

### Manual del Administrador

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.

Número de Parte: BSIGAdministrador3.10

## Contenido

#### Capítulo 1. ¿Cómo utilizar este manual?

1.1 Simbología y convenciones	1 - 1
1.1.1. Recomendaciones y Advertencias	1 - 1
1.2 Objetivo de este manual	1 - 1
1.3 Nueva Funcionalidad	1 - 1
Capítulo 2. Acuerdos Multilaterales en bigned	
2.1 El funcionamiento de l'Signel	2 - 1
2.2 Requerimientos para usar bSigned	2 - 3
2.3 Conceptos y terminología usados en liqued	2 - 3
2.3.1. Estado de los acuerdos	2 - 3
2.3.2. Archivo Adjunto	2 - 4
2.3.3. Participantes	2 - 4
2.3.4. Grupos	2 - 5
2.3.5. Tipos de firma	2 - 6
2.3.6. Fecha de expiración	2 - 6
2.3.7. Asignación de Participantes por Coordinador de Grupo	2 - 6
2.3.8. Notificaciones	2 - 6
2.3.9. Orden de los participantes	2 - 7
2.3.10. Tipos de acuerdo	2 - 7
Capítulo 3. Sesiones de administración en bSigned	
3.1 La Interfaz de bSigned	3 - 2
3.2 Acceso a la administración de ligned	3 - 2
3.3 Administración del Servidor bigned	3 - 6
-	

3 - 8
3 - 9
3 - 13
3 - 17
3 - 23
3 - 28
3 - 30
3 - 36
3 - 48
3 - 49
3 - 50
3 - 51

#### Capítulo 4. Configuración de Plantillas para bSigned Office Connector

#### 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

Permite elaborar y administrar acuerdos electrónicos eliminando la necesidad de usar pluma y papel, permitiendo recolectar las firmas electrónicas legalmente válidas, de manera segura y automática usando Microsoft® Internet Explorer.

#### 1.3 Nueva Funcionalidad

A continuación se enumeran las nuevas funcionalidades de luqued versión 3.10:

 En el detalle de los acuerdos, se muestra el nombre de la organización a la que pertenecen cada uno de los participantes del acuerdo, deslizando el ratón sobre el nombre del mismo.



- Presenta un mensaje de alerta (15 días antes), que indica que el certificado del usuario está por expirar.
- Se incrementó a 6000 caracteres la longitud de la razón por la cual un participante declina un acuerdo.
- Se agregó un distintivo a los acuerdos que se encuentran en el estado de A Firmar para diferenciarlos de los acuerdos que aun no se han firmado, o que ya se firmaron en desacuerdo.
- Se incluyeron los acuerdos que tienen secuencia de firma, en el estado A Firmar, únicamente para los usuarios que en ese momento estén utilizando bijund y les toque su turno de firmar dicho acuerdo.
- Se modificaron los filtros de fechas, para que no se tome en cuenta la fecha de expiración del acuerdo que el iniciador determinó, sino que ahora los acuerdos que finalizaron su gestión se presenten en los acuerdos Completados.
- bliqued Web funciona también en el navegador FireFox, solo para los usuarios.

#### CAPÍTULO 2

# Acuerdos Multilaterales en

## **bSigned**

En este capítulo se explica de manera general el funcionamiento de blimet, así como los conceptos que se usan en el siguiente capítulo para operar blimet.

Aún cuando la interface de limel es bastante intuitiva, se recomienda leer completo este capítulo para comprender la terminología y facilitar la operación de la aplicación.

En caso de existir alguna duda, le recomendamos acudir al personal de soporte técnico o al administrador bisiquel.

## 2.1 El funcionamiento de bijned

Esimel es una herramienta que facilita el proceso de recabar firmas electrónicas multilateralmente, con validez legal para cualquier tipo de documento o acuerdo electrónico confidencial, como puede ser un contrato, una solicitud de crédito, información sensible, registros médicos o financieros, etc.

La infraestructura de liquel facilita la administración y manejo de los documentos de manera segura y confiable.



Actordo

onitre
insperity big
insperity
in

La forma en que opera bligned se esquematiza en la Figura 2.1.

Figura 2.1 Funcionamiento de bigned

El iniciador (Participante 1) ingresa a simel por medio de Microsoft® Internet Explorer, autenticándose por medio de su certificado ante el servidor simel y crea el acuerdo, indicando el archivo adjunto que se firmará, los participantes, la fecha de expiración e inicia la gestión del acuerdo.

El servidor lumacena el acuerdo en la base de datos y comienza a enviar las notificaciones por medio de correo electrónico a los participantes requeridos.

Los participantes ingresan a liqued utilizando Microsoft® Internet Explorer. Se autentican los participantes por medio de su certificado. El servidor valida en cada operación, que el certificado del usuario sea válido (vigente y no revocado), y que sean emitidos por una Autoridad Certificadora reconocida o dada de alta en liqued. El servidor liqued se conecta a un servidor OCSP solicitando al servidor TSP una estampilla de tiempo que indica el momento en que cada evento sucedió. Estos registros forman parte de la evidencia que recopila liqued.

Al terminar de firmar los *n* participantes, el servidor signel envía un correo electrónico a todos ellos para notificar que el acuerdo concluyó su gestión.

Finalmente, simul recopila todos los eventos relacionados con el acuerdo y arma un paquete descargable por cualquiera de los participantes, facilitando las labores de auditoría.

Para el usuario final de luquel, esta mecánica se limita a realizar los siguientes pasos:

- El iniciador configura el nuevo acuerdo a través de su navegador e indica a signel que comience a gestionarlo
- 2. Espera a que todos los participantes firmen el acuerdo
- 3. Recibe la notificación del servidor biquel, de que todas las firmas fueron recabadas y puede proceder a descargar su copia del documento con todas las firmas electrónicas

Las variantes que pudieran existir para los casos en que los participantes no firmen o que declinen el contenido del acuerdo se pueden monitorear con gran facilidad, dado que sime cuenta con una interface sencilla y se opera de la misma forma en que se navega en sitios Web.

## 2.2 Requerimientos para usar Signed

Para que un usuario pueda acceder a limed deberá de contar con los siguientes elementos:

- Un equipo que tenga instalado Microsoft® Internet Explorer Versión 5.5 o superior
- Acceso a Internet, red local o a la Intranet desde donde sea accesible el servidor l\( \) internet.
- La URL para acceder a bigned
- Un certificado digital X.509 con su llave privada, instalados en el repositorio de certificados de Microsoft® Internet Explorer. Para mayor información sobre cómo cargar su certificado en el repositorio, deberá consultar la ayuda en línea del navegador
- Ser dado de alta por el administrador de bundo o bien ser incluido en un acuerdo por un usuario que ya esté registrado previamente en el servidor

## 2.3 Conceptos y terminología usados en bimed

Los documentos manejados por líquel se denominan *acuerdos*, identificados en la interface de líquel como PAM (procesos de Acuerdos Multilaterales). Un acuerdo es un documento electrónico formado por:

- un archivo adjunto acerca del cual cada uno de los participantes firmará electrónicamente
- un grupo de participantes que serán requeridos para firmar el acuerdo
- un grupo de parámetros que definen la forma en que se deberá gestionar el documento

#### 2.3.1 Estado de los acuerdos

Cuando los acuerdos creados inician su gestión, se dice que están en *ejecución*. Mientras esté en ejecución, podrán aceptarse firmas para el acuerdo.



Los acuerdos pueden encontrarse en distintos estados y bijmel los mantendrá agrupados para facilitar su administración. Los estados posibles se describen en la Tabla 2.1.

Tabla 2.1 Estados de un acuerdo

En la categoría	se encuentran los acuerdos que
En Edición	aún no inician su ejecución por no tener todas sus partes configuradas o bien no se desea que comiencen a ejecutarse
En Proceso	son los acuerdos que se encuentran en ejecución en espera de firmas de otros usuarios
A Firmar	son los acuerdos que se encuentran en ejecución en espera de la firma del usuario actual de hisimal y posiblemente de otros usuarios
Completados	son los acuerdos que terminaron su ejecución y recibieron todas las firmas necesarias antes de la fecha de expiración
No Ejecutados	son los acuerdos que alcanzaron la fecha de expiración sin recabar todas las firmas necesarias
Declinados	son los acuerdos no ejecutados en donde la firma del usuario actual de logned, no se recabó o no se aplicó.

