

¿Qué ofrece Autentia Real Business Solutions S.L?

Somos su empresa de **Soporte a Desarrollo Informático**.
 Ese apoyo que siempre quiso tener...

1. Desarrollo de componentes y proyectos a medida



2. Auditoría de código y recomendaciones de mejora

3. Arranque de proyectos basados en nuevas tecnologías

1. Definición de frameworks corporativos.
2. Transferencia de conocimiento de nuevas arquitecturas.
3. Soporte al arranque de proyectos.
4. Auditoría preventiva periódica de calidad.
5. Revisión previa a la certificación de proyectos.
6. Extensión de capacidad de equipos de calidad.
7. Identificación de problemas en producción.



4. Cursos de formación (impartidos por desarrolladores en activo)

Spring MVC, JSF-PrimeFaces /RichFaces,
 HTML5, CSS3, JavaScript-jQuery

Gestor portales (Liferay)
 Gestor de contenidos (Alfresco)
 Aplicaciones híbridas

Tareas programadas (Quartz)
 Gestor documental (Alfresco)
 Inversión de control (Spring)

Control de autenticación y
 acceso (Spring Security)
 UDDI
 Web Services
 Rest Services
 Social SSO
 SSO (Cas)

JPA-Hibernate, MyBatis
 Motor de búsqueda empresarial (Solr)
 ETL (Talend)

Dirección de Proyectos Informáticos.
 Metodologías ágiles
 Patrones de diseño
 TDD

BPM (jBPM o Bonita)
 Generación de informes (JasperReport)
 ESB (Open ESB)



[Home](#) | [Quienes Somos](#) | [Empleo](#) | [Foros](#) | [Tutoriales](#) | [Servicios Gratuitos](#) | [Contacte](#)

	Tutorial desarrollado por: Roberto Canales Mora 2003-2005 Creador de AdictosAlTrabajo.com y Director General de Autentia S.L. Recuerda que me puedes contratar para echarle una mano: Desarrollo y arquitectura Java/J2EE Asesoramiento tecnológico Web Formación / consultoría integrados en tu proyecto No te cortes y contacta: 655 99 11 72 rcanales@autentia.com.	 autentia real business solutions
---	--	---

Descargar este documento en formato PDF [ssltomcat.pdf](#)

Free SSL Certificates

Issued in mins installed in seconds
 Low price single root 128/256 bit

Certificados SSL VeriSign

Servidor seguro con SSL de 128 bits
 Descargar ahora la guía gratis.

SPW S.L.

Soluciones en SSL-VPN
 Watchguard y Enkoo

CertiSign Site Seguro Pro

Segurança on-line é coisa séria.
 Certificados SSL 128 bits
 CertiSign

Anuncios Goooooogle

Anunciarse en este sitio

SSL en Tomcat

En el desarrollo de aplicaciones profesionales, la seguridad es un elemento clave.

Si trabajas para compañías importantes, puede que tu aplicación haga lo que tiene que hacer pero ... si no cumple ciertos estandares de seguridad... es posible que nunca te la dejen instalar

La seguridad es muchas cosas en este caso vamos a resolver solo una de ellas ... como proporcionar un acceso seguro SSL a ella.

Hay muchas otras cosas que veremos en capítulos dedicados como:

- Almacenamiento de passwords (codificación y acceso)
- Administración centralizadas de usuarios y roles (normalmente mediante LDAP)
- Políticas de contingencia y precedimientos de restauración.
- Puertos que debe mantener abiertos para funcionar (y posibilidad de tunelización de protocolos)
- Y otras muchas cosas

Para poder proporcionar acceso SSL en Tomcat tenemos que seguir los siguientes pasos.

