SeguriSign Service

versión 8.6

Manual de Servicio

Revisión 1.0

SeguriData

SeguriData Privada, S.A. de C.V.

Av. Insurgentes Sur #2375, 3er. piso,
Col. Tizapán, Del. Alvaro Obregón,
C.P. 01000, México, D.F.

Tel. +52 (55) 3098-0700
Fax. +52 (55) 3098-0702

http://www.seguridata.com

Número de Parte: SIGNService_8.6_Win

Contenido

Capítulo 3. Configuración de SeguriSign Server

CAPÍTULO 1

¿Cómo utilizar este manual?

1.1 Simbología y convenciones

En todo el manual se hace uso de una simbología específica para hacer más sencilla la identificación del tipo de información que se expone, así como de convenciones tipográficas, para hacer más clara la documentación.

1.1.1 Recomendaciones y Advertencias

En los lugares que resulte más oportuno, se insertarán comentarios sobre el contenido del texto.

Importante

Este tipo de anotaciones contienen sugerencias y aclaraciones que facilitan el uso de la aplicación.

Precaución

Este tipo de anotaciones advierten sobre posibles riesgos en las operaciones descritas en el texto y que pueden causar pérdida de funcionalidad o datos.

1.2 Objetivo del Manual

Proporcionar los requerimientos de hardware y certificados, así como los pasos a seguir para la configuración e instalación del Servicio de SeguriSign.

1.3 Objetivo del Producto

Permitir al usuario configurar cada una de las partes que conforman al servicio SeguriSign, con el propósito de iniciar e instalar un nuevo servicio.

1.4 CBitácora de Cambios

En la siguiente tabla se actualizan los cambios de este manual. (Tabla 1.1)

Tabla 1.1

Versión	Fecha de la modificación	Modificación
8.6	28-Jun-2011	* Se corrige defecto detectado en Windows2008 que provocaba que la configuración desde el portal WEB no pudiera completarse, así como el proceso de verificación de transacciones firmadas. El mensaje de error obtenido incluía cualquiera de dos variantes del mensaje (“...error al leer/recibir respuesta de SeguriSign”=) * Habilita la funcionalidad para verificar si un documento es parte de un proceso de firma multilateral. La API para Java habilita el mensaje y el servidor responde de acuerdo al identificador del proceso y el documento o información asegurada. * Permite configurar un parámetro a fin de definir un tiempo en milisegundos para el manejo de timeout para lectura de bytes en los sockets establecidos para las conexiones entrantes al servidor.

CAPÍTULO 2

Instalación de SeguriSign

El siguiente capítulo explica cómo se debe llevar acabo la instalación de SeguriSign versión 8.6. Las actividades enumeradas deberán ser realizadas por personal que cuente con los conocimientos sobre instalación y administración de sistemas, además de tener una cuenta con privilegios de administrador en el sistema.

Se asume que la persona que realizará la instalación es el administrador que cuenta con privilegios de acceso equivalentes y cuenta con conocimientos acerca de:

- el uso de programas bajo Windows,
- instalación de aplicaciones de Windows y
- configuración de servicios de red bajo Windows

2.1 Requerimientos de Hardware

Los requerimientos para el equipo en que se hará la instalación, son:

- Procesador Dual Core a 2.6 GHZ o superior
- 4 GB de memoria RAM o superior
- 90 GB de espacio en disco duro como mínimo
- Unidad CD-ROM
- Conexión a red

2.2 Sistemas Operativos soportados por el Servidor

Los sistemas operativos soportados por el servidor se enumeran a continuación:

- Windows Server 2000. Todos los Upgrades de seguridad disponibles
- Windows Server 2003. Todos los Upgrades de seguridad disponibles
- Windows Server 2008 (Inglés y Español)
- Linux.

2.3 Sistemas Operativos soportados por el Cliente

Los sistemas operativos por el Cliente, se enumeran a continuación:

- Windows Server 2000
- Windows Server 2003
- Windows Server 2008
- Windows XP
- Windows Vista
- Windows 7
- Solaris 10
- Linux
- RedHat Linux 5
- Mac OS 10

2.4 Requerimientos para Windows Server 2008 a 32 bits.

Los requerimientos para Windows Server 2008 a 32 bits son:

- Memoria de 2.0 GB de RAM
- 512 MB de espacio en Disco Duro
- Cliente en Base de Datos: SQL 2008, Oracle 11g ó 10g.

2.4.1 Explorador de Internet soportados por el ActiveX (sólo sobre Windows)

- Internet Explorer 6.0 o superior

2.4.2 Explorador de Internet soportados por el Applet (Windows, Solaris [32&64], Linux, Mac OS 10)

- Internet Explorer 6.0 o superior
- Mozilla FireFox 2.0 o superior

2.5 Idiomas soportados del Sistema Operativo

Los idiomas soportados del sistema operativo son:

- Español
- Inglés

2.6 Procesador

El procesador para el sistema operativo es:

- Procesador a 32 bits

2.7 Ambientes Soportados

Los ambientes soportados para la aplicación son:

- Instancia(s) independiente(s)
- Activo-Pasivo (software de cluster Microsoft)
- Balanceo de Cargas

2.8 Base de datos soportadas

Las bases soportadas son:

- Oracle 9i (32 bits) / 10g(32&64 bits) español e ingles
- MS SQL 2000 (32 bits) sp1 y sp2 / MSQL 2005 (32 bits) sp1 y sp2 / MS SQL 2008 (32 bits)
- IBM DB2 7.2/8.1 español e ingles
- Cliente de base de datos en función del manejador de base de datos instalado

Para la funcionalidad y configuración de SeguriSign se deben instalar las siguientes aplicaciones adicionales:

- Contar con el cliente de base de datos adecuado en el equipo en que residirá el Servidor SeguriSign, como puede ser: Oracle 9i y 10g; DB2 7.1 y 8.2; MSSQL 2000, 2005 y 2008.
- JDBC para manejador de Base de Datos versión 2.0
- JRE 1.6 build 20 o superior
- Tomcat v6.0 o superior

2.9 Requerimientos necesarios para la Instalación

El procedimiento de instalación de SeguriSign requiere de lo siguiente:

- Número de puerto donde estará corriendo el servicio de SeguriSign
- Conocer la dirección IP y puerto donde está corriendo SeguriNotary, en caso de utilizarlo
- Conocer la dirección IP y puertos de la Infraestructura Extendida de Seguridad (IES) (Si aplica)
- Contar con un par de llaves (Pública/Privada) del Cliente IES, y conocer la clave de acceso de la Llave Privada.
- Creación de una base de datos para el servidor que se va a utilizar
- Crear un usuario ligado a la base de datos
- Conocer el Alias, Usuario y Clave de Acceso de la base de datos creada para SeguriSign
- Dirección IP y puerto del Servicio SeguriNom (Si aplica)
- Servidor SMTP y puerto para peticiones (Si aplica)
- Usuario y clave de acceso válidos ante el servidor SMTP (Si aplica)