Para definir las condiciones en que un acuerdo termina su ejecución, se deberá indicar tanto el tipo de documento (Ver "2.3.10 Tipos de acuerdo" en la página 2-7), como la fecha de expiración del acuerdo (Ver "2.3.6 Fecha de expiración" en la página 2-6).

#### 2.3.2 Archivo Adjunto

Un archivo adjunto es el motivo de la solicitud de firma del acuerdo.

El archivo adjunto puede ser de cualquier tipo. Por ejemplo, puede tratarse de un documento de Microsoft® Word, un libro de trabajo de Microsoft® Excel, un diseño de AutoCAD<sup>TM</sup> o bien un documento en formato PDF.

El archivo adjunto será almacenado de forma segura en la base de datos de lisimel a través del servidor lisimel.

Los participantes tendrán la posibilidad de consultar su situación en todo momento y examinarlo cuando sea requerida su firma. En todo momento, signidad asegurará su integridad y confidencialidad.

#### 2.3.3 Participantes

Los participantes serán los individuos o representantes de una organización, que firmarán el acuerdo, indicando su aceptación o rechazo sobre el archivo adjunto.

Cuando se crea un nuevo acuerdo, se seleccionarán los participantes y tendrán una función de *Firmante*, misma que se puede modificar según convenga.

El usuario que crea un nuevo acuerdo se denomina iniciador.

Al asignar una función a cada participante, facilita la organización del proceso de recolección de firmas, adaptándose a los flujos preestablecidos en una organización.

Las funciones que pueden tener los participantes se indican en la Tabla 2.2.

Tabla 2.2 Funciones de los participantes

Función	Puede firmar	Descripción
Revisor	Si	Son testigos y destinatarios que podrán firmar el acuerdo de aceptación o desacuerdo.
Firmante	Si	Participante que puede firmar el acuerdo de aceptación o desacuerdo.
Testigo	Si	Participante que puede firmar el acuerdo de aceptación o desacuerdo
Destinatario	No	Participante que recibe una notificación de que el documento ejecutado está disponible al terminar de recabarse las firmas.
Lector	No	Los lectores son participantes que solo pueden ver la gestión del acuerdo, pero no pueden firmar.
		Importante Un usuario pierde la función de lector, cuando
		deja de pertenecer al grupo, y obtienen la función de lector los nuevos integrantes.

#### 2.3.4 Grupos

En blimed existen tres tipos de grupos de participantes:

- Grupos Personalizados: Estos grupos son creados por el iniciador del acuerdo. Cualquier usuario que tenga el atributo de Iniciador, podrá crear sus propios grupos personalizados. Estos grupos se crean con la finalidad de agilizar la inclusión de varios participantes a un acuerdo en solo paso.
- Grupos Predefinidos. Estos grupos son creados exclusivamente por el administrador del sistema, y su propósito es poder delegar la responsabilidad de la asignación de participantes de un PAM a los coordinadores del grupo predefinido, que son especificados por el administrador al momento de agregar miembros al grupo durante la configuración del PAM, y es así como el iniciador delega la responsabilidad de la asignación de participantes a los coordinadores de cada grupo predefinido incluido. Se selecciona el número de usuarios de un grupo predefinido y la función que ejercerán cada uno de ellos. El coordinador deberá elegir a cada participante requerido.
- Grupos de Lectores. Estos grupos los define el administrador, teniendo como única función consultar el acuerdo donde fueron incluidos. Estos grupos NO son creados por el administrador, son los mismos grupos predefinidos, pero dados de alta como grupos



de lectores. Estos grupos toman sentido cuando hay alta rotación de personal y el acceso a los participantes es de alcance grupal o por área.

#### 2.3.5 Tipos de firma

Cuando un participante procede a firmar un acuerdo, ya sea ingresando al sitio de limito o bien usando la referencia que se envía en la notificación de solicitud de firma, tiene las siguientes alternativas:

- Firmar aceptando el documento
   En este caso el participante registra su firma y se incorpora al acuerdo. Esta situación no es reversible.
- Firmar su desacuerdo con el documento adjunto
   Cuando un usuario firma un desacuerdo, tiene la posibilidad de que se registre su firma junto con un texto explicando la razón del mismo.
   En caso de cambiar de opinión, puede ingresar nuevamente a biquel y firmar la aceptación del documento mientras el documento no haya expirado.
- No firmar y firmar posteriormente

#### 2.3.6 Fecha de expiración

La fecha de expiración marca el límite de espera del servidor bijned, para recibir firmas de los participantes.

La fecha de expiración considera mes, día y hora.

#### 2.3.7 Asignación de Participantes por Coordinador de Grupo

La función de coordinador la asigna el Administrador de lime, con el propósito de que cuando se crea un acuerdo y se integran *n* numero de participantes de un grupo predefinido para la firma del mismo, el coordinador es quien asigna a los participantes de su grupo que se requieren.

#### 2.3.8 Notificaciones

Cuando un usuario es requerido para firmar el documento, se le envía un correo electrónico a la dirección que indica su certificado de usuario signed, o bien a la cuenta de correo configurado por el administrador para el usuario en específico, un mensaje que hace referencia al acuerdo que está en ejecución y una liga que lo lleva directamente al inicio del proceso de firma dentro de liqued.

Si el usuario no firma el documento, el servidor buel enviará recordatorios como seguimiento a las firmas faltantes. El número de notificaciones que recibe el participante es configurable al momento de crear el acuerdo.

#### 2.3.9 Orden de los participantes

Una vez que se han definido los participantes de un acuerdo, es posible establecer un orden particular para recabar las firmas, permitiendo apegarse a procedimientos particulares de una organización.

El orden de los participantes solamente se puede establecer en los acuerdos de tipo Obligatorio (Ver "2.3.10 Tipos de acuerdo" en la página 2-7).

#### 2.3.10 Tipos de acuerdo

Los tipos de acuerdo impactan tanto la forma en que se ejecuta un documento, como el momento en que termina su ejecución.

Dependiendo del tipo de acuerdo, signed ajustará la manera en que dará seguimiento al acuerdo y tomará las acciones necesarias para aplicar los criterios establecidos por el usuario para cada caso.

El tipo de acuerdo se indica estableciendo el requerimiento de firma y los valores posibles se explican en la Tabla 2.3.

Tabla 2.3 Tipos de requerimiento de firma

El requerimiento de firma	consiste en	y la ejecución termina cuando
Obligatorio	recabar las firmas de todos los participantes	se recabaron las firmas de todos los participantes o bien cuando se cumple a la fecha de expiración del acuerdo
Adhesión	recabar la mayor cantidad de firmas	se cumple la fecha de expiración
Adhesión limitada	recabar al menos <i>n</i> firmas de una lista de <i>m</i> participantes (nbm)	se cumple la fecha de expiración o cuando ha transcurrido un tiempo predeterminado, después de que se han recabado <i>n</i> firmas (sin que se haya cumplido la fecha de expiración)

#### CAPÍTULO 3

# Sesiones de administración en bigned

Para acceder a Signal, deberá ejecutar Microsoft® Internet Explorer e introducir el URL desde el cual se accede a la aplicación.



#### Importante

Asegúrese de que su certificado esté instalado antes de iniciar su sesión de Mignel.



#### Precaución

Antes de entrar al sitio de simil, asegúrese que en las preferencias de Microsoft® Internet Explorer para el manejo del caché, se encuentre en actualización automática para evitar que se despliegue información no actualizada durante su sesión.

Este parámetro se puede ajustar desde el Panel de Control, en Internet Options o bien abriendo Microsoft® Internet Explorer y desde el menú:

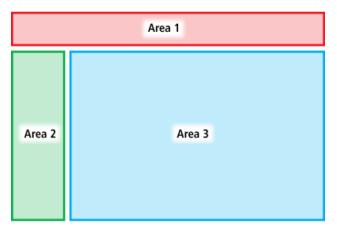
Tools @ Internet Options

Se desplegará el panel y deberá hacer clic en el botón Settings... de la sección Temporary Internet Files bajo la pestaña General. En el cuadro de diálogo que aparece, seleccione Automatically seguido de un clic en OK. Finalmente, cierre el panel haciendo clic en el botón OK.

