Administración y configuración

Gestión de la seguridad

Meta4 Spain, S.A.
Centro Europa Empresarial
Edificio Roma
C/ Rozabella, 8
Ctra. de La Coruña, km. 24,200
28230 Las Rozas, Madrid
SPAIN
http://www.meta4.com

Tecnología. Versión 3.21

Tabla de contenidos

Gestión de la seguridad

Acerca de este documento

Este documento presenta las distintas posibilidades de mantenimiento de la seguridad. Meta4Mind Set®© es un sistema de gestión integral de recursos humanos y, como tal, maneja información confidencial. Por tanto, el sistema debe disponer de mecanismos de protección frente a intrusiones externas.

El documento se estructura de la siguiente manera:

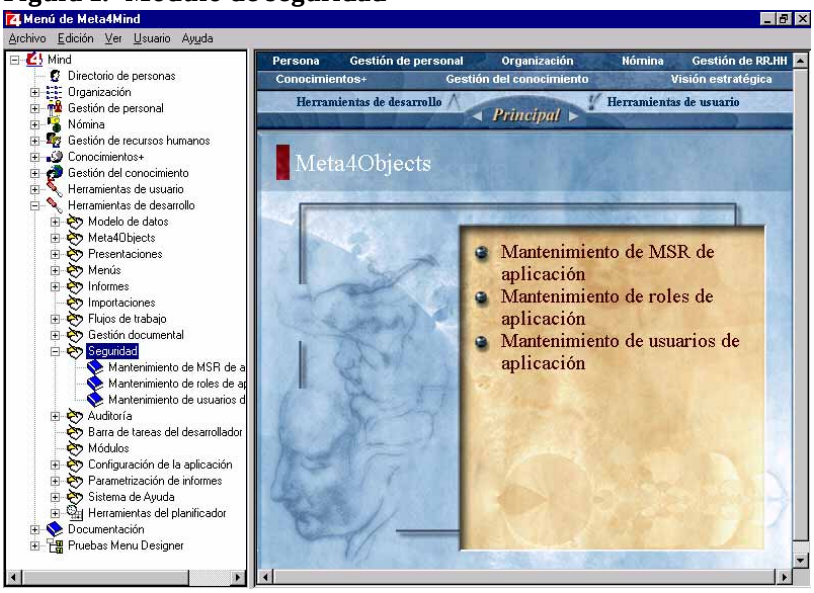
- Mantenimiento de MSR de aplicación
  - Seguridad a nivel de tablas
  - Seguridad a nivel de Meta4Objects
  - Seguridad desde las herramientas de diseño
- Mantenimiento de roles de aplicación
  - Creación de un rol de aplicación
  - Edición de un rol de aplicación
  - Borrado de un rol de aplicación
- Mantenimiento de usuarios de aplicación
  - Creación de un usuario de aplicación
  - Asignación de roles fijos a un usuario
  - Establecimiento de una nueva contraseña
  - Información de la conexión del usuario
  - Borrado de un usuario de aplicación
  - Rol de aplicación por defecto

Introducción

La herramienta de seguridad de Meta4Mind Works 3.2 permite el mantenimiento, a diferentes niveles, de la seguridad de la información y los procesos con los que trabaja el sistema. Así, la aplicación cuenta con los mecanismos necesarios para:

- Impedir el acceso al sistema de usuarios no autorizados
- Garantizar la confidencialidad de los datos delicados: datos personales, información salarial, etc.
- Impedir la ejecución de acciones y procesos por parte de usuarios que carezcan de autorización
- Registrar todas las acciones ejecutadas sobre las tareas del sistema: grabación de datos en tablas, ejecución de procesos, etc.

Figura 1. Módulo de seguridad



El mantenimiento de la seguridad se aplica, de forma integral, desde el módulo de seguridad disponible en Meta4Mind Works. Dicho módulo ofrece la posibilidad de definir seguridad a tres niveles y para ello cuenta con las siguientes herramientas:

NOTA:
MSR es el modelo de sistema de roles.

- **Mantenimiento de MSR de aplicación**: permite definir seguridad en forma de permisos a nivel de tablas y de Meta4Objects a través de máscaras. El término *máscara* hace referencia al conjunto de permisos concedidos a un Meta4Object en un mismo MSR. Para definir seguridad a nivel de registros se ha incorporado la herramienta *Diseñador de filtros*.

- **Mantenimiento de roles de aplicación**: permite definir roles de aplicación, es decir, perfiles de seguridad sobre tareas. El único permiso que se puede conceder sobre una tarea es el de ejecución. En el caso de que una tarea esté asociada a datos de Meta4Objects, será necesario disponer de permisos sobre dichos Meta4Objects para poder ejecutarla.
- **Mantenimiento de usuarios de aplicación**: permite definir los parámetros de seguridad a nivel de usuario (identificación, contraseña, número de intentos permitidos, etc.). Asimismo, permite asignar a un usuario uno o más perfiles de seguridad fijos, que se unirán a aquéllos que le correspondan como consecuencia de las reglas de elegibilidad.

NOTA:

También es posible definir la seguridad a nivel de Meta4Objects y de tablas en tiempo de diseño desde las correspondientes herramientas de diseño, tal como se describe en el apartado *Seguridad desde las herramientas de diseño*.

Hay una estrecha relación entre las tres opciones de la herramienta de seguridad, dado que:

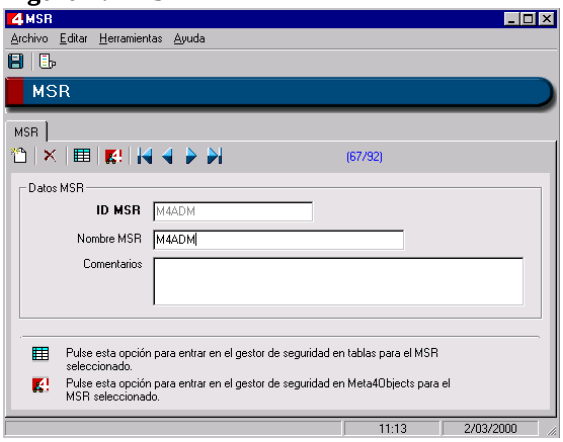
- El perfil de seguridad asignado a un usuario desde **Mantenimiento de usuarios de aplicación** proviene de los roles de aplicación previamente definidos.
- Una máscara sobre un Meta4Object puede definirse de manera independiente desde **Mantenimiento de MSR de aplicación**. Esto tiene sentido cuando se incorpora a un MSR de aplicación, a través de éste a un rol de usuario y a través de éste último a un usuario de la aplicación.

Mantenimiento de MSR de aplicación

Esta herramienta permite definir las opciones de seguridad sobre los Meta4Objects y sus componentes (nodos y elementos), así como sobre las tablas. Para tener acceso a ella, seleccione **Mind|Herramientas de desarrollo|Seguridad|Mantenimiento de MSR de aplicación** en el árbol de menús de la aplicación Meta4Mind Works.

