

Manual de Instalación

Revisión 1.0



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

Derechos Reservados © SeguriData IP S.A. de C.V., Av. Insurgentes Sur #2375, 3er. piso, Col. Tizapán, Del. Alvaro Obregón, C.P. 01000, México, D.F.. Derechos Reservados © SeguriData Privada S.A. de C.V., Av. Insurgentes Sur #2375, 3er. piso, Col. Tizapán, México, D.F., México, 1998. Este producto constituye una obra intelectual protegida por las leyes nacionales y tratados internacionales en materia de derechos de autor, y queda prohibida su reproducción o uso total o parcial, que no sean autorizadas por su titular.

BSIGInstalación3.10

Contenido

Capítulo 1. ¿Cómo utilizar este manual?

1 0	
1.1 Simbología y convenciones	1 - 1
1.1.1. Recomendaciones y Advertencias	1 - 1
1.2 Objetivo de este manual	1 - 1
Capítulo 2. Instalación de bSigned Server Wizard	
2.1 Requerimientos de Hardware	2 - 1
2.2 Configuraciones válidas de bSigned Server Wizard	2 - 1
2.2.1. Configuración de cuatro servidores (Recomendada)	2 - 2
2.2.2. Configuración de tres servidores	2 - 3
2.2.3. Configuración de dos equipos	2 - 4
2.3 Requerimientos necesarios para la Instalación	2 - 4
2.4 Requerimientos de Certificación	2 - 4
2.5 Componentes de Software adicionales	2 - 5
2.6 Ejecución del Instalador	2 - 5
2.7 Instalación de Adobe PDF IFILTER 5.0	2 - 12
2.8 Configuración del Servidor bSigned 2 - 16	
2.9 Configuración de la Base de Datos 2 - 18	
2.10 Configuración del Servidor de Correo Electrónico	2 - 19
2.11 Habilitar la Sincronización del Estado de Revocación	2 - 20
2.11.1. Agregar el usuario de la Autoridad Certificadora a la Base de Datos	de bSigned2 -
20	
2.11.2. Creación del Trigger de sincronización	2 - 21
2.11.3. Verificación de la ejecución del Trigger	2 - 21
2.12 Configuración de Componentes de Software Adicionales	2 - 22
2.13 Verificación de la instalación del Servicio de Licencia	2 - 22
2.14 Verificación de la instalación del Servidor de bSigned	2 - 23
2.15 STS	2 - 24

Capítulo 3. Instalación de bSigned Web Wizard 3.1 Requerimientos de Hardware 3 - 13 - 1 3.2 Requerimientos de Hardware 3.3 Configuraciones válidas de bSigned Web Wizard 3 - 2 3 - 2 3.3.1. Configuración de cuatro servidores (Recomendada) 3 - 3 3.3.2. Configuración de tres servidores 3 - 4 3.3.3. Configuración de dos equipos 3 - 4 3.4 Información necesaria para la Instalación 3 - 4 3.5 Ejecución del Instalador de bSigned Web Wizard 3.6 Configuración de los Valores de bSigned Web Wizard 3 - 103 - 11 3.7 Configuración del Sitio Web 3.8 Configuración del Servidor bSigned 3 - 133 - 133.8.1. Configuración de la Licencia de bSigned 3.9 Configuración de la Certificación 3 - 143.10 Configuración de la Base de Datos 3 - 163.11 Configuración de las Aplicaciones 3 - 173 - 19 3.12 Configuración del Certificado del sitio de bSigned en el servidor web 3.13 Configuración de los Directorios Seguros de bSigned 3 - 253.13.1. Configuración de cgi-bin (Directorio Virtual) 3 - 253 - 293.13.2. Configuración del directorio Secured 3.14 Limpiar el caché del navegador 3 - 323.15 Configuración del equipo del Administrador 3 - 343.16 Configuración del Servidor bSigned 3 - 353.16.1. Arranque del Servidor bSigned 3.17 Descarga de Acuerdos (nueva funcionalidad) 3 - 373.17.1. Reemplazo de archivos 3 - 373 - 403.17.2. Creación de carpetas 3 - 423.17.3. IIS 3.17.4. bSigned Agreements DwnldServer 3 - 463.17.5. Instalación de bSigned Agreements Download 3 - 473.17.6. Configuración 3 - 503.17.7. Configuración del horario 3 - 533 - 543.17.8. Configuración del correo electrónico Capítulo 4. Desinstalación Capítulo 5. Uso del CGI de bSigned 5.1 Funcionamiento del CGI 5 - 1 5 - 7 5.2 Invocación del CGI 5.3 Mensajes de Error 5 - 8 5.4 Estructura de Tablas de bSigned 5 - 10

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 mas 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 de este manual

El objetivo de este manual es de servir como referencia al Administrador para la instalación y configuración de bigned Server y bigned Web Wizard.

¿Cómo utilizar este manual?



CAPÍTULO 2

Instalación de bSigned Server

El presente documento es una guía para la instalación de bSigned Server versión 3.10. Esto considera la instalación de la Base de Datos, el Servidor bSigned y el Servicio de Licencia.

Éstas 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 del sistema.

2.1 Requerimientos de Hardware

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

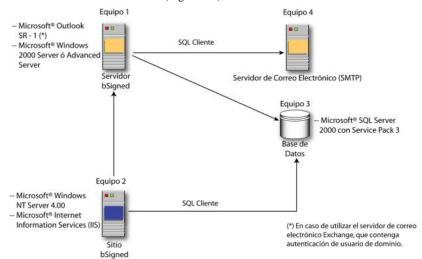
- Procesador Pentium IV 1GHz
- Espacio en disco duro 90GB
- 2GB en RAM
- Unidad lectora de CD-ROM
- Tener instalado FrameWork ASP .Net MVC 3
- Tener instalado BCL Easy PDF Loader versión 6.3

2.2 Configuraciones válidas de bSigned Server

Existen tres posibles configuraciones que se diferencian según la ubicación de los componentes.

2.2.1 Configuración de cuatro servidores (Recomendada)

El primer servidor contiene al servidor bSigned. El segundo equipo contiene al servidor web con el sitio de bSigned. En un tercer equipo se encuentra la base de datos de bSigned. Finalmente, el



cuarto contiene al servidor de correo. (Figura 2.1).

Figura 2.1 Instalación en cuatro equipos

2.2.2 Configuración de tres servidores

El primer servidor contiene al servidor bSigned y la base de datos de bSigned. El segundo equipo contiene al servidor web con el sitio de bSigned. Finalmente, el tercero contiene al servidor de

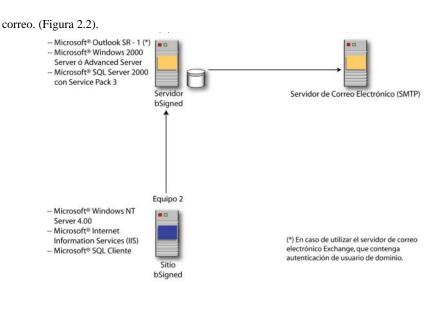


Figura 2.2 Instalación en tres equipos

2.2.3 Configuración de dos equipos

El primer servidor contiene el servidor web con el sitio de bSigned, el servidor bSigned y la base de datos de bSigned. El segundo equipo contiene al servidor de correo. (Figura 2.3).

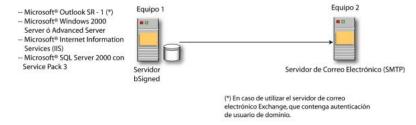


Figura 2.3 Instalación en dos equipos

2.3 Requerimientos necesarios para la Instalación

El procedimiento de instalación de bSigned Server requiere de lo siguiente:

- Tener creadas 2 cuentas de correo electrónico en el servidor de correo electrónico, una para el Notificador de bSigned y otra para el Administrador de bSigned
- Dirección IP y puerto del servidor de correo electrónico
- Dirección IP y puerto donde está corriendo el servicio de la Autoridad Certificadora
- Dirección IP y puerto del Respondedor de OCSP (si aplica)
- Dirección IP y puerto del Servicio de Estampilla de Tiempo (TSP)

2.4 Requerimientos de Certificación

El procedimiento de instalación de bSigned Server requiere de los siguientes certificados:

- Certificado Digital de la Autoridad Certificadora (Formato X.509)
- Certificado Digital y Llave Privada en formato PKCS#12 (pfx) del sitio del bSigned
- Certificado Digital del Administrador de bSigned (Formato X.509) y PKCS#12 (pfx)
- Certificado Digital y Llave Privada en formato PKCS#12 (pfx) del Servicio de Estampillas de Tiempo

Si utiliza SeguriSERVER, debe contar con los siguientes certificados en formato X.509:

Respondedor de OCSP (si aplica)

- Servicio OCSP (Online Certificate Service Protocol)
- Agente Certificador



Importante

Si no cuenta con una Autoridad Certificadora, puede instalar SeguriSERVER, de lo contrario utilice la Autoridad Certificadora que corresponde.

2.5 Componentes de Software adicionales

Para la funcionalidad y configuración de bSigned se deben instalar las siguientes aplicaciones adicionales en el siguiente orden:

- Instalación de SeguriServer, en caso de no contar con una Autoridad Certificadora (Ver Manual SeguriSERVER)
- Instalación del Servicio OCSP (si aplica)
- Instalación del Agente Certificador (Ver Manual Agente Certificador)
- Instalación de los CGIs de la Autoridad Certificadora (Ver Manual CGIs)
- Instalación de SeguriTOOLS (Ver Manual SeguriTOOLS)
- Instalación del Servicio de Estampilla de Tiempo (TSP) en caso de manejo de dos
 certificados, uno para autentica y otro para firmar debe usar el software TSP Gateway
 v1.0 para sellos de tiempo.

2.6 Ejecución del Instalador

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 bSigned Server en el lector de CD-ROM y con ayuda del explorador de archivos localice el archivo SetupbSigned3.10.exe. Ejecútelo haciendo doble clic en el nombre del archivo.

Se presentará una ventana, que permite seleccionar el idioma que se utilizará para la instalación. (Figura 2.4).



Figura 2.4 Selección del Idioma

Seleccione el idioma y haga clic en el botón OK.

El asistente de instalación mostrará una nueva ventana con la identificación del producto. (Figura 2.5).



Figura 2.5 Identificación del Producto

Para comenzar la instalación, haga clic en el botón Siguiente >.

A continuación el instalador le pregunta si desea que se integre un servidor STS a bSigned, de ser así, seleccione la casilla como se muestra a continuación. (Figura 2.6)



Figura 2.6 Integración con STS.

Para continuar, haga clic en el botón Siguiente >.



La funcionalidad de la integración de STS a bSigned es para que los documentos procesados exitosamente por bSigned (archivos 2bv) sean almacenados en la Infraestructura de STS (Sistema de Storage Seguro STS).

A continuación, el asistente solicitará la ubicación del lugar donde se instalará la aplicación. (Figura 2.7).

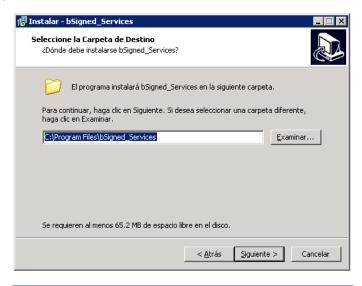


Figura 2.7 Selección de la Carpeta Destino

Para continuar con el proceso, haga clic en el botón Siguiente >.