En la página principal, encontrará la bienvenida al sitio de liquel, con una breve explicación acerca de liquel. Para comenzar a interactuar con la aplicación deberá hacer clic en el botón Entrar.

3.1 La Interfaz de bigned

En la siguiente página, verá el ambiente de trabajo de ligned. La interfaz de ligned está organizada en tres áreas, mismas que siempre estarán presentes:



- Area 1. En ella se mostrará la identificación del usuario que esté usando limed en ese momento. Es particularmente importante cuando varios usuarios acceden a limed usando el mismo equipo.
- Area 2. Contendrá siempre el menú de operación de blimel. Las operaciones disponibles se desplegarán siempre en esta área.
- Area 3. Es el área de trabajo en donde el administrador realizará la configuración y administración del servidor blimet.



#### **Importante**

La imagen de lo puede personalizarse de acuerdo a colores institucionales de la organización que lo utilice o bien colocar un logotipo personalizado en el extremo derecho del Area 1.

Consulte al soporte técnico de Seguillata para mayor información sobre la personalización de la interfaz de lisigned.

3.2 Acceso a la administración de bSigned

Al entrar a la página principal, en el área del menú se encuentran la opción Usar bSigned, que permite ingresar al área segura de la aplicación, así como las operaciones relacionadas con los certificados que respaldan la identidad de los usuarios, éstas son Requerimiento de Certificación, Instalar Certificado y Renovar Certificado.

Para ingresar a la aplicación haga clic en la liga Usar bSigned del menú. (Figura 3.1).



Figura 3.1 Menú



A continuación se desplegará una ventana en la que deberá seleccionar el certificado que se va a utilizar. (Figura 3.2).

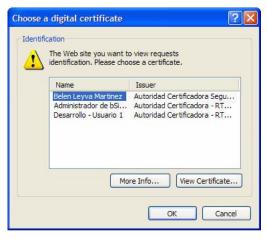


Figura 3.2 Selección del Certificado

Seleccione el certificado correspondiente y haga clic en el botón OK.

Recuerde que el certificado que seleccione deberá tener permisos de Administrador.



Recuerde que el certificado que use, es lo que lo identificará ante bimel y el uso que se haga bajo este certificado será imputable al propietario del certificado.

A continuación aparecerá otra ventana confirmando que el certificado que se usará es el mismo que seleccionó, y en caso de ser correcto deberá de hacer clic en OK.

Si el certificado se generó con un nivel de alta seguridad, en esa misma ventana se solicitará la clave de uso del certificado y deberá proporcionarla antes de hacer clic en el botón OK. (Figura 3.3).



Figura 3.3 Clave de Acceso para Utilizar el Certificado

Una vez que haya ingresado a signet todas las operaciones que realice se gestionarán desde el navegador como transacciones seguras y bajo la identidad del certificado actual.



En tanto no cierre la sesión de limel, su certificado estará en uso. Asegúrese de hacer clic en la opción Cerrar Sesión del menú, para garantizar que se cierre su sesión cuando haya terminado de utilizar limel.

#### Precaución

Si algún otro usuario requiere acceder a liqued en el mismo equipo después de que usted lo ha hecho, se recomienda cerrar todas las otras sesiones de Microsoft® Internet Explorer, independientemente del contenido de las otras páginas antes de que otro usuario ingrese a la aplicación.



## 3.3 Administración del Servidor bigned

Una vez que se encuentre en el menú de blimel, el administrador tendrá acceso a la opción que permite configurar los parámetros principales del servidor blimel. Para accesar a esta funcionalidad haga clic en la opción Administración del Servidor. (Figura 3.4).



Figura 3.4 Menú de Administración



Si la liga Adm. del Servidor no aparece en el menú de lignel, deberá de habilitar su certificado que contenga permisos de administrador.

Al ingresar al área de administración, en el menú habrá tres opciones:

Iniciar/Detener Servicio

Permite iniciar o detener el servicio de ligned. La liga cambiará automáticamente según el estado del servicio.

Para cambiar el estado del servicio bastará con hacer clic en la liga y esperar un momento para que se muestre el estado del servidor bijmel.

Configurar Servidor

Despliega el menú que permite configurar al servidor blimed.

· Licencia del Servidor

Permite conocer el estado de la licencia de uso de ligned, así como activar una nueva licencia.

Esta opciones se muestran en la Figura 3.5.



Figura 3.5 Opciones de Administración

#### 0

#### **Importante**

Cuando se requiera dar mantenimiento a limel o modificar la configuración, deberá de detenerse el servicio antes de realizar cualquier modificación. De manera similar, después de realizar las modificaciones deberá de iniciarse nuevamente el servicio.



#### 3.4 Configurar Servidor

La configuración del servidor considera todos los parámetros que requiere bijent para gestionar acuerdos.

Al hacer clic en la liga Configurar Servidor del menú, se mostrarán las opciones de configuración disponibles:

- Parámetros de Operación
- AC(s)
- Certificados de Usuarios
- Respondedor TSP
- Administración de Grupos
- Administración de Rutas Predefinidas

#### 3.4.1 Parámetros de Operación

Al hacer clic en esta liga, en el área de trabajo se desplegarán todos los parámetros que usa signed para gestionar los acuerdos como se muestra en la Figura 3.6.

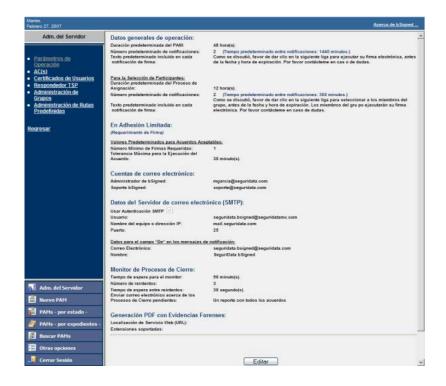


Figura 3.6 Parámetros de Operación

Para modificarlos deberá hacer clic en el botón Editar.



A continuación se presenta una ventana que permite editar los parámetros de operación, como se muestra en la Figura 3.7.

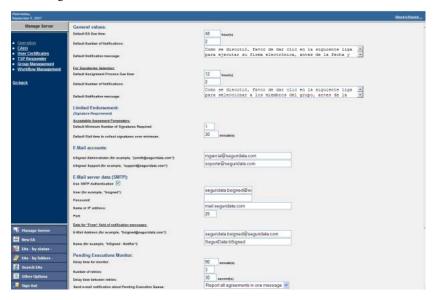


Figura 3.7 Edición de los Parámetros de Operación



#### Importante

Los datos de las secciones Cuentas de correo electrónico y Datos del Servidor de correo electrónico, corresponden a la información proporcionada en el Wizard de instalación de los servicios. Demás secciones, son datos predefinidos por el sistema. La sección Generación PDF con evidencias forences, estará en blanco.

En la Tabla 3.1 se explican los parámetros predefinidos para la creación de PAMs y Rutas.

Tabla 3.1 Parámetros de Operación

El parámetro	es
Datos generales de operación	
Duración predeterminada del PAM	el tiempo en que deberán. recabarse las firmas requeridas para la ejecución del acuerdo
Número predeterminado de notificaciones	el número de notificaciones a enviar a los participantes que deberán firmar el documento.