2.10Otros Requisitos

El procedimiento de instalación de SeguriSign requiere de los siguientes certificados:

- Certificado(s) Digital(es) de la(s) Autoridad(es) Certificadora(s) en formato X.509 binario
- Certificado Digital de la Autoridad Registradora de la IES en formato X.509 binario, (Si aplica)
- Certificado Digital en formato X.509 binario y Llave Privada en formato binario y según el estándar PKCS#8 con encripción PKCS#5, del cliente IES, (Si aplica)
- Certificado Digital en formato X.509 binario y Llave Privada en formato binario y según el estándar PKCS#8 con encripción PKCS#5, para el servicio de Autenticación

- Certificado Digital de SeguriNotary, (Si aplica, recomendado). Si se configura SeguriNotary v4.x se requerirá configurar el certificado del emisor del Servicio de estampillas de tiempo
- Certificado Digital del Servicio SeguriNom (Si aplica)
- Certificado Digital en formato X.509 binario y Llave Privada en formato binario y según el estándar PKCS#8 con encripción PKCS#5, para el solicitante de constancias SeguriNom (Si aplica)
- Detalles de compatibilidad y del solicitante de constancias (Si aplica)
- Número de servidor SeguriNom (Si aplica)
- Usuario y clave para identificación ante el FEC (Si aplica)
- Nombre y puerto del Servidor ITFEA (Si aplica)
- URL al servidor OCSP para ITFEA (Si aplica)
- Certificado Digital en formato X.509 binario, a utilizar como referencia en la resolución de cadenas de certificación (Si aplica)
- Certificado Digital en formato X.509 del(os) respondedor(es) OCSP de confianza (Si aplica)

2.11 Instalación de la Aplicación

La instalación de SeguriSign se divide en tres etapas que deben ejecutarse en el siguiente orden:

- Instalación del Cliente de la Base de Datos a utilizar (Ver documentación propia del cliente de base de datos a instalar)
- Instalación de SeguriSign
- Configuración de SeguriSign

2.12 Ejecución del Instalador de SeguriSign

Para iniciar la instalación deberá contar con el CD de la aplicación. Se recomienda leer el procedimiento de instalación para asegurarse de que se cuenta con todos los elementos necesarios para la instalación, así como tenerlo a la mano como referencia.

Finalmente, para el eventual caso de que requiera apoyo del Soporte Técnico de SeguriData, encontrará nuestros teléfonos en las primeras páginas de este manual.

Inserte el CD de la aplicación en el lector de CD-ROM y con ayuda del explorador de archivos localice el archivo *Setup.exe*. Ejecútelo haciendo doble clic en el nombre del archivo.

El asistente de instalación mostrará la siguiente ventana con la identificación del producto. Para comenzar la instalación, deberá de hacer clic en el botón *Next >*. (Figura 2.1).

Figura 2.1 Inicio del Asistente de Instalación

A continuación, el asistente solicitará la ubicación en donde se instalará SeguriSign. (Figura 2.2).

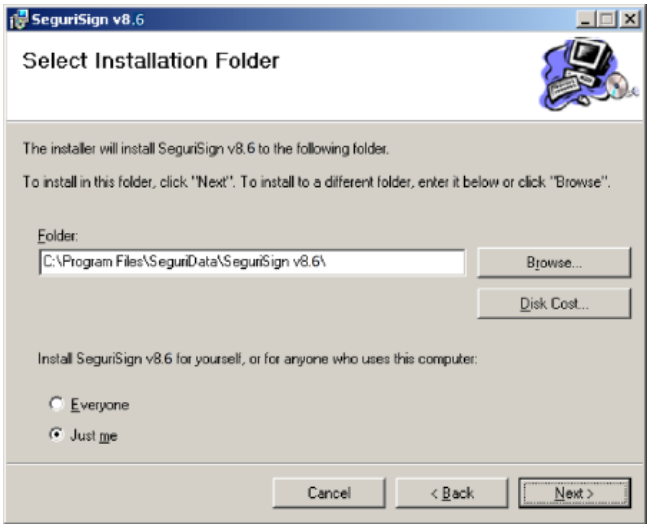

Figura 2.2 Selección de la Carpeta de Instalación

El valor recomendado es el directorio:

C:\Program Files\SeguriData\SeguriSignv8.6

Al finalizar, el asistente mostrará un mensaje de confirmación indicando el resultado de la instalación. (Figura 2.3).

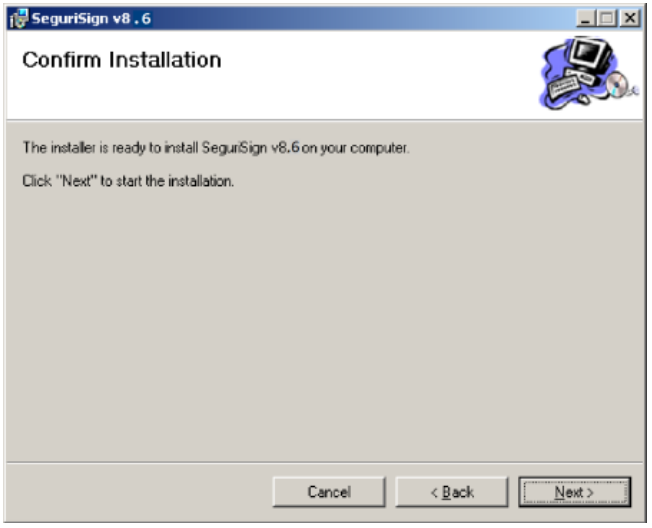

Figura 2.3 Resultado de la Instalación

Haga clic en el botón *Next*.

CAPÍTULO 3

Configuración de SeguriSign Server

Para la configuración de SeguriSign Servicio seleccione el menú:

Start > Programs > SeguriData > SeguriSign v8.6 > Configuración

A continuación se presentará la siguiente ventana con la identificación del producto. (Figura 3.1).

Figura 3.1 Identificación del Producto

A continuación se presentará la siguiente ventana. (Figura 3.2).

