Bloque III

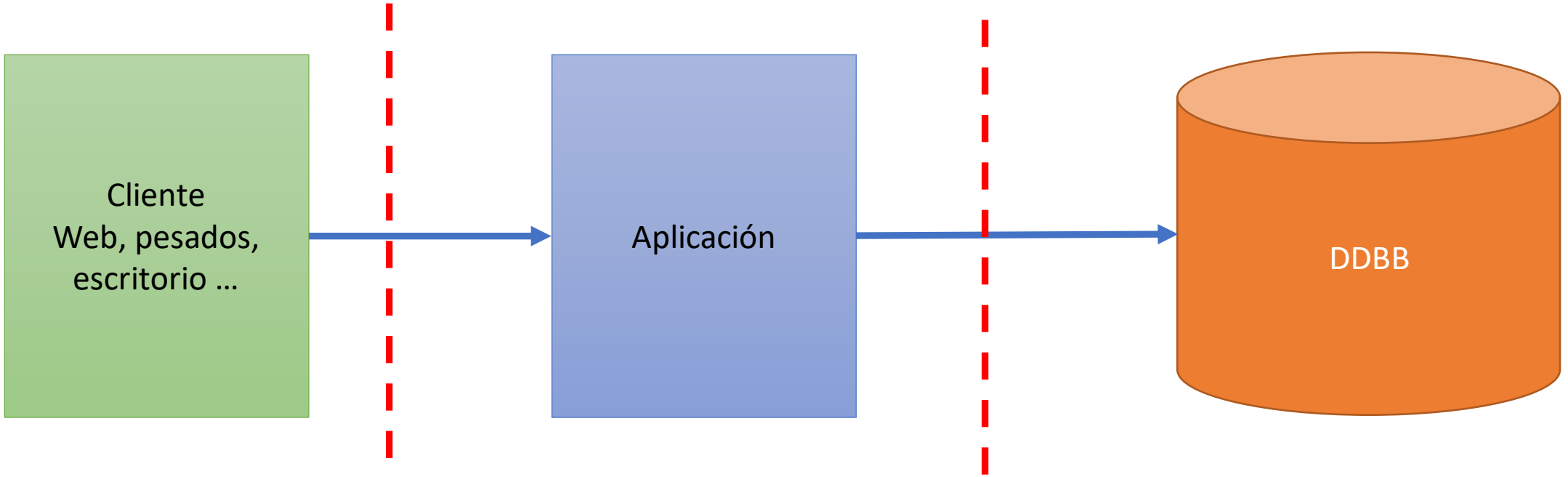
Taller mitigación y pruebas Web con Java

Contenidos

1. Arquitecturas servidor java, transiciones de páginas, SPAs y apis REST.
2. Spring MVC y Spring Boot: especificaciones vs frameworksEstándares OWASP y OWASP Testing Guide
3. Verificación de la gestión de sesiones
4. Verificación del control de acceso
5. Verificación de entrada maliciosa
6. Verificación de la criptografía
8. Verificación del logging y manejo de errores
9. Verificación de la protección de datos
10. Verificación de la seguridad en las comunicaciones
11. Verificación de la configuración de seguridad HTTP
12. Verificación de los controles maliciosos
13. Verificación de la lógica de negocio
14. Verificación de los recursos y ficheros