Tabla 3.1 Parámetros de Operación (Continuación)

El parámetro	es
Texto predeterminado incluido en cada notificación de firma	el texto predeterminado para las notificaciones de firma.
Para la Selección de Participantes	
Duración predeterminada del proceso de Asignación	el tiempo en que los coordinadores deberán asignar a los miembros de los grupos predefinidos como participantes de un PAM.
Número predeterminado de Notificaciones	número de notificaciones a enviar a los coordinadores de grupos predefinidos, que deberán asignar participantes a un PAM.
Texto predeterminado incluido en cada notificación de firma	Mensaje predeterminado para las notificaciones de asignación que aparecerán al agregar un grupo predefinido a un acuerdo nuevo.
En Adhesión Limitada	
Número Mínimo de Firmas Requeridas	el número mínimo de firmas requeridas para la ejecución de un acuerdo. Aparecerá al elegir como tipo de requerimiento de firma: Adhesión Limitada.
Tolerancia Máxima para la Ejecución del Acuerdo	el tiempo de espera para recabar una mayor cantidad de firmas, y ejecutar un acuerdo una vez recolectado el número mínimo de firmas requeridas. Aparecerá al elegir como tipo de requerimiento de firma Adhesión Limitada.
Cuentas de correo electrónico	
Administrador de bSigned	la dirección de correo electrónico del administrador de lSigned.
Soporte bSigned	la dirección de correo electrónico del encargado de soporte técnico.
Datos del Servidor de correo electrónico	
Usar Autenticación SMTP	marque la casilla si el servidor de correo electrónico que se usará para enviar las notificaciones de firma de asignación y mensajes, requiere autenticación de usuario.
Usuario	el usuario que se usa para establecer la conexión con el servidor de correo electrónico.
Contraseña	la contraseña asociada al usuario (campo anterior).
Nombre del equipo o dirección IP	el nombre o dirección IP del equipo en donde se encuentra instalado el servidor de correo electrónico.
Puerto	el puerto asociado a la dirección del equipo (campo anterior).
Monitor de Procesos de Cierre	



Tabla 3.1 Parámetros de Operación (Continuación)

El parámetro	es
Tiempo de espera para el monitor	la duración de las pausas que hace el servicio que monitorea el tiempo que debe transcurrir antes de verificar si hay PAMs con proceso de cierre pendiente.
Número de reintentos	el número de intentos que hace el Servidor lumel para ejecutar el proceso de cierre por cada PAM.
Tiempo de espera entre reintentos	el tiempo de espera entre cada intento (campo anterior).
Enviar correo electrónico acerca de los Procesos de Cierre pendientes	la forma de notificar al Administrador acerca de los PAMs con proceso de cierre pendiente.
Generación PDF con Evidencias Forences	
	Las opciones Localización del Servicio Web (URL) y Extensiones Soportadas deberán configurarse sólo si se ha adquirido el módulo de generación de la versión imprimible de los PAMs, hacer lo contrario provocará que los PAMs no concluyan su ejecución satisfactoriamente.
Localización del Servicio Web (URL)	escriba la dirección URL del Web Service de ligned.
Extensiones Soportadas	son los tipos de documentos de los cuales se generará su versión imprimible.
	Los tipos de documentos o extensiones soportadas por logand son: documentos de Office (*.doc, *.xls, *.ppt), archivos de texto (*.txt) y PDFs.

Al terminar de actualizar los parámetros de operación, deberá hacer clic en el botón Actualizar.

Si desea re-establecer todos los parámetros desechando los anteriores, puede hacer clic en el botón Limpiar.

#### $3.4.2 \, AC(s)$

Al hacer clic en esta liga, en el área de trabajo se desplegarán todas las autoridades certificadoras reconocidas. Esto significa que solamente aquellos certificados que provengan de alguna de las autoridades certificadoras de esta lista, podrán acceder a liguel y ser utilizados como participantes de acuerdos. (Figura 3.8).

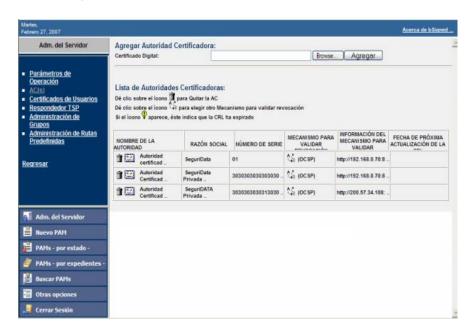


Figura 3.8 Administración de las Autoridades Certificadoras

Es posible agregar nuevas autoridades haciendo clic en el botón Browse... para localizar el certificado de una autoridad que se desee agregar, seguido de un clic en el botón Agregar.

También es posible eliminar una autoridad certificadora haciendo clic en el ícono del bote de basura a la izquierda del renglón.



No se podrá eliminar una Autoridad Certificadora cuando se haya utilizado un certificado en algún acuerdo, que haya sido emitido por ésta.



Para configurar el mecanismo para validar el estado de revocación de los usuarios emitidos por determinada autoridad, haga clic en la columna MECANISMO PARA VALIDAR REVOCACION del usuario correspondiente.

A continuación se presentará la siguiente ventana. (Figura 3.9).

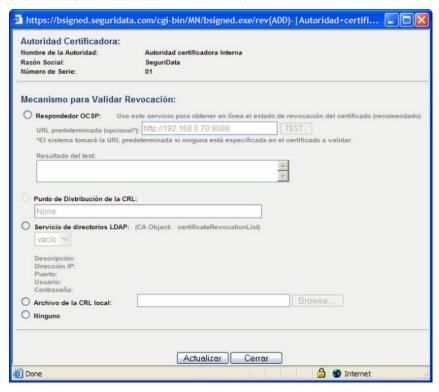


Figura 3.9 Mecanismo para Validar Revocación

A continuación se describen cada uno de los mecanismos disponibles, como se muestra en la Tabla 3.2.

Tabla 3.2 Mecanismos de Verificación de Revocación

Mecanismo	Descripción
Respondedor OCSP	Este mecanismo es recomendado para obtener el línea el estado de revocación de certificados. Marque esta opción e indique la URL y puerto de este servicio en el campo URL predeterminada (opcional). Si desea haga clic en el botón TEST para verificar la conexión, el resultado de la verificación se presentará en el campo Resultado del test.
Punto de Distribución de la CRL	Si desea utilizar una CRL para verificar la revocación de certificados, marque esta opción e indique la URL donde se encuentra la CRL.
Servicios de directorios LDAP	Si hand cuenta con este tipo de servicios, marque esta opción y seleccione del combo, el servicio LDAP disponible.
Archivo de la CRL local	Marque esta opción si en su equipo cuenta con una CRL. Haga clic en el botón Browse y localice la lista correspondiente.
Ninguno	Si no cuenta, o no desea utilizar ningún servicio de verificación de revocación, marque esta opción.

Haga clic en el botón Actualizar.



Para ver el detalle del certificado de una autoridad, haga doble clic en el icono de la critificadora correspondiente, que presenta la siguiente ventana. (Figura 3.10).

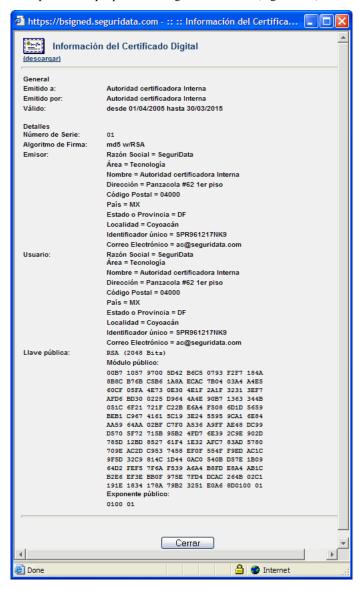


Figura 3.10 Detalle de un Certificado

#### 3.4.3 Certificados de Usuarios

Al hacer clic en esta liga, en el área de trabajo se desplegarán todos los certificados registrados en bliqued. (Figura 3.11).



Figura 3.11 Administración de Certificados de Usuarios



La página anterior permite consultar el estado y detalle de un certificado de un usuario, haciendo clic en el icono . (Válido, Expirado, Revocado o Revocado y Expirado). (Figura 3.12).

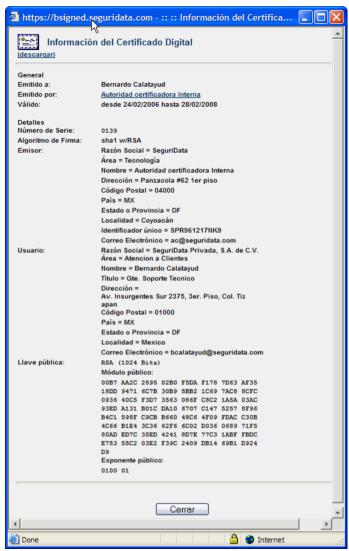


Figura 3.12 Detalle del Certificado de un Usuario

También se pueden agregar nuevos usuarios haciendo clic en el botón Browse... para localizar el certificado de un usuario que se desee agregar, seguido de un clic en el botón Agregar.

Además permite asignar atributos especiales a los usuarios modificando los indicadores de la última columna del lado derecho, (Ninguno, Administrador o Auditor).



#### **Importante**

Para asignar el atributo de Iniciador de PAMs a un usuario, deberá marcar la opción Inic. del usuario correspondiente, como se muestra en la Figura 3.13.