Primero instalárnoslo (jeje)

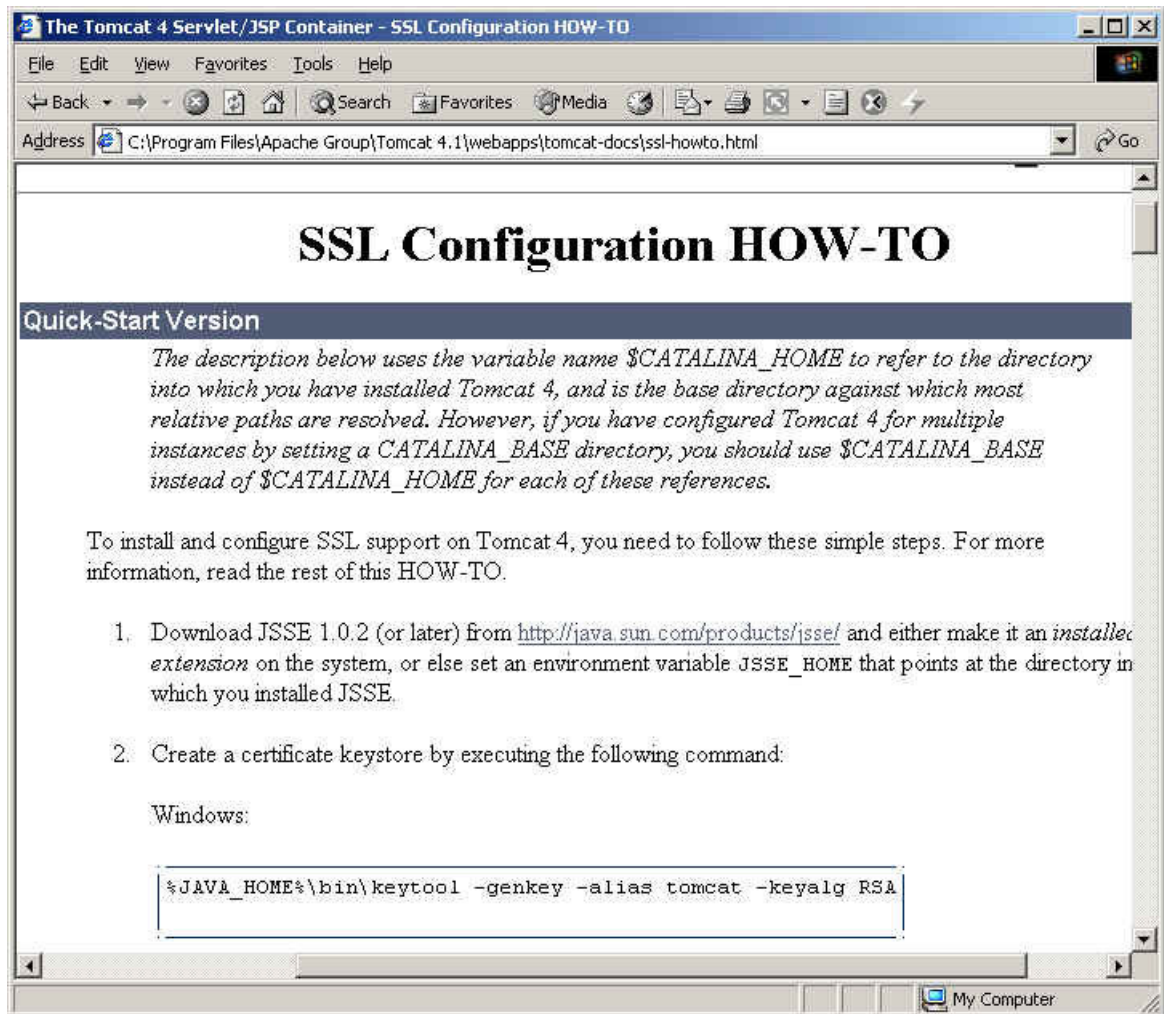
Posteriormente hay dos modos de trabajar... uno ... en modo digamos "de andar por casa" y otro utilizando certificado X509 y entidades certificadoras