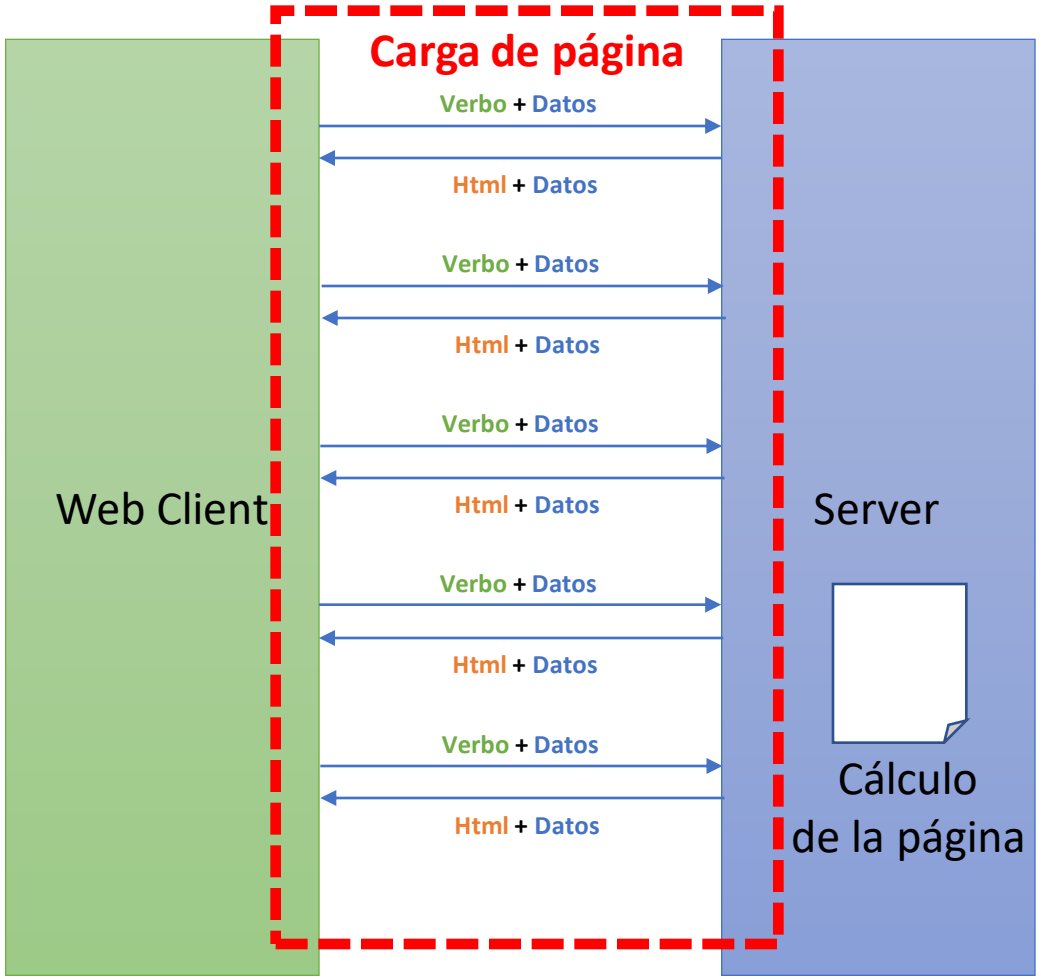
1. Arquitecturas servidor java, transiciones de páginas, SPAs y apis REST