Figura 3.13 Atributo de Iniciador

En el caso de que desee eliminar un certificado de un usuario, deberá tener en cuenta el estado de éste, como se explica en la Tabla 3.3.

Tabla 3.3 Descripción de los Iconos

Icono	Descripción
<b>⊗</b>	Certificado de un usuario que pertenece a un grupo y/o ruta. Si desea eliminar al usuario, el creador del grupo y/o ruta tendrá que darlo de baja para poder eliminarlo.
	Certificado que si es posible eliminar.
iii	



Para consultar el listado de grupos y/o rutas donde un usuario está incluido, haga clic en el icono del usuario correspondiente, que presenta la siguiente ventana. (Figura 3.14).

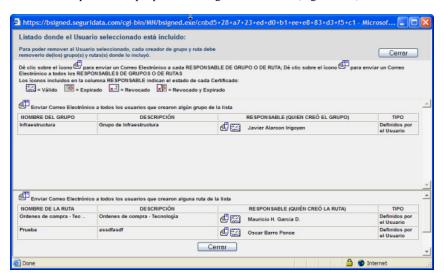


Figura 3.14 Listado donde el Usuario seleccionado está incluido

Si desea enviar un correo electrónico al responsable quien creó el Grupo o Ruta, haga clic en el icono del responsable correspondiente.

Para cambiar el certificado o correo electrónico de un usuario, haga clic sobre el nombre de éste para que se presente la siguiente ventana. (Figura 3.15).

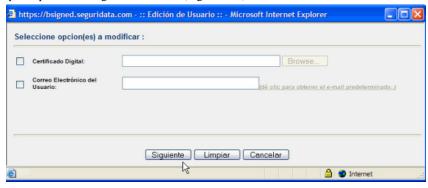
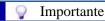


Figura 3.15 Opciones a Modificar

Para cambiar el certificado digital, marque la opción Certificado Digital y haga clic en el botón Browse... para localizar el nuevo certificado.

Para cambiar el correo electrónico, marque la opción Correo Electrónico del Usuario e indique el nuevo correo.



El nuevo correo electrónico asignado al usuario, es el que utilizará para recibir las notificaciones del servidor bijned.

Para continuar haga clic en el botón Siguiente.



A continuación se presentará la siguiente ventana para firmar los cambios del usuario. (Figura 3.16).

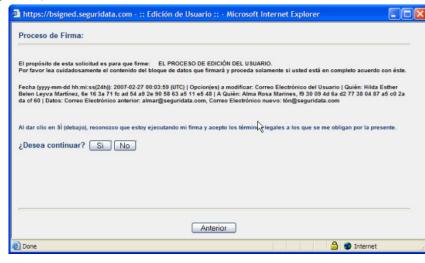


Figura 3.16 Proceso de Firma

Si desea continuar haga clic en el botón Si para que se presente el siguiente mensaje. (Figura 3.17).

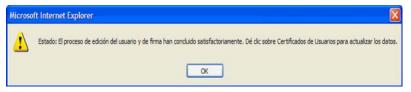


Figura 3.17 Mensaje

#### 3.4.4 Uso de certificados de autenticación y certificado de firma.

Un certificado de autenticación es aquel que se configura únicamente para autenticar al usuario en el acceso a blimet, y un certificado de firma es el que se configura para firmar acuerdos en blimet. (Figura 3.18)

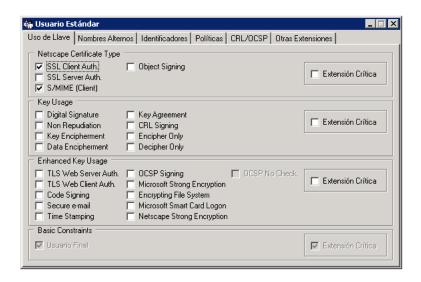


Figura 3.18 Certificado de Autenticación.



En la pestaña de Politicas se debe de seleccionar la casilla Incluir CPS (Figura 3.19) .

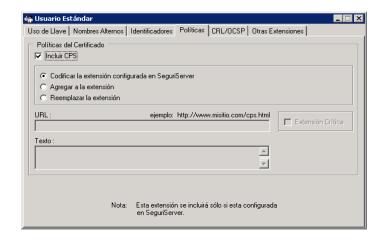


Figura 3.19 Políticas.

En la pestaña CRL/OCSP se debe de seleccionar las casillas Incluir CDP y la casilla Incluir AIA. (Figura 3.20)

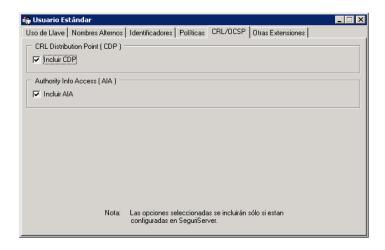


Figura 3.20 Pestaña CRL/OCSP.



Es importante recalcar que debe existir el par de certificados para poder operar bligned.

Debe cuidarse que el identificador del requerimiento llamado CURP coincida en ambos certificados, normalmente el dato que se asigna a este campo es el identificador de la máquina del usuario, aunque puede ser cualquier otro dato. Además los datos del subject de los certificados deben ser idénticos. (Figura 3.21)

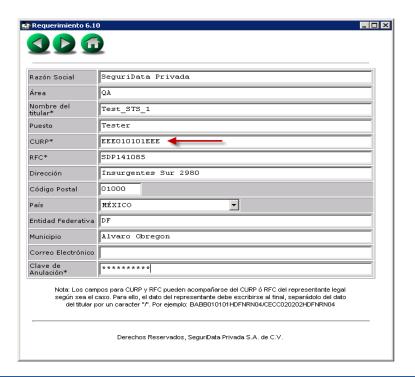


Figura 3.21 Requerimientos de los Certificados.



El certificado de firma debe ser agregado a la base de datos de blima, es decir, agregarlo en esta sección de certificados de usuarios y registrarlo en la máquina. El certificado de autenticación únicamente debe ser registrado en la máquina. (Figura 3.22)

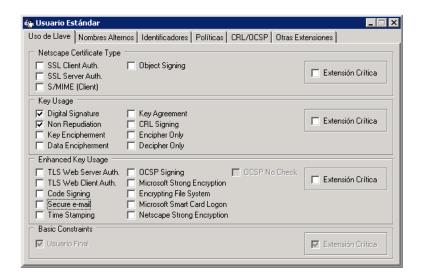


Figura 3.22 Certificado Firma.

Uso de Llave Nombres Alternos Identificadores Políticas CRL/DCSP Otras Extensiones

Políticas del Certificado
Incluir CPS

C Codificar la extensión configurada en SeguriServer
Agregar a la extensión
Reemplazar la extensión

URL: ejemplo: http://www.misitio.com/cps.html

Texto:

Nota: Esta extensión se incluirá sólo si esta configurada en SeguriServer.

En la pestaña de Politicas se debe de seleccionar la casilla Incluir CPS (Figura 3.23) .

Figura 3.23 Pestaña Políticas.

En la pesta $\tilde{n}$ a CRL/OCSP se debe de seleccionar las casillas Incluir CDP y la casilla Incluir AIA. (Figura 3.24) .

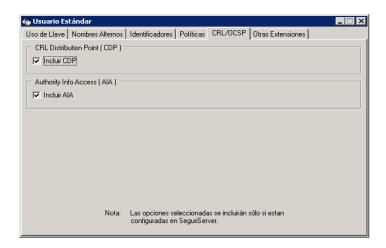


Figura 3.24 Pestaña CRL/OCSP.



# 3.4.5 Respondedor TSP

Al hacer clic en esta liga, en el área de trabajo se desplegarán los datos del servidor de TSP, que emite estampillas de tiempo para bijmel. Para modificarlo, deberá hacer clic en el botón Editar, como se muestra en la Figura 3.25.

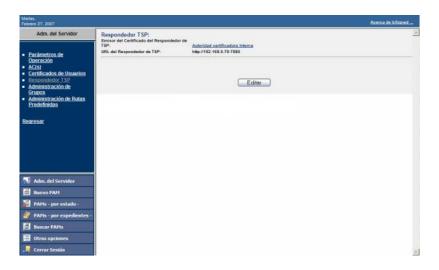


Figura 3.25 Respondedor TSP

Marine 27, 2007

Adm. del Servidor

Parámetros de Operación

Administrosón de Usuarios
Parámetrosón de Ratas
Prodefinidas

Resputado del test

Resputado del test

TEST...