NOTA:
MSR es el modelo de sistema de roles.

Figura 2. MSR



Los permisos de selección, inserción, actualización y borrado que se conceden sobre tablas y sobre Meta4Objects se agrupan en los MSR. Dado que los Meta4Objects están definidos a partir de tablas, se emplea la misma herramienta para definir permisos sobre ambos tipos de elementos. Únicamente es preciso prestar atención a la superposición de los permisos concedidos sobre ambos tipos de elementos, de modo que no se produzcan conflictos entre ellos.

Desde la ventana de **MSR**, se puede obtener un listado de los MSR ya existentes mediante el botón **Ver lista** de la barra de herramientas.

También pueden definirse nuevos MSR haciendo clic en el botón **Crear registro**. Los datos que identifican un nuevo MSR son:

- **ID MSR:** código identificativo del modelo de sistema de roles
- **Nombre MSR:** nombre del modelo de sistema de roles

Para dotar de contenido a un nuevo MSR desde este formulario, dispone de los botones **Seguridad tablas** y **Seguridad Meta4Objects**. Haga clic en uno u otro botón, según desee asociar al MSR permisos sobre tablas o sobre Meta4Objects, respectivamente.

Seguridad a nivel de tablas

En este nivel de seguridad, se indica qué acciones podrá ejecutar un grupo de usuarios sobre las tablas. Hay tablas sin seguridad, para las que no existe ninguna restricción de acceso, y tablas con seguridad.

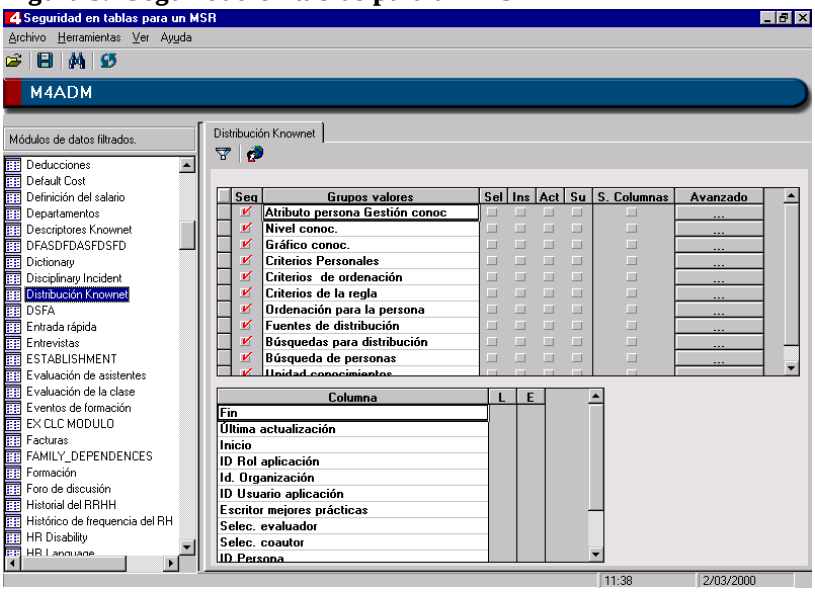
En este segundo caso, el gestor definirá los privilegios que se van a aplicar sobre las acciones ejecutables en esas tablas:

- Lectura de los registros de la tabla
- Incorporación de nuevos registros a la misma
- Modificación de registros de la tabla
- Borrado de registros de la tabla

Es importante recordar que cuando se indique que una tabla tiene seguridad, se desactivarán todos los permisos sobre la misma. El gestor deberá proceder entonces a conceder permisos sobre la tabla.

En la barra de herramientas del **MSR**, haga clic en el botón **Seguridad tablas** para tener acceso a la ventana de definición de seguridad sobre tablas.

Figura 3. Seguridad en tablas para un MSR



La concesión de permisos sobre tablas en el marco de un MSR se realiza desde el formulario **Seguridad en tablas para un MSR**.

Una instancia determinada de **Seguridad en tablas para un MSR** está asociada al MSR del que procede, y las operaciones de asignación de seguridad sobre tablas que se realicen en ella quedarán igualmente asociadas a dicho MSR.

Este formulario se compone de tres paneles:

- En el panel de navegación, a la izquierda de la interfaz, aparece un listado de los diferentes módulos de datos filtrados que componen la aplicación. Cada uno de esos módulos contiene una serie de tablas, a las que se puede asignar seguridad desde la herramienta Seguridad en tablas.
- Al seleccionar uno de los módulos de la aplicación, en el panel de tablas de la parte superior derecha, aparece la lista de las tablas incluidas en dicho módulo. Desde este panel, puede asignar seguridad a las tablas a través de una serie de opciones que se describen más adelante.
- Al seleccionar una de las tablas sobre el panel anterior, puede ver la lista de las columnas, situado en la parte inferior. Desde esta ventana, puede asignar seguridad a nivel de columnas de las tablas.

En el panel de tablas, aparece la casilla de verificación **Seg.** a la izquierda de los nombres de las tablas. Para asignar seguridad a una tabla determinada, active la casilla **Seg.** correspondiente. En ese caso, a la derecha del nombre del objeto, se activa una tabla sobre la que se puede definir el tipo de permiso que se desea asignar a la tabla. Hay seis clases de permisos:

- **Sel.**: permiso de lectura de registros de la tabla.
- **Ins.**: permiso de inserción de registros en la tabla.
- **Act.**: permiso de actualización de registros.
- **Su.**: permiso de borrado de registros.
- **S. columnas**: permisos de escritura y lectura sobre todas las columnas de la tabla.

- **Avanzado**: opciones de seguridad avanzada para la tabla.

  Al hacer clic en este botón, aparecen varias casillas de verificación con las diferentes opciones de seguridad aplicables sobre la tabla seleccionada:

  – **Actualizar la fecha de cierre**: permite trabajar sobre tablas cerradas, modificando en caso necesario las fechas de cierre de los registros.

  – **Adaptar los datos históricos**: permite asignar seguridad a nivel de columnas sobre las tablas de histórico mencionadas anteriormente.

  – **Borrar en cascada**: habilita el borrado de las tablas hijas para las que se haya definido esta propiedad en la relación.

  – **Actualizar la fecha de inicio en cascada**: permite determinar una nueva fecha de inicio y que ésta se asigne automáticamente al resto de las columnas asociadas.