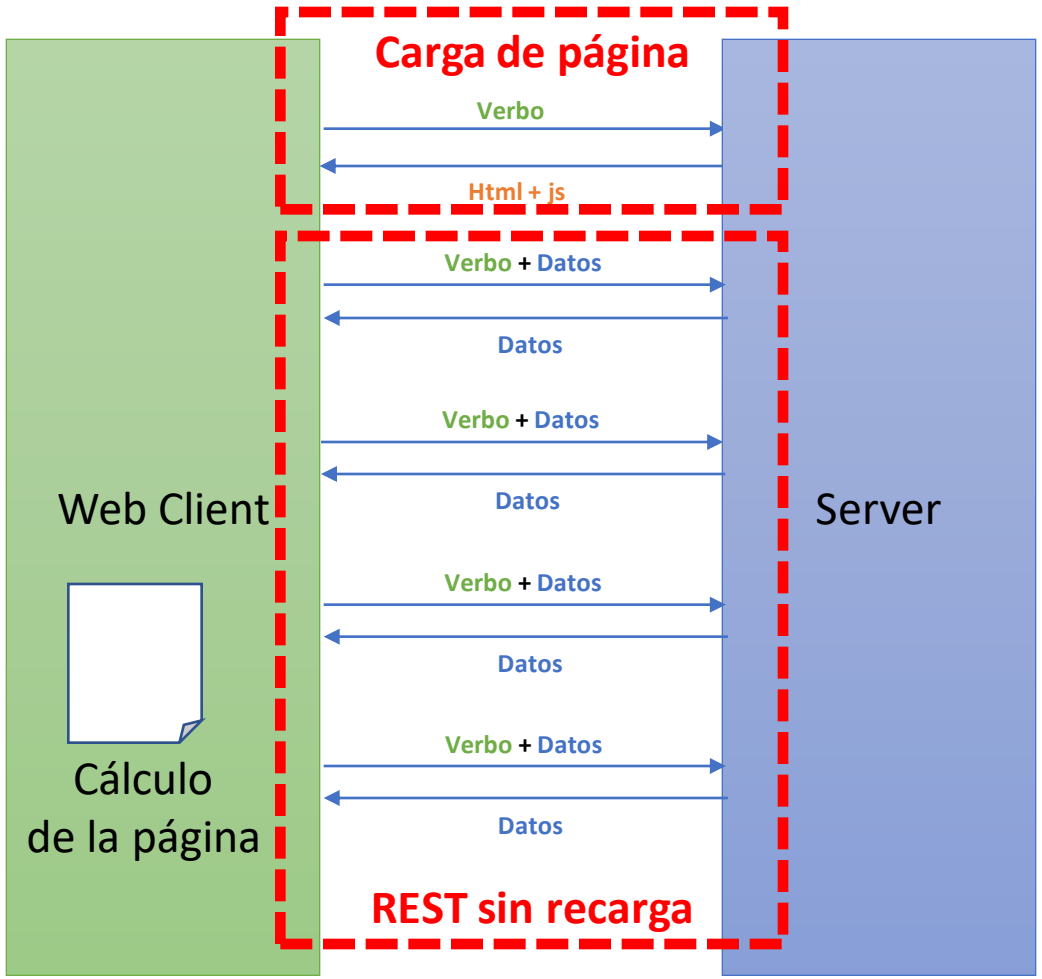
Arquitecturas: Evolución



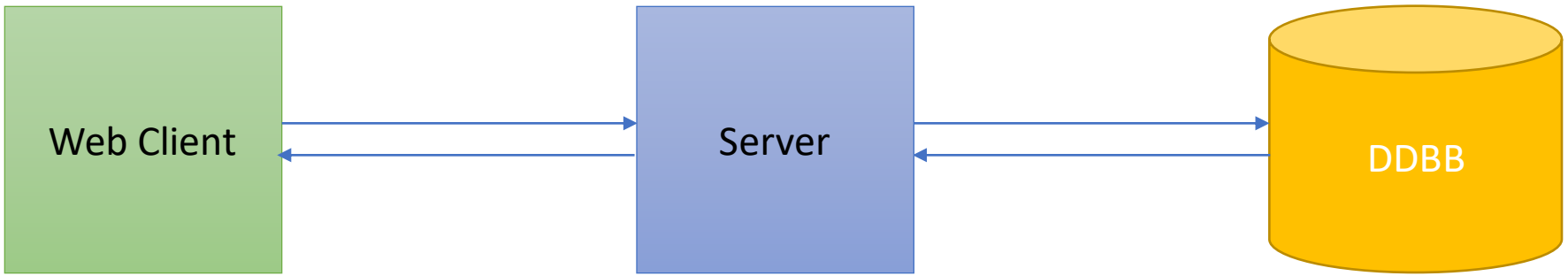
MPA vs SPA

(Multiple Page Application vs Single Page Application)