Seleccione la Carpeta del Menú Inicio
¿Dónde deben colocarse los accesos directos del programa?

El programa de instalación creará los accesos directos del programa en la siguiente carpeta del Menú Inicio.

Para continuar, haga clic en Siguiente. Si desea seleccionar una carpeta distinta, haga clic en Examinar.

SeguriData\bSigned_Services V3.10

Examinar...

No crear una carpeta en el Menú Inicio

< Atrás Siguiente > Cancelar

Indique donde se va a colocar los accesos directos bSigned en el Menú de Inicio. (Figura 2.8).

Figura 2.8 Selección de los accesos directos.

Si no necesita que se cree la carpeta en el Menú de Inicio seleccione la casilla "No crear una carpeta en el Menú de Inicio".

Para continuar con el proceso, haga clic en el botón Siguiente >.

En esta sección puede seleccionar las tareas adicionales que se desea realizar, en este caso, la tarea adicional es Crear un icono en el escritorio. (Figura 2.9)



Figura 2.9 Crear un icono en el escritorio.

Para continuar, haga clic en el botón Siguiente >.

Se presentará un resumen de los valores seleccionados en las ventanas anteriores, como se muestra en la Figura 2.10.

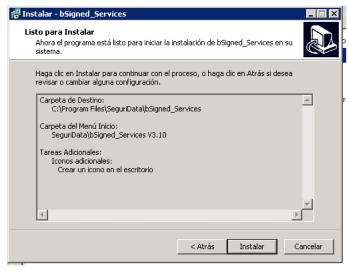


Figura 2.10 Resumen de los Valores seleccionados

Para comenzar la instalación, haga clic en el botón Instalar.



En caso de ser necesario, puede regresar a las ventanas anteriores por medio del botón < Atrás y modificar los parámetros de instalación.

El proceso de copia de archivos se iniciará y se mostrará el avance de la instalación. (Figura 2.11).

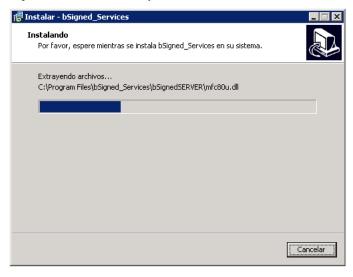


Figura 2.11 Avance de la Instalación

Al termino de la instalación, el asistente mostrará un mensaje indicando el resultado de la instalación. (Figura 2.12).



Figura 2.12 Resultado de la Instalación

Haga clic en el botón Terminar.



La aplicación Adobe PDF IFILTER 5.0 debe ser instalada cuando no haya ningún usuario conectado al servidor de SQL Server, ni en el equipo donde reside el servidor de SQL, ni en el equipo donde reside SQL Server.

2.7 Instalación de Adobe PDF IFILTER 5.0 Se presentará una ventana para indicar el idioma que se utilizará para la instalación. (Figura 2.13).



Figura 2.13 Selección del Lenguaje

Haga clic en el botón Next >.

En esta ventana se presenta el Contrato de Licencia del Usuario Final para utilizar esta aplicación. (Figura 2.14).



Figura 2.14 Contrato de Licencia de para el Usuario Final

Haga clic en el botón Accept.



Como siguiente paso, indique la ubicación donde se instalará la aplicación. (Figura 2.15).

Figura 2.15 Selección del folder destino

Si desea cambiar la ruta haga clic en el botón Browse... En caso de ser necesario, puede regresar a las pantallas anteriores por medio del botón < Back y modificar los parámetros de instalación.

Para continuar con el proceso, haga clic en el botón Next >.

El proceso de copia de archivos se iniciará y se presentará el avance de la instalación. (Figura 2.16).



Figura 2.16 Barra de Avance de Instalación

Al termino de la instalación, el asistente mostrará un mensaje indicando el resultado de la instalación. (Figura 2.17).



Figura 2.17 Termino de la Instalación

Haga clic en el botón OK para terminar con la instalación.

2.8 Configuración del Servidor bSigned

En esta ventana indique los parámetros solicitados para la configuración del Servidor bSigned. (Figura 2.18).



Figura 2.18 Configuración del Servidor bSigned



Importante

Si en la configuración del SERVER se habilita la opción de "Usar Licencia" y en la casilla de "Usar registro" con la opción "SI" entonces, en la configuración WEB se debe de indicar que también "Use Licencia" (en WEB queda deshabilitada la opción de "Usar registro").

Los datos que se solicitan se muestran en la Tabla 2.1.

Tabla 2.1 Datos para la configuración del Servidor bSigned

Información	Dato
bSigned server port	Indique el número de puerto del servidor bSigned por donde escuchará las peticiones el servidor bSigned.
Generate Trace	Marque la casilla en caso de requerir una bitácora de las operaciones realizadas en bSigned. Es recomendado para analizar algún proceso de acuerdo bilateral. Posteriormente puede ser habilitado.
Use licence service	Marque la casilla si se requiere el servicio de licencia para bSigned para resolver operaciones relacionadas con el licenciamiento de bSigned. Este servicio es necesario cuando el servidor bSigned se encuentre instalado en un equipo diferente al de bSigned servidor web. De lo contrario los CGIs de bSigned resolverán las operaciones de Licenciamiento.
bSigned licence port	Indique el número de puerto del servicio de licencia de bSigned.
Use Registry	Seleccione Yes, si desea que los datos de licencia queden almacenados en el Registro de Microsoft® Windows, de lo contrario seleccione No.

Haga clic en el botón Next.

2.9 Configuración de la Base de Datos

En la siguiente ventana indique los parámetros solicitados para la configuración de la Base de Datos. (Figura 2.19).

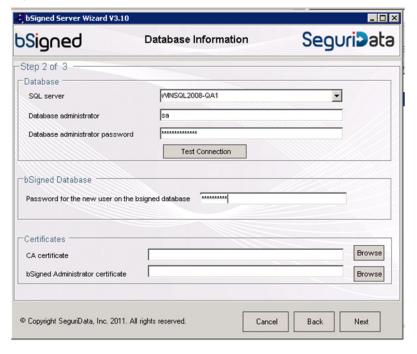


Figura 2.19 Configuración de la Base de Datos

Los datos que se solicitan se muestran en la Tabla 2.2.

Tabla 2.2 Información de la Base de Datos

Información	Dato
SQL Server	Indique el nombre del equipo donde se encuentra el servidor SQL Server.
Database administrator	Proporcione el nombre del administrador de SQL Server.
Data base administrator password	Proporcione la clave de acceso del administrador de SQL Server.
Botón Test Connection	Haga clic en este botón para verificar la conexión con la base de datos.
Password for the new user on the bSigned database	Proporcione una clave de acceso para el nuevo usuario (bSigned) de la Base de Datos bSigned. El usuario bSigned es creado por el Wizard de configuración de bSigned Server.

Tabla 2.2 Información de la Base de Datos (Continuación)

Información	Dato
Directory where the bSigned Database files will be created in the selected SQL Server	Haga clic en el botón Browse para seleccionar la carpeta donde quedarán guardados los archivos de la base de datos de bSigned.
CA certificate	Seleccione el certificado de la Autoridad Certificadora que corresponde, en formato X509, haciendo clic en el botón Browse
bSigned Administrator certificate	Seleccione el certificado del Administrador de bSigned en formato X.509, haciendo clic en el botón Browse

Haga clic en el botón Next.

2.10 Configuración del Servidor de Correo Electrónico En esta ventana indique los parámetros solicitados para la configuración del Servidor de Correo Electrónico. (Figura 2.20).



Figura 2.20 Configuración del servidor de Correo Electrónico

Si desea que Local System sea el usuario de arranque del servidor bSigned, marque la opción Use the Local system account to run bSigned e indique los datos que se solicitan como se muestra en la

Tabla 2.3.

Tabla 2.3 Datos para la configuración del servidor de correo electrónico

Información	Dato
Use an SMTP server	Si utiliza un servidor de correo electrónico (SMTP), marque esta opción y proporcione la dirección IP (SMTP server) y el número de puerto donde se localiza este servidor (SMTP port).
Use SMTP authentication	Marque esta opción si se requiere autenticación SMTP y proporcione el nombre de usuario (SMTP user) y clave de acceso de dominio (SMTP password).
Notifier	Cuenta de correo electrónico con la cual se enviarán las notificaciones de firma. Esta cuenta debe estar habilitada para envio de correo electrónico.
bSigned Administrator	Proporcione la dirección del correo electrónico del administrador de bSigned.
bSigned Support	Proporcione la dirección de soporte técnico de SeguriData.

Si desea que bSigned sea iniciado manualmente marque la opción Use a especific account to run bSigned e indique los datos que se solicitan, como se muestra en la Tabla 2.4.

Tabla 2.4 Datos para la configuración del servidor de correo electrónico

Información	Dato
Account user	Indique la cuenta de correo electrónico del usuario que iniciará bSigned.
Account Password	Indique la clave de acceso de la cuenta de correo electrónico del usuario anterior.

Haga clic en el botón Finish para finalizar las configuraciones.

Terminando de hacer estas configuraciones, se debe de ejecutar el Query "procedures_and_functions_required_by_WSs.sql" (Figura 2.21).

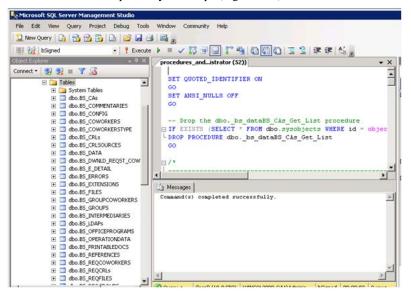


Figura 2.21 Ejecutar el Query

2.11 Habilitar la Sincronización del Estado de Revocación

Las siguientes tareas se realizan sólo en caso de utilizar SeguriServer como Autoridad Certificadora:

- 2.11.1 Agregar el usuario de la Autoridad Certificadora a la Base de Datos de bSigned
 - Ejecute el Enterprise Manager desde el menú de inicio: Start > Programs > Microsoft SQL Server > Enterprise Manager
 - 2. Seleccione el Servidor de SQL Server y conéctese con el usuario bSigned.
 - 3. Expanda la carpeta del Servidor.
 - 4. Expanda la carpeta Databases.
 - Expanda la carpeta bsigned.
 - 6. Seleccione Users.
 - 7. Haga clic con el botón derecho del ratón.
 - 8. Seleccione New Database User en el menú emergente.

- Seleccione como "Login name" el usuario creado para la base de datos de la Autoridad Certificadora, asegúrese que el rol del usuario sea public.
- 10. Haga clic con el botón derecho del ratón sobre el nuevo usuario.
- 11. Seleccione All Tasks > Manager permissions.... en el menú emergente.
- Habilite los permisos de Consulta (SELECT) y Actualización (UPDATE) en el objeto BS COWORKERS.

2.11.2 Creación del Trigger de sincronización

- Ejecute el Query Analizer desde el menú de inicio: Start > Programs > Microsoft SQL Server > Query Analyzer
- Seleccione como "Login name" el usuario creado para la base de datos de la Autoridad Certificadora para resolver la autenticación.
- Abra el archivo trigger.sql.
 (ubicado en el directorio bSigned_services\bSignedSERVER\[SQL]\)
- 4. Ejecute el Script.