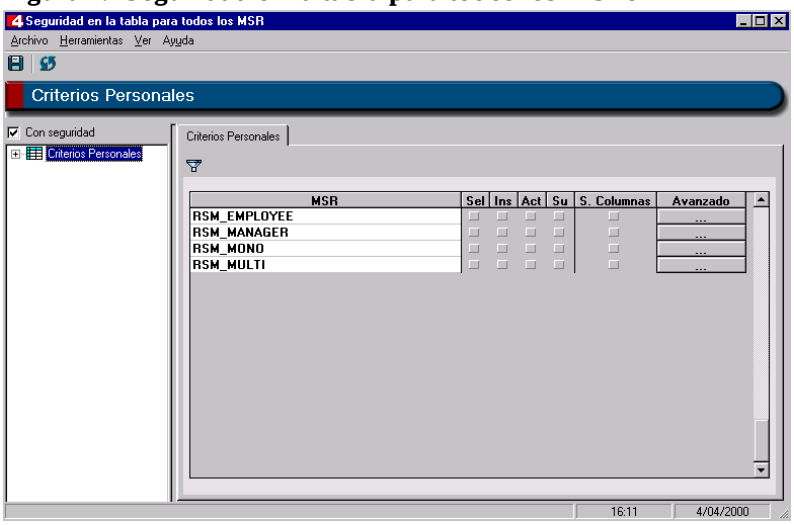
- **Actualización la fecha de fin en cascada**: permite determinar una nueva fecha de fin y que ésta se asigne automáticamente al resto de las columnas asociadas.
- **Actualizar la clave en cascada**: permite corregir la clave de una columna determinada y la de todos los elementos que dependan de ella.

En el panel de columnas de la parte inferior aparece, como ya se ha dicho, la lista de las columnas que contiene la tabla seleccionada en la ventana inmediatamente superior. Junto al nombre de cada columna, se encuentran dos casillas (**L** y **E**), desde las que es posible asignar permisos de lectura y escritura sobre cada columna con sólo activarlas. Estas casillas están desactivadas por defecto.

Por otra parte, la herramienta de asignación de seguridad a nivel de tablas presenta también la opción de visualización de los permisos concedidos sobre una tabla determinada desde todos y cada uno de los MSRs definidos.

Para activar esta opción, haga clic en el botón **Vista tabla-MSR** dentro de la pestaña o seleccione la opción **Herramientas|Vista tabla-MSR** de la barra de menús. Aparece la siguiente ventana:

Figura 4. Seguridad en la tabla para todos los MSRs



En esta ventana se muestran los diferentes MSRs y los permisos que cada uno de ellos tiene definidos sobre la tabla seleccionada. También se pueden ver los permisos a nivel de columna para los distintos MSRs: despliegue la estructura de la tabla sobre el panel de navegación de la izquierda y seleccione cualquiera de las columnas que la componen.

Finalmente, desde esta ventana puede realizar modificaciones sobre los permisos asignados desde los distintos MSRs a nivel de tablas, columnas o registros, desde la herramienta Diseñador de filtros.

Permisos a nivel de registro: filtros

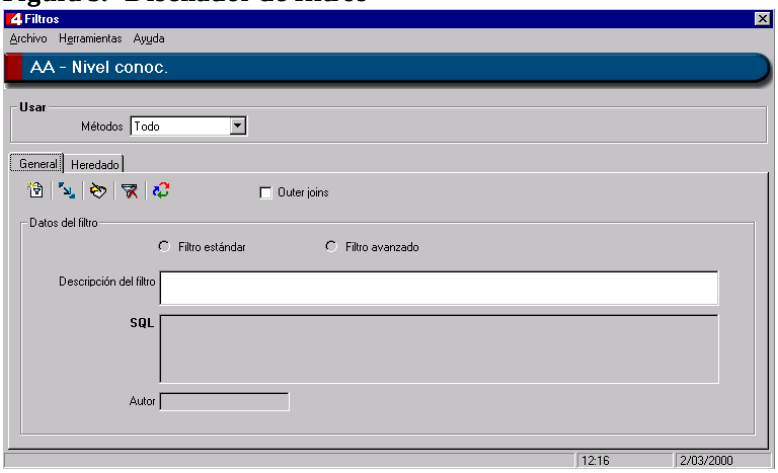
La ventana **Seguridad en tablas para un MSR** presenta también la opción de asignación de permisos a nivel de registro desde el Diseñador de filtros. Permite asignar permisos sobre registros individuales o grupos de registros.

Por ejemplo, en una tabla con información sobre las evaluaciones de los empleados de todas las unidades organizativas, se puede diseñar un perfil de seguridad que sólo permita leer los registros correspondientes a los empleados adscritos a la misma unidad organizativa que el usuario que ejecuta la acción de lectura. Esto no se puede hacer definiendo permisos sobre la tabla completa, ni siquiera sobre las columnas de dicha tabla, sino únicamente asignando permisos a nivel de registro.

En este caso, se recurre a los filtros para asignar un permiso determinado sobre todos aquellos registros que cumplen la condición expresada en el filtro.

Para tener acceso al Diseñador de filtros, haga clic en el botón **Filtros** que se muestra al margen.

Figura 5. Diseñador de filtros



Los filtros diseñados desde esta herramienta, al igual que los permisos ya definidos anteriormente, quedan también asociados al MSR al que pertenecen. Así, un MSR se compone de una serie de permisos, tanto a nivel general como a nivel de columnas, sobre tablas asociadas a módulos de la aplicación. Asimismo, incluye una serie de filtros sobre elementos que hacen posible la recuperación de información a nivel de registro.

El Diseñador de filtros se compone de dos pestañas:

- **General**: contiene la herramienta de diseño de filtros.
- **Heredado**: contiene una herramienta adicional para la herencia de filtros, es decir, para reutilizar los filtros asignándolos a otras tablas.

La ventana del Diseñador de filtros presenta, en primer lugar, una barra de título en la que se muestran el MSR y la tabla a la que pertenece el filtro que se va a definir

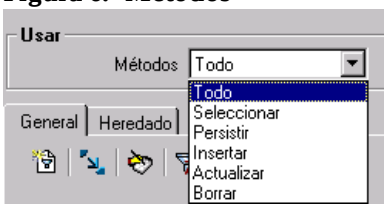
Asignación de filtros

La pestaña **General** tiene un cuadro de grupo de datos llamado **Usar** que presenta el cuadro de lista desplegable **Métodos**. Aquí, se define el tipo de permiso que se va a asignar a los registros que cumplan la condición del filtro. Es posible definir filtros para las siguientes acciones:

- **Seleccionar**: lectura
- **Persistir**: grabación
- **Insertar**: escritura
- **Actualizar**: modificación
- **Borrar**: borrado

La opción **Guardar** equivale a las operaciones de escritura y modificación. También se puede definir el filtro **Todo**, que es equivalente a la suma de todas las condiciones anteriores.

Figura 6. Métodos



La pestaña **General** cuenta con una barra de herramientas que contiene los siguientes botones:

- **Nuevo filtro**: define un nuevo filtro documentado o estándar.

- **Convertir filtro**: convierte un filtro estándar o documentado en un filtro avanzado o semidocumentado.

- **Editar filtro**: edita la instrucción SQL que compone el filtro.