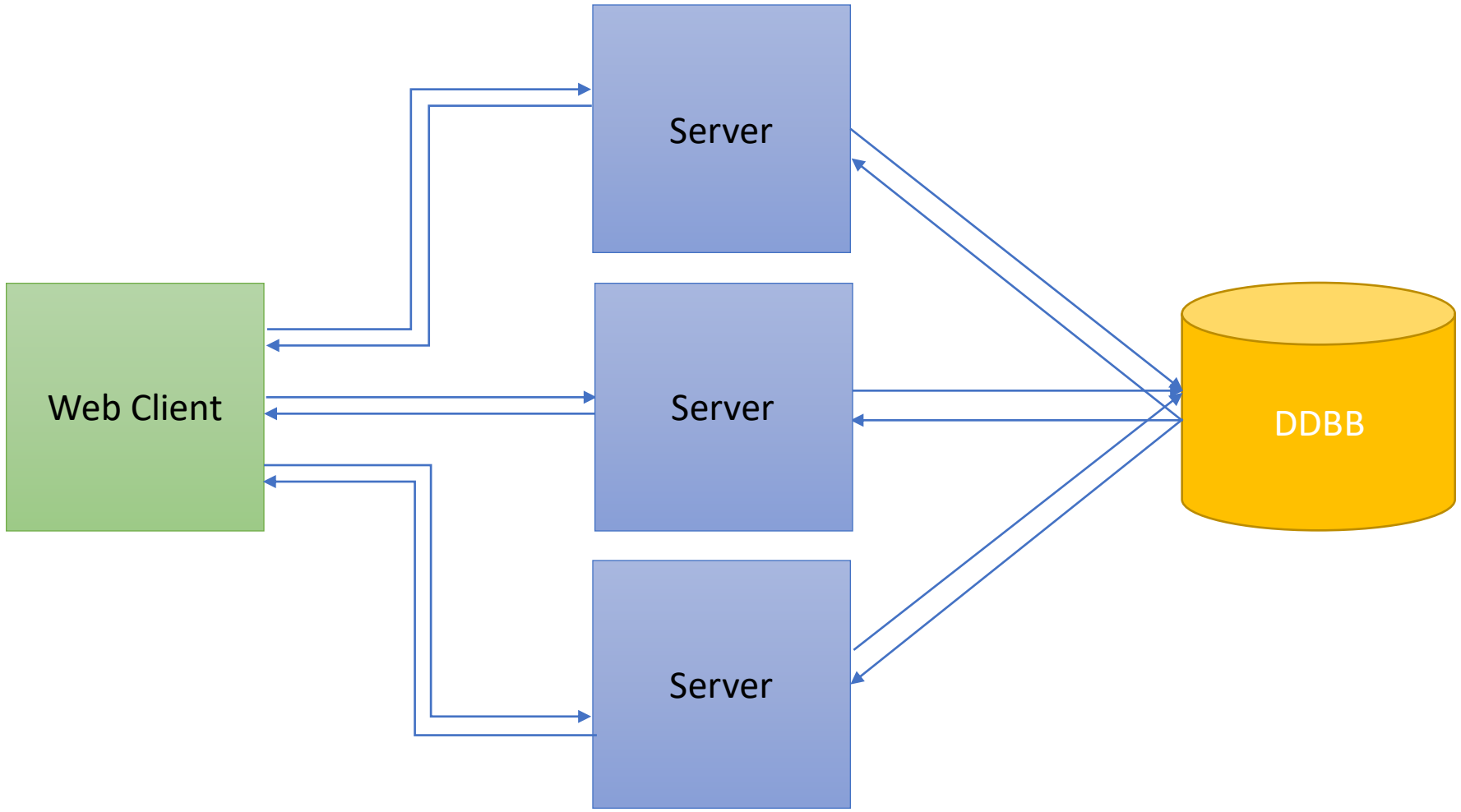




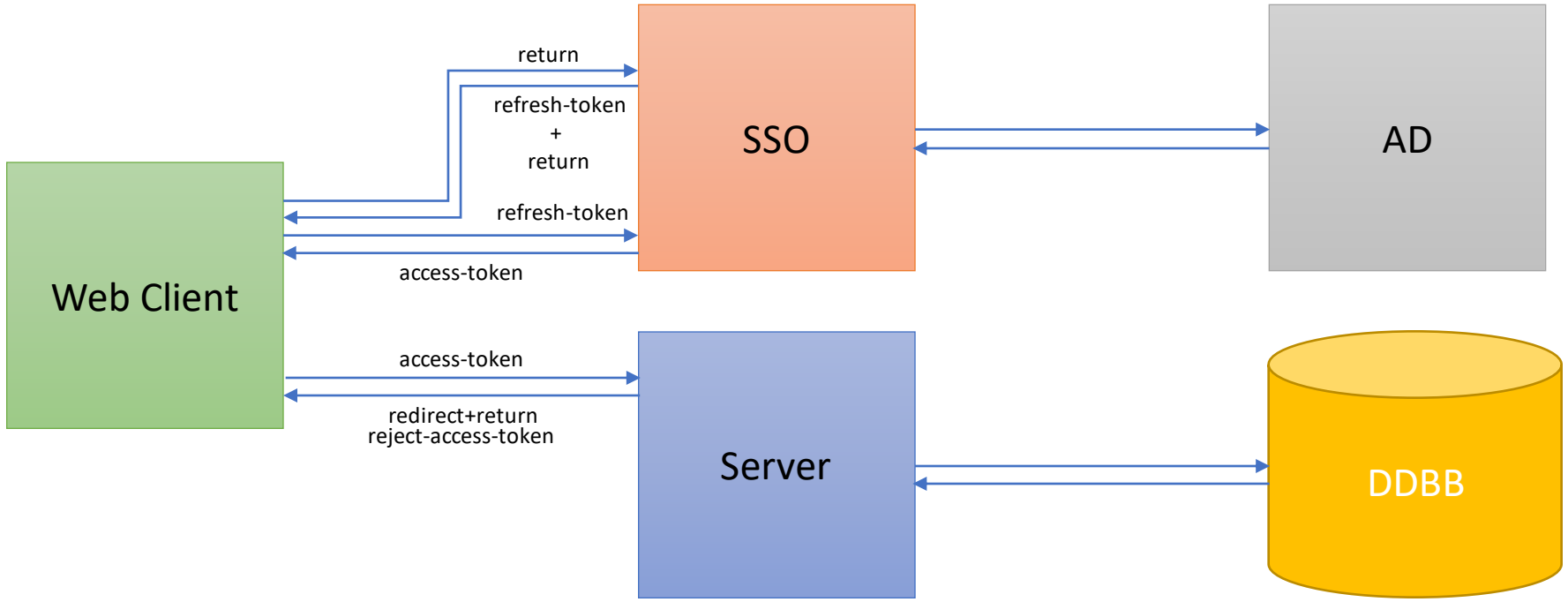
Single Servers: SessionID (stateful)



Multiple Servers: JWT (stateless)



