidor DNS de almacenamiento en caché, tan solo debemos modificar el archivo *named.conf.options* que se encuentra dentro de el directorio *named.conf*, debemos editarlo con permisos de administrador (sudo), escribiremos lo siguiente:

```
sudo nano named.conf.options

options{
        directory “var/cache/bind”;
        dnssec-validation auto;
        auth-nxdomain no;     #conform to RFC1035
        listen-on-v6 {any;};
}
```

Ahora, configuraremos una lista de direcciones IP o rangos de red en las que confiamos. Encima del bloque de opciones, crearemos un nuevo bloque llamado acl y para este grupo creamos una etiqueta, en este debemos enumerar las direcciones IP o redes que pueden usar este servidor DNS, por supuesto debemos agregar localhost y localnets para que tanto nuestro servidor como el servidor cliente puedan operar dentro de la misma subred/24 automáticamente:

```
acl.goodclients{
        localhost;
        localnets;
}

options{
        directory “/var/cache/bind”;
        recursion yes;
        ALLOW-QUERY { goodclients; }
        dnssec-validation auto;
        auth-nxdomain no;
        Listen-on-v6 { any; };
}
```

Para que el servidor ya no intente realizar consultas recursivas, cambiamos la configuración. Configuraremos una lista de servidores de almacenamiento en caché para reenviar nuestras solicitudes, dentro del bloque *options{}*, creamos un bloque de reenviadores que contienen las direcciones IP de los servidores de nombres recursivos a los que queremos reenviar las solicitudes:

```
options{
        directory “/var/cache/bind”;
        recursion yes;
```

```
        allow-query { goodclients; }
        forwarder{
                10.0.109.15
                8.8.8.8
        }
}
```

Después debemos establecer la directiva de reenvío en “solo”, ya que este servidor reenviará todas las solicitudes y no debe intentar resolver las solicitudes por sí solo.

```
acl goodclients {
        localhost;
        localnets,
};

options{
        directory “/var/cache/bind”;
        recursion yes;
        allow-query { goodclients ;};
        forwarders {
                10.0.109.15
                8.8.8.8;
        }
        forward only;
        dnssec-validation auto;
        auth-nxdomain no;      #conform to RFC1035
        Listen-on-v6 { any; }
};
```

Ahora tenemos que reiniciar el servidor BIND, las herramientas de BIND verifican la sintaxis de nuestros archivos de configuración, si no hay errores el indicador de shell no mostrará ninguna salida:

```
sudo named-checkconf
sudo service bind9 restart
sudo tail -f /var/log/syslog
```

WINDOWS:

En windows utilizaremos la plataforma MicrosoftDNS, que tan solo funcionan en Windows y la plataforma En concreto utilizaremos WindowsServer 2019 sin interfaz gràfica.

El primer paso es instalar el rol de Servicios de dominio de Active Directory, así que primero abrimos el powershell e instalamos el AD-Domain-Services y ya que estamos instalamos todas las herramientas de gestión que puedan aplicarse a esta característica, escribiendo:

```
powershell
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

Una vez instalado hemos de llevar a cabo la promoción, para esto necesitamos los *cmdlets* contenidos en el módulo *ADDSDeployment a la sesión de trabajo actual*, utilizamos la siguiente sintaxis:

```
Import-Module ADDSDeployment
```

Ahora debemos crear un controlador de dominio;

```
Install-ADDSForest
```

Tras este commando, el sistemo nos pide el nombre que tendrá el dominio y la contraseña de administracion para el modo seguro, en nuestro caso el nombre del dominio será “2daw.iesmariaenriques.es” y la contraseña “123Daw” (para que cumpla con los parámetros de seguridad). Tras esto comienza la instalación de un nuevo bosque y cuando termine se reiniciará el equipo.

Y para comprobar que la promoción ha sido correcta ejecutamos el comando *sconfig* y ya podremos ver el nombre de nuestro dominio.