

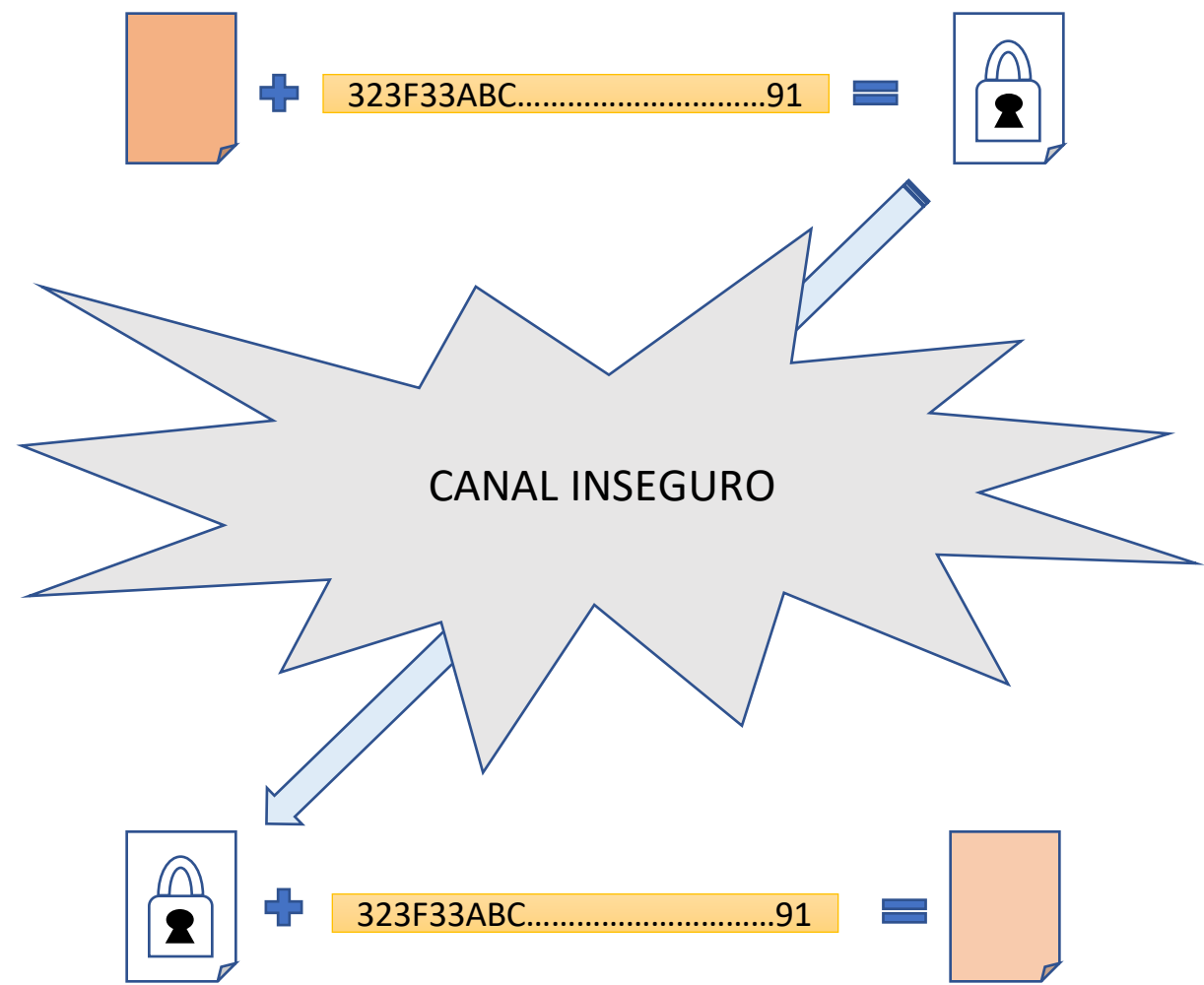
Ejemplo práctico

A8 - Insecure Deserialization

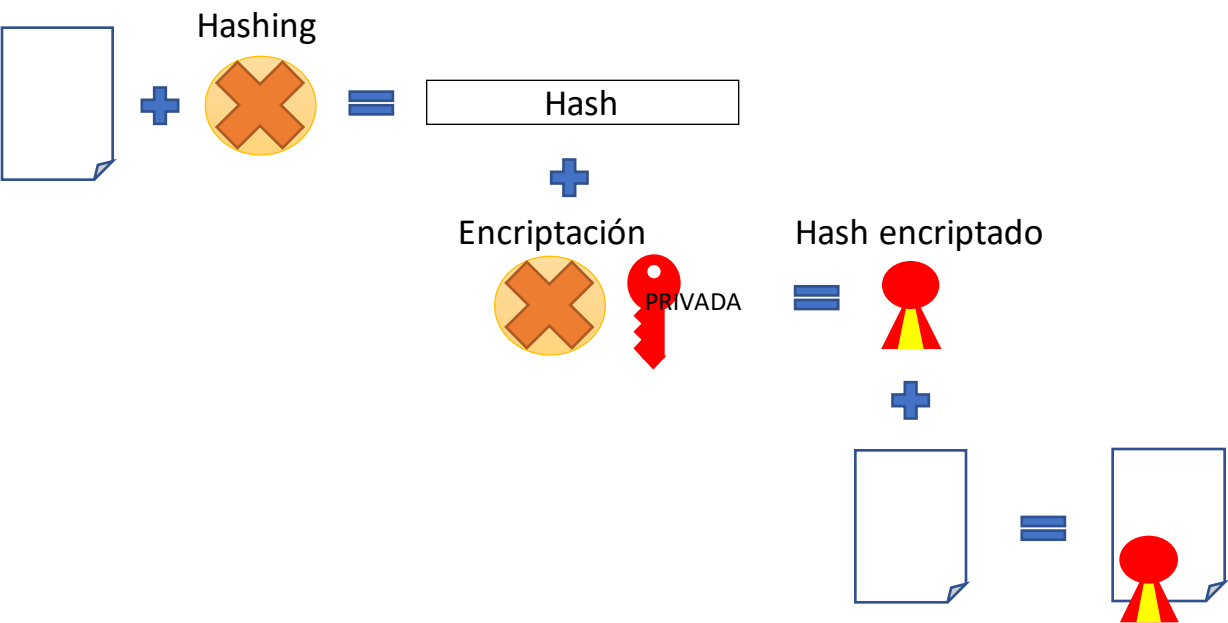
Insecure Serialization

7. Verificación de la criptografía

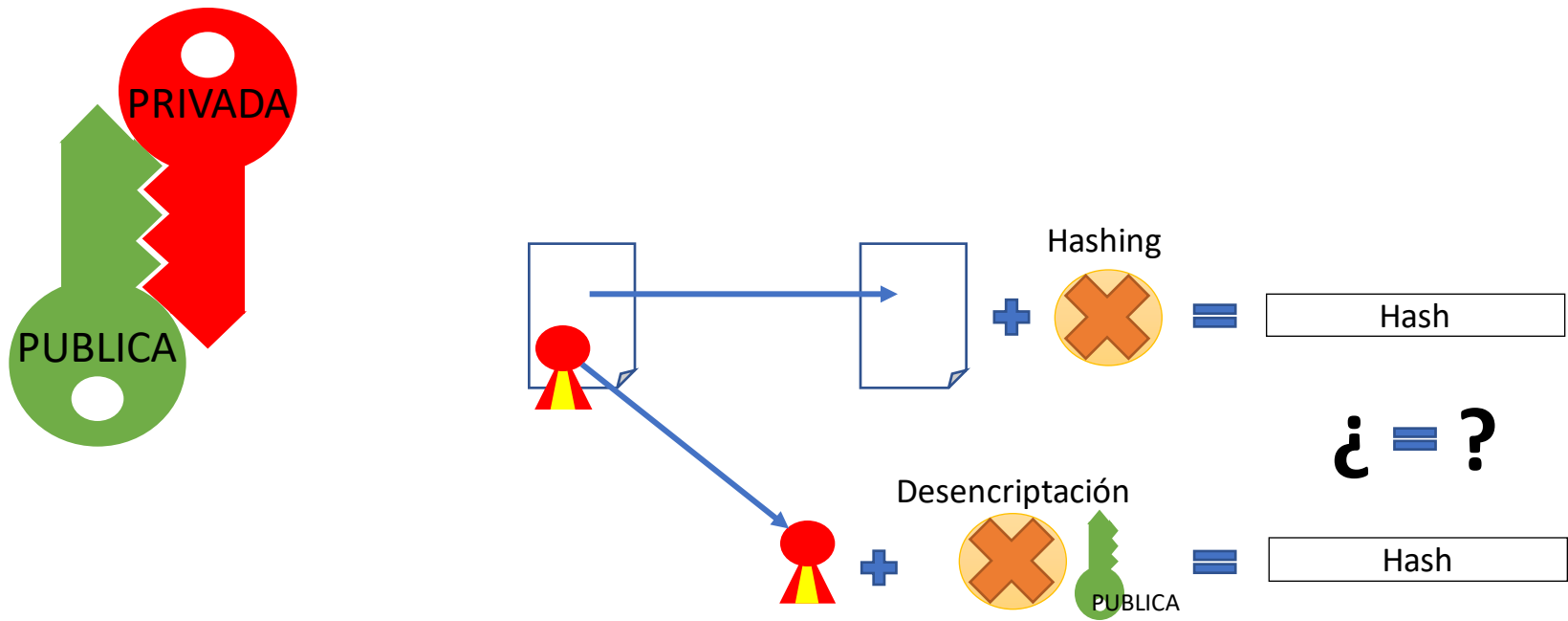
Clave simétrica



Clave pública: Firma



Clave pública: Verificación



JWT y criptografía

HEADER.PAYLOAD.SIGNATURE

Ejemplo práctico

A3 - Sensitive Data Exposure
Insecure Login - Insecure Login

8. Verificación del logging y manejo de errores

Ejemplo práctico

A10 - Insufficient Logging & Monitoring

NO WebGoat

9. Verificación de la protección de datos

10. Verificación de la seguridad en las comunicaciones

Ejemplo práctico

A2 - Broken Authentication (cont.)

[JWT Tokens - Decoding a JWT token](#)

11. Verificación de la configuración de seguridad HTTP

12. Verificación de los controles maliciosos

CSRF token operaciones no seguras...¿y REST?

...

```
<form method='POST (PUT o DELETE no soportado en HTML)'>
```

```
  <input name='campo1' value='DATO_1'>
```

```
  <input name='campo2' value='DATO_2'>
```