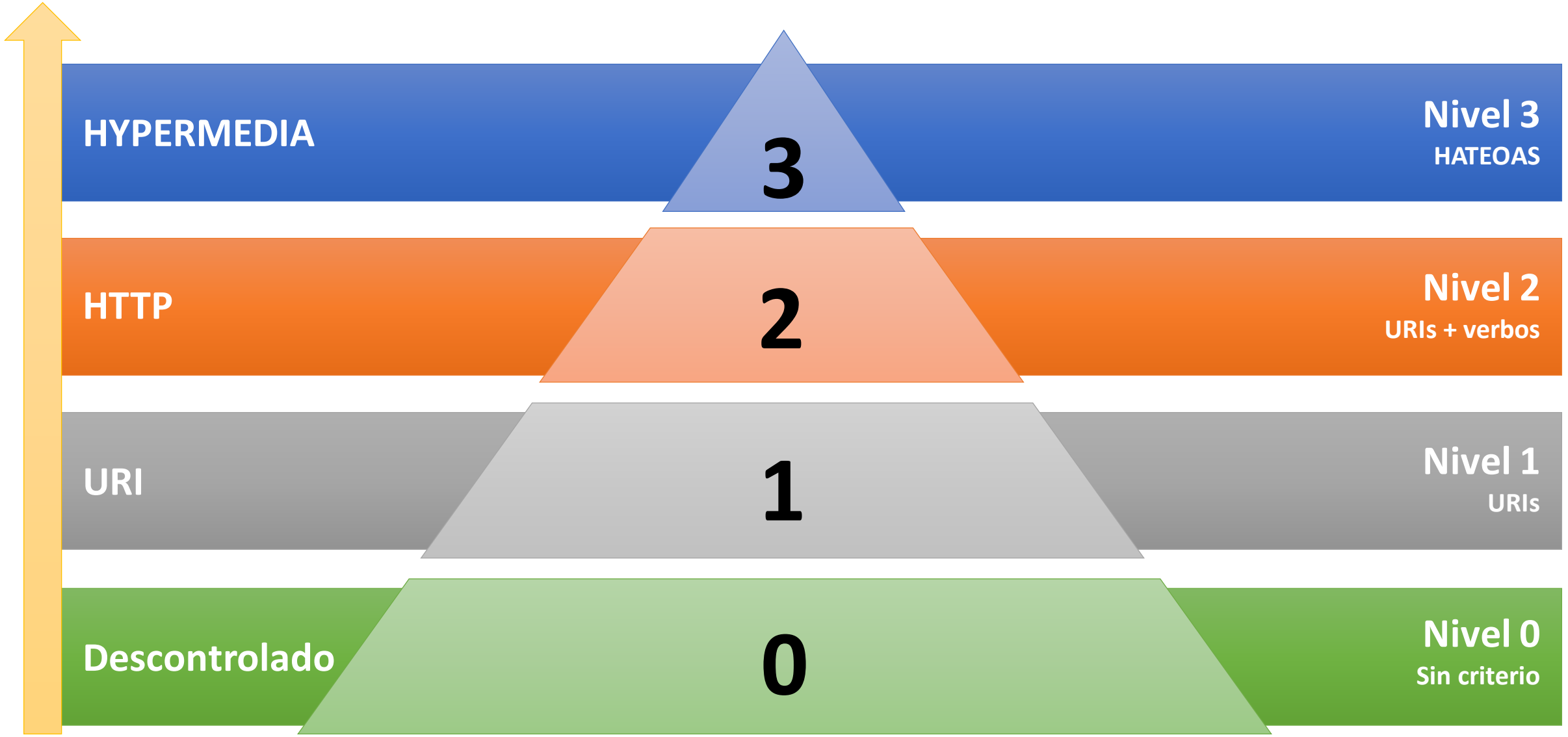
SSO Flow


return
refresh-token
+
return
refresh-token
access-token
SSO
AD
Web Client
access-token
redirect+return
reject-access-token
Server
DDBB