- **Marcar filtro para borrar**: elimina filtros no válidos o desactualizados.

- **Propagar**: activa la opción de propagación de filtros, que hace que el filtro definido sobre una tabla se extienda a todos los elementos relacionados con ésta.
- **Outer joins**: esta casilla de verificación se activa para que el filtro estándar sea de tipo Outer join. Si está desactivada, el filtro estándar será de tipo Inner join. Por defecto, la casilla de verificación aparece desactivada.

El cuadro de texto **Datos del filtro** contiene los siguientes campos:

NOTA:
Los cambios introducidos no tendrán validez hasta que se haga clic en el botón **Guardar** de la barra de herramientas.

- **Descripción del filtro**: comentario explicativo de la funcionalidad del filtro que se está definiendo.
- **SQL**: definición del filtro propiamente dicha en forma de sentencia SQL.
- **Autor**: identificación de usuario del autor del filtro que se introduce automáticamente.

Al hacer clic en **Nuevo filtro**, aparecen los siguientes tipos de definición de filtros:

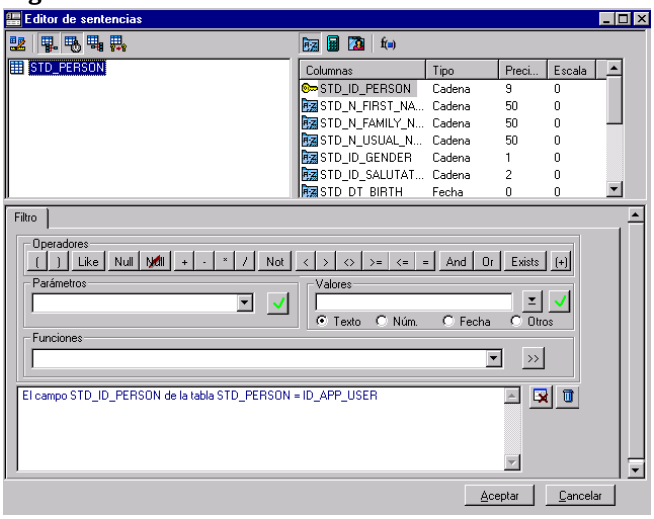
- Filtro estándar o documentado
- Filtro avanzado o semidocumentado
- Filtro existente

Filtro estándar o documentado

Se define un nuevo filtro estándar o *documentado* desde el *Editor de sentencias SQL*, desde donde se puede crear una sentencia SQL con la que se recuperarán los registros que cumplan una condición.

NOTA:
Los filtros documentados se registran en las tablas del repositorio que recogen información referente a las sentencias SCH_SENTENCES, SCH_SENT_OBJECTS, SCH_SENT_OBJ_FIELD, SCH_SENT_OBJ_REL, etc.

Figura 7. Editor de sentencias



En la sentencia SQL que se crea, se distinguen las siguientes partes:

- El nombre de la tabla de la que se extraen los datos sería la cláusula FROM.
- El nombre de las columnas de la tabla que se quieren recuperar darían lugar a la cláusula SELECT.
- Las condiciones que deben cumplir los registros recuperados serían la cláusula WHERE.

La ventana Editor de sentencias se compone de tres partes diferenciadas:

1. En la parte superior izquierda, aparece la tabla seleccionada. Si lo necesita, puede unir dos o más tablas para realizar la consulta en función de los siguientes criterios:
   - Unión de tablas con relación uno a muchos
   - Unión de tablas con relación muchos a uno
   - Unión de tablas históricas
   - Creación de relaciones personalizadas

2. En la parte superior derecha, aparecen las columnas que forman la tabla seleccionada. Puede indicar qué columnas desea visualizar seleccionando los siguientes botones:
   - **Columnas**: se visualizan todas las columnas de la tabla.
   - **Columnas seleccionadas**: se visualizan sólo las columnas seleccionadas para la creación del filtro.
   - **Campos calculados**: se muestran las expresiones de cálculo que hayan sido creadas para este filtro.
   - **Editar campos calculados**: si hace clic en este botón, podrá crear o editar los campos calculados que necesite para su consulta.
3. En la parte inferior es donde se construirá el filtro.

La sentencia se crea desde la pestaña **Filtro**, donde, una vez seleccionadas las columnas, se creará la condición por la que se recuperarán los registros.

Los distintos elementos que se pueden utilizar para crear la condición de filtrado son:

- **Operadores**: botones con los que se puede restringir los registros que se recuperan.
- **Valores**: para establecer filtros de comparación, puede que necesite conocer los valores que toma una determinada columna. Seleccione una columna y haga clic en el botón de remonte. En la tabla que aparece, se muestran todos los valores que existen para la tabla y columna seleccionadas.
- **Funciones**: son operaciones que se realizan sobre los datos y que modifican sus características. Un ejemplo sería la conversión del texto "editor de sentencias" a mayúsculas, para lo que debería utilizar la función CONVERTIR A MAYÚSCULA. Para obtener mayor información sobre las funciones existentes, lea el capítulo "Consulta" del manual *Herramientas de usuario*.

EJEMPLO

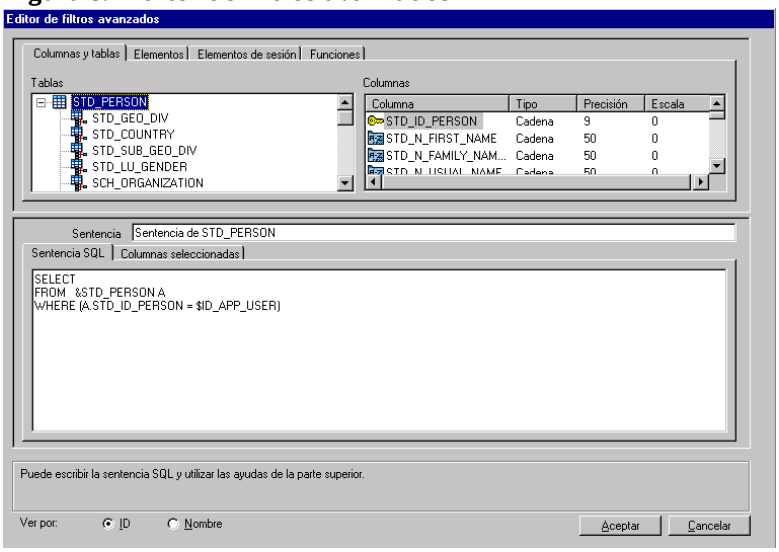
```
El campo STD_ID_PERSON de la tabla STD_PERSON =
ID_APP_USER
```

Esta sentencia recupera las filas de la tabla PERSONA cuyo identificador de la persona sea igual al identificador del rol que ha iniciado la sesión.

Filtro avanzado o semidocumentado

Se define un nuevo filtro avanzado o *semidocumentado* escribiendo directamente la instrucción SQL en la ventana de definición de filtros.