2.11.3 Verificación de la ejecución del Trigger

- 1. Ejecute el Enterprise Manager desde el menú de inicio: Start > Programs > Microsoft SQL Server > Enterprise Manager
- 2. Seleccione el Servidor de SQL Server e ingrese el usuario de la Autoridad Certificadora.
- 3. Expanda la carpeta del Servidor.
- 4. Expanda la carpeta Databases.
- Expanda la carpeta de la base de datos de la Autoridad Certificadora. (Si utilizó el predeterminado se llama AC SOL).
- Seleccione Tables.
- 7. Seleccione la tabla REVOCADOS.
- 8. Haga clic con el botón derecho del ratón sobre la tabla de revocados.
- 9. Seleccione All Tasks > Manager Triggers.... en el menú emergente.
- 10. Verifique que en la lista de triggers, aparezca uno con nombre: bs_coworkers_upd.

2.12 Configuración de Componentes de Software Adicionales

Modifique los siguientes servicios para que queden en modo automático y dependan de SQL Server (Consultar Manuales):

- SeguriServer, Sección 3.7.6 (Login Automático)
- SeguriNOTARY TSP1 y ENCADENAMIENTO

SeguriData

2.13 Verificación de la instalación del Servicio de Licencia

Verificar que el servicio de licencia bsLS esté iniciado en modo automático, y que dependa de SQL SERVER. Esto se realiza seleccionando:

Start > Programs > Administrative Tools > Services

- 1. Buscar en la lista de Servicios el servicio bsLS V3.0 y seleccionarlo.
- 2. Hacer clic con el botón derecho del ratón en el servicio seleccionado.
- 3. Seleccionar la opción Properties.
- 4. Seleccionar la carpeta General, y verificar que el modo de arranque (Startup type) este configurado en modo automático.
- Seleccionar la carpeta Dependencias.
- 6. Verificar que el nombre del servicio de SQL Server esté incluido en la lista. En caso de no estar incluido siga los siguientes pasos:
 - Obtener el nombre del servicio para SQL Server en el registry seleccionando: Start > Run > regedt34 o Start > Run > regedit (dependiendo de la versión del Sistema Operativo)
 - Seleccionar:

Mi Computer > HKEY_LOCAL_MACHINE > SYSTEM > ControlSet001 > Services

- Buscar el directorio relacionado con SQL Server.
- Buscar la carpeta bsLS en el lado izquierdo de la pantalla y seleccionarla.
- Hacer clic con el botón derecho del ratón en la parte derecha de la pantalla.
- En el menú emergente seleccionar:

New > String Value

- Escriba en la ventana el texto del String: "DependOnService" y haga doble clic con el ratón.
- En el área del texto de la ventana escriba el nombre que obtuvo en el paso [a].
- Haga clic en el botón OK.

2.14 Verificación de la instalación del Servidor de bSigned

Verificar que el servicio asociado con el servidor bSigned bsServer dependa de SQL Server y que el modo de inicio de la aplicación sea también automático. Esto se realiza seleccionando:

Start > Programs > Administrative Tools > Services

- 1. Buscar en la lista de Servicios el servicio bsServer V2.b y seleccionarlo.
- 2. Hacer clic con el botón derecho del ratón en el servicio seleccionado.
- 3. Seleccionar la opción Properties.
- 4. Seleccionar la carpeta General, y verificar que el modo de arranque (Startup type) este configurado en modo automático.
- 5. Seleccionar la carpeta Dependencias.
- 6. Verificar que el nombre del servicio de SQL Server esté incluido en la lista. En caso de no estar incluido siga los siguientes pasos:

• Obtener el nombre del servicio para SQL Server en el registry seleccionando:

Start > Run > regedt34

Seleccionar:

 $\label{eq:micomputer} \mbox{Mi Computer} > \mbox{HKEY_LOCAL_MACHINE} > \mbox{SYSTEM} > \mbox{ControlSet001} > \mbox{Services}$

- Buscar el directorio relacionado con SQL Server.
- Buscar la carpeta bsLS en el lado izquierdo de la pantalla y seleccionarla.
- Hacer clic con el botón derecho del ratón en la parte derecha de la pantalla.
- En el menú emergente seleccionar:

New > String Value

- Escriba en la ventana el texto del String: "DependOnService" y haga doble clic con el ratón.
- En el área del texto de la ventana escriba el nombre que obtuvo en el paso [a].
- Haga clic en el botón OK.

2.15 STS

STS es un sistema de resguardo de información el cual almacena los documentos procesados en bSigned, conservando la integridad de sus propiedades con alta disponibilidad.



Al terminar la instalación de bSigned Server, se despliega la pantalla de configuración para STS, en caso de no configurar en ese momento, localice el STS Wizard.

Para configurar el STSWizard, vaya a la ruta en donde se encuentra instalado: (Figura 2.22) Inicio > Todos los Programas > bSigned_Services > Wizards > STSWizard



Figura 2.22 Configuración STS.

Guardar

Configuración STS. **bSigned** Configuración STS Seguri**D**ata Base de Datos de bSigned Servidor SQL: QA-2K3-SQL5-226 Base de datos: bSigned Contraseña: Nombre de usuario: Propiedades del Servidor STS Información archivo de llaves VAR PKCS12 Examinar Contraseña: Archivo de Llaves: Información de usuario ID del VAR: E-Mail: Contraseña: ID Profile ▼ ID Folder ▼ Obtener IDs URL del servidor STS: Seguridad para la ejecución de la aplicación La aplicación se ejecutara como Contraseña: Usuario:

A continuación aparecerá la pantalla de configuración de STS. (Figura 2.22)

Figura 2.23 Configuración STS.

Para la configuración se debe de colocar los siguientes datos:

© Copyright SeguriData, Inc. 2011. Todos los derechos reservados.

Tabla 2.5

Parámetro	Descripción
Archivo de llaves	Haga clic en el botón Examinar para seleccionar la carpeta donde esta el archivo PKCS12 con las llaves definidas para el VAR (Value Added Reseler)
Contraseña	Coloque la contraseña que corresponde a las llaves que se colocaron
ID de VAR	ID del VAR (Value Added Reseler)
E-Mail	Coloque el e-mail del usuario de STS

Tabla 2.5

Parámetro	Descripción
Contraseña	Indique la contraseña que corresponde al correo electrónico proporcionado.
URL del Servidor STS	Coloque la URL que corresponda al servicio de STS
ID Profile	Coloque el ID del Profile
ID Folder	Coloque ID del Folder
La aplicación se ejecutará como	LocalSystem: Esta opción es para que el servicio que se comunica con el STS se ejecute con la cuenta predeterminada del sistema (Se recomienda esta opción) Otro Usuario: Esta opción es para que el servicio que se comunica con el STS se ejecute con la cuenta predeterminada del sistema.



Importante

Para obtener los IDs del Profile y Folder se pude usar un programa adjunto que permite la consulta de esos valores.

Al termino de un clic en el botón Guardar.



Importante

Una vez que se guarde la configuración se genera el servicio b Signed STS Connector V $3.10\,$

CAPÍTULO 3

Instalación de Signed Web

El presente documento es una guía para la instalación de limed Web versión 3.10. Esto considera la instalación del sitio de limed (páginas HTML y CGIs), la instalación de los certificados de la Autoridad Certificadora, el sitio en el repositorio de Microsoft® Windows y la creación de directorios virtuales.

La instalación deberá ser realizada por personal que cuente con los conocimientos sobre instalación y administración de sistemas, además de tener una cuenta con privilegios de administrador del equipo.

La instalación se divide en dos etapas que deben ejecutarse en el siguiente orden:

- 1. Instalación de Signed Web
- 2. Configuración de Web Server y Microsoft® Internet Information Services

3.1 Requerimientos de Hardware

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

- Procesador Pentium IV @1GHz
- Espacio en disco duro 12GB
- 1GB en RAM
- Unidad lectora de CD-ROM

3.2 Requerimientos de Hardware

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

- Procesador Pentium IV @1GHz
- Espacio en disco duro 12GB
- 1GB en RAM
- Unidad lectora de CD-ROM



3.3 Configuraciones válidas de bigned Web

Existen tres posibles configuraciones que se diferencian según la ubicación de los componentes.

3.3.1 Configuración de cuatro servidores (Recomendada)

El primer servidor contiene al servidor l'signed. El segundo equipo contiene al servidor web con el sitio de l'signed. En un tercer equipo se encuentra la base de datos de l'signed. Finalmente, el cuarto contiene al servidor de correo. (Figura 3.1).

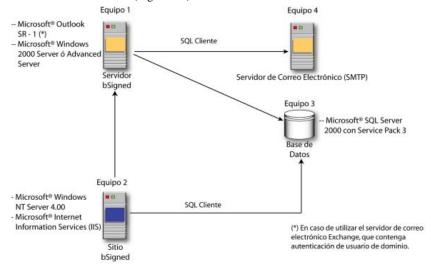


Figura 3.1 Instalación en cuatro equipos

3.3.2 Configuración de tres servidores

El primer servidor contiene al servidor homed y la base de datos de homed. El segundo equipo contiene al servidor web con el sitio de homed. Finalmente, el tercero contiene al servidor de correo. (Figura 3.2).

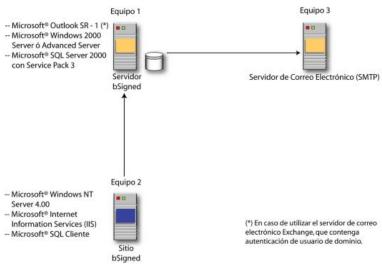


Figura 3.2 Instalación en tres equipos

3.3.3 Configuración de dos equipos

El primer servidor contiene el servidor web con el sitio de bliqued, el servidor bliqued y la base de datos de bliqued. El segundo equipo contiene al servidor de correo. (Figura 3.3).

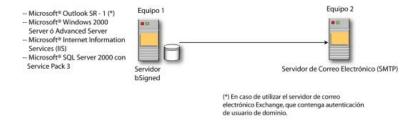


Figura 3.3 Instalación en dos equipos

3.4 Información necesaria para la Instalación

El procedimiento de instalación de lúmed Web requiere que la siguiente información se conozca antes de iniciarlo:

- Instalación del servidor SQL Server donde reside la Base de Datos de Minel
- El nombre de la Base de Datos de bigned
- La clave de acceso a la Base de Datos de l\(\)signed
- La dirección IP y puerto del Servicio de Licencia
- La contraseña de la cuenta del administrador del equipo, donde se instalará el sitio de b\u00edimed
- La dirección IP y puerto del servidor bligned
- La dirección IP del servidor SMTP

Disponer del certificado de la Autoridad Certificadora en formato X.509 y el certificado del sitio en formato PKCS#12 y su contraseña.

3.5 Ejecución del Instalador de bigned Web

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 Seguillata, 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 bSigned Web Wiz 3_10.exe. Ejecútelo haciendo doble clic en el nombre del archivo.

El asistente de instalación mostrará una ventana que permite elegir el idioma que se utilizará durante la instalación, éste puede ser Español o Inglés como se muestra en la Figura 3.4.



Figura 3.4 Selección del Idioma

Seleccione el idioma y haga clic en el botón OK

El asistente de instalación mostrará la siguiente ventana con la identificación del producto. Para comenzar la instalación, haga clic en el botón Siguiente >. (Figura 3.5).