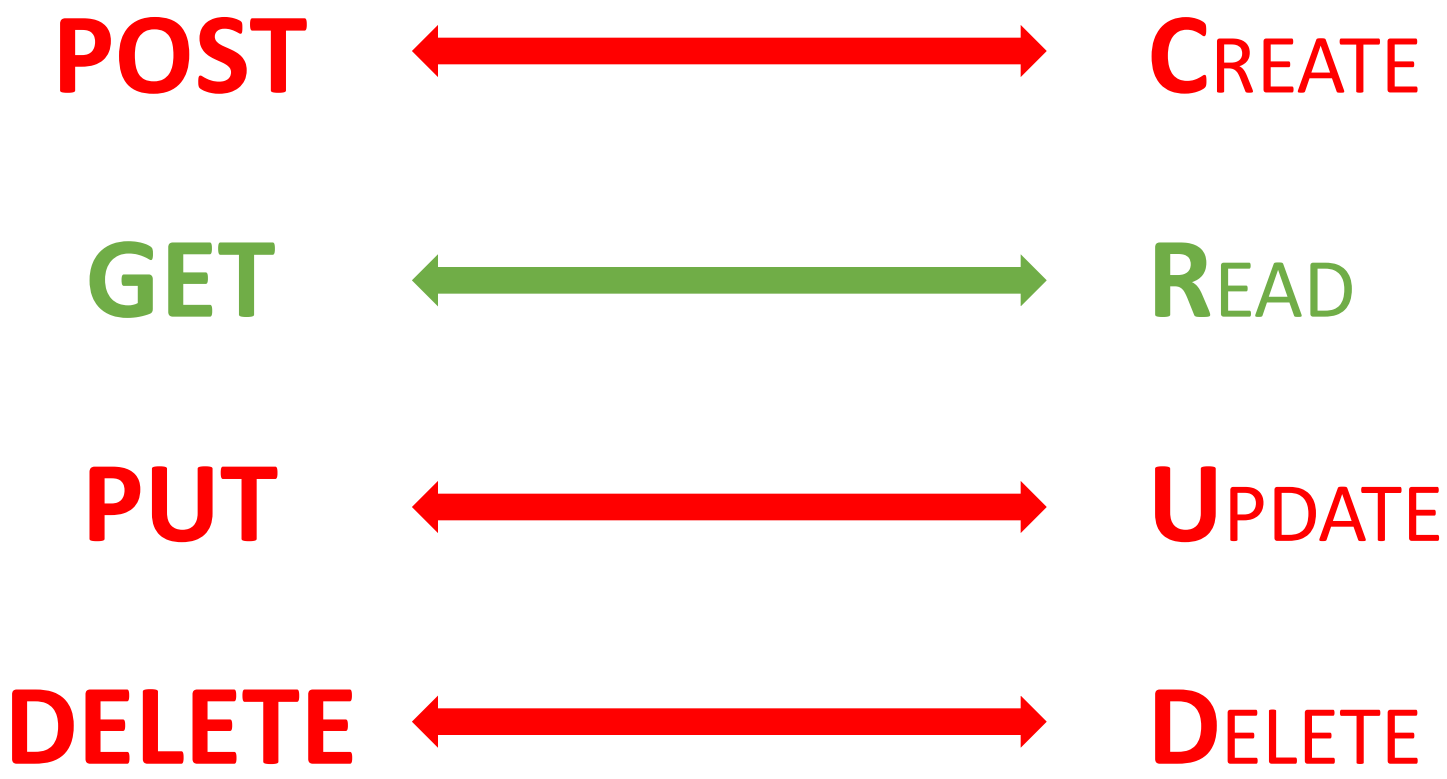
Páginas mezclando datos + presentación

```
<html>
  <head>

  </head>
  <body>

      DATO_X

      <form method='METHOD'>
          <input name='campo1' value='DATO_1'>
          <input name='campo2' value='DATO_2'>
      </form>
      DATO_Y
  </body>
</html>
```

Modelo de madurez de Richardson



Verbos (http) – Acciones (CRUD)