Vamos a empezar por el primero... basado en tecnología Java

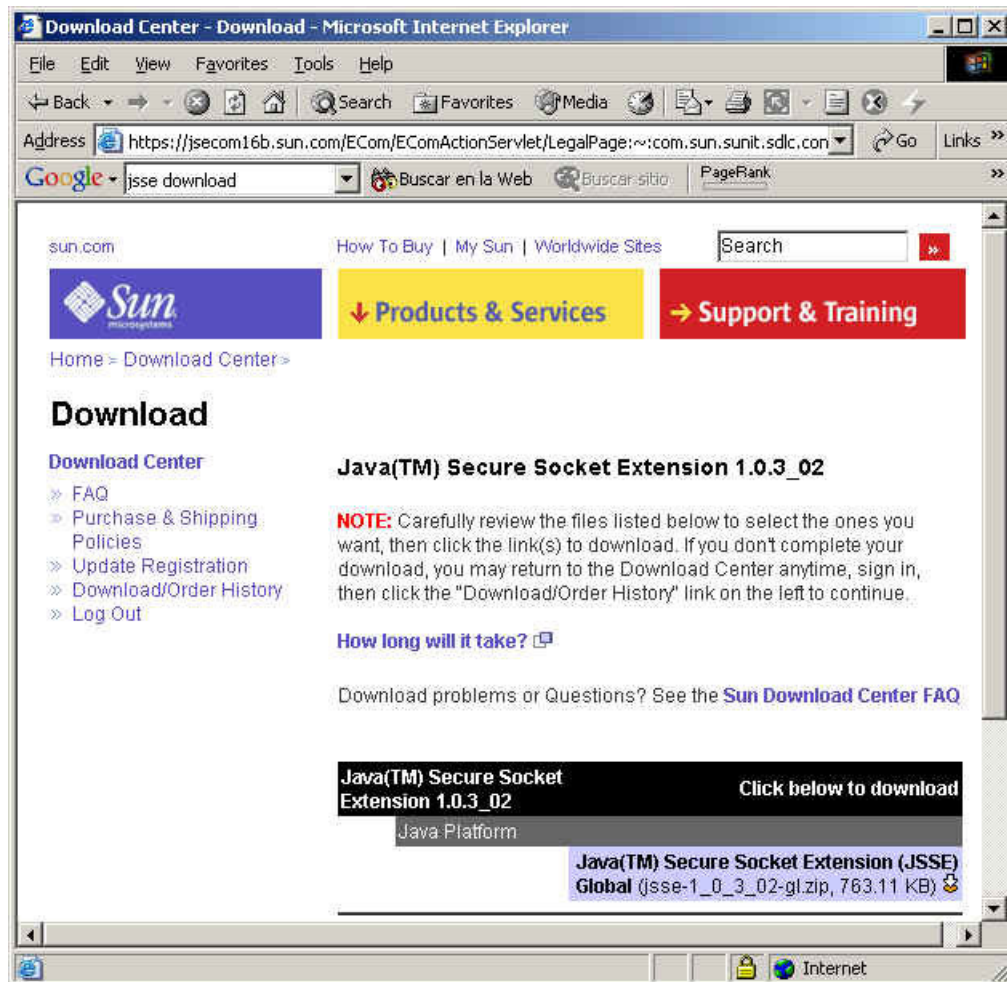
Instalación simple de soporte SSL

Como siempre .. lo más adecuado es buscar en la documentación del propio Tomcat

Yo lo tengo instalado en local en **C:\Program Files\Apache Group\Tomcat 4.1\webapps\tomcat-docs\ssl-howto.html**



Seguimos la instrucciones.. nos descargamos el JSSE de la página de SUN

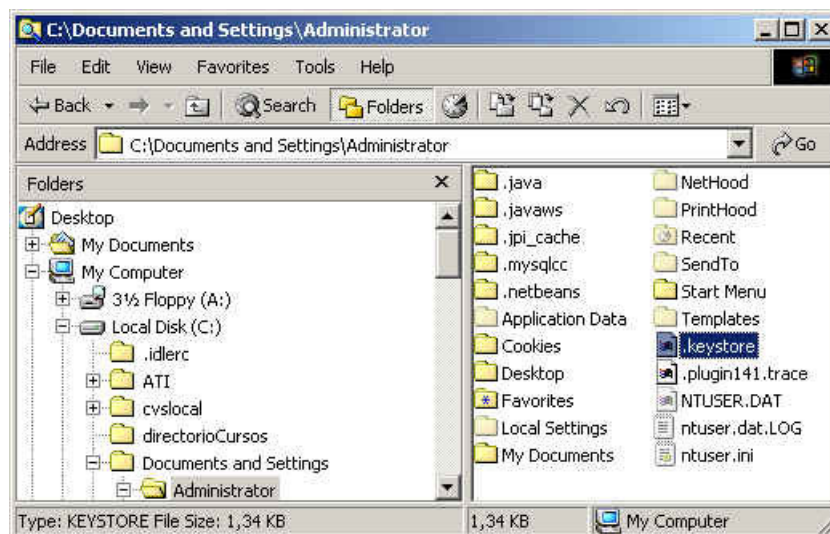


Como indica en el propio documento de ayuda de apache establecemos la variable de entorno JSSE al directorio donde hemos descomprimido el zip que nos descargamos.

