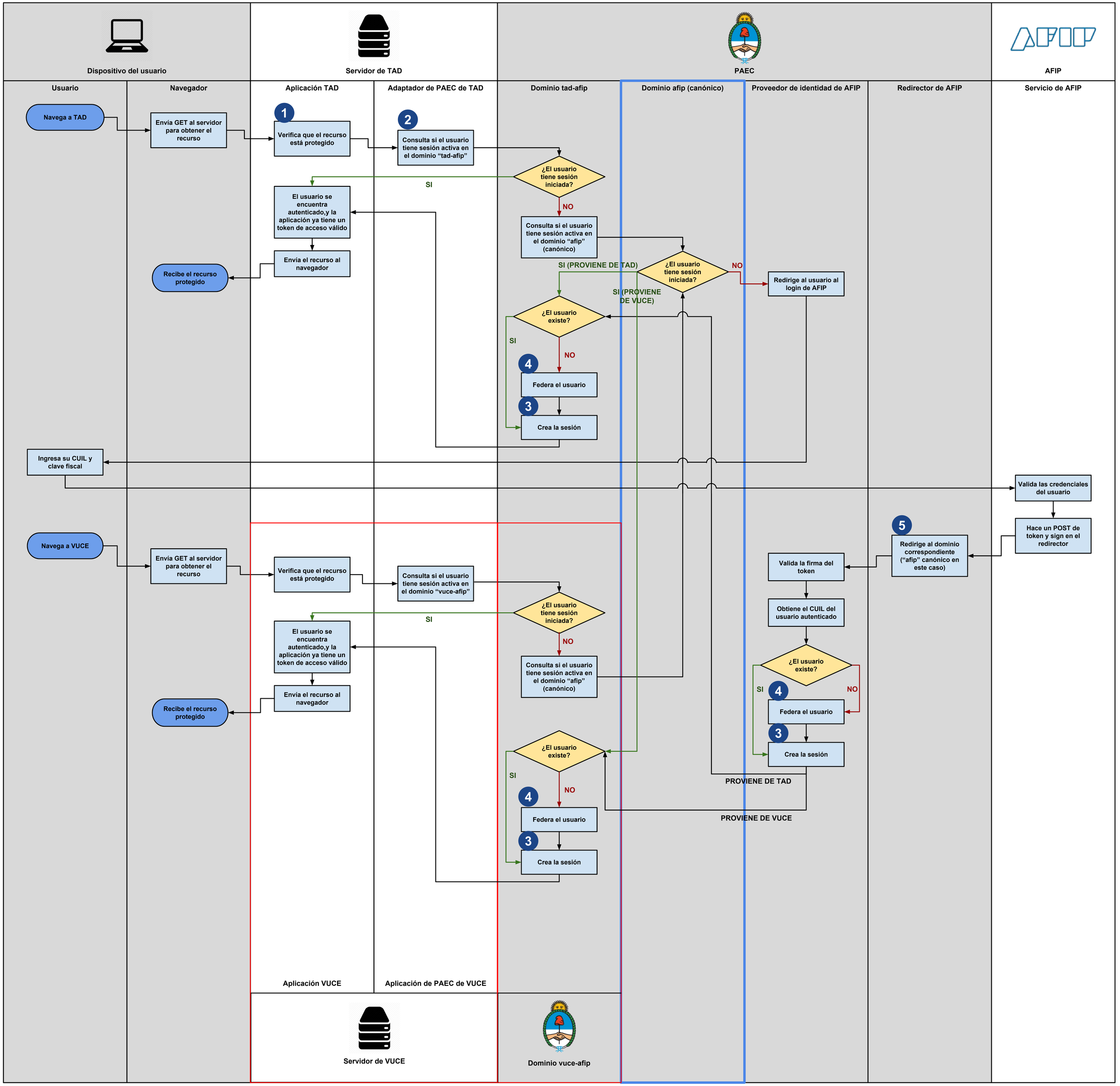

1) Depende de la tecnología:
   a) Angular/Javascript: El adaptador se encuentra en el cliente, y al acceder al recurso verifica si el cliente tiene una sesión activa o no.
   b) Java/web services: Se agregan security-constraints en el archivo web.xml. El adaptador valida la sesión o inicia un login cuando se accede a un recurso protegido.
2) El adaptador obtiene los datos para acceder al servidor de PAEC de un archivo JSON local.
3) El usuario (identificado por CUIL) debe existir en la base de datos de PAEC. *Ver 4.*
4) “Federar” un usuario es crear un usuario de PAEC, vinculado a la identidad del mismo en AFIP. Este usuario federado guarda los datos que después se expondrán en el ID Token a las aplicaciones cliente. Solamente puede guardar y exponer los datos devueltos por AFIP.
5) Como AFIP hace el POST a una URL única por cliente, se implementa un redirector para redirigir el POST a distintos dominios. Esto sirve para que los clientes que no usen el dominio canónico no tengan que dar de alta un sistema propio en AFIP.