Figura 3.5 Presentación del Producto



A continuación, el asistente solicitará la ubicación de la carpeta destino en donde se instalará la aplicación blimed Web. (Figura 3.6).

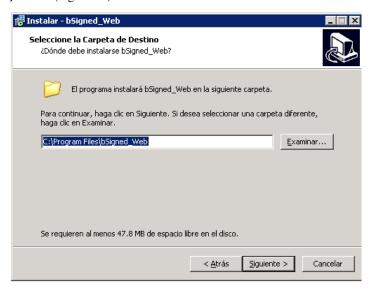


Figura 3.6 Selección de la Carpeta Destino

A continuación, haga clic en el botón Siguiente >.

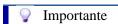
A continuación, el asistente solicitará la ubicación de la carpeta en donde se va a colocar los accesos directos de l\(\) med en el Men\(\) de Inicio. (Figura 3.7).



Figura 3.7 Selección de la Carpeta bSigned Web

Si necesita que no se cree la carpeta en el Menú de Inicio seleccione la casilla "No crear una carpeta en el Menú de Inicio.

Para continuar, haga clic en el botón Siguiente >.



Se recomienda que el directorio bSigned_Web se instale en un subdirectorio Inetpub o Apache de su Web Server.



Cerciórese que aparezca la ruta completa después de haber dado doble clic en el directorio seleccionado.



En esta sección puede seleccionar las tareas adicionales que se desea realizar, en este caso, la tarea adicional es Crear un icono en el escritorio. (Figura 3.8)



Figura 3.8 Selección de tareas adicionales.

Para continuar, haga clic en el botón Siguiente >.

En la siguiente ventana, se muestra un resumen de los valores seleccionados en las etapas anteriores. (Figura 3.9).

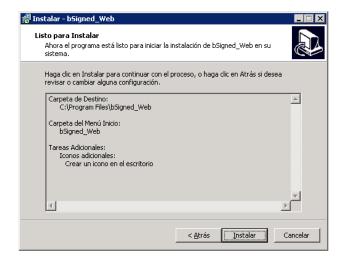
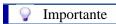


Figura 3.9 Resumen de Valores seleccionados

Si son correctos, haga clic en el botón Instalar.



En caso de ser necesario, puede regresar a las ventanas anteriores por medio del botón < Atrás y modificar los parámetros de instalación.



El proceso de copia de archivos se iniciará mostrando el avance de la instalación. (Figura 3.10).

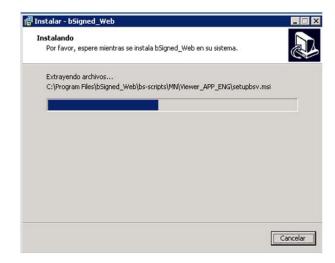


Figura 3.10 Avance de la Instalación

A continuación aparece un mensaje, en el cual se le indica que se instalo con éxito la dll de CapiCom.dll. (Figura 3.11)

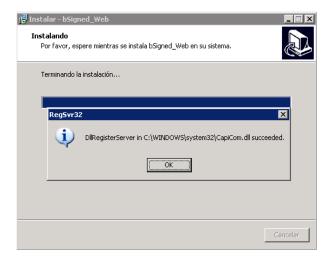


Figura 3.11 Resultado de la Instalación de la DLL.



Importante

Este mensaje aparece como resultado de la instalación en el sistema operativo, ya que se puede instalar a 32 0 64 bits.



Al finalizar, el asistente mostrará un mensaje indicando el resultado de la instalación. (Figura 3.12).



Figura 3.12 Resultado de la Instalación

Haga clic en el botón Terminar.

Marque la casilla Ejecutar bSigned Web, si desea configurar los valores de lo contrario, desmarque la opción y realice la configuración posteriormente. Ver Sección "3.6 Configuración de los Valores de bSigned Web".

3.6 Configuración de los Valores de ligned Web

La configuración de los valores de ligned Web se realiza desde el menú de inicio:

Start > Programs > bSigned Web > bSigned Web 3.10

Esta aplicación muestra las siguientes ventanas.

3.7 Configuración del Sitio Web

Consola que permite configurar los parámetros del Servidor Web, como se muestra en la Figura 3.13.

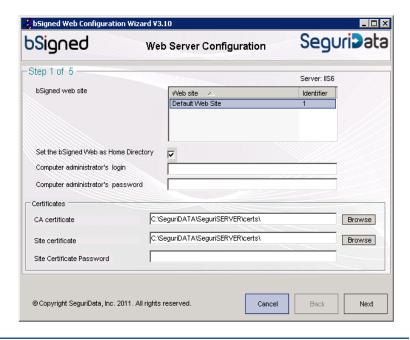


Figura 3.13 Configuración del Sito Web

Seleccione el Sitio Web (Web Site), donde signed Web se instalará.

Seleccione Set the bSigned Web as Home Directory si desea que el sitio de bSigned sea el predeterminado en el servidor de web.

Proporcione los datos que se solicitan, como se muestran en la Tabla 3.1.



Tabla 3.1 Parámetros de Bigned como Home Directory

Parámetro	Dato
Computer Administrator's login	Proporcione el nombre del administrador del equipo.
Computer Administrator's password	Proporcione la contraseña del administrador del equipo.
CA Certificate	Haga clic en el botón Browse para localizar el archivo que contiene el certificado de la Autoridad Certificadora en formato X509.
Site certificate	Haga clic en el botón Browse para localizar el archivo que contiene el certificado del sitio de liquel en formato PKCS12.
Site Certificate Password	Proporcione la clave de uso del certificado del sitio de l\(\)signet.

Haga clic en el botón Next > para continuar.

3.8 Configuración del Servidor Mignel

Consola que permite configurar los datos del Servidor Mint, como se muestra en la Figura 3.14.



Figura 3.14 Configuración del Servidor Signed



Importante

Si en la configuración del SERVER se habilito la opción de "Usar Licencia" y de igual manera se selecciono en la casilla de "Usar registro" la opción "SI" entonces, en la configuración WEB se debe de indicar que también se "Use Licencia" (con esta configuración en WEB queda deshabilitada la opción de "Usar registro").

En el campo bSigned server operation mode seleccione el modo de operación Standard y proporcione los datos que se solicitan como se muestra en la Tabla 3.2.

Tabla 3.2 Parámetros de Configuración del Servidor Mignel

Parámetros	Dato
IP address	Indique la dirección IP del equipo donde se encuentra bSigned Server. (Esta puede ser la misma máquina).
bSigned server port	Seleccione el número de puerto del servidor bligned.

3.8.1 Configuración de la Licencia de liqued

Si el servidor web está en el mismo equipo donde se instaló som Server, NO debe utilizar el servicio de licencia. Sólo configure el lugar donde se almacenarán los datos de la licencia para mejor desempeño de la aplicación. Estos datos se podrán almacenar en dos lugares:

- Registry
- Archivos Locales



Importante

Se recomienda que los datos de la licencia se almacenen en el Registry, a menos que exista alguna restricción para la lectura o escritura, en caso contrario los datos se guardarán en archivos locales.

En caso contrario, seleccione la opción Use License Service y proporcione el número de puerto por donde escuchará este servicio.

Haga clic en el botón Next >.



3.9 Configuración de la Certificación

La consola permite realizar un Test Conection para los certificados de Requerimiento y de la Instalacion, como se muestra en la Figura 3.15.



Figura 3.15 Certificación



Se recomienda realizar esta prueba para validad la conexión.

3.10 Configuración de la Base de Datos

Consola que permite configurar la base de datos, como se muestra en la Figura 3.16.



Figura 3.16 Configuración de la Base de Datos

Proporcione los siguientes datos como se muestra en la Tabla 3.3.

Tabla 3.3 Parámetros para la Configuración de la Base de Datos

Parámetro	Dato
SQL server	Seleccione de la lista el nombre del servidor SQL.
Database login	Indique el usuario con el nombre de "bsigned".
Database password	Indique la clave de acceso del usuario del campo anterior.
Database name	Seleccione de la lista el nombre de la base de datos.

Para comprobar la conexión con el Servidor SQL, haga clic en el botón Test Connection.

Haga clic en el botón Next >.



3.11 Configuración de las Aplicaciones

Consola que permite configurar los parámetros requeridos para el CGI de Inicialización de Acuerdos Electrónicos (NE: New Electronic Agreement) y CGI de búsqueda (SE: Search) (Figura 3.17).



Figura 3.17 Configuración de las Aplicaciones

Proporcione los siguientes datos como se muestra en la Tabla 3.4.

Tabla 3.4 Datos para la bitácora

Parámetro	Dato
GDP Log	Indique si desea habilitar la escritura de la bitácora en el CGI de inicialización.
SE Configuration	Indique el número de registros a desplegar en el resultado de la búsqueda.



Para el campo anterior, se recomienda 30 renglones.

Para finalizar, haga clic en el botón Finish.

Signed Web Configuration Wizard V3.10

Summary

Configuration settings applied ...

© Copyright SeguriData, Inc. 2011. All rights reserved.

Cancel Back Close

Al terminar la configuración se presenta el resultado de la configuración. (Figura 3.18).

Figura 3.18 Final de la Configuración

Haga clic en el botón Close para salir de la configuración.



3.12 Configuración del Certificado del sitio de lume en el servidor web Se lleva a cabo esta configuración con la finalidad de proteger el canal de comunicación entre el servidor blimed y el usuario final. Para esta configuración, seleccione:

Start > Programs > Administrative Tools > Administración de Servicios de Internet

Se presentará la siguiente ventana, que permite seleccionar el sitio web predeterminado. (Figura 3.19).

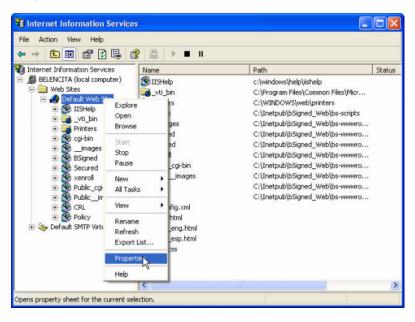


Figura 3.19 Selección del sitio web

Haga clic en el botón derecho del ratón y seleccione la opción Properties del menú emergente.

Default Web Site Properties Web Site ISAPI Filters Home Directory Documents Directory Security HTTP Headers Custom Errors Server Extensions Anonymous access and authentication control Enable anonymous access and edit the authentication methods for this resource. Edit. IP address and domain name restrictions Grant or deny access to this resource using IP addresses or internet domain names. Secure communications Require secure communications and Server Certificate. enable client certificates when this resource is accessed. View Certificate OK Cancel Help

En la siguiente ventana seleccione la carpeta Directory Security. (Figura 3.20).

Figura 3.20 Carpeta Directorio de Seguridad

Haga clic en el botón Server Certificate... para comenzar la instalación del certificado del sitio blimel.



El asistente de instalación mostrará una ventana con la identificación del producto. Para comenzar la instalación, haga clic en el botón Next >. (Figura 3.21).



Figura 3.21 Inicio de la instalación del certificado de Signed

En la siguiente ventana marque la opción Assign and existing certificate y haga clic en el botón Next > como se muestra en la Figura 3.22.