Ahora ... generamos nuestro certificado utilizando la utilidad **keytool** de Java

keytool -genkey -alias tomcat -keyalg RSA

Al generar el fichero de claves, se genera en nuestro home para el usuario actual



Observar que hemos puesto la password **roberto**

```

C:\WINNT\System32\cmd.exe

C:\java\j2sdk1.4.1\bin>keytool -genkey -alias tomcat -keyalg RSA
Escriba la contraseña del almacén de claves: roberto
¿Cuáles son su nombre y su apellido?
[Unknown]: Roberto Canales
¿Cuál es el nombre de su unidad de organización?
[Unknown]: casa
¿Cuál es el nombre de su organización?
[Unknown]: adictosaltrabajo
¿Cuál es el nombre de su ciudad o localidad?
[Unknown]: Torrejon
¿Cuál es el nombre de su estado o provincia?
[Unknown]: Madrid
¿Cuál es el código de país de dos letras de la unidad?
[Unknown]: es
¿Es correcto CN=Roberto Canales, OU=casa, O=adictosaltrabajo, L=Torrejon, ST=Madrid, C=es?
[No]: si

Escriba la contraseña clave para <tomcat>
<ENTER> si es la misma contraseña que la del almacén de claves:

C:\java\j2sdk1.4.1\bin>

```

Ahora... debemos activar en el fichero **server.xml** el conector para soporte SSL (que viene comentado ... buscando la cadena "**Define a SSL Coyote HTTP/1.1 Connector on port 8443**") , y lo hacemos activando el **puerto 8443**

Ahora.. como hemos creado nuestro certificado con una password distinta de la que espera Tomcat por defecto (**changeit**), debemos especificarlo

```

server.xml - Notepad
File Edit Format Help

%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA (windows)
$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA (unix)
with a password value of "changeit" for both the certificate and
the keystore itself.

By default, DNS lookups are enabled when a web application calls
request.getRemoteHost(). This can have an adverse impact on
performance, so you can disable it by setting the
"enableLookups" attribute to "false". When DNS lookups are disabled,
request.getRemoteHost() will return the string version of the
IP address of the remote client.

-->

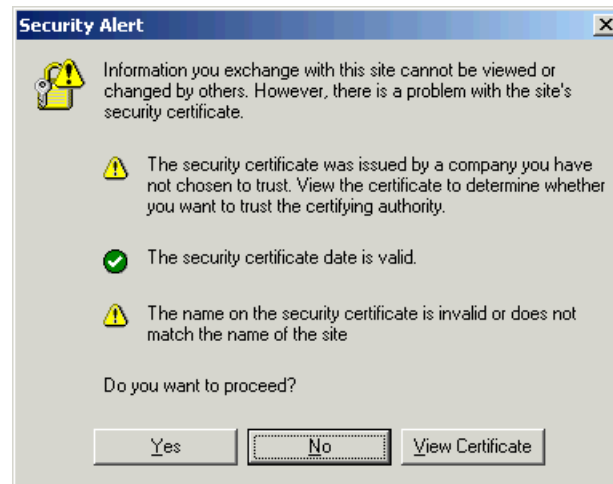
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8080"
minProcessors="5" maxProcessors="75"
enableLookups="true" redirectPort="8443"
acceptCount="100" debug="0" connectionTimeout="20000"
useURValidationHack="false" disableUploadTimeout="true" />
<!-- Note : To disable connection timeouts, set connectionTimeout value
to -1 -->
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"
useURValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
keystorePass="roberto" clientAuth="false" protocol="TLS" />
</Connector>

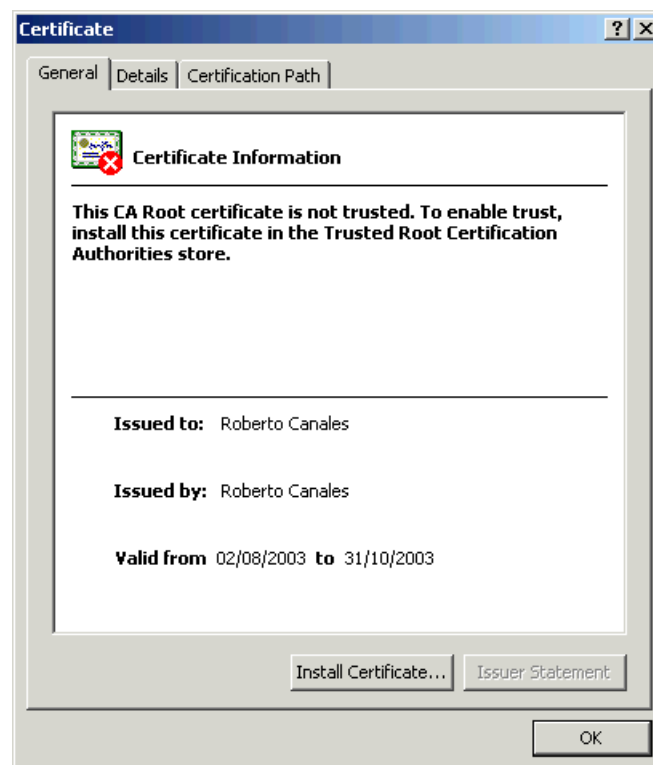
```