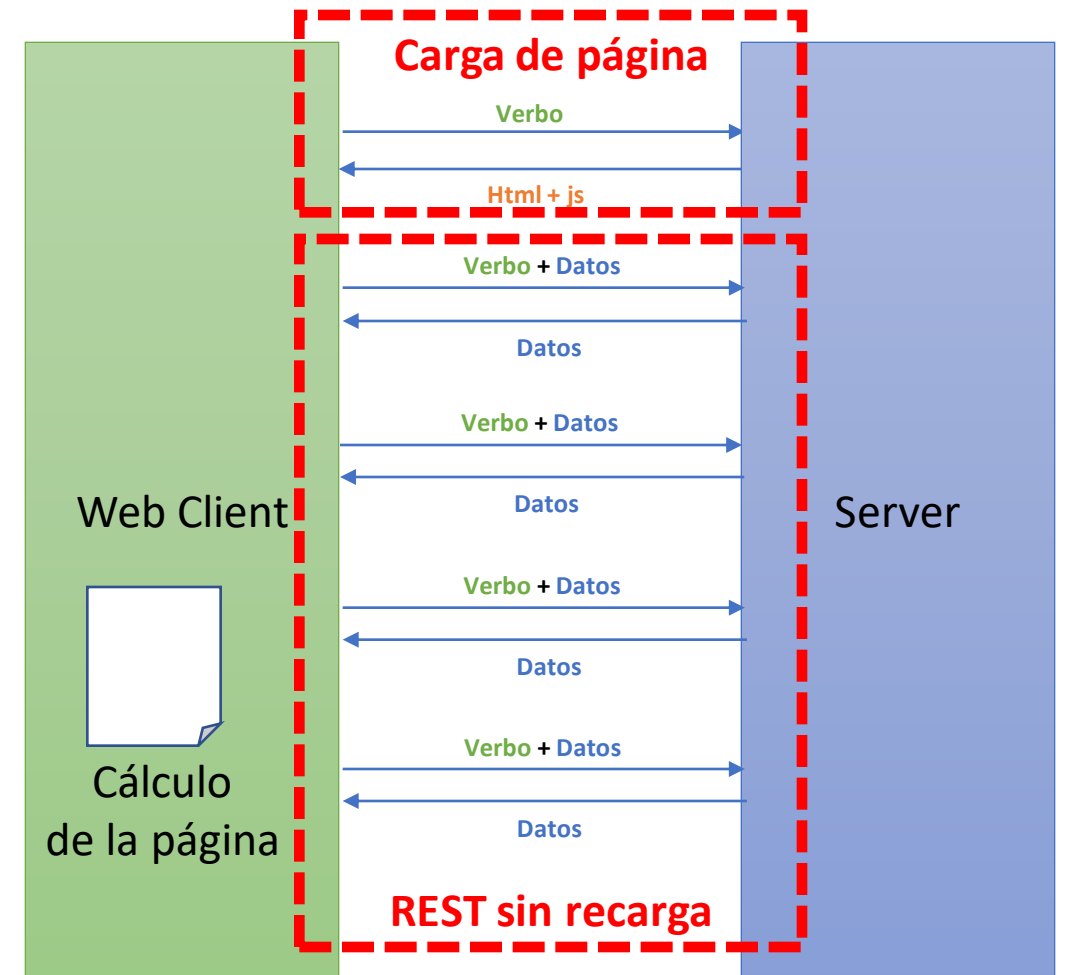
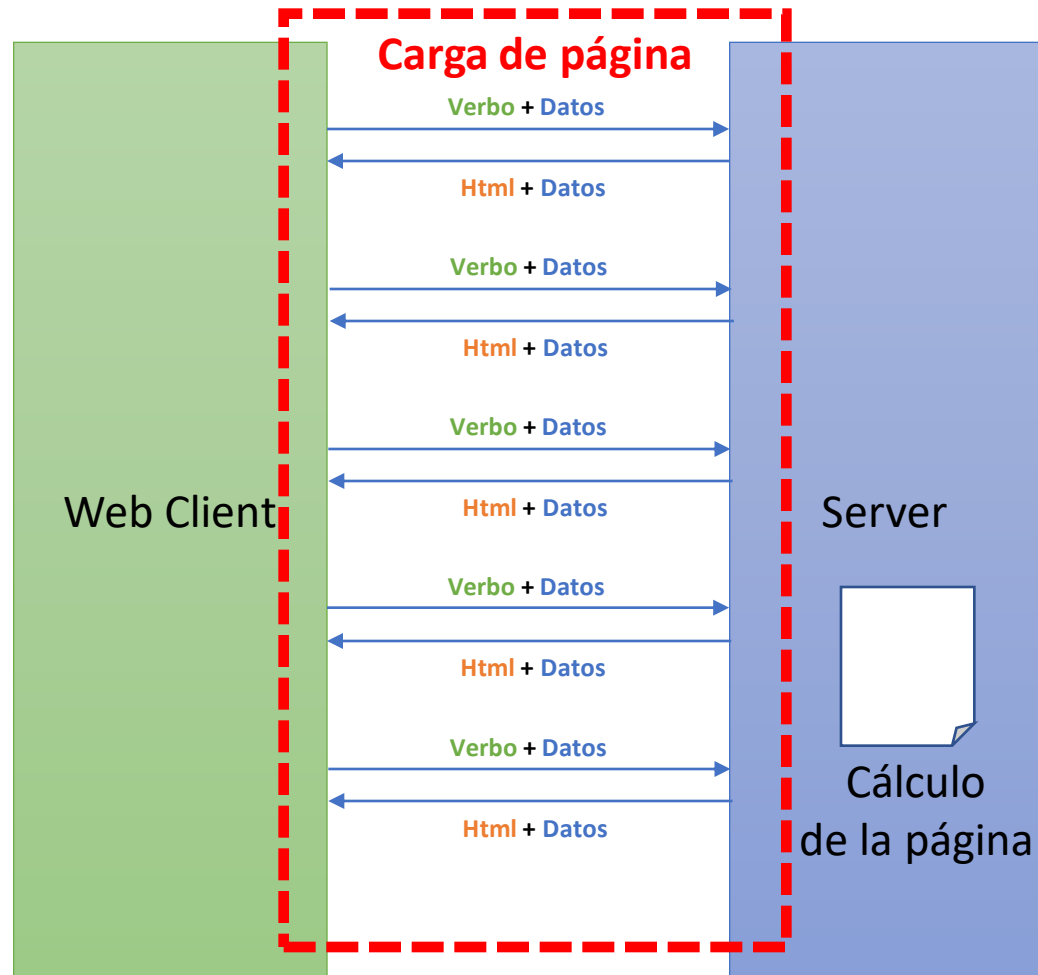
```
  <input name='x-csrf-token' value='token'>
```

```
</form>
```