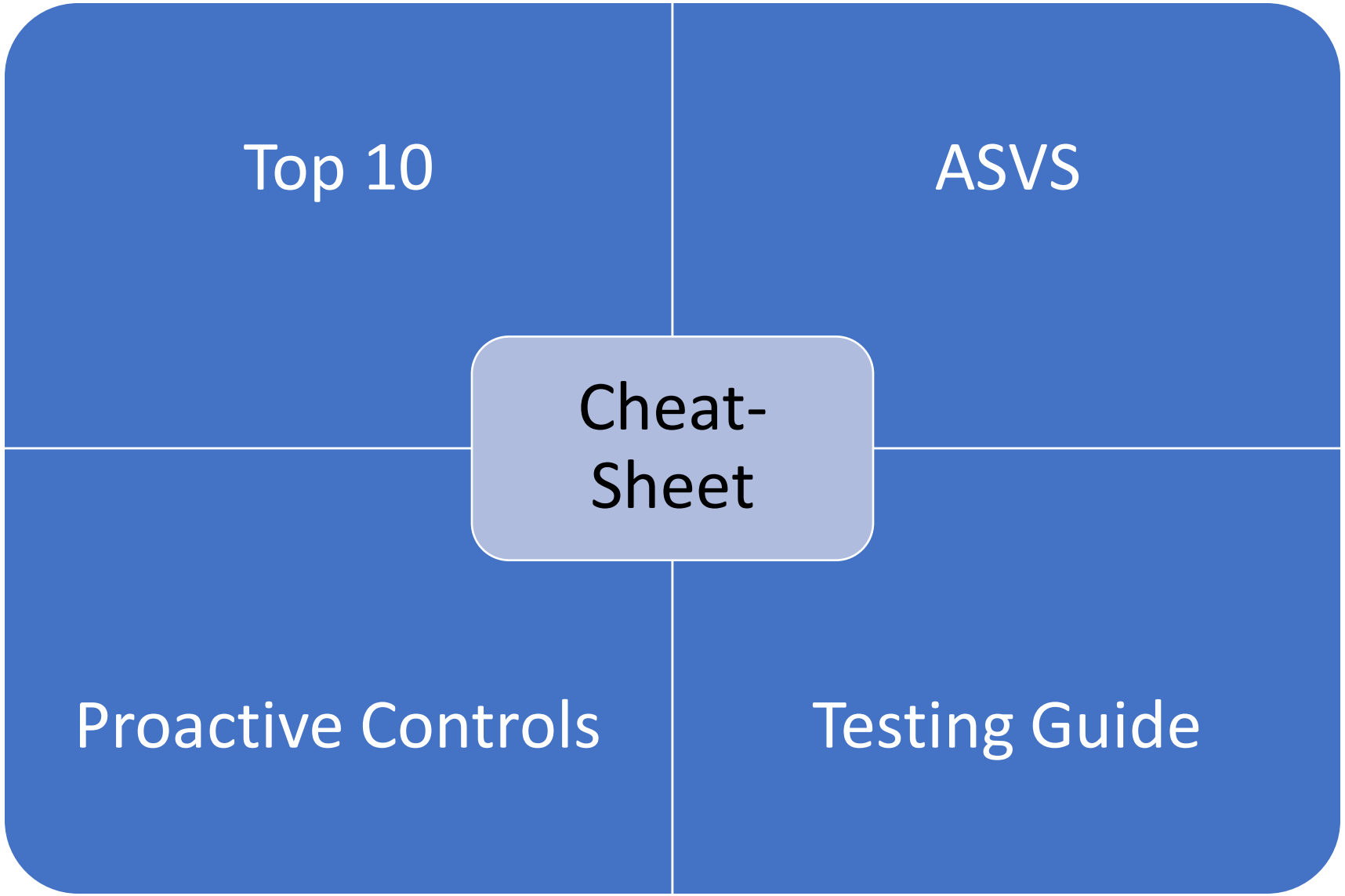


2. Spring MVC y Spring Boot: especificaciones vs frameworks

Un poco de historia

- Java: ¿Lenguaje para lavadoras?
- Evolución relativamente rápida, soporte para aplicaciones Web
- Muy relacionado con el mundo Open Source
- Durante unos años se extendió a otros modelos: aplicaciones móviles
- Las controversias con Oracle
- Spring, modelo alternativo a JEE (JakartaEE)
- Inyección de dependencias… revisited

3. Estándares OWASP y OWASP Testing Guide


Top 10
ASVS
Cheat-Sheet
Proactive Controls
Testing Guide

Pen-Testing

1. Planificación y reconocimiento
2. Escaneo
3. Obteniendo acceso
4. Mantener el acceso
5. Análisis y contramedidas
6. … vuelta al 1

4. Verificación de la gestión de sesiones

En esta primera sesión

- Threat Model
- Implicaciones
- Conocemos nuestras herramientas:
  - WebGoat
  - Firefox
  - Zap
- Entendiendo los protocolos
- Un ejemplo simple de ataque: 2017 - A2 Broken authentication
- Mejores prácticas:
  - https://docs.microsoft.com/en-us/previous-versions/ms178194(v=vs.140)?redirectedfrom=MSDN
  - https://docs.microsoft.com/en-us/previous-versions/aspnet/zdh19h94(v=vs.100) Antiguo