Figura 3.22 Instalación de un certificado ya existente

Available Certificates

The certificates you can use for your Web server are listed below.

Select a certificate:

Issued To Issued By Expiration Date Intended Purpose being Autoridad Certifi... 5/10/2014 Server Authentic...

A continuación seleccione el certificado del sitio blimel que se instalará. (Figura 3.23).

Figura 3.23 Selección del certificado del sitio bigned

Haga clic en el botón Next >.



En la siguiente ventana se presentan el detalle del certificado seleccionado anteriormente. (Figura 3.24).



Figura 3.24 Datos del certificado seleccionado

Haga clic en el botón Next > para iniciar la instalación.

Al finalizar, el asistente mostrará un mensaje indicando el resultado de la instalación. (Figura 3.25).



Figura 3.25 Resultado de la instalación

Haga clic en el botón Finish para finalizar la instalación.



3.13 Configuración de los Directorios Seguros de Binnel

3.13.1Configuración de cgi-bin (Directorio Virtual)

Para elegir el directorio virtual cgi-bin, seleccione la siguiente ruta desde del menú de inicio: Start > Programs > Internet Information Services

Se presentará la siguiente ventana. (Figura 3.26).

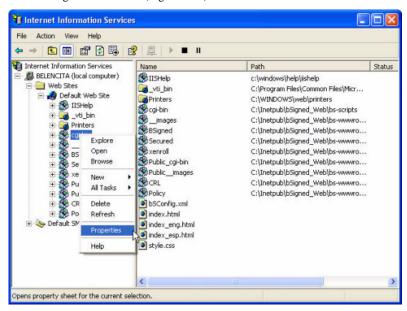
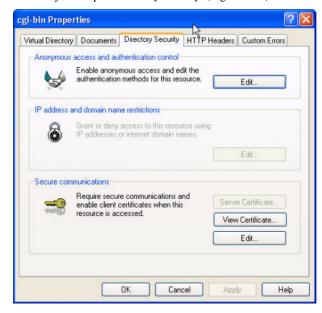


Figura 3.26 Selección del archivo cgi-bin

Seleccione el directorio cgi-bin y haga clic con el botón derecho del ratón y elija Properties del menú emergente.



En la siguiente ventana elija la carpeta Directory Security. (Figura 3.27).

Figura 3.27 Carpeta Directory Security

Elija el apartado Secure communications y haga clic en el botón Edit... (Figura 3.28).



Figura 3.28 Secure communications



En esta ventana marque la opción Require secure channel (SSL) y la opción Require client certificates como se muestra en la Figura 3.29.

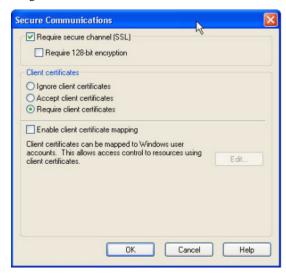


Figura 3.29 Selección de Opciones

Haga clic en el botón Ok.



El producto por default deja habilitada la opción de "Ignore client certificates", al levantar el servicio de bSigned marca un error de "Violación de Memoria".

Para finalizar y guardar las configuraciones, haga clic en el botón Apply y después haga clic en el botón OK. (Figura 3.30).



Figura 3.30 Termino de la configuración



3.13.2Configuración del directorio Secured

Para elegir el directorio, seleccione la siguiente ruta desde del menú de inicio:

Start > Programs > Internet Information Services

Se presentará la siguiente ventana. (Figura 3.31).

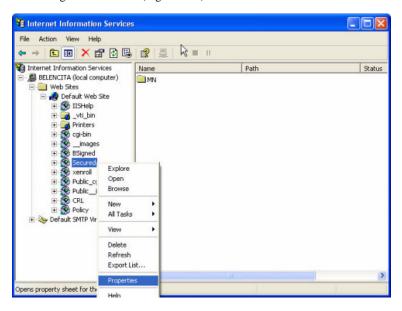
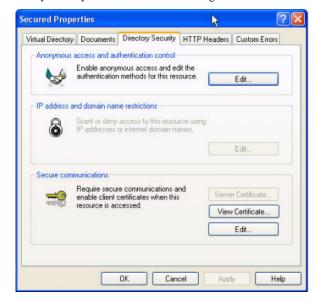


Figura 3.31 Selección del directorio Secured

Seleccione el directorio Secured, y haga clic con el botón derecho del ratón y elija Properties del menú emergente.



Elija la carpeta Directory Security como se muestra en la Figura 3.32.

Figura 3.32 Carpeta Directory Security

Elija el apartado Secure communications y haga clic en el botón Edit... (Figura 3.33).



Figura 3.33 Secure communications



En la siguiente ventana marque la opción Require secure channel (SSL) y la opción Require client certificates como se muestra en la Figura 3.34.

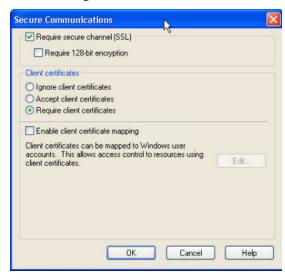


Figura 3.34 Selección de opciones

Haga clic en el botón Ok.

Para finalizar y guardar las configuraciones haga clic en el botón Apply, y después haga clic en el botón OK. (Figura 3.35).

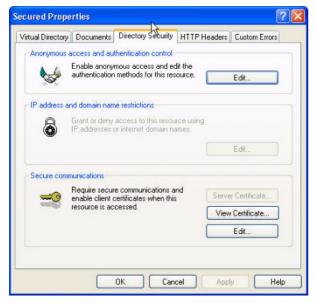


Figura 3.35 Termino de la configuración



Importante

En el caso de instalar l\(\) med en Windows 2003, deber\(a \) agregar los usuarios con todos los privilegios a la carpeta f\(\) fisica donde est\(a \) los webservices:

- *) Network Service
- *) ASPNET
- *) Internet User

En los permisos del Event Log los siguientes:

- *) ASPNET
- *) Internet User
- *) Network Service

Y para el caso de que se tenga el IIS versión 6.0, adicionar los permisos de correr CGI y ASPNET.

3.14 Limpiar el caché Se recomienda limpiar el caché de su navegador para que éste tome la última configuración. del navegador

Para limpiarlo, ejecute su navegador de Internet y seleccione el siguiente menú:

Tools > Internet Options... > Carpeta General

como se muestra en la Figura 3.36.

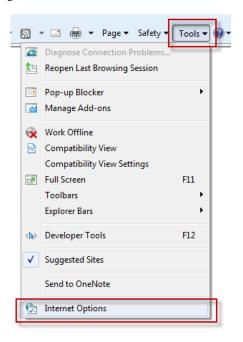


Figura 3.36 Selección del menú

En la ventana siguiente, elija el apartado Temporary Internet Files y haga clic en el botón Delete Files.. para eliminar los archivos temporales y actualizar la última configuración del sitio, como se muestra en la Figura 3.37.



Figura 3.37 Eliminación de archivos temporales

Por ultimo se presentará la confirmación de eliminación de archivos temporales. Haga clic en el botón OK para eliminarlos como se muestra en la Figura 3.38.

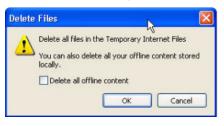


Figura 3.38 Mensaje de confirmación

3.15 Configuración del equipo del Administrador

La configuración del equipo del Administrador se realiza mediante las actividades listadas en la Tabla 3.5.

Tabla 3.5 Configuración del equipo del Administrador

	Actividad	Comentarios
1.	Importación del PKCS#12 al navegador del administrador de bSigned	Desde el Panel de Control o desde el menú de Microsoft® Internet Explorer seleccione: Tools > Internet Options > Content > Certificates > Import



3.16 Configuración del Servidor bigned

La configuración del Servidor de \mathfrak{b} se realiza mediante las actividades listadas en la Tabla 3.6.

Tabla 3.6 Configuración del Servidor bigned

	Actividad	Comentarios
Configuración del Servidor l\(\) Signed	Obtener Licencia	 Ejecute el explorador de Internet e indique la dirección donde reside el sitio de bijnel.
		 Seleccione el idioma y haga clic en el botón Entrar.
		 Haga clic en la liga Usar bSigned.
		Seleccione el certificado del administrador de bsigned.
		 Seleccione del menú de l\(\)signed: Administración del Servidor > Servidor de Licencia > Obtener Identificador
		Enviar el Identificador obtenido a soporte técnico de suribata para obtener el archivo de licencia.
	Instalación de la Licencia	 Una vez que se obtuvo el archivo de Licencia seleccione del menú de l\(s\)imid:
		Usar bSigned > Administración del Servidor > Servidor de Licencia > Instalar Licencia
		Proporcione el nombre del archivo de Licencia.
		Seleccione del menú de limed: Administración del Servidor > Configurar Servidor > Parámetros de operación
		 Haga clic en el botón Edit y establezca los siguientes parámetros según lo requiera: Vigencia de Documentos Número de notificaciones Texto de Notificaciones Parámetros de Adhesión limitada
		 Verificar las cuentas de correo.

Tabla 3.6 Configuración del Servidor Migned (Continuación)

Ac	tividad	Comentarios
•	Configurar el mecanismo para validar la Revocación	Seleccione del menú de ligned: Administración del Servidor > Configurar Servidor > AC(s)
		 Verificar que se encuentre el certificado de la Autoridad Certificadora en la tabla.
		 Hacer clic en el icono Mecanismo para Validar Revocación.
		 Marque la opción Respondedor OCSP e indique la URL del Respondedor OCSP.
2.	Verificar el Certificado del Administrador de l'Signed	 Seleccione del menú de l\(\) Signed: Administración del Servidor > Configurar Servidor > Certificados de Usuarios
		 Verificar que se encuentre el certificado del Administrador de b\(\sigma\)jmed.
3.	Respondedor TSP	Seleccione del menú de himd: Administración del Servidor > Configurar Servidor > Respondedor TSP
		 Haga clic en el botón Edit.
		 Indique el certificado de la Autoridad Certificadora que certifica al Respondedor de TSP e indique la URL del Respondedor TSP.



3.16.1 Arranque del Servidor Signed

Después de completar la configuración del servidor, inicie el servicio bigned desde la consola de servicios, o bien desde el menú de bigned:

Administración del Servidor > Iniciar Servicio

En caso de que se presente algún error, verifique las bitácoras de blimel. (Tabla 3.7).

