UD3. SERVIDOR DE APLICACIONES

Servidor de aplicaciones
El despliegue de una aplicación en un servidor de aplicaciones. Tener en cuenta algunos aspectos:

- el descriptor de despliegue
- el servidor de aplicaciones donde se va a desplegarse la aplicación
- la seguridad de la aplicación
- cómo se van a autenticar los usuarios
- la administración de sesiones,
- los registros de logs de la aplicación

Modelo-Vista-Controlador (MVC)
La arquitectura que se emplea en este tipo de aplicaciones es un patrón software que separa la lógica de negocio y los datos de la parte representativa que observa el usuario, los eventos y las comunicaciones entre los distintos componentes.

Modelo: es el componente que se encarga de representar la información con la que la aplicación trabaja. Por lo que su función es la de realizar las consultas y modificaciones con base en los privilegios definidos previamente en el análisis de requisitos de la aplicación. La petición llega por parte del controlador y este componente ejecuta la acción y la presenta a la Vista.

Vista: visualiza el modelo con un tipo de representación para interactuar con el usuario. Normalmente es la interfaz de la aplicación, ya que puede ser una aplicación web, aplicación de escritorio, o cualquier aplicación en cualquier entorno o sistema operativo.

Controlador: es el módulo más importante, como su propio nombre indica, que con#trola a los otros dos componentes. Responde a peticiones realizadas por el usuario (pulsar un botón de la interfaz), y partir de ahí se comunica con el modelo para manipularlo haciendo cambios en la vista. Se puede concluir que es el mediador entre el Modelo y la Vista.

Servidores de aplicaciones.
Tomcat, Wildfly, IBM WebSphere, Oracle Weblogic

Tomcat.
Conocer carpetas bin, conf, lib, webapp y logs
Conocer ficheros server.xml, context.xml, web.xml y tomcat-users.xml

Seguridad

Configurar el servidor de aplicaciones con soporte SSL/T

Una vez que se ha desplegado una aplicación web, no se puede olvidar proteger a la aplic web y al servidor de aplicaciones de accesos malintencionados. Por otro lado, controla personas ajenas a la aplicación no intercepten información susceptible a través de Interne

5.9.1. Seguridad y autenticación

Para llevar a cabo las soluciones ante las anteriores amenazas, un sistema de seguridad se ba tres conceptos clave, que son los siguientes:

a) *Autenticación:* proceso para identificar quién entra a la aplicación es quién dice ser, y pueda acceder a los recursos.
b) *Confidencialidad:* solamente los extremos de la comunicación conocen la inform que se intercambia.
c) *Integridad:* la información que se transmite de extremo a extremo no es modificad agentes externos.

Con relación a la seguridad, lo importante es que el servidor de aplicaciones controle las comunicaciones entre los distintos elementos que intercambian información a lo largo del flujo de la aplicación. Esto se realiza de forma transparente al usuario. El fichero web.xml es el que se encarga de esta función con las marcas que se han explicado anteriormente.

Por otro lado, se puede controlar la seguridad mediante la programación de servlet y ficheros .jsp que permitan la seguridad de la aplicación.

Con relación a la autenticación, se tienen distintos tipos que se pueden implementar en una aplicación web. Son los siguientes:

- Autenticación digest: es una variante de basic. En lugar de viajar la password por la red, viaja encriptada mediante una función hash. Todos los servidores no soportan este tipo de autentificación.
- Autenticación basic: se basa en solicitar datos al usuario, como un nombre y una contraseña. Esta información no va codificada, por lo que es peligroso usar este tipo de autenticación.
- Autenticación basada en formularios: se basa en solicitar datos al usuario mediante un formulario que introduzca el usuario y una password. Este mecanismo es débil de cara a los hackers, ya que se puede obtener esta información de forma fácil.
- Certificados digitales y SSL: lo ideal es usar el protocolo HTTPS que funciona con el puerto 443 que permite la confidencialidad y la integridad de la información y, por otro lado, se tiene asegurada la autenticación. Todo ello se basa en la criptografía de clave pública. Este método es el que se implementará a continuación.