Figura 8. Editor de filtros avanzados



Esta ventana cuenta con unas pestañas de ayuda que facilitan la creación de la sentencia SQL y proporcionan un listado con todos los elementos que pueden componer la sentencia SQL. Estos elementos se pueden seleccionar y son:

- **Columnas y tablas**: se visualizan todas la columnas y tablas.
- **Elementos**: se visualizan los elementos de la estructura de nodo (campos, propiedades, métodos y conceptos).
- **Elementos de sesión**: se visualizan únicamente los elementos que pertenecen a las sesión.
- **Funciones**: son operaciones que se realizan sobre los datos y que modifican sus características.

EJEMPLO

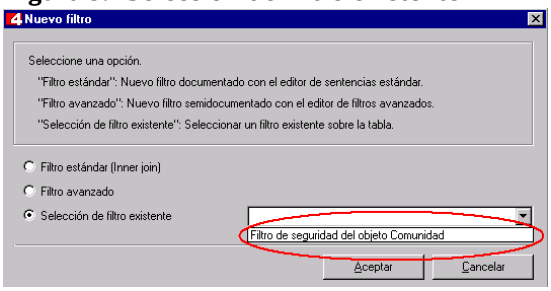
```
SELECT
FROM &STD_PERSON A
WHERE (A.STD_ID_PERSON = $ID_APP_USER)
```

Esta sentencia recupera las filas de la tabla PERSONA cuyo identificador de la persona sea igual al identificador del rol que ha iniciado la sesión.

Filtro existente

Posee un cuadro de lista desplegable donde se puede seleccionar un filtro que exista sobre la tabla.

Figura 9. Selección de filtro existente



Propagación y herencia de filtros

La herramienta de asignación de seguridad permite reutilizar filtros definidos para distintos componentes. La reutilización de filtros evita tener que definir muchos filtros y facilita el diseño de los modelos de seguridad. Mediante el Diseñador de filtros, el administrador del sistema puede realizar las siguientes acciones:

NOTA:
Las relaciones entre tablas se establecen mediante claves externas. En el manual *Metodología de diseño del modelo de datos* tiene más información sobre las distintas relaciones que se pueden establecer entre tablas.

- Propagar el filtro diseñado sobre una tabla al resto de tablas con las que ésta esté relacionada. La propagación copiará el filtro que se define para un componente al resto de componentes con los que esté relacionado.
- Copiar al componente al que se está definiendo la seguridad, un filtro diseñado para otra tabla. De este modo, se produce una *herencia* del filtro de la tabla padre al elemento hijo.

Propagación de filtros

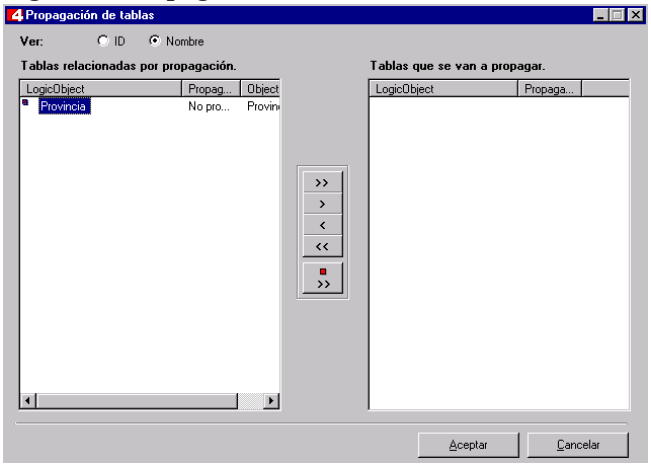
Los filtros definidos sobre una tabla pueden propagarse mediante una clave externa a todas las tablas con las que ésta esté relacionada.

Se establece una relación de clave externa entre dos tablas siempre que una de ellas contenga una o más columnas que sean claves externas. Al propagar un filtro definido sobre una tabla X, el filtro se aplicará a todas las tablas que contengan una clave externa definida sobre la clave primaria de la tabla X.

A efectos prácticos, la propagación de filtros implica que únicamente se leerán de las tablas hijas aquellos registros que estén relacionados con los registros visibles en la tabla padre.

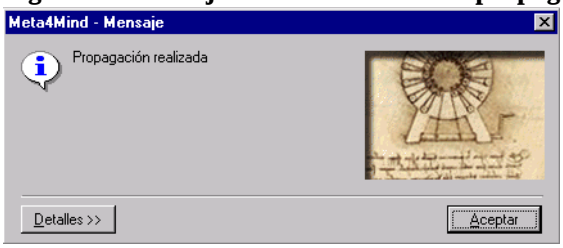
La propagación de un filtro definido sobre una tabla a todas aquellas tablas con las que ésta esté relacionada mediante una clave externa, se realizará automáticamente al hacer clic en el botón **Propagar** de la barra de herramientas de la pestaña **General** del Diseñador de filtros.

Figura 10. Propagación de tablas



El programa detecta las tablas relacionadas con la tabla original y les asigna el filtro en propagación. Al finalizar la operación, muestra en pantalla el siguiente mensaje:

Figura 11. Mensaje de conclusión de la propagación del filtro



Herencia de filtros

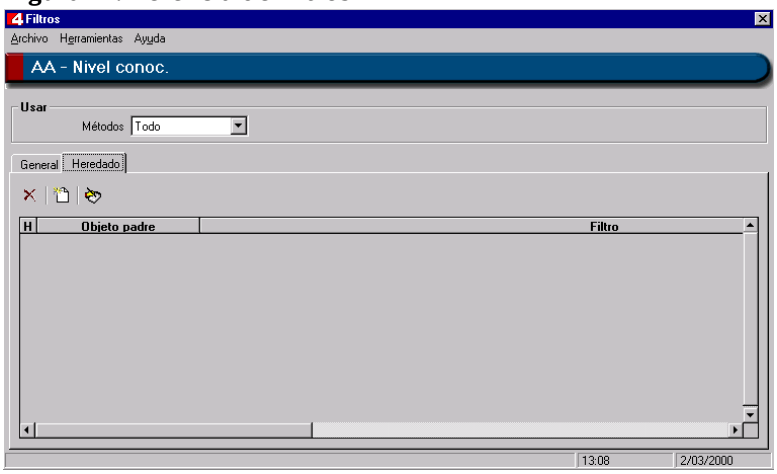
La herramienta de asignación de seguridad a las tablas permite aplicar sobre una tabla un filtro definido con anterioridad para otra tabla.

Al heredar un filtro, se está indicando al sistema que, de todos los registros de la tabla que hereda el filtro, únicamente se podrá trabajar con aquéllos que se correspondan con los registros visibles de la tabla de la que se hereda el filtro.

NOTA:
Para poder heredar un filtro de otra tabla, es necesario definir una relación entre ambas que indique qué registros de la tabla que hereda el filtro se corresponden con los registros visibles o no visibles de la tabla cuyo filtro se hereda.