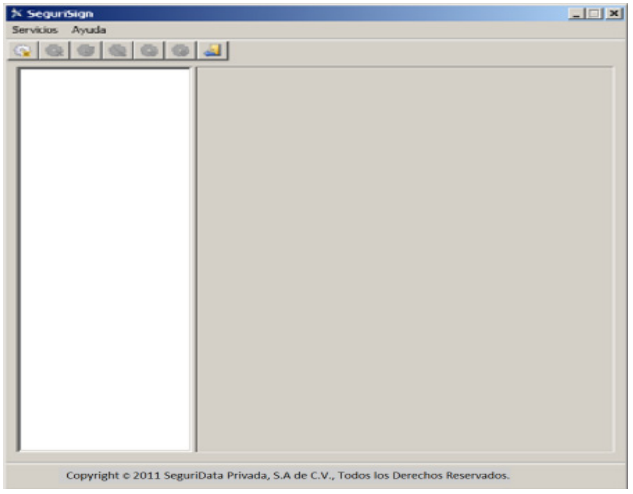

Figura 3.2 Configuración de SeguriSign

3.1 Configuración del Servicio

3.1.1 Configuración inicial del Servicio

Como primer paso haga clic la opción de Servicios para desplegar los datos a configurar, como se muestra en la Figura 3.3.

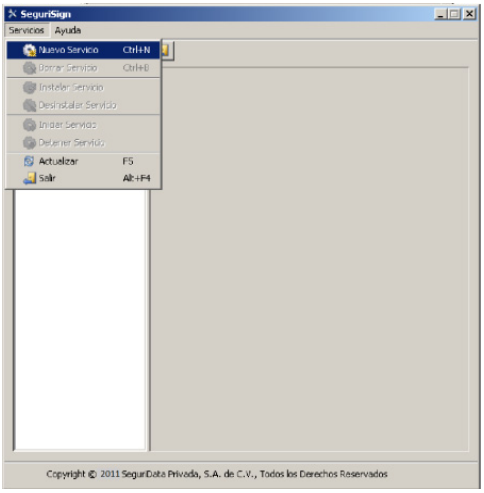

Figura 3.3 Parámetros Generales

Tabla 3.1 Detalle de elementos de la Interfaz

Parámetro	Descripción
Servicios	Dentro de esta opción se encuentran las tareas adminitraivasde los servicios SeguriSign en el sistema.
Ayuda > Acerca de...	Da acceso a la interfaz descriptiva del producto y su "Publisher".

3.1.2 Detalles del Administrador

A continuación haga clic en la opción *Nuevo Servicio*, como se muestra en la Figura 3.4.

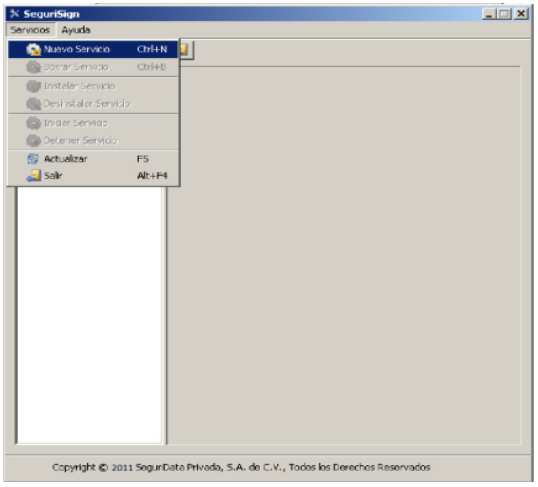

Figura 3.4 Nuevo Servicio.

3.1.3 Detalles del Servidor SeguriSign

Haga clic en *SeguriSign* para configurar los parámetros correspondientes. (Figura 3.5).

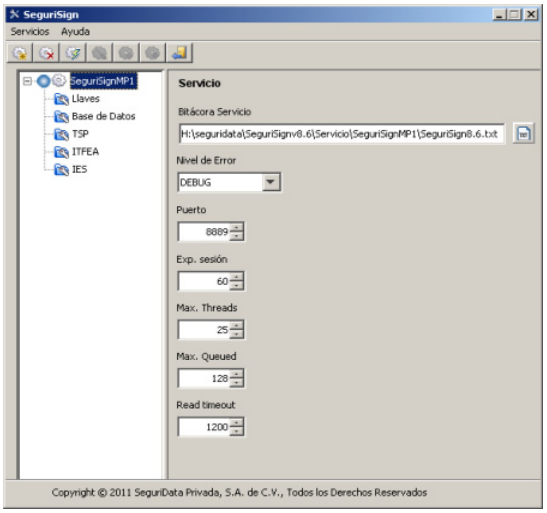

Figura 3.5 Configuración de SeguriSign

Indique los parámetros que se solicitan como se muestra en la Tabla 3.2.

Tabla 3.2 Parámetros de SeguriSign

Parámetro	Descripción
Bitácora Servicio	Define la ruta y nombre de archivo donde serpa escrita la bitácora de eventos y errores que se presentan en el servicio.
Nivel de Error	Es posible además especificar el nivel de mensajes de error a escribir a bitácora: ERROR y DEBUG.
Puerto	Puerto por el que se atienden peticiones relacionadas con procesos de firma unilateral o multilateral. Puede ser definido por el administrador y debe corresponder a un puerto libre y/o no reservado en el equipo.
Exp. Sesión	Se refiere al tiempo en segundos definido para que se den por expiradas las llaves de sesión negociadas entre el servidor y los clientes (Java API). Aplica sólo cuando el Java API se ha habilitado para tal fin.

Tabla 3.2 Parámetros de SeguriSign

Parámetro	Descripción
Max. Threads	Número de threads en el servicio, para atender peticiones encoladas. Se sugiere ampliamente definir máximo 25 hilos por procesador en el equipo.
Max. Queued	Define el número máximo de transacciones encoladas
Read timeout	Define un tiempo en milisegundos para el manejo de timeout para lectura de bytes en los sockets establecidos para las conexiones entrantes al servidor.

Importante

Se ha creado un nuevo servicio SeguriSign, mismo que debe ser configurado e instalado.

3.2 Llaves

3.2.1 Configuración de las Llaves.

Haga clic en *Configuración -> Llaves* para configurar los parámetros correspondientes. (Figura 3.6).