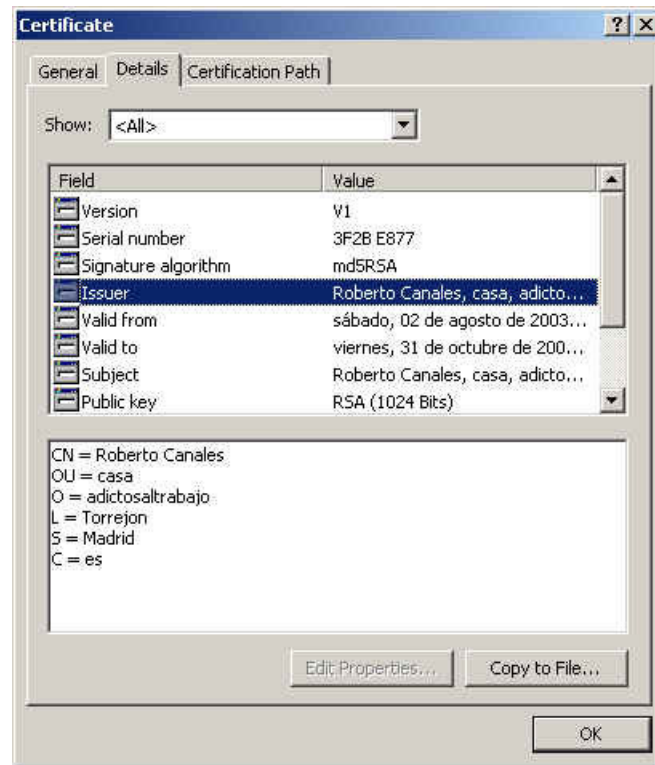
Arrancamos el servidor

Si ahora accedemos a nuestro servicio de modo seguro **https://127.0.0.1:8443**

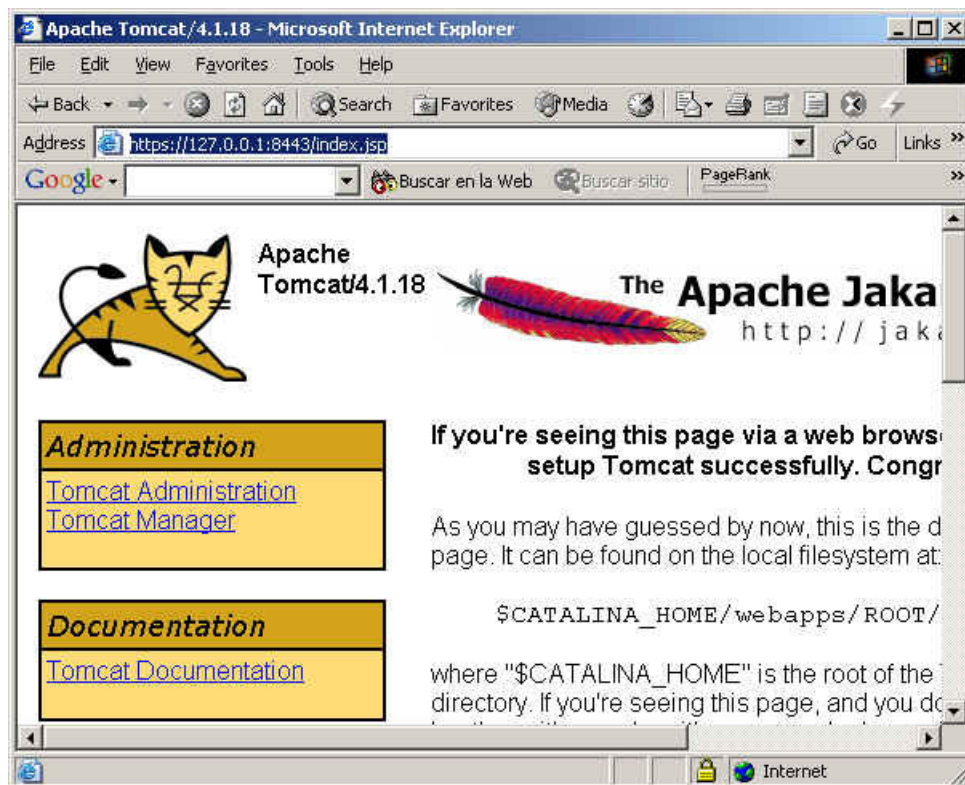


Si vemos los detalles





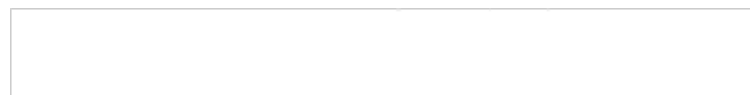
Y despues de aceptar el certificado vemos la página de resultado .. podemos ver el candado amarillo indicando que el enlace es seguro ..



En próximos tutoriales os enseñaremos a hacerlo utilizando entidades certificadoras externas

[Sobre el Autor ..](#)

Si desea contratar formación, consultoría o desarrollo de piezas a medida puede contactar con



[Autentia S.L.](#) Somos expertos en:
J2EE, C++, OOP, UML, Vignette, Creatividad ..

y muchas otras cosas

Nuevo servicio de notificaciones

Si deseas que te enviemos un correo electrónico cuando introduzcamos nuevos tutoriales, inserta tu dirección de correo en el siguiente formulario.

Subscribirse a Novedades	
e-mail	
	Enviar

Otros Tutoriales Recomendados ([También ver todos](#))

Nombre Corto