Para que el sistema pueda saber qué registros de la tabla que hereda el filtro se corresponden con cada uno de los registros de la tabla de la cual se hereda, es necesario establecer una relación o *Join* entre las dos tablas. Esto se hace desde la pestaña **Heredado** del Diseñador de filtros.

Figura 12. Herencia de filtros



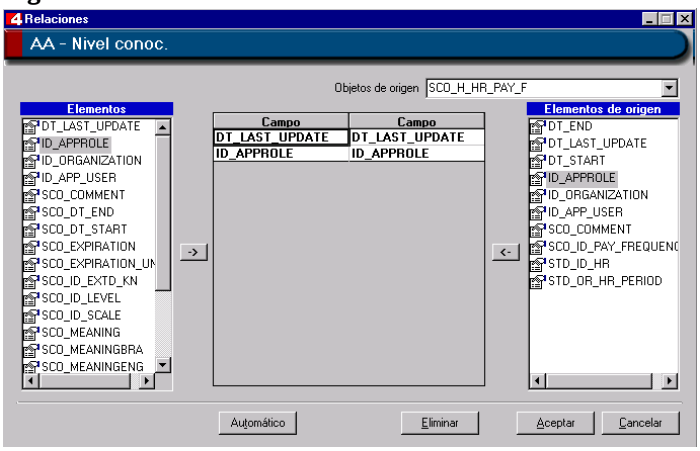
Se pueden heredar filtros de dos formas: por propagación o por creación manual. Los filtros manuales se pueden editar desde la pestaña **Heredado**, que incluye los siguientes botones:

- **Marcar relación para borrar**: marca una relación entre dos tablas creada con anterioridad para que sea eliminada.

- **Nueva relación**: al hacer clic en este botón, aparece el formulario **Relaciones**, donde se incluyen las características de una relación establecida. En este formulario, defina una herencia de filtros indicando las columnas de las tablas cuyo valor desea igualar.

- **Editar relación**: permite la edición de las relaciones que hay entre las tablas.

Figura 13. Relaciones entre tablas



En el cuadro **Elementos** situado a la izquierda, se enumeran las columnas de la tabla que va a heredar el filtro, es decir, la tabla para la cual se están definiendo las condiciones de seguridad.

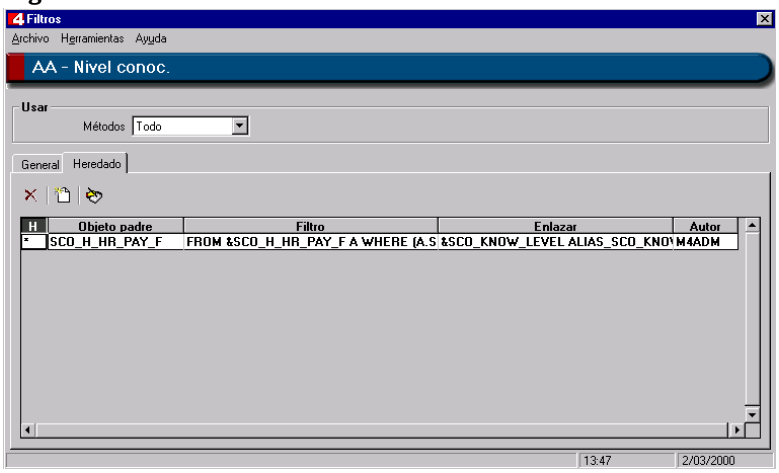
En el cuadro de lista desplegable **Objetos de origen** situado en la esquina superior derecha, se incluyen todas las tablas para las que se ha definido un filtro de seguridad en el marco del mismo MSR que se está utilizando.

En el cuadro **Elementos de origen** situado a la derecha, se muestran los elementos de la tabla origen cuyo filtro se quiere heredar.

En las columnas **Campo**, se incluyen los pares de columnas que se quieren igualar para crear la relación entre las dos tablas. La relación entre las columnas puede establecerse manualmente, mediante los botones de flecha, o automáticamente, haciendo clic en el botón **Automático**. En este caso, el programa detecta las columnas comunes entre los elementos de ambos extremos de la ventana (elemento origen y elemento destino) y los incluye en la tabla central.

Si desea borrar alguna de las relaciones a nivel de columna, seleccione las columnas que va a eliminar de la herencia y haga clic en **Eliminar**. Al hacer clic en **Aceptar,** se define la relación entre columnas registrada en la tabla central, y se vuelve a la ventana del Diseñador de filtros. Aquí se pueden ver las características de la relación que se ha establecido entre las tablas.

Figura 14. Relación establecida entre las tablas



En esta ventana, se incluyen los siguientes parámetros:

- **Objeto padre**: elemento origen del que se hereda el filtro.
- **Filtro**: sentencia SQL del filtro heredado.
- **Enlazar**: sentencia de igualación de las columnas que constituye la relación establecida entre las tablas origen y destino del filtro.
- **Autor**: código identificativo de usuario del autor del filtro.

NOTA:
Los cambios introducidos no tendrán validez hasta que se haga clic en el botón **Guardar** de la barra de herramientas.

Finalmente, existe el cuadro de grupo **Usar**, que presenta un cuadro de lista desplegable, **Métodos**, donde se define el tipo de permiso que caracteriza al filtro que se hereda (Seleccionar, Persistir, Insertar, Actualizar, etc.)

Seguridad a nivel de Meta4Objects

Una tabla puede utilizarse en la definición de una o más estructuras de nodo. A su vez, estas estructuras de nodo pueden utilizarse en múltiples Meta4Objects.

El Meta4Object actúa como interfaz entre la base de datos y la aplicación diseñada con la aplicación Meta4®. Todos los accesos y operaciones que se hagan sobre los datos de la base de datos, emplearán Meta4Objects.

Un Meta4Object no sólo recoge información de la base de datos, sino que también encapsula las instrucciones de procesamiento que se pueden ejecutar sobre estos datos. Las instrucciones de procesamiento se definen mediante elementos de tipo método o concepto. El administrador del sistema podrá conceder permisos sobre los Meta4Objects y sobre cada uno de sus componentes: nodos y elementos.

Al igual que sucedía con las tablas, mediante los MSRs es posible diseñar perfiles de seguridad que incluyan un conjunto de permisos sobre uno o más Meta4Objects.

Un mismo MSR recoge los diferentes permisos sobre uno o más Meta4Objects. El conjunto de permisos correspondientes a un Meta4Object conforman una máscara.