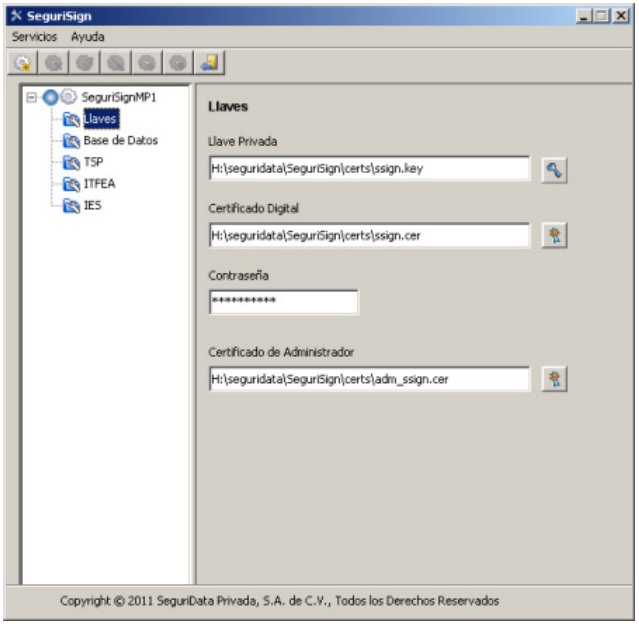

Figura 3.6 Parámetros de Configuración de las Llaves

Tabla 3.3 Parámetros de la Base de Datos

Parámetro	Descripción
`Llave privada`	Seleccione la llave privada asignada al servicio de firmas.
`Certificado Digital`	Certificado digital correspondiente a la llave privada del servicio de firmas.
`Contraseña`	Clave de acceso para la llave privada.
`Certificado de Administrador`	Certificado digital del administrador autorizado para comunicarse con este servicio.

3.3 Configuración de la Base de Datos

3.3.1 Configuración de la Base de Datos

Haga clic en *Configuración -> Base de Datos* para configurar los parámetros correspondientes. (Figura 3.7).

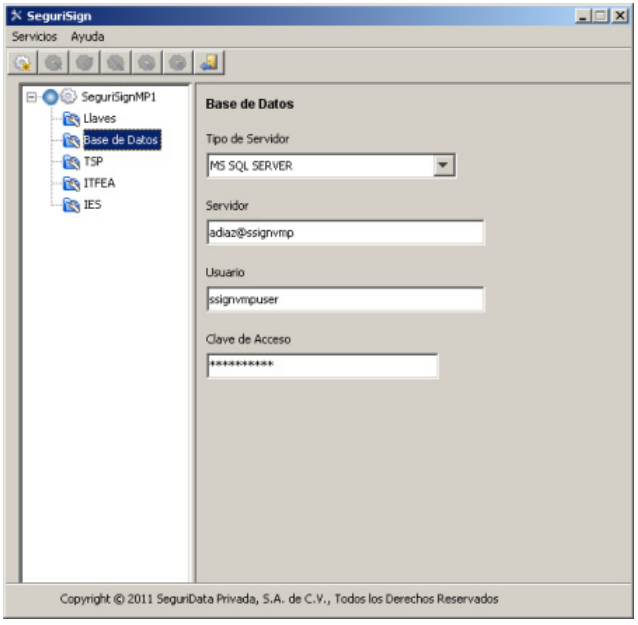

Figura 3.7 Parámetros de Configuración de la Base de Datos

Seleccione el *Tipo* de Base de Datos y proceda a indicar los parámetros que se solicitan, como se muestra en la Tabla 3.4.

Tabla 3.4 Parámetros de la Base de Datos

Parámetro	Descripción
`Tipo de Servidor`	Corresponde al proveedor del manejador de base de datos: Oracle, MS SQL Server, DB2.
`Servidor`	Se indica el servidor que contiene la base de datos. Para el caso de oracle corresponde a la instancia configurada en el cliente.
`Usuario`	Usuario para conexión a la base de datos configurada.
`Clave de Acceso`	Clave correspondiente al usuario para la Base de Datos.

Importante

Proporcione los detalles para conexión a la base de datos del producto: el usuario y los objetos debieron haber sido previamente creados. La base de datos debe ser "resolvible" desde el servidor SeguriSign y el cliente para la misma debió haber sido instalado antes.

3.3.2 Configuración de Estampas

Cuando una transacción de autenticación de firma digital es aceptada, se ampara la firma del mensaje criptográfico recibido, mediante una estampilla de tiempo que se solicita en línea a un Servidor de Estampas de tiempo. (Figura 3.8).

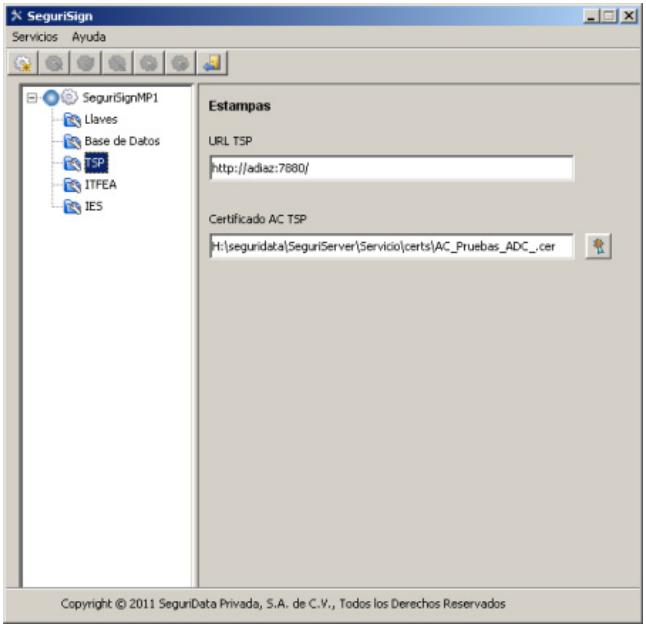

Figura 3.8 Parámetros de Configuración de las Estampas

Indique los parámetros que se solicitan como se muestra en la Tabla 3.5

Tabla 3.5 Parámetros de las Estampas

Parámetro	Descripción
URL TSP	URL para conexión con el servicio generador de estampas de tiempo.
Certificado AC TSP	Archivo de certificado digital en binario y formato X.509. Corresponderá al certificado digital de la autoridad certificadora emisora del servicio de emisión de estampas.

3.4 Instalar Servicio

Una vez configuradas las Estampas, se procederá a instalar el servicio, como se muestra en la siguiente consola. (Figura 3.9).

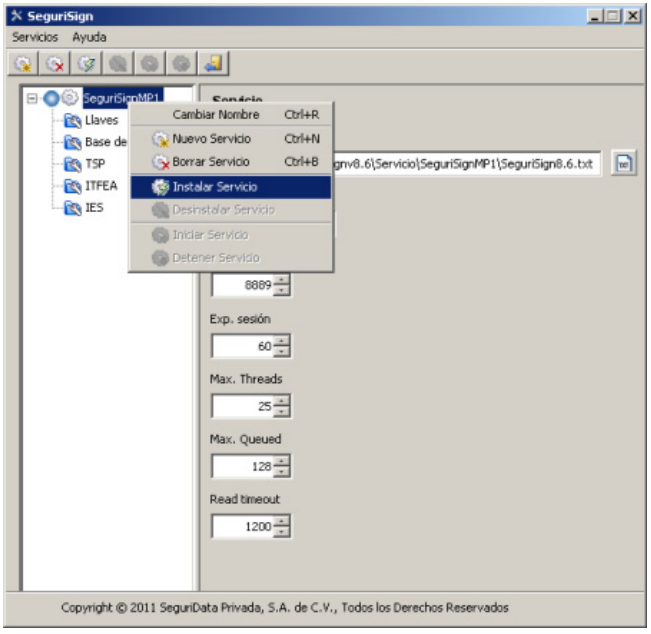

Figura 3.9 Instalar Servicio

Seleccione el nombre del servicio ya creado, y haga clic en la opción *Servicios*, seleccione la opción *Instalar Servicio* del menú emergente.