[Activación de la seguridad en Apache](#)

[Activar SSL en IIS](#)

Descripción

Alejandro Pérez nos enseña como securizar Apache a través de autenticación básica y certificados de seguridad SSL.

Os mostramos como activar el soporte de https en IIS, creando vuestros propios certificados autofirmados, usando OpenSSL

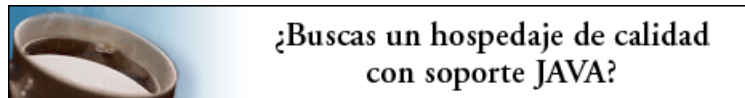
Nota: Los tutoriales mostrados en este Web tienen como objetivo la difusión del conocimiento.

Los contenidos y comentarios de los tutoriales son responsabilidad de sus respectivos autores.

En algún caso se puede hacer referencia a marcas o nombres cuya propiedad y derechos es de sus respectivos dueños. Si algún afectado desea que incorporemos alguna reseña específica, no tiene más que solicitarlo.

Si alguien encuentra algún problema con la información publicada en este Web, rogamos que informe al administrador rcanales@adictosaltrabajo.com para su resolución.

[Patrocinados por enredados.com Hosting en Castellano con soporte Java/J2EE](#)



www.AdictosAlTrabajo.com Optimizado 800X600