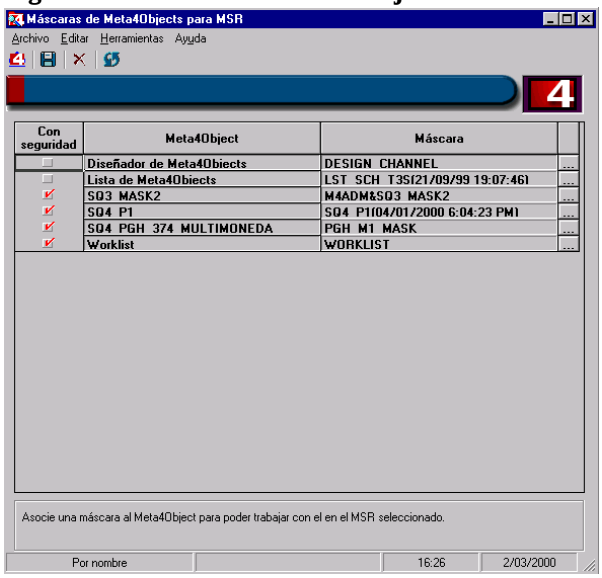
Las máscaras pueden reutilizarse en más de un MSR; es decir, se puede encontrar dos MSRs que compartan una misma máscara para un mismo Meta4Object. De este modo, ambos MSRs tendrán idénticos permisos sobre el Meta4Object.

En la barra de herramientas de **MSR**, haga clic en el botón **Seguridad Meta4Objects** para tener acceso a la ventana de definición de seguridad sobre Meta4Objects. Aparecerá la ventana **Máscaras de Meta4Objects para MSR**, con los Meta4Objects y las máscaras que componen el MSR seleccionado.

NOTA:

Sobre un Meta4Object pueden definirse tantas máscaras como se desee, aunque, posteriormente, al asignar permisos sobre tareas a un usuario mediante el Diseñador de roles de aplicación, no se podrá asignar más que una máscara para cada Meta4Object.

Figura 15. Máscaras de Meta4Objects



En la barra de herramientas se incluyen los siguientes botones:

- **Añadir Meta4Object a la lista**: agrega un nuevo Meta4Object al MSR, que se seleccionará mediante un filtro.

- **Graba la seguridad de los Meta4Object**: archiva las modificaciones realizadas.

- **Elimina el Meta4Object seleccionado de la lista**: elimina un Meta4Object del MSR.

Para visualizar las diferentes máscaras definidas para un mismo Meta4Object, haga clic en el botón que aparece junto a la columna **Máscara**; se abrirá la siguiente ventana:

Figura 16. Máscaras del Meta4Object

Desde esta ventana, puede realizar las siguientes operaciones:

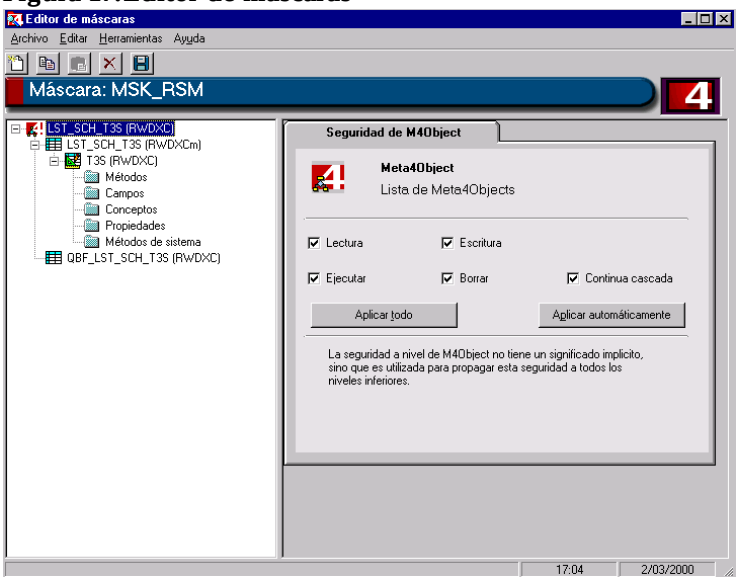
- **Editor de máscaras**: edita la máscara seleccionada.

- **Nuevo**: crea una nueva máscara para el Meta4Object seleccionado.

- **Borrar**: elimina una máscara.

Al hacer clic en **Editor de máscaras**, se visualizan las características de la máscara seleccionada.

Figura 17. Editor de máscaras



A la izquierda de la ventana, aparece un panel de navegación, donde se muestra el Meta4Object al que pertenece dicha máscara. Para ver la estructura del Meta4Object, despliegue sus sucesivas entradas sobre el panel de navegación.

A la derecha, se encuentra el panel de atributos de seguridad. Selecciónelos en el panel de navegación para ver los permisos definidos sobre los diferentes elementos del Meta4Object mostrado a la izquierda.

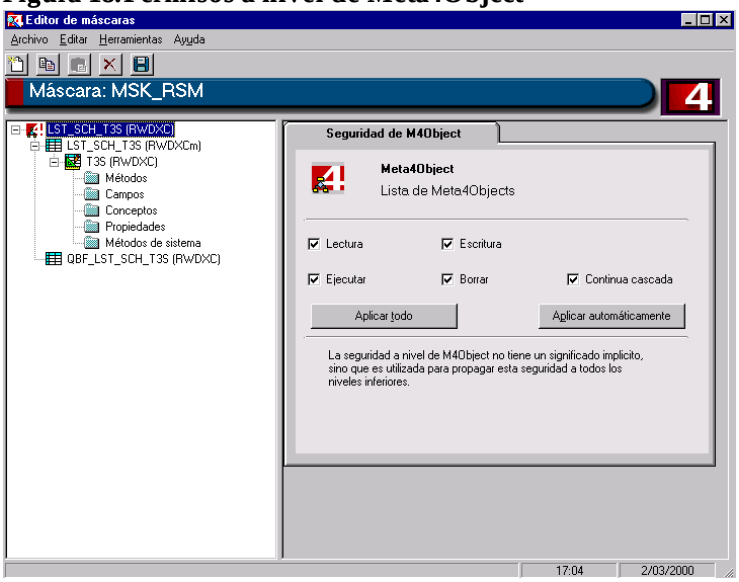
Es posible conceder permisos a nivel de Meta4Object, de nodo, de estructura de nodo y de elemento. Además, existen opciones para que los permisos concedidos a nivel de Meta4Object sean heredados por todos sus componentes. De la misma forma, los permisos que se concedan a nivel de nodo podrán ser heredados por la estructura de nodo sobre la que se hayan definido y por sus correspondientes elementos. Finalmente, los permisos que se concedan sobre estructuras de nodo podrán ser heredados por todos sus elementos.

Los permisos que pueden asignarse varían en función del componente de la estructura del Meta4Object sobre el que se trabaje. A continuación, se explican los permisos disponibles para cada uno de los niveles.

Permisos a nivel de Meta4Object

A nivel de Meta4Object, se pueden conceder permisos de lectura, escritura, borrado, ejecución y continua cascada, si bien, para que tengan efecto, deberán existir los permisos necesarios a nivel de elemento. Así, los permisos a nivel de Meta4Object tienen como principal objetivo simplificar la asignación de permisos a niveles inferiores por propagación.