Como resultado, el ícono circular cambiará a color rojo indicando que el servicio se ha instalado exitosamente. (Figura 3.10).

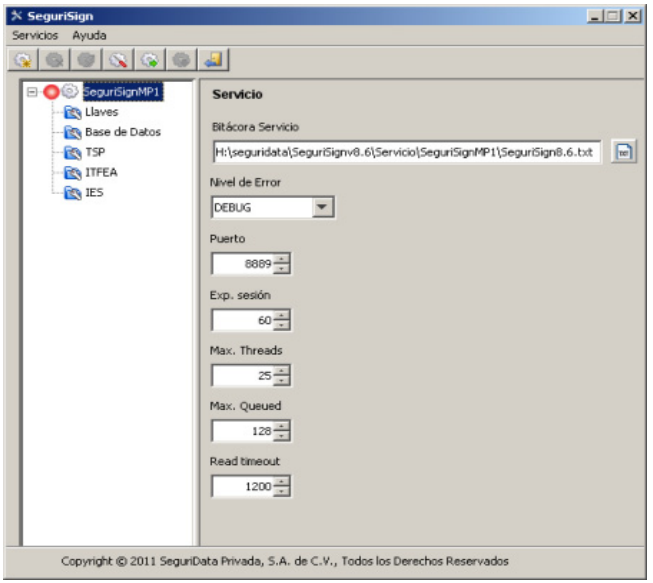

Figura 3.10 Servicio Instalado

3.5 Iniciar Servicio

Una vez que el el servicio ha sido creado, se procederá a iniciarlo. (Figura 3.11).

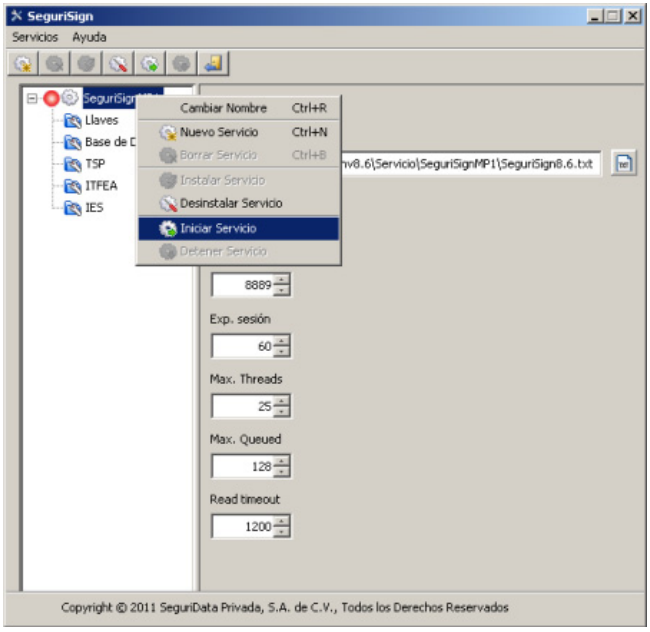

Figura 3.11 Iniciar Servicio

Seleccione el servicio y haga clic en la opción *Servicios* y seleccione la opción *Iniciar Servicio* del menú.

Como resultado, el icono circular cambiará a color verde indicando que el servicio ha sido iniciado con los parámetros que se le han definido. (Figura 3.12).

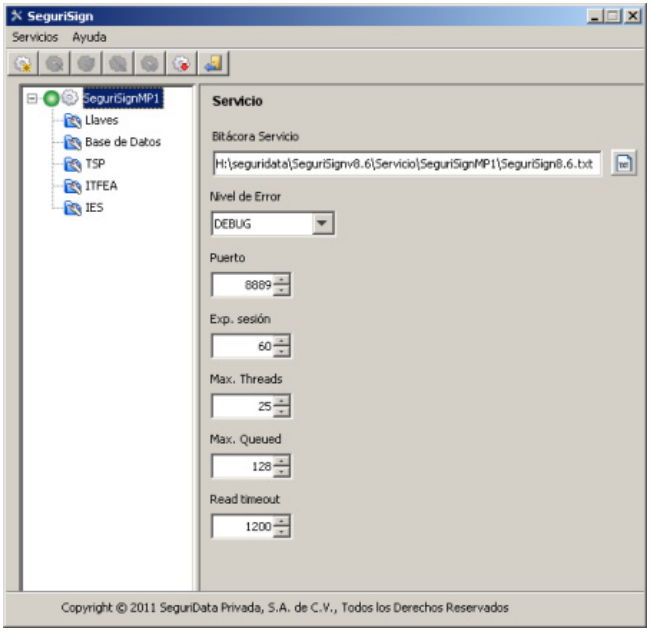

Figura 3.12 Iniciar Servicio

3.6 Configuración WEB.

Una vez que se ha creado, instalado, configurado e iniciado un servicio de autenticación de firmas, debe procederse a finalizar su configuración WEB. Primero debe desplegarse la aplicación WEB de administración.
Localice el archivo “segurisign.war“, esto se encuentra dentro de la ruta de instalación. (Figura 3.13).

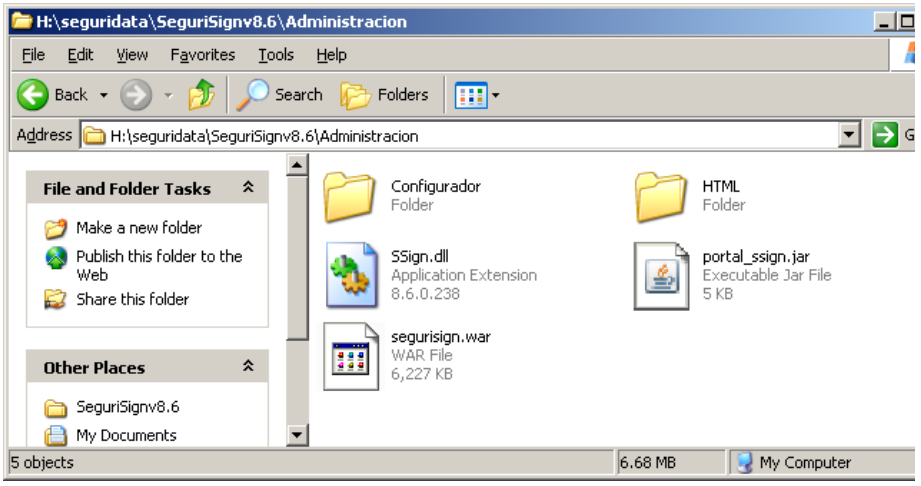

Figura 3.13 Archivo de Cofiguración.