Resputado del test

TEST...

Adm. del Servidor

Muevo PAH

PAHs - por estado 
PAHS - po

A continuación se presentará una ventana para configurar el Respondedor TSP. (Figura 3.26).

Figura 3.26 Configuración del Respondedor TSP

En el área de trabajo aparecerán dos campos en los que se debe proporcionar el certificado de la Autoridad Certificadora en la que se confía para emitir el certificado del servidor de TSP. En el otro campo proporcione la URL en la cual se atienden las peticiones, en el formato http://dirección IP:Puerto.

Una vez especificados los campos anteriores, haga clic en el botón TEST para verificar que los datos sean correctos antes de actualizarlos en limed.

Si todo es correcto, proporcione nuevamente el certificado de la Autoridad Certificadora y haga clic en el botón Actualizar.



#### **Importante**

El certificado del Respondedor TSP deberá ser emitido por alguna de las Autoridades Certificadoras registradas en bsignet.



#### 3.4.6 Administración de Grupos

Esta opción permite al administrador crear grupos predefinidos que son de alcance organizacional. Podrán ser incluidos como grupos predefinidos o grupos de lectores durante la creación de PAMs o Rutas, los cuales se quedan registrados en el sistema, y el iniciador de un PAM pueda seleccionar estos grupos para la firma de un acuerdo.

En la siguiente ventana el Administrador puede crear los grupos predefinidos, permitiendo asignar a los usuarios la función de Coordinador. (Figura 3.27).



Figura 3.27 Administración de Grupos

Para crear un grupo haga clic en el botón Agregar Grupo.

En esta ventana puede crear el nuevo grupo, proporcionando el Nombre del Grupo y una breve Descripción del grupo. (Figura 3.28).

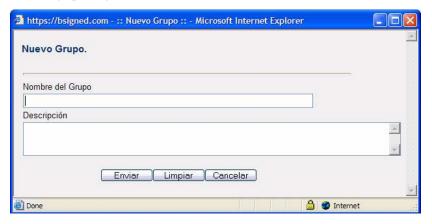


Figura 3.28 Creación del nuevo grupo



No necesariamente los miembros de un grupo deben pertenecer a la misma área.

Haga clic en el botón Enviar para crear el nuevo grupo.



Posteriormente se presentará en el área de trabajo el nombre del grupo creado y su descripción. (Figura 3.29).



Figura 3.29 Grupo Creado

Para agregar los miembros correspondientes al grupo creado, haga clic en el botón Agregar Miembro.

En esta ventana deberá indicar los criterios de búsqueda para localizar a los usuarios que se agregarán como miembros o integrantes del grupo. (Figura 3.30).

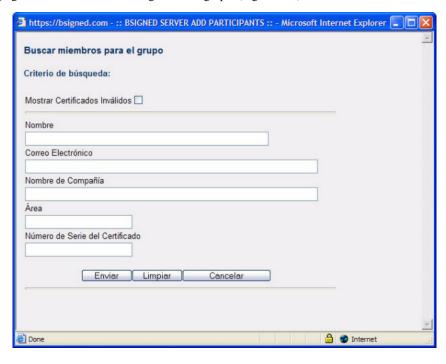


Figura 3.30 Criterios de Búsqueda

La ventana se divide en las siguientes secciones:

#### Mostrar Certificados Inválidos

Esta opción funciona conjuntamente con las siguientes secciones, extendiendo la búsqueda a usuarios con certificados vencidos o revocados. Para activarla haga marque la casilla Mostrar Certificados Inválidos.



#### Criterios de búsqueda

En esta sección podrá llenar los campos que le sean útiles para localizar a los usuarios que le interesan, seguido de un clic en el botón Enviar.

Si antes de enviar la búsqueda desea borrar todos los campos para definir otro criterio podrá usar el botón Limpiar.

Las búsquedas se pueden realizar tantas veces como se desee, hasta localizar a todos los usuarios requeridos para el grupo predefinido. Al llenar los criterios de búsqueda podrá escribir solamente parte del texto que busca.

Haga clic en el botón Enviar.

El resultado de la búsqueda será una lista con los usuarios correspondientes como se muestra en la Figura 3.31.

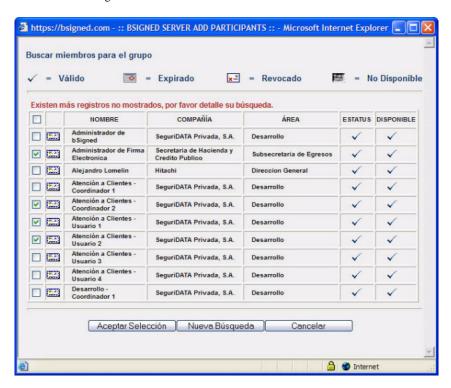


Figura 3.31 Lista de Miembros

Marque la(s) casilla(s) que se encuentra del lado izquierdo del renglón para seleccionar a los miembros para el grupo.

Haga clic en el botón Aceptar Selección.

Si en esta lista no se encuentran los usuarios que le interesan, podrá repetir la búsqueda haciendo clic en el botón Nueva Búsqueda.

En el área de trabajo se mostrarán los miembros del grupo que se integraron, y podrá marcar la casilla (COORD) de la última columna, para asignar al usuario la función de Coordinador. (Figura 3.32).



Figura 3.32 Miembros del Nuevo Grupo



# Importante

Para regresar al menú anterior haga clic en la liga Regresar. La función de Coordinador se basa en asignar quiénes de los miembros de un grupo podrán firmar el acuerdo.



#### 3.4.7 Administración de Rutas Predefinidas

Esta opción permite pre-configurar los parámetros necesarios de un PAM, para agilizar su configuración y por lo tanto su gestión. (Figura 3.33).

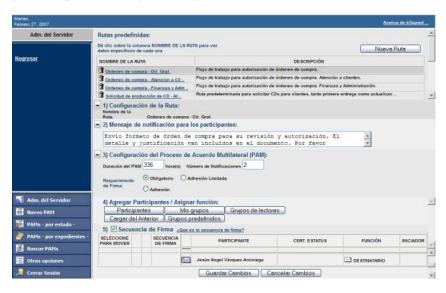


Figura 3.33 Rutas Predefinidas

A Internet

Nueva Ruta.

Nombre de la Ruta

Pago de Vacaciones

Descripción

Pago de mis vacaciones del mes de Julio del 2002

Para crear una ruta, seleccione el botón Nueva Ruta que presenta la siguiente ventana. (Figura 3.34).

Figura 3.34 Creación de una Nueva Ruta

Proporcione el Nombre de la nueva ruta y una breve Descripción de la misma.

Haga clic en el botón Enviar, para crear la ruta.



Posteriormente se presentará en el área de trabajo el nombre de la ruta creada y su descripción. (Figura 3.35).

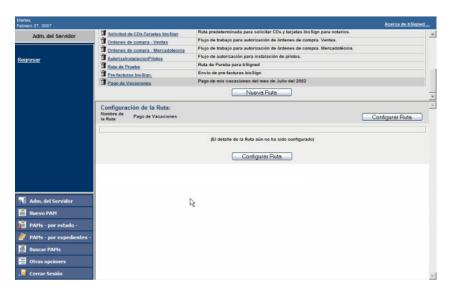


Figura 3.35 Ruta Creada

Como siguiente paso será Configurar la Ruta.

Para la configuración de la ruta, haga clic en el botón Configurar Ruta, que presenta la siguiente ventana. (Figura 3.36).



Figura 3.36 Configuración de la Nueva Ruta



#### Importante

En el paso uno, dos y tres de la configuración, se presenta un ícono que permite expander la sección, o contraer la misma .

Configure los siguientes parámetros.

1. Configuración de la Ruta. (Figura 3.37).



Figura 3.37 Configuración de la Ruta

Esta parte, sólo presenta el nombre de la Ruta a configurar.



2. Mensaje de notificación para los participantes.(Figura 3.38).



Figura 3.38 Configuración del Mensaje de Notificación

Presenta el mensaje predefinido en la administración del servidor (parámetros de operación), si desea cambiarlo escriba un nuevo mensaje de notificación que se les enviará a los participantes de la firma del PAM.