Tabla 3.7 Bitácoras de bigned

Bitácora	Resultado
\bsigned_Services\bsignedServer\LOGS	%day% [TRACE].txt: Rastreo de los procesos en background del Servidor de Firma Electrónica del día %day%
	%day.txt: Bitácora de errores de los procesos en background del Servidor de Firma Electrónica del día %day%
\bsigned_Services\bsignedServer\LOGScb	%day% [TRACE].txt: Rastreo del proceso de Callback llamado por el Servidor de Firma Electrónica del día %day%
	%day.txt: Bitácora de errores del proceso de Callback llamado por el Servidor de Firma Electrónica del día %day%
$ b signed_Services b signedServer _TRACE$	%day% [TRACE].txt: Rastreo de los procesos de inicio y firma de un documento en el Servidor de Firma Electrónica del día %day%
	%day.txt: Bitácora de errores de los procesos de inicio y firma de un documento en el Servidor de Firma Electrónica del día %day%

Después de corregir los errores que se identifiquen en las bitácoras, inicie el servicio nuevamente.

bigned - Versión 3.10 Descarga de Acuerdos

3.17 Descarga de Acuerdos

3.17.1 Reemplazo de archivos

En el CD de instalación visualizará las siguientes tres carpetas: (Figura 3.39)

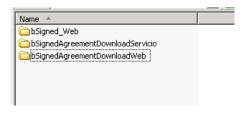


Figura 3.39 Contenido del CD de instalación.

bSignedWeb

Dentro de la carpeta de bSignedWeb, se encontrará la carpeta bs-scripts, la cuál contendrá las carpetas de MN y NE. (Figura 3.40)



Figura 3.40 Directorio de bSignedWeb

Dentro de la carpeta MN, se encontrarán los archivos de bsigned.exe y left(6).htm, los cuáles tendrán que ser remplazados al servidor destino. (Figura 3.41)

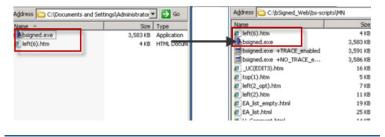


Figura 3.41 Contenido de la carpeta MN.



Dentro de la carpeta de NE, se encontrará el archivo NE.exe, el cuál debe ser reemplazado al servidor destino. (Figura 3.42)

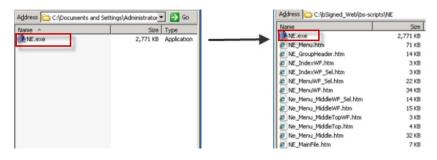


Figura 3.42 Contenido de la carpeta NE.

Dentro de la carpeta de bSignedWeb, también se encontrará la carpeta bs-wwwroot, la cuál contendrá las carpetas de _images y Public. (Figura 3.43)

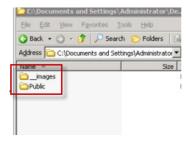


Figura 3.43 Contenido de la carpeta bs-wwwroot...

Dentro de la carpeta _images, se encuentra el archivo Splash_bSigned_Esp.gif, el cuál deberá ser reemplazado al servidor destino. (Figura 3.44)



Figura 3.44 Contenido de la carpeta _images.

Dentro de la carpeta MN se encuentra la carpeta Public, la cuál contiene la carpeta Public_cgibin, y dentro la cuál se encuentra el archivo bsigned.exe el cuál deberá ser reemplazado en el servidor destino. (Figura 3.45)

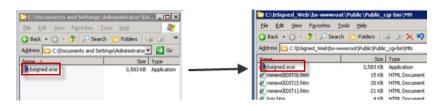


Figura 3.45 Contenido de la carpeta Public_cgi-bin.



3.17.2 Creación de carpetas

Se debe de crear un directorio llamado bSignedAgreementsDwnldWeb dentro de la carpeta de bSigned_Web. (Figura 3.46)

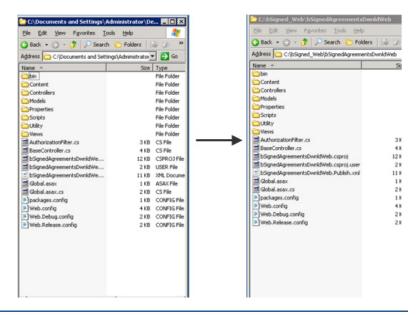


Figura 3.46 Directorio bSignedAgreementsDwnldWeb en la carpeta de bSigned_Web.



Esta carpeta debe de estar dentro de bSigned_Web.

Abrir el archivo Web.config y localizar la cadena de la base de datos y poner los valores del servidor destino (Figura 3.47)

```
<add name="bsignedEntities"
connectionString="metadata=res://"/Models.bsignedModel.csdlires://"/Models.bsignedModel.csdlires://"/Models.bsignedModel.csdlires://"/Models.bsignedModel.csdlires://"/Models.bsignedModel.csdlires://"/Models.bsignedModel.csdlires://"/Models.bsignedModel.csdlires://"/Models.bsignedBodels.bsignedEntition.csdlires://"/Models.bsignedBodels.bsignedEntition.csdlires://"/Models.bsignedModels.bsignedEntition.csdlires://
Latalog=bsignedEntition.csdlires://
Latalog=bsign
```

Figura 3.47 Web.config

Por último, se le tiene que proporcionar los permisos necesarios al usuario NETWORK SERVICE. (Figura 3.48)

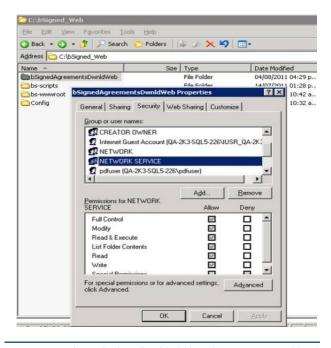


Figura 3.48 Directorio de aplicación bSignedAgreementsDwnldWeb



3.17.3 IIS

Se debe de crear el directorio de aplicación con el nombre de bSignedAgreementsDwnldWeb. (Figura 3.49)

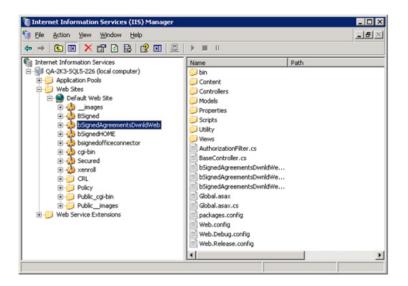


Figura 3.49 Directorio de aplicación bSignedAgreementsDwnldWeb

Seleccione el directorio creado y de un clic derecho para desplegar el submenú de properties (Figura 3.50)

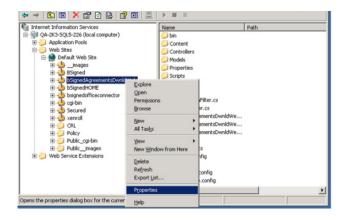


Figura 3.50 Submenú properties.

Se desplegará la siguiente ventana. (Figura 3.51)

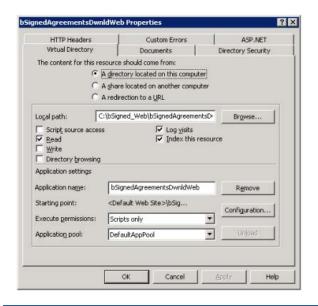


Figura 3.51 bSignedAgreementsDwnldWeb Properties.



Dar clic en el botón *Configuration*. (Figura 3.52)

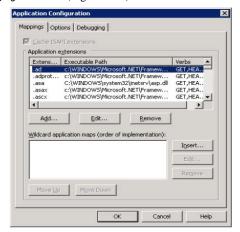


Figura 3.52 Configuration

Dar clic en el botón Add. (Figura 3.53)

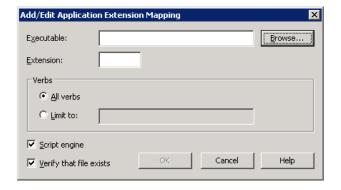


Figura 3.53 Add.

Dar clic en el botón *Browse* y seleccionar la ruta del ejecutable del Framework (aspnet_isapi.dll). (Figura 3.54)

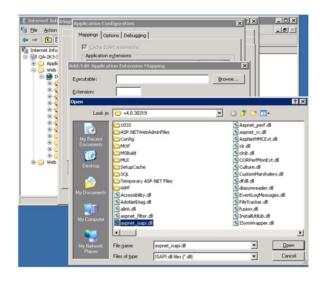


Figura 3.54 Ruta del ejecutable del Framework.

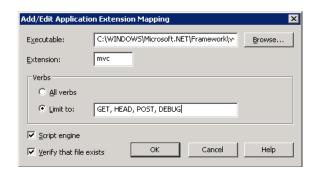


Figura 3.55 Browse.



Importante

En el campo de Extensión se tiene que poner .mvc y en el campo de Limit To poner GET,HEAD,POST,DEBUG.



3.17.4 bSigned Agreements DwnldServer

Se debe de abrir una instancia de SQL y ejecutar el Query Create Table bn_DWNLD_Reqst.sql (Figura 3.56)

Figura 3.56 Create Table bn_DWNLD_Reqst.sql

3.17.5 Instalación de bSigned Agreements Download

Para instalar esta funcionalidad debemos localizar la carpeta con el nombre de bSignedAgreementsDwnldServiceSetup, ya que en su contenido esta el archivo Setup.exe al cual hay que ejecutar.

La primer pantalla que aparece es la bienvenida al instalador de bSigned Agreements Dowload. (Figura 3.57).



Figura 3.57 Bienvenida al instalador de bSigned Agreements Download.

Para continuar de un clic en el botón Next>



A continuación aparece un mensaje para confirmar la instalación. (Figura 3.58)

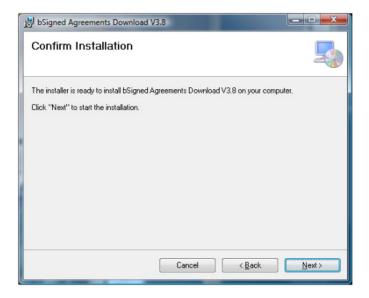


Figura 3.58 Confirmar la instalación..

Para continuar de un clic en el botón Next>

Installation Complete

bSigned Agreements Download V3.8 has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Por último aparece un mensaje indicando que ha concluido la instalación. (Figura 3.59)

Figura 3.59 Instalación finalizada..

Para finalizar de clic en el botón Close.



3.17.6 Configuración

Después de la instalación se debe de configurar este servicio, para esto vaya a la ruta donde se instaló bSigned Agreements Download. (Figura 3.60)

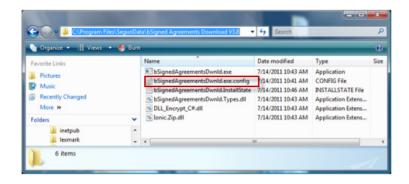


Figura 3.60 Configuración..

En esta carpeta localice archivo bSignedAgreementsDownload.exe.config y ábralo con un editor de texto. (Figura 3.61)

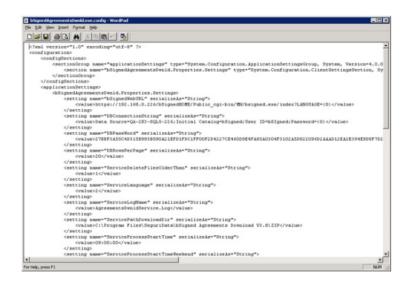


Figura 3.61 bSignedAgreementsDownload.exe.config.



Precaución

Es importante respetar el formato (tipo de dato) que se localiza en el archivo de configuración, ya que el sistema tomará los valores definidos por default.

Para iniciar la configuración, empezaremos con la línea bSignedAgreementsDwnld.Properties.Settings.

En esta línea se debe de cambiar la IP predefinida por la IP en la que reside el servicio de bSigned. (Figura 3.62).

Figura 3.62 bSignedAgreementsDwnld.Properties.Settings.

Configuración de la base de datos

En la siguiente línea setting name="DBConnectionString" serializeAs="String" contiene la información de la base de datos de bSigned,para la configuración de está se deben de seguir los siguientes pasos:

Primero se debe de configurar el nombre de la máquina donde se aloja a base de datos. (Figura 3.63)

Figura 3.63 Máquina donde se aloja la BD

A continuación se debe de colocar el nombre de la base de datos de bSigned. (Figura 3.64)

Figura 3.64 Nombre de la base de datos.