Copie el archivo “segurisign.war“ de la aplicación WEB en la carpeta de Tom Cat Server (Un ejemplo de ruta para Tomcat puede ser C:\Program Files\ Apache Software Foundation\Tomcat 6.0)

Importante

El servicio de TomCat debe de estar instalado antes de realizar la configuración.

como se muestra en la Figura 3.14.

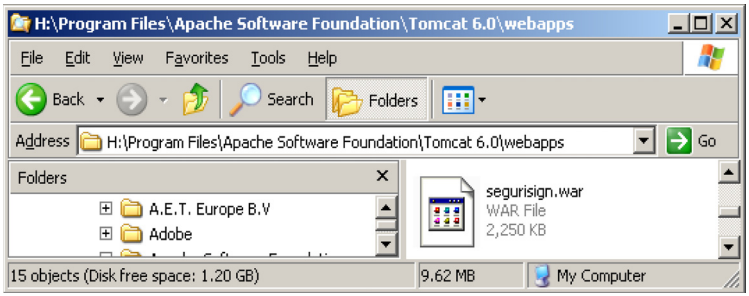

Figura 3.14 Carpeta de TomCat Server.

Importante

El servicio de TomCat debe de estar configurado para realizar el autodespliegue de aplicaciones dispuestas en un war, de ser esto correcto TomCat realizará el despliegue de la aplicación.

Una vez desplegada la aplicación se observará una carpeta bajo webapps llamada segurisign. (Figura 3.15).

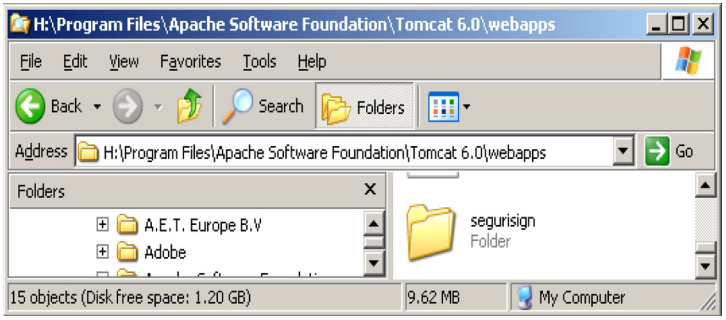

Figura 3.15 Carpeta Webapps

Localice el archivo portal_ssign.jar y cópielo bajo la carpeta de librerías de Tomcat. (Figura 3.16).

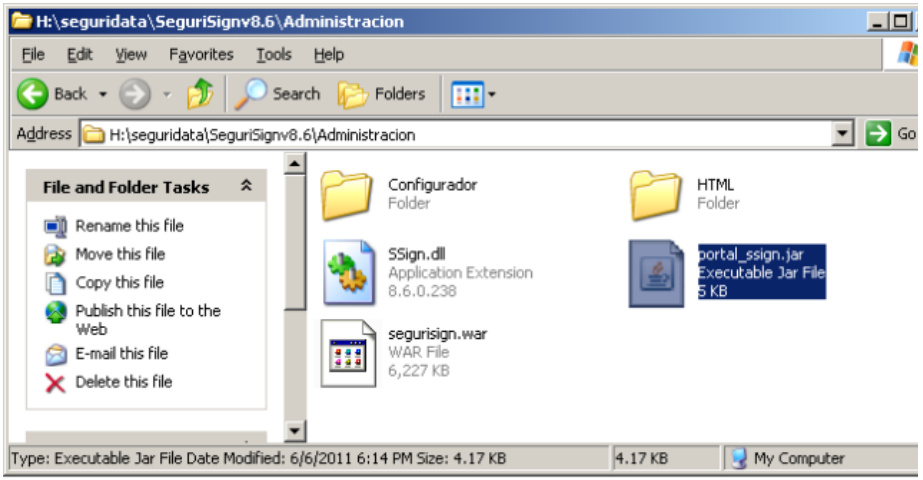

Figura 3.16 Archivo portal_ssign.jar

Deberá estar incluido en dicha carpeta tal cual se muestra en la Figura 3.17.

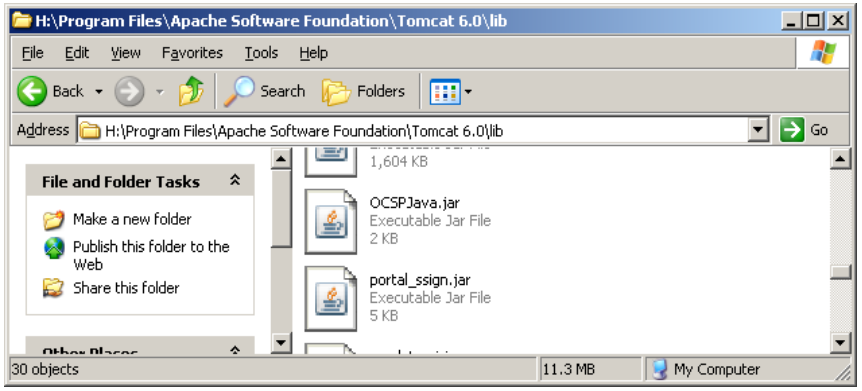

Figura 3.17 Guardar Cambios

Localice la librería SSign.dll y sitúela en la carpeta de ejecutables de Tomcat.(Figura 3.18).

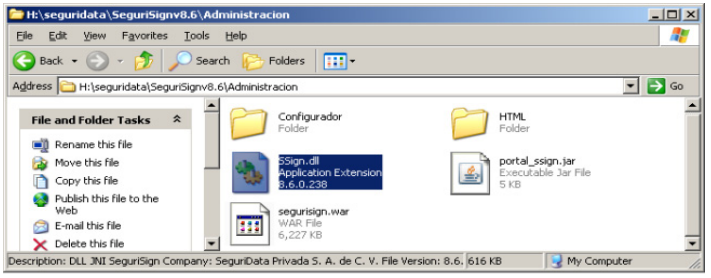

Figura 3.18 Librería SSign.dll

Deberá poder visualizarse como se muestra. (Figura 3.19).