3. Configuración del Proceso de Acuerdo Multilateral (PAM). (Figura 3.39).



Figura 3.39 Configuración del PAM

Configure los siguientes parámetros presentados en la Tabla 3.4.

Tabla 3.4 Parámetros de Configuración

Parámetro	Descripción
Duración del PAM	Indique el tiempo en horas de la duración del PAM.
Número de Notificaciones	Indique el número de notificaciones para los participantes.
Requerimiento de Firma	Seleccione el tipo de requerimiento de firma del PAM. (Obligatorio, Adhesión y Adhesión Limitada).

Cuando se elige el tipo de requerimiento Adhesión Limitada se presentarán dos parámetros más para configurar. (Figura 3.40).



Figura 3.40 Adhesión Limitada

Número Mínimo de Firmas Requeridas. Indique el número de firmas requeridas para la ejecución del acuerdo.

Tolerancia Máxima para la Ejecución del Acuerdo. Indique el número de minutos que deberán transcurrir para que se ejecute el acuerdo a partir de haberse recolectado el número mínimo de firmas requeridas.



#### 4. Agregar Participantes/Asignar Función

En esta parte se eligen a los participantes y posteriormente se le asigna su función a cada uno de ellos. (Figura 3.41).

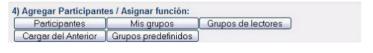


Figura 3.41 Agregar Participantes/Asignar Función



### Importante

Al crear un nuevo PAM usando Rutas, si el iniciador no está configurado como participante, siempre se incluirá al PAM como destinatario.

Elija a los participantes, seleccionando alguno de los siguientes botones:

4.a *Botón Participantes*. Puede agregar participantes a un acuerdo, buscando en la base de datos de usuarios registrados en limel, haciendo clic en el botón Participantes, que presenta la siguiente ventana. (Figura 3.42).

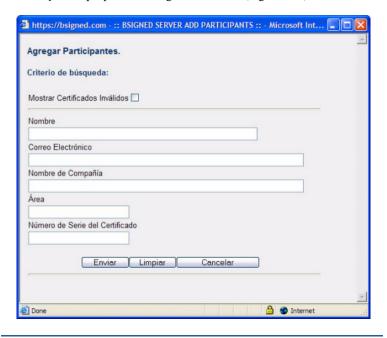


Figura 3.42 Agregar Participantes

La ventana se divide en las siguientes secciones:

#### Mostrar Certificados Inválidos

Esta opción funciona conjuntamente con las siguientes secciones, extendiendo la búsqueda a usuarios con certificados vencidos o revocados. Para activarla haga marque la casilla Mostrar Certificados Inválidos.

#### Criterios de búsqueda

En esta sección podrá llenar los campos que le sean útiles para localizar a los usuarios que le interesan, seguido de un clic en el botón Enviar.



El resultado de la búsqueda será una lista con los usuarios correspondientes, como se muestra en la Figura 3.43



Figura 3.43 Resultado de búsqueda

Marque la(s) casilla(s) que se encuentra del lado izquierdo del renglón para seleccionar a los participantes. Haga clic en el botón Aceptar Selección.

Si en esta lista no se encuentran los usuarios que le interesan, podrá repetir la búsqueda haciendo clic en el botón Nueva Búsqueda.

Las búsquedas se pueden realizar tantas veces como se desee hasta localizar a todos los participantes requeridos para el acuerdo.

Si antes de enviar la búsqueda desea borrar todos los campos para definir otro criterio podrá usar el botón Limpiar.

Al llenar los criterios de búsqueda podrá escribir solamente parte del texto que busca.

- 4.b Botón Cargar del Anterior. Puede agregar participantes al PAM, haciendo clic en el botón Cargar del Anterior. Aparecerán automáticamente los participantes del acuerdo más reciente que haya creado el iniciador. Esta lista sirve como un inicio rápido y se puede modificar posteriormente.
- 4.c *Botón Mis Grupos*. En el botón Mis Grupos, el administrador puede elegir un grupo de participantes que él mismo haya creado, esto con la finalidad de facilitar el proceso de firma con muchos participantes. (Figura 3.44).

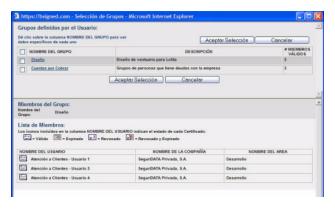


Figura 3.44 Mis Grupos

En esta ventana se presentarán todos los grupos creados por el usuario, su descripción y número de miembros.

En la parte Grupos definidos por el Usuario, se muestra una tabla con las siguientes secciones:

Nombre del grupo. Nombre del grupo existente

Descripción. Texto que describe el propósito, o bien que define los integrantes del mismo.

# Miembros Válidos. Total de participantes que integran el grupo, excluyendo integrantes expirados o revocados.

Marque la casilla correspondiente al grupo que desea agregar. Si desea ver los miembros o integrantes del grupo seleccionado, haga clic sobre el nombre del grupo y éstos se presentarán en la parte de la ventana Miembros del Grupo, donde podrá ver además, el estatus de cada uno de los certificados de cada miembro o integrante del grupo.

Para ver el detalle de los certificados, haga clic sobre el icono.

Una vez elegido(s) el (los) grupo(s) haga clic en el botón Aceptar Selección.



 Botón Grupos Predefinidos. También puede agregar participantes a un PAM, eligiendo un grupo(s) de usuario(s) creado(s) por el administrador del sistema. Haga clic en el botón Grupos Predefinidos que presenta la siguiente ventana. (Figura 3.45).



Figura 3.45 Grupos Predefinidos

En la parte Grupos predefinidos se muestra una tabla con las siguientes secciones:

- Nombre del grupo. Nombre del grupo existente
- Descripción. Area a la que pertenece el grupo
- #Miembros Válidos. Total de participantes que integran el grupo
- #Requeridos. Indique el número de participantes que requiere para la firma del acuerdo

Marque la columna del grupo predefinido que desea agregar. Si desea que el coordinador del grupo seleccionado, asigne a sus participantes, marque la columna Usando Coordinador e indique en la columna #Requeridos el número de participantes que requiere para la firma.

Si desea ver los participantes que integran el grupo seleccionado, haga clic sobre el nombre del grupo y éstos se presentarán en la parte Miembros del Grupo donde podrá ver el estatus de los certificados de cada uno de los participantes.

Para ver el detalle de los certificados, haga clic sobre el icono.

Una vez elegidos los grupos, haga clic en el botón Aceptar Selección.



#### **Importante**

El grupo predefinido que no contenga participantes o coordinadores, no se podrá seleccionar.

Cada Grupo Predefinido deberá tener al menos un coordinador, el cual elige cuales de sus miembros participarán en cada PAM donde el grupo fue incluido.

5.a Para que el proceso de firma de un acuerdo sea visto por integrantes de uno o más grupos predefinidos, haga clic en el botón Grupos de Lectores. (Figura 3.46).

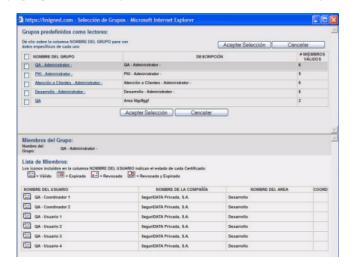


Figura 3.46 Grupos de Lectores

Seleccione el grupo de lectores que corresponde, los participantes de este grupo se presentaran en el área Miembros del Grupo para ver el estatus de su certificado. Haga clic en el botón Aceptar Selección.



#### **Importante**

Los Grupos de Lectores son creados por el administrador del sistema, teniendo como única función consultar el acuerdo donde fueron incluidos. (Ver Capítulo 2 "2.3.4 Grupos" en la página 2-5)



6. Cuando el tipo de requerimiento es Obligatorio, es posible asignar orden a los participantes para la firma del acuerdo, esto con la condición de que exista más de un participante. (Figura 3.47).



Figura 3.47 Secuencia de Firma

Cuando se marca la casilla Secuencia de Firma, aparecerán tres columnas más en la lista de participantes, como se muestra en la Figura 3.48.