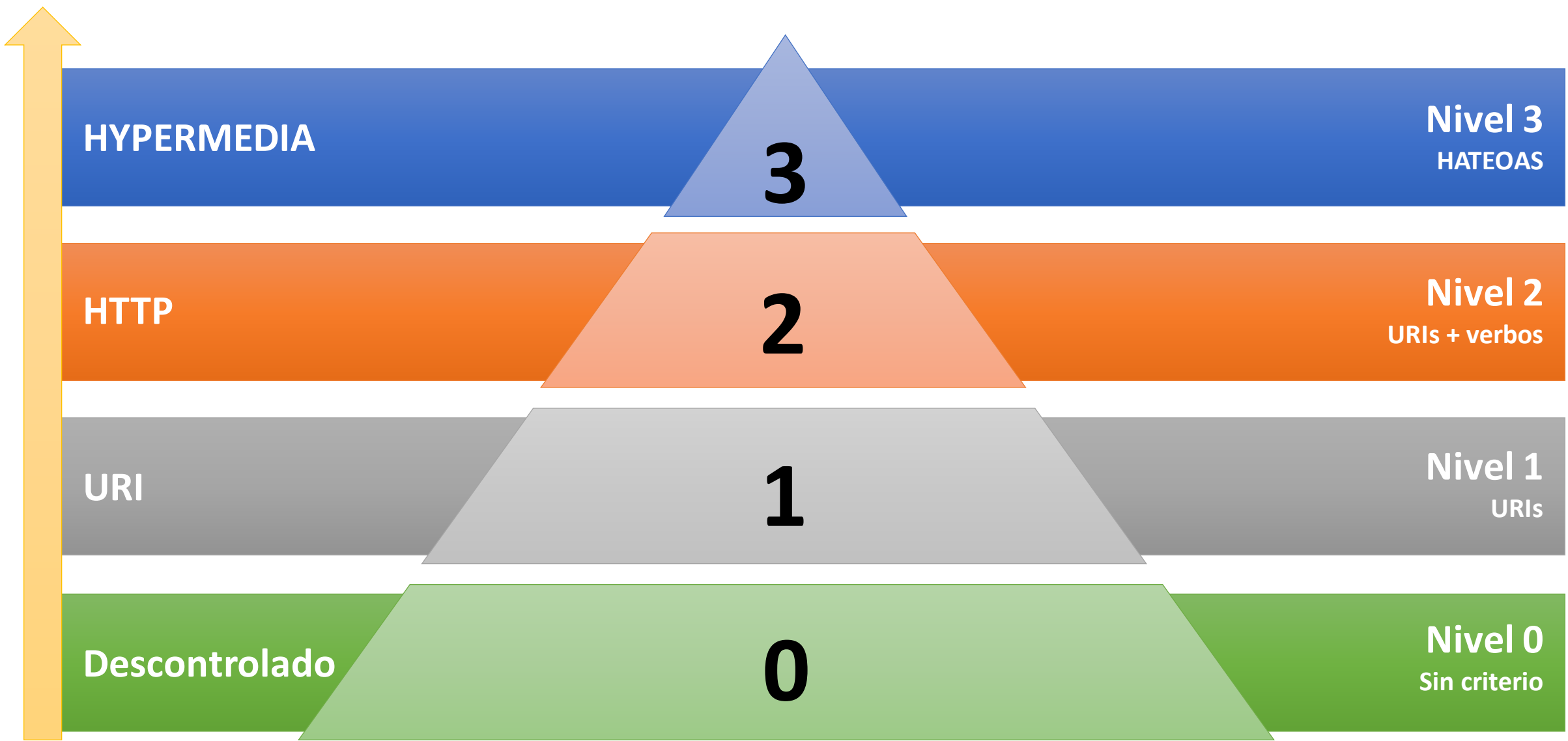
...