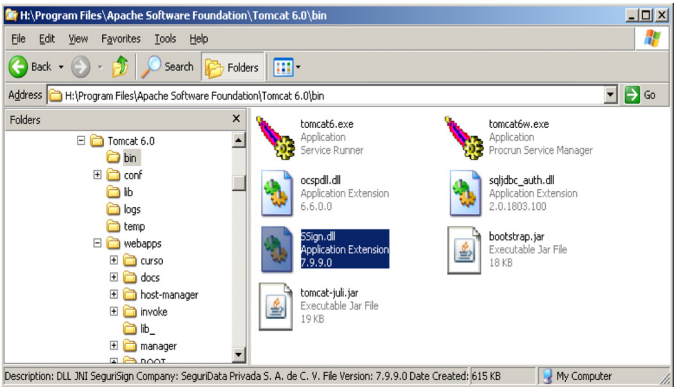

Figura 3.19 Librería SSign.dll

Importante

Nunca copiar las librerias ya mencionadas (SSign.dll y portal_ssign.jar) bajo la aplicación WEB desplegada, ya que debido al manejo de JNI no es conveniente cuando se tiene más de una aplicación WEB que la consuma (en caso de que aplique).

Localice los las clases para JDBC del proveedor de BD y cópielas en la carpeta lib de Tomcat. De igual modo afecte la variable de ambiente classpath para que contenga la ruta y nombre de cada archivo jar del driver para JDBCs. (Figura 3.20).

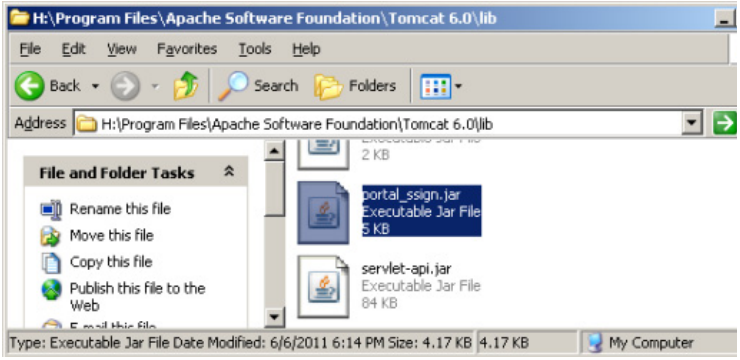

Figura 3.20 Clases para JDBC

Iníciese la aplicación para configuración del administrador WEB. (Figura 3.21).

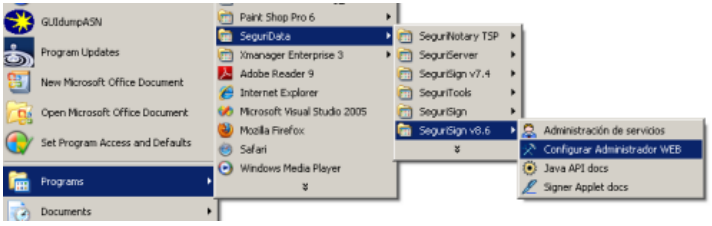

Figura 3.21 Aplicación WEB

La aplicación abrirá como se muestra en la siguiente imagen. (Figura 3.22).

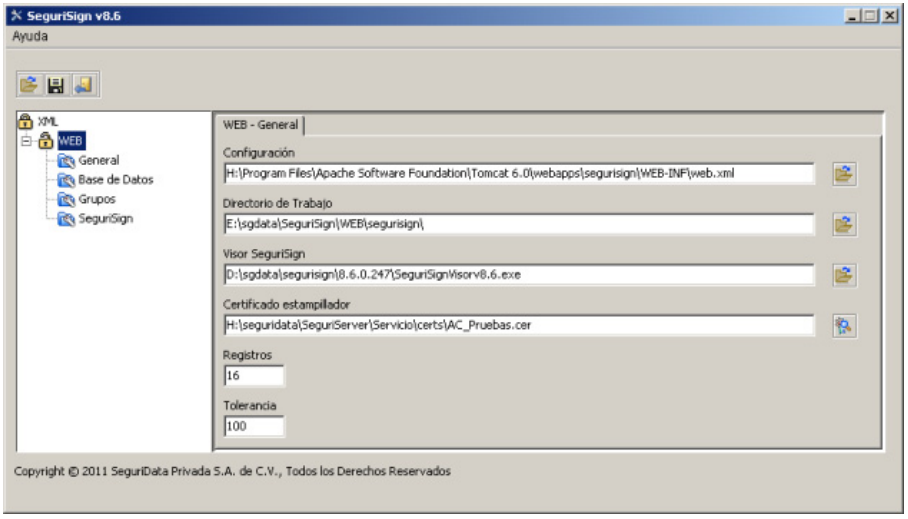

Figura 3.22 SeguriSign WEB

Indique los parámetros que se solicitan como se muestra en la Tabla 3.6

Tabla 3.6 Parámetros de la aplicación WEB

Parámetro	Descripción
Configuración	Indique un archivo nuevo a crear o en su defecto localice y abra el archivo de configuración de la aplicación anteriormente desplegada.
Directorio de Trabajo	Localice el directorio HTML bajo la carpeta Administracion dentro de la ruta de instalación del producto.
Visor SeguriSign	Ruta y nombre de archivo para el instalador del Visor SeguriSign a descargar de la liga habilitada para tal fin en el portal WEB de Administración.
Certificación de Estampillador	Archivo de certificado digital en binario y formato X.509. Corresponderá al certificado digital de la autoridad emisora del servicio de estampas.
Registros	Número de líneas a desplegar para reportes

Tabla 3.6 Parámetros de la aplicación WEB

Parámetro	Descripción
Tolerancia	Tiempo de tolerancia para autenticación de usuario administrador

Especifique la base de datos creada para el producto y en la que ya se ha corrido el script adecuado para creación de objetos, como pudiera haber sido el caso de la siguiente figura. (Figura 3.23).

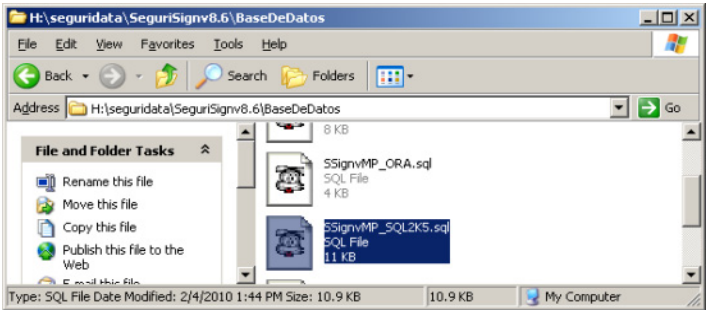

Figura 3.23 Especificación de la Base de Datos

Abra la interfaz para especificar los detalles para la Base de Datos del servicio, vea la siguiente Figura 3.24.