Después se debe de colocar el usuario de la base de datos. (Figura 3.65)

```
User ID=bSIgned; Password={0}</value>
```

Figura 3.65 Usuario de la base de datos.

Por último tenemos el password de la base de datos. (Figura 3.66)

```
User ID=bSIgned;Password={0}</value>
```

Figura 3.66 Password de la base de datos.



Importante

No se debe quitar o cambiar el valor predefinido en Password = $\{0\}$.

A continuación ingrese el password encriptado. (Figura 3.67)

Figura 3.67 Password encriptado de la base de datos.



Importante

Para realizar la encriptación del password se debe utilizar la herramienta llamada PassEncrypt.exe la cuál se puede encontrar en C:/bSigned_Services/PassEncrypt.

Ruta de descarga.

En el siguiente párrafo se colocará la ruta de descarga, en la cuál se almacenarán los archivos .Zip que contienen los acuerdos descargados de acuerdo a lo solicitado por el usuario. (Figura 3.68)

Figura 3.68 Ruta de descarga.



Importante

Debe cuidar el espacio disponible de la ruta proporcionada.

3.17.7 Configuración del horario

Ahora se deben colocar los horarios en los cuáles va a trabajar el servicio.



Importante

El formato que se maneja es de 24 hrs.

• Hora de inicio en formato HH:MM:SS

Figura 3.69 Hora de inicio.

• Hora de inicio durante el fin de semana en formato HH:MM:SS

Figura 3.70 Hora de inicio durante el fin de semana.



• Horario en el que se va a detener el servicio en formato HH:MM:SS.

Figura 3.71 Horario en el que se va a detener el servicio.

• Tiempo de espera del servicio, el tiempo se coloca en milisegundos.

Figura 3.72 Tiempo de espera.

3.17.8 Configuración del correo electrónico.

A continuación se configura el correo electrónico en el cuál se enviará el aviso de la descarga de los acuerdos al usuario que lo solicitó.

Dirección del correo electrónico

Figura 3.73 Correo electrónico.

• Nombre del Usuario de la cuenta de correo electrónico.

Figura 3.74 Nombre de usuario.

Después se coloca el password cifrado de la cuenta de correo electrónico.

Figura 3.75 Password.



Importante

Para realizar la encriptación del password se debe utilizar la herramienta llamada PassEncrypt.exe la cuál se puede encontrar en C:/bSigned_Services/PassEncrypt.

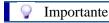
En este párrafo se coloca el usuario SMTP.

Figura 3.76 Usuario SMTP.



En los párrafos siguientes se muestra el cuerpo del correo, puede ser en inglés o en español. (Figura 3.77)

Figura 3.77 Cuerpo del correo electrónico.



No modificar los {0} ya que son variables que se definieron en la parte superior.

A continuación configure el tipo de escritura a la bitácora del servicio. (Figura 3.78)

Figura 3.78 Tipo de escritura.



VerboseMode (True) escribe a bitácora paso a paso lo cuál sólo es recomendable en caso de que el servicio no se pueda iniciar.

Una vez terminando de configurar ha que salvar los cambios que sufrió el archivo de configuración. A continuación se debe de abrir una ventana de servicios para levantar el servicio de bSigned Agreements Download. (Figura 3.79)

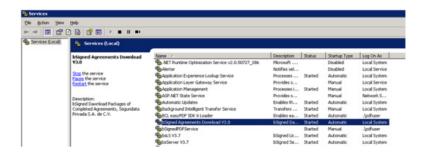


Figura 3.79 Servicio levantado del bSigned Agreements Download.

Instalación de bSigned Web



Capítulo 4

Desinstalación

Para la desinstalación de la aplicación seleccione el siguiente menú:

Start < Programs < SeguriData < bSigned Server Configuration Wizard < Uninstall bSigned Server Configuration Wizard

Se presenta la siguiente ventana de confirmación de desinstalación. (Figura 4.1).



Figura 4.1 Mensaje de Confirmación

Para continuar con la desinstalación haga clic en el botón Yes.



En la siguiente ventana se muestra el avance de la desinstalación. (Figura 4.2).

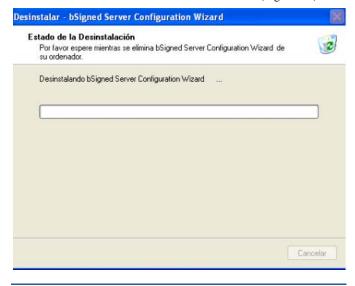


Figura 4.2 Avance de la Desinstalación

Al finalizar se presenta un mensaje con el resultado de la desinstalación. (Figura 4.3).

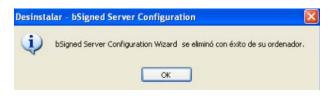


Figura 4.3 Resultado de la Desinstalación

Haga clic en el botón Ok para finalizar.

Capítulo 5

Uso del CGI de bigned

El CGI de simel, permite la gestión de documentos que se encuentran en una base de datos de terceros, a través de aplicaciones basadas en Web. Y éste debe ser ejecutado por un usuario con privilegios de la máquina donde se encuentra instalado simel Server.

5.1 Funcionamiento del CGI

Al ser invocado el CGI, éste realiza el siguiente procedimiento para iniciar la gestión del documento.

Tabla 5.1 Funcionalidad del CGI

Paso	Acción					
1	Extrae del Registry los valores INSTANCE, PASSWORD y USER para acceder a las tablas de trabajo: GDP_NE (Oracle), GDP_NE_COWORKERS (Oracle) y la tabla de Oracle cuyo nombre está indicado a su vez, en la siguiente referencia en SQL Server: BS_GDPCONFIG.<[Table]> La llave del Registry que contiene estos valores es: HKEY_LOCAL_MACHINE\SOFTWARE\SeguriDATA\bSigned					
2	Se conecta a Oracle.					
3	Lee el archivo de configuración: :\bSigned\Config\bSConfig.xml para obtener los parámetros necesarios para conectarse con el servidor de SQL Server, abriendo una sesión a la base de datos de limed. Los valores que se toman de este archivo y que están incluidos en la variable "CONN"son:					
	Clave de Acceso (Password)					
	• Usuario (User ID)					
	Nombre del Servidor (Data Source)					



Tabla 5.1 Funcionalidad del CGI (Continuación)

Paso	Acción					
4	Se conecta a SQL Server.					
5	Obtiene el número de serie del certificado del inicializador de la tabla GDP_NE_COWORKERS (Oracle).					
6	Valida que el inicializador esté dado de alta en bigned, en la tabla: BS_COWORKERS (SQL Server).					
7	Valida que le certificado con el que se accedió a la página, sea el certificado inicializador.					
8	Elimina de las tablas temporales de limid, los documentos que sean generados por dicho certificado (certificado del inicializador).					
9	Obtiene de la tabla GDP_NE los siguientes datos del documento:					
	• document_id					
	• system_id					
	• email_body					
	• document_file					
	• document_name					
	• signature_requirement					
	• sign_sequence					
	expiration_date					
	• tries_num					
	• lend_minnumofsgtrs					
	lend_additionaltime					
10	Calcula la digestión del certificado del inicializador.					
11	Calcula la digestión del documento.					
12	Calcula el tamaño del documento.					
13	Calcula el tiempo de duración del documento en minutos.					
14	Calcula el tiempo entre notificaciones de firma.					
15	Valida que los certificados utilizados estén dados de alta en el sistema lignel. Tabla BS_COWORKERS					

Tabla 5.1 Funcionalidad del CGI (Continuación)

Paso	Acción				
16	Inserta en la tabla de ligned BS_REQUIREMENTS los siguientes valores:				
	• ReqID				
	• ReqDesc				
	• ReqType				
	• [Date]				
	• ReceptionTime				
	• StatusID				
	• ErrorID				
	• Busy				
	DocumentName				
	• DocumentPath				
	• DocumentSize				
	• TimeToWartATSR				
	• TriesNum				
	• SubscriptionDOC				
	ExpirationDate				
	• DigestDOC				
	• Document				
	EXTERNSYSTEM_ID				
	• EXTERN_SYSTEM				
	EXTERN_DOC_ID				
	• EMail_BODY				
	• doc_extension				
	LEnd_MinNumOfSGTRS				
	LEnd_AdditionalTime				



Tabla 5.1 Funcionalidad del CGI (Continuación)

Paso	Acción					
17	Inserta en la tabla de lignet BS_REQCOWORKERS la siguiente información:					
	• ReqID					
	• CoWorkerID					
	• CertDigest					
	• TypeID					
	• Seq					
	• Tries					
	• Starter					
18	Envía petición de procesamiento al Servidor limed a través del llamado: SendNE_DOC (ReqID, StarterID, Starter_CertDigest, HTTPHost)					
19	Muestra reporte de estatus.					

Una vez que concluye el proceso de firma, el Servidor Signel realiza el siguiente proceso de Callback.

Tabla 5.2 Funcionalidad del Callback

	14514 5.2 I dictonantata dei Canbaca					
Paso	Acción					
1	Obtiene de la tabla de lisigned los valores de BS_REQUIREMENTS:					
	 EXTERN_SYSTEM_ID 					
	EXTERN_DOC_ID					
	De acuerdo a ReqID					
2	Obtiene de la tabla de liquel los valores de BS_GDPCONFIG:					
	• [table]					
	• stored_proc					
	• col_doc_id					
	• col_reqid					
	• col_receipt					
	• col_status					
	• nombres_columnas.txt					
	• SGTR_TABLE					
	SGTR_COL_DOC_ID					
	• SGTR_COL_SERIAL_NUMBER					
	 SGTR_COL_ACCEPTANCE_SIGNATURE_TIME 					
	 SGTR_COL_DECLINED_SIGNATURE_TIME 					
	 SGTR_COL_ACCEPTANCE_SIGNATURE 					
	 SGTR_COL_DECLINED_SIGNATURE 					
	 SGTR_COL_DISAGREE 					
	de acuerdo a EXTERN_SYSTEM_ID					
3	Cerrar sesión de SQL Server y abrir una nueva sesión a la base de datos Oracle.					
4	En caso de que el proceso de firma haya concluido sin error, deposita en la tabla BS_GDPCONFIG.<[Table]> (de Oracle), el recibo criptográfico en la					
	columna col_receipt, en caso de que el proceso de firma haya concluido con o					
	sin error, actualiza el status del documento en la columna col_status e inserta el identificador del documento en la columna col_regid.					
	Las actualizaciones se harán en el registro donde el contenido de la columna					
	col_doc_id sea igual a EXTERNDOC_ID.					
5	En caso de haberse especificado, se ejecuta el procedimiento almacenado stored_proc.					
	-					



Tabla 5.2 Funcionalidad del Callback (Continuación)

Paso	Acción	
6	Se cierra la sesión de Oracle.	

bigned - Versión 3.10 Invocación del CGI

5.2 Invocación del CGI

El CGI deberá de ser invocado desde una página web. A continuación se presenta un ejemplo de la manera en que se recomienda el uso del CGI.

```
[1] <html>
        <head>
          <meta http-equiv="content-type" content="text/html;charset=iso-8859-1">
 [4]
          <meta name="generator" content="Adobe GoLive 5">
 [5]
          <title>Welcome to bSigned </title>
 [6]
        </head>
        <body bgcolor="#ffffff" topmargin="0" leftmargin="0">
          <SCRIPT LANGUAGE="JavaScript">
 [8]
           var addWindow
 [9]
           function subpop()
             if (!addWindow || addWindow.closed)
[14]
               addWindow = window.open("https://< hostname > /cgi-bin/NE_GDP/
[15]
                NE_GDP.exe?document_id=1",
[16]
                "cal","width=450,height=380,resizable=0,status=1,
                menubar=0,scrollbars=0,fullscreen=0")
[18]
              addWindow.focus()
            }
            else
            {
              addWindow.focus()
            }
          </SCRIPT>
          <a href="javascript:subpop()">GDP_bSigned</a>
        </body>
[28] </html>
```

La función subpop() desplegará una ventana en la que se mostrará el estatus de la transacción, evitando que se modifique el contenido de la ventana desde la cual se invoca el CGI.