Figura 3.48 Orden de Firma

Cuando se marca la casilla de un participante SELECCIONE PARA MOVER, aparecerán dos botones con flechas que permiten desplazar hacia arriba y hacia a bajo al participante, según convenga.

#### 3.5 Licencia del Servidor

bijimel puede ser usado por organizaciones bajo una licencia que autoriza su uso por un número de usuarios, o bien por documentos ejecutados.

Al hacer clic en la liga Licencia del Servidor desde el menú de administración, se mostrarán las opciones de manejo de licencia:

#### 3.5.1 Estado de la Licencia

Despliega en el área de trabajo la situación de la licencia indicando el número de acuerdos amparados por la licencia, ejecutados y restantes; o bien el número de usuarios autorizados y los que están en uso, dependiendo del tipo de licencia que se haya adquirido. (Figura 3.49).

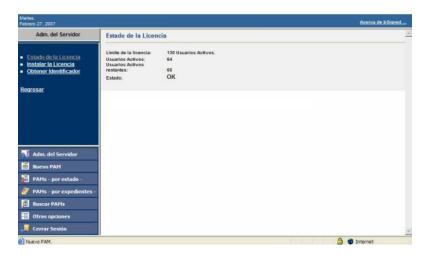


Figura 3.49 Estado de la Licencia de Uso



#### 3.5.2 Instalar la Licencia

Al hacer clic en esta liga, podrá instalar el archivo que contiene la licencia de uso. (Figura 3.50).

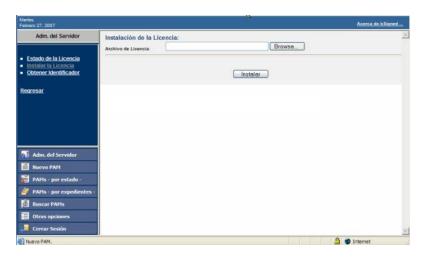


Figura 3.50 Instalar Licencia

Para cargar el archivo haga clic en el botón Browse..., y seleccione el archivo que contiene la licencia, posteriormente de clic en el botón Instalar. Este archivo será entregado por Supribata al obtener su licencia de uso.

#### 3.5.3 Obtener Identificador

Presenta el ID del servidor para gestionar la licencia de uso. (Figura 3.51).

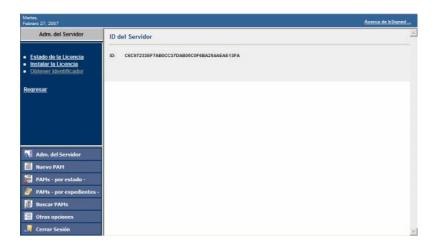


Figura 3.51 Obtener Identificador

Para obtener la licencia de uso, deberá de proporcionar este código a sumbta para que sea generado su archivo de licencia.

Al terminar de usar las opciones de manejo de licencia, podrá regresar al menú anterior haciendo clic en la liga Regresar.



Es importante mencionar que cuando la licencia va a expirar, se le envía al administrador por correo electrónico un mensaje que describe la expiración de la licencia y por lo tanto deberá renovarla.

# CAPÍTULO 4

# Configuración de Plantillas para bigned Office Connector

Las plantillas que se utilizan en bijnel Office Connector, son elaboradas y dadas de alta por el Administrador. Esta plantillas pueden ser elaboradas para las aplicaciones:

- Microsoft® MS Word 2003
- Microsoft® MS Word 2007
- Microsoft® MS Excel 2003
- Microsoft® MS Excel 2007
- Microsoft® MS Power Point 2007

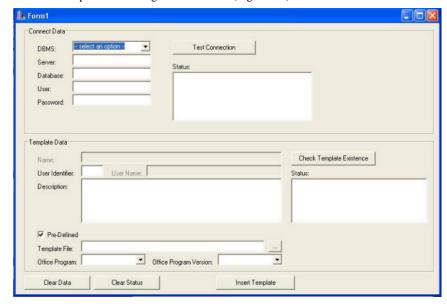
Para dar de alta las plantillas deberá ejecutar la aplicación app\_add\_templates.exe.



#### Importante

Cerciórese que esta aplicación se encuentre en la misma carpeta donde se encuentra la dll sqlapi.dll.





A continuación se presentará la siguiente ventana. (Figura 4.1).

Figura 4.1 Forma para dar de alta Plantillas

Indique los parámetros que se le solicitan como se muestra en la Tabla 4.1.

Parámetro	Descripción
DBMS	Seleccione el manejador de base de datos que l\( \) utiliza.
Server	Nombre del Servidor de base de datos. Este dato se presenta por omisión, después de haber seleccionado el manejador de base de datos. Si este dato no corresponde, puede cambiarlo.
Database	Nombre de la base de datos. Este dato se presenta por omisión, después de haber seleccionado el manejador de base de datos. Si este dato no corresponde, puede cambiarlo.
User	Nombre del usuario de la base de datos. Este dato se presenta por omisión, después de haber seleccionado el manejador de base de datos. Si este dato no corresponde, puede cambiarlo.
Password	Escriba la clave de acceso del usuario a la base de datos.

Tabla 4.1 Parámetros de Configuración de la Base de Datos

№ Form1 Connect Data SQL Server Test Connection + DBMS: ga1 Server: bsigned We are connected! We are disconnected! bsigned Heer Password Template Data Check Template Existence User Name: User Identifier Status Description: ✓ Pre-Defined Template File:

Haga clic en el botón Test Connection para probar la conexión a la base de datos. Si ésta es correcta se presentará un mensaje en el campo Status. (Figura 4.2).

Figura 4.2 Mensaje de Conexión

Office Program:

Clear Data

select an option -- 🕶

Clear Status

A continuación deberá indicar los siguientes datos, como se muestra en la Tabla 4.2.

Office Program Version

Parámetro Descripción User Identifier Indique el número de identificador de su certificado digital. Indique una breve descripción de la plantilla de dará de alta. Descripción Pre- Defined Marque esta opción si desea que la plantilla que dará de alta, será predefinida. Template File Indique la ruta y nombre de la plantilla que dará de alta. Office Program Seleccione el programa donde se dará de alta la plantilla. Office Program: select an option Word Clear Data PowerPoint 1 8 1

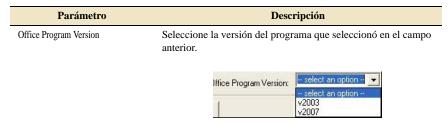
Tabla 4.2 Parámetros de Configuración de Plantillas

- select an option --

Insert Template



Tabla 4.2 Parámetros de Configuración de Plantillas



A continuación haga clic en el botón Check Template Existence para validar si ya existe una plantilla con el mismo nombre de la que se agregó. El resultado de este proceso se presentará en el campo Status.

Y haga clic en el botón Insert Template para insertar la plantilla. Este proceso envía un mensaje con el resultado de la inserción de la plantilla en el campo Status, como se muestra en la Figura 4.3.

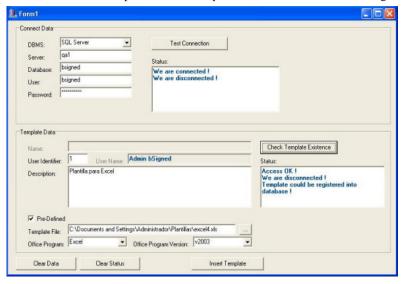


Figura 4.3 Resultado de la Inserción de la Plantilla

# APÉNDICE A

# Configuración del archivo java.policy

En caso de que algún usuario vaya a utilizar el navegador Mozilla FireFox, es necesario realizar el siguiente procedimiento, para que lume funcione correctamente.

Para Mozilla FireFox en Microsoft Windows:

- Localizar el archivo .java.policy en la ruta donde se instaló b@gned:
   C:\..\bSigned Web\bs-wwwroot\Public
- Copiar el archivo
- Instalarlo en la máquina(s) del (los) usuario(s) que utilizarán Mozilla FireFox, en el directorio HOME:
  - C:\Documents and Settings\"Nombre del Usuario"

#### Para Mozilla FireFox en Macintosh:

- Localizar el archivo .java.policy en la ruta donde se instaló bsigned: C:\..\bSigned\_Web\bs-wwwroot\Public
- Copiar el archivo
- Instalarlo en la máquina(s) del (los) usuario(s) que utilizarán Mozilla FireFox, en el directorio HOME:
  - C:\Users\"Usuario"