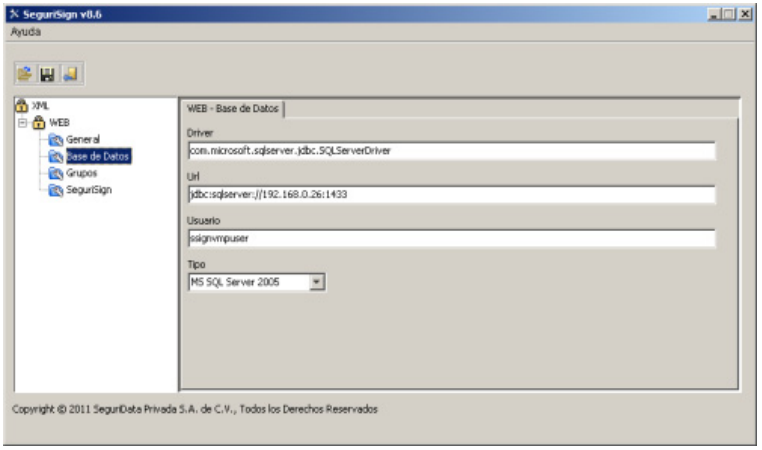

Figura 3.24 Especificación de la Base de Datos

Indique los parámetros que se solicitan como se muestra en la Tabla 3.7

Tabla 3.7 Especificación de la Base de Datos

Parámetro	Descripción
`Driver`	Driver que corresponde al proveedor nativo del manejador de base de datos a utilizar. Los drivers para base de datos debieron haber sido copiados a la carpeta lib de la aplicación y reflejados en CLASSPATH de las variables de ambiente del sistema.
`URL`	Url JDBC para la base de datos
`Usuario`	Usuario de la base de datos.
`Tipo`	Tipo de base de datos a utilizar. Para MSSQL 2005 y 2008 se selecciona como MS SQL Server 2005.

Abra la interfaz para especificar los detalles para los Grupos del servicio, vea la siguiente Figura 3.25.

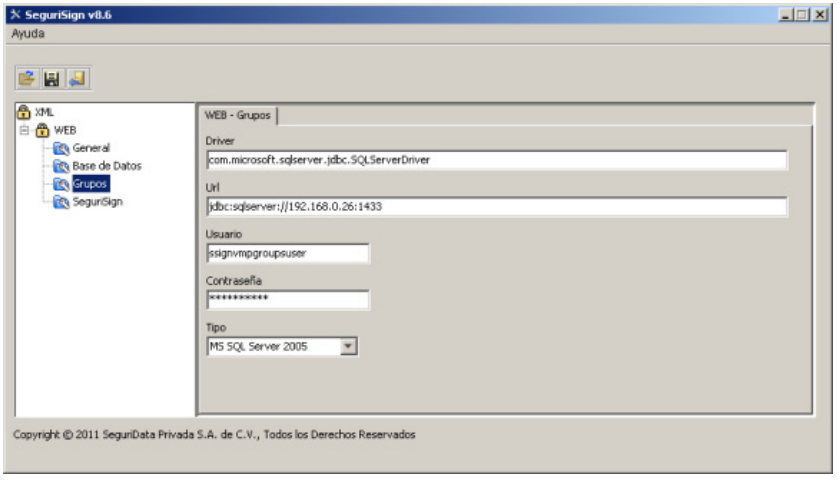

Figura 3.25 Especificación de los Grupos

Indique los parámetros que se solicitan como se muestra en la Tabla 3.8

Tabla 3.8 Especificación de los Grupos

Parámetro	Descripción
`Driver`	Driver que corresponde al proveedor nativo del manejador de base de datos a utilizar. Los drivers para base de datos debieron haber sido copiados a la carpeta lib de la aplicación y reflejados en CLASSPATH de las variables de ambiente del sistema.
`URL`	Url JDBC para la base de datos, donde se generaron los objetos para el administrador WEB.
`Usuario`	Usuario de la base de datos.
`Contraseña`	Clave para el usuario de la base de datos.
`Tipo`	Tipo de base de datos a utilizar. Para MSSQL 2005 y 2008 se selecciona como MS SQL Server 2005.

Finalmente especifique el servidor SeguriSign principal a administrar y salve el archivo. (Figura 3.26).

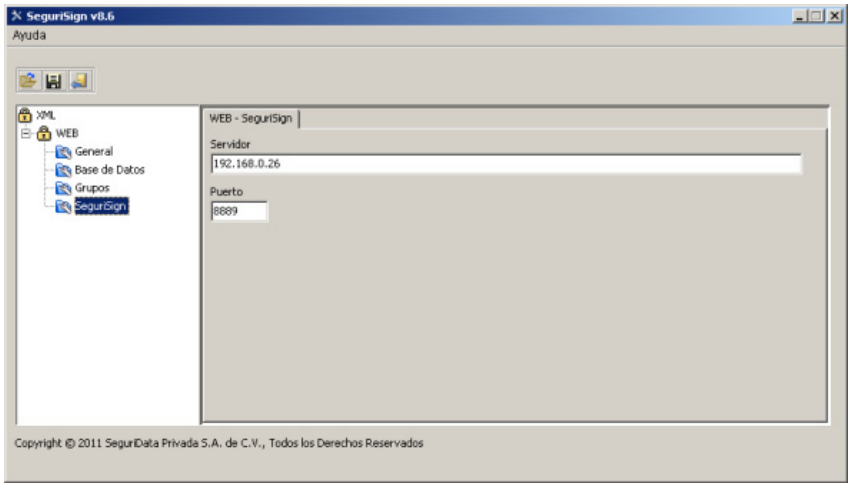

Figura 3.26 Especificación del Servidor

Indique los parámetros que se solicitan como se muestra en la Tabla 3.7

Tabla 3.9 Especificación de la Base de Datos

Parámetro	Descripción
Servidor	Dirección IP del Servidor SeguriSign.
Puerto	Puerto del Servicio.

Una vez grabada la configuración se visualizará un mensaje como el siguiente (Figura 3.27).

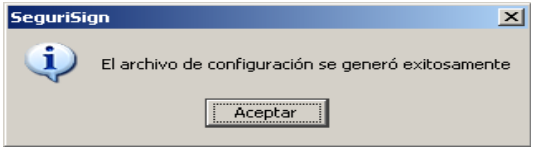

Figura 3.27 Mensaje de Confirmación

Importante

En caso de haber generado un archivo nuevo deberá ser reemplazado el archivo web.xml de la aplicación WEB.