5.3 Mensajes de Error

En caso de que ocurra algún error al momento de procesar un documento, el CGI enviará algunos de los siguientes mensajes para facilitar la corrección de la situación que se presente.

El código de Error corresponde a los valores de la tabla BS_GDPCONFIG.<[Table]> en el campo BS_GDPCONFIG. $<col_status>$

Tabla 5.1 Mensajes de Error Emitidos por el CGI de bligned

Descripción	Código de Error
ERROR el Documento ya está en proceso.	90
ERROR al extraer información de la tabla GDP_NE: SYSTEM_ID, EMAIL_BODY. [EOracleError]	91
ERROR No se encontró el registro del documento que se someterá a firma. [GDP_NE.DOCUMENT_ID= <document_id_value>]</document_id_value>	91
ERROR al extraer información de la tabla GDP_NE: DOCUMENT_FILE, DOCUMENT_NAME, SIGNATURE_REQUIREMENT, SIFGN_SEQUENCE, EXPIRATION_DATE, TRIES_NUM, LEnd_MinNumOfSGTRS, LEnd_AdditionalTime	91
ERROR al extraer información de la tabla GDP_NE_COWORKERS: STARTER SERIAL_NUMBER.	92
ERROR No se encontró el registro del iniciador del documento que se someterá a firma. [GDP_NE_COWORKERS.DOCUMENT_ID= <document_id_value>]</document_id_value>	93
ERROR El Número de Serie del Iniciador no ha sido especifi-cado. [GDP_NE_COWORKERS.DOCUMENT_ID= <document_id_value>]</document_id_value>	111
ERROR No se puede procesar este documento, es necesario entrar a la página con el certificado del inicializador.	94
ERROR El participante con Certificado Número: <serial_number_value> no está dado de alta en bSigned.</serial_number_value>	95
ERROR El Participante marcado como iniciador, no puede iniciar gestión de documentos, Certificado Número: <serial_number_value></serial_number_value>	97
ERROR Los siguientes certificados de participantes no están dados de alta en bSigned: <serial_number_list_value></serial_number_list_value>	96
ERROR La Fecha de Expiración del documento que se someterá a firma no es válida. [GDP_NE.EXPIRATION_DATE= <expiration_date_value>]</expiration_date_value>	109
ERROR El proceso de digestión del documento en B64 que se someterá a firma no fue completado. [<filenameb64>]</filenameb64>	99
ERROR El proceso de inserción a SQL SERVER (BS_REQUIREMENTS) no fue completado.	100

Tabla 5.1 Mensajes de Error Emitidos por el CGI de bliquel (Continuación)

Descripción	Código de Error
ERROR al obtener el status del documento que se someterá a firma.	89
ERROR No se encontró el registro del documento que se someterá a firma. [BS_GDPCONFIGTable.DOCUMENT_ID= <document_id_value>]</document_id_value>	89
ERROR Estatus inválido del documento que se someterá a firma. [BS_GDPCONFIGTable.DOCUMENT_ID= <document_id_value>]</document_id_value>	89
ERROR al inicializar socket.	101
ERROR al abrir socket.	102
ERROR al establecer conexión con el servidor bSigned.	103
ERROR al codificar petición de envío del requerimiento.	104
ERROR al enviar al servidor bSigned la petición de procesar el nuevo documento.	105
ERROR al leer respuesta del servidor bSigned.	106
ERROR al menos un certificado ha sido revocado o está vencido.	107
ERRORES devueltos por servidor bSigned durante el proceso de un documento > {ERRORES INTERNOS; CONSULTAR LOG DE BSIGNED}	108



De la misma forma, en la tabla BS_GDPCONFIG.<[Table]> queda registrado el estado de la gestión de cada documento.

Tabla 5.2 Estatus del CGI bSigned

	Descripción	
1		PROCESO DE FIRMA NO INICIADO
2		PROCESO DE FIRMA INICIADO

Tabla 5.3 Estatus del Callback

Código de Error o Exito	Descripción		
3	PROCESO DE FIRMA CONCLUÍDO SIN ERROR		
4	PROCESO DE FIRMA CANCELADO POR TIMEOUT		
5	PROCESO DE FIRMA CANCELADO POR CERTIFICADO FUERA DEL RANGO DE VALIDEZ -VENCIDO (Validado al momento de la firma).		
6	PROCESO DE FIRMA CANCELADO POR CERTIFICADO REVOCADO (AtoSignReq_W) (Validado al momento de la firma)		

5.4 Estructura de Tablas de Signed

Las siguientes tablas son utilizadas por el CGI para leer los componentes del documento e iniciar su gestión.

Estas tablas deberán ser cargadas antes de invocar el CGI.

Tabla 5.4 Estructura de la Tabla GDP_NE (Oracle)

Campo	Tipo	Longitud	Descripción
DOCUMENT_ID	Number	5	Identificador del Documento.
DOCUMENT_FILE	Blob		Documento a ser firmado.
DOCUMENT_NAME	VarChar2	255	Nombre del documento.
SIGNATURE_REQUIREMENT	Char	1	0 Firma obligatoria 1 Firma de adhesión 2 Firma de adhesión limitada
SIGN_SEQUENCE	Char	1	0 Sin orden 1 Con orden preestablecido
EXPIRATION_DATE	Date		Fecha de expiración del documento.
TRIES_NUM	Number	5	Número máximo de notificaciones de firma.
SYSTEM_ID	Number	5	Clave de configuración en BS_GDPCONFIG.

Tabla 5.4 Estructura de la Tabla GDP_NE (Oracle) (Continuación)

Campo	Tipo	Longitud	Descripción
EMAIL_BODY	VarChar2	255	Texto del correo electrónico que será enviado en las notificaciones de firma.
LEND_MINNUMOFSGTRS	Number	5	Mínimo número de firmas requeridas para los documentos con tipo de firma de adhesión limitada.
LEND_ADDITIONALTIME	Number	5	Tiempo de tolerancia para recabar más firmas una vez alcanzado el mínimo de número de firmas requeridas.

 $Tabla~5.5~Estructura~de~la~Tabla~GDP_NE_COWORKERS~(Oracle)$

Campo	Tipo	Longitud	Opcional	Descripción
DOCUMENT_ID	Number	5		Identificador del Documento.
SERIAL_NUMBER	VarChar2	255		Número de serie del certificado digital del usuario, del cual se requiere la firma.
TYPE_ID	Char	1		Rol del participante: R - Revisor S - Firmante W - Testigo A - Destinatario
SEQ	Number	5	X	Número que indica el orden en que firmará el usuario, en caso de que se establezca orden de firma.
STARTER	Char	1		Indica si el usuario es el inicializador del proceso de firma: 0 - Falso 1 - Verdadero
ACCEPTANCE_SIGNATUR E_TIME	Date		X	Fecha y hora en que fue aplicada la firma de aceptación.
DECLINED_SIGNATURE_ TIME	Date		X	Fecha y hora en que fue aplicada la firma de desacuerdo.
ACCEPTANCE_SIGNATUR E	Blob		X	Firma de aceptación.
DECLINED_SIGNATURE	Blob		X	Firma de desacuerdo.
DISAGREE	VarChar2	255	X	Motivo o razón de desacuerdo.

Tabla 5.6 Estructura de la Tabla BS_GDPCONFIG.Table (Oracle)

Campo	Tipo	Longitud	Opcional	Descripción
DOCUMENT_ID	Number	5		Identificador del Documento.
FILENAME	VarChar2	350		Nombre del Documento.
REQID	VarChar2	32	X	Identificador del Documento en la base de datos de la signed.
RECEIPT	Blob		X	Recibo criptográfico del Documento concluido.
STATUS	Char	1		Estatus de firma del Documento.

La siguiente tabla es utilizada por el Callback para determinar la ubicación del estatus del documento concluido, recibo criptográfico e identificador del documento en la base de datos de bliqued.

Tabla 5.7 Estructura de la Tabla BS_DGDPCONFIG (SQL Server)

Campo	Tipo	Longitud	Opcional	Descripción
SYSTEM_ID	Integer	4		Clave de configuración.
INSTANCE	Char	255		Nombre de la instancia de Oracle.
[TABLE]	Char	255		Nombre de la tabla en que se depositará el recibo criptográfico, estatus de firma e identificador del documento en la base de datos de bijned.
[USER]	Char	255		Nombre del usuario de la base de datos.
Passwd	Char	255		Contraseña del usuario de la base de datos de Oracle.
STORED_PROC	Char	255	X	Procedimiento almacenado a ejecutar una vez concluido el proceso de firma.
COL_DOC_ID	Char	255		Nombre de la columna que contiene el identificador del documento a firmar.
COL_REQID	Char	255		Nombre de la columna que contiene el nombre del identificador del documento en la base de datos de bisped.

Tabla 5.7 Estructura de la Tabla BS_DGDPCONFIG (SQL Server) (Continuación)

Campo	Tipo	Longitud	Opcional	Descripción
COL_RECEIPT	Char	255		Nombre de la columna que contiene el recibo criptográfico del documento concluido.
COL_STATUS	Char	255		Nombre de la columna en que se reflejará el estatus de firma.
SGTR_TABLE	Char	255		Nombre de la tabla en donde se registran datos relacionados con las firmas recibidas por el servidor bigned.
SGTR_COL_DOC_ID	Char	255		Nombre de la columna que contiene el identificador del documento a firmar.
SGTR_COL_SERIAL_NUMBER	Char	255		Nombre de la columna que contiene el número de serie de los participantes del documento que envían su firma al servidor bijund.
SGTR_COL_ACCEPTANCE_SIGN ATURE_TIME	Char	255		Nombre de la columna que contiene la fecha y hora en que la firma de aceptación fue enviada por el usuario al servidor bigned.
SGTR_COL_DECLINED_SIGNAT URE_TIME	Char	255		Nombre de la columna que contiene la fecha y hora en que la firma de desacuerdo fue enviada por el usuario al servidor bigned.
SGTR_COL_ACCEPTANCE_SIGN ATURE	Char	255		Nombre de la columna que contiene la firma de aceptación enviada por el usuario al servidor bigned.
SGTR_COL_DECLINED_SIGNAT URE	Char	255		Nombre de la columna que contiene la firma de desacuerdo enviada por el usuario al servidor bigned.
SGTR_COL_DISAGREE	Char	255		Nombre de la columna que contiene el motivo o razón de haber firmado en desacuerdo.