Seguridad dentro de la aplicación WEB

Administración de TOMCAT

- Configurar la aplicación
  - Se usa el fichero web.xml
  - Se define a nivel de “security constraint”

```
<security-constraint>
      <web-resource-collection>
         <web-resource-name>Ejemplo de REALM MEMORY</web-resource-name>
         <url-pattern>/*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
         <role-name>usuario</role-name>
      </auth-constraint>
   </security-constraint>
```

Administración de TOMCAT

- Configurar la aplicación
  - Especificamos el rol de seguridad

```
<security-role>
      <role-name>usuario</role-name>
   </security-role>
```

- Luego se define el mecanismo de login

```
<login-config>
      <auth-method>BASIC</auth-method>
      <realm-name>APLICACION EJEMPLO</realm-name>
   </login-config>
```

Administración de TOMCAT

- Tipos de autenticación
  - BASIC: a través de usuario y password y la información se manda en texto plano
  - DIGEST: similar a BASIC pero la password se manda codificada
  - FORM: el cliente se autentica mediante un formulario HTML. Tanto los campos como el “action formm” se definene en la especificación servlet
  - CLIENT_CERT: utiliza SSL mediante certificado entre cliente y servidor