MPA vs SPA

(Multiple Page Application vs Single Page Application)



Modelo de madurez de Richardson



Verbos (http) – Acciones (CRUD)

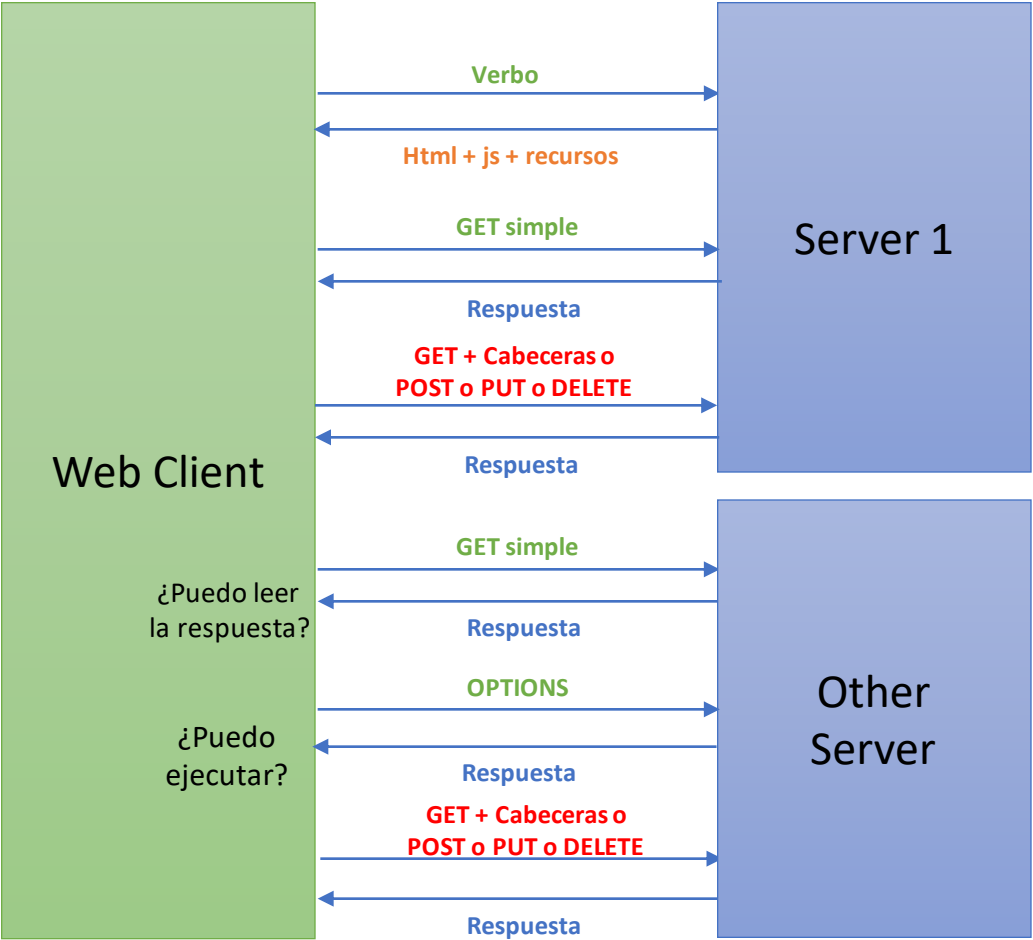
POST ↔ **C**REATE

GET ↔ **R**EAD

PUT ↔ **U**PDATE

DELETE ↔ **D**ELETE

CORS (Cross-Origin Resource Sharing) y Same Origin



Ejemplo práctico

A7 - XSS

Cross Site Scripting - Reflected XSS

Ejemplo práctico

A8 (2013) - CSRF

Cross Site Request Forgery - Confirm Flag

Ejemplo práctico

A9 - Vulnerable Components

NO WebGoat

13. Verificación de la lógica de negocio

Ejemplo práctico

A2 - Broken Authentication (cont.)

Password Reset - Security Questions

14. Verificación de los recursos y ficheros

Ejemplo práctico

A10 (2021) - SSRF

Server Side Request Forgery - Show Jerry