Figura 18. Permisos a nivel de Meta4Object



- **Lectura**: los usuarios incluidos en el perfil de seguridad podrán leer todos los datos recuperables por el Meta4Object, siempre que tengan permisos de lectura sobre los elementos necesarios, así como sobre las tablas sobre las que se ha definido el Meta4Object. Los permisos de lectura sólo se pueden aplicar a los elementos de tipo columna, concepto y propiedad.
- **Escritura**: los usuarios incluidos en el perfil de seguridad podrán agregar nuevos registros en el Meta4Object, y modificar los valores de los registros recuperados por el Meta4Object, siempre que tengan permisos de escritura y actualización sobre los elementos necesarios, así como sobre las tablas sobre las que se ha definido el Meta4Object. Los permisos de escritura sólo se pueden aplicar a los elementos de tipo columna, concepto y propiedad.
- **Borrar**: los usuarios incluidos en el perfil de seguridad podrán borrar los registros recuperados por el Meta4Object, siempre que tengan permisos de borrado sobre los elementos correspondientes, así como sobre las tablas sobre las que se ha definido el Meta4Object. Los permisos de borrado sólo se pueden aplicar a los elementos de tipo columna, concepto y propiedad.
- **Ejecutar**: los usuarios incluidos en el perfil de seguridad podrán ejecutar los métodos y conceptos del Meta4Object, siempre que tengan los permisos necesarios a nivel de elemento.
- **Continua cascada**: el usuario decide si quiere detener la ejecución en cascada o no, habilitando el borrado de los nodos hijos cuando se detecten errores. Esto sólo tiene sentido a nivel de método y concepto.

Permisos a nivel de nodo

Se puede conceder a cada nodo permisos de escritura, lectura, borrado, ejecución y continua cascada. Estos permisos tienen el mismo significado y las mismas restricciones que los permisos del mismo nombre definidos a nivel de Meta4Object en el apartado anterior. A nivel de nodo se puede definir además otro tipo de permiso:

- **Filtro dinámico**: si activa este permiso, podrá cambiar las condiciones de las sentencias de la estructura de nodo.

NOTA:
En el caso de que se produzca un conflicto entre los permisos asignados a dos elementos relacionados jerárquicamente, el sistema siempre adoptará los permisos más restrictivos.

Además de estos permisos, se puede definir un **Nuevo filtro estándar** a nivel de nodo o un **Nuevo filtro avanzado**, de modo similar a como se hacía a nivel de tabla.

Es importante recordar que, si se ha diseñado un filtro de seguridad sobre una tabla, este filtro se aplicará a todas las estructuras de nodo y nodos que se hayan definido a partir de esa tabla. Si se produce un conflicto entre el filtro de seguridad definido sobre un nodo y el definido sobre la tabla a partir de la cual se ha diseñado el nodo, el sistema unirá las condiciones de los dos filtros y optará por la fórmula más restrictiva posible.

Permisos a nivel de estructura de nodo

Para cada una de las estructuras de nodo de un Meta4Object, se podrán conceder permisos de lectura, escritura, borrado, ejecución y continua cascada. Al igual que en el caso de los permisos a nivel de Meta4Object, cuando se asigna un permiso a una estructura de nodo, los elementos heredan ese permiso.

El significado de los permisos coincide con los de los definidos a nivel de Meta4Object:

- **Lectura**: el usuario puede leer los registros recuperados por la estructura de nodo.
- **Escritura**: el usuario puede agregar nuevos registros a la estructura de nodo y modificar los valores de los registros recuperados por la estructura de nodo.
- **Borrar**: el usuario puede borrar registros del conjunto de registros recuperados por la estructura de nodo.
- **Ejecutar**: el usuario puede ejecutar los elementos de tipo método y concepto definidos en la estructura de nodo.
- **Continua cascada**: el usuario decide si quiere detener la ejecución en cascada o no, habilitando el borrado de los nodos hijos cuando se detecten errores. Esto sólo tiene sentido a nivel de método y concepto.

En todos los casos anteriores, para que los permisos definidos sobre la estructura de nodo funcionen correctamente, será necesario que el usuario disponga de ese mismo permiso sobre los correspondientes elementos, así como sobre las tablas sobre las que se ha diseñado la estructura de nodo.

Permisos a nivel de elemento

El último nivel de permisos se puede conceder a nivel de elemento. En este caso se pueden conceder los siguientes permisos:

- **Lectura**: sólo se aplica sobre los elementos de tipo campo, concepto y propiedad. Si se activa este permiso, el usuario podrá leer el valor del elemento, siempre que se haya concedido permiso de lectura sobre la columna y la tabla de las cuales toma valor el elemento de la estructura de nodo.
- **Escritura**: sólo se aplica sobre los elementos de tipo campo, concepto y propiedad. Si se activa este permiso, el usuario podrá escribir o sobrescribir el valor del elemento (dependiendo de si se inserta un nuevo registro o se actualiza uno existente), siempre que se haya concedido permiso de escritura sobre la columna y tabla de las que toma valor el elemento de la estructura de nodo.

NOTA:
Por ejemplo, si se ha concedido permiso de borrado a nivel de estructura de nodo, pero no en todos los elementos de la estructura de nodo, el usuario no podrá borrar los registros de la estructura de nodo. Es preciso recordar que, ante un conflicto de permisos, el sistema siempre adoptará los permisos más restrictivos.

- **Borrar**: sólo se aplica sobre los elementos de tipo campo, concepto y propiedad. Como no es posible borrar el valor de un elemento de una estructura de nodo (sólo se pueden borrar registros completos), el gestor deberá comprobar que se ha concedido este permiso a todos los elementos de una estructura de nodo para la que se haya concedido permiso de borrado.
- **Ejecutar**: sólo se aplicará a elementos de tipo concepto o método.
- **Continua cascada**: sólo se aplicará a elementos de tipo concepto o método. Permite cortar la ejecución en cascada.

Se ha creado un elemento nuevo llamado *Métodos de sistema*, que recoge todos los métodos que tiene el sistema. A estos elementos se les puede asignar los mismos permisos que a los elementos de tipo método.

El **Editor de máscaras** presenta una serie de botones adicionales para la concesión de permisos sobre los nodos y las estructuras de nodo de un Meta4Object:

- **Aplicar todo**: aplica un perfil de seguridad definido a nivel de Meta4Object o nodo a todos los componentes y, en particular, a los elementos. Esta herramienta simplifica la tarea de asignar determinados permisos sobre la totalidad de los elementos de un Meta4Object.

- **Aplicar automáticamente**: tiene la misma función de propagación de permisos que la herramienta anterior, con la diferencia de que conserva los permisos previos que pueda haber a nivel de elemento.

NOTA:
Las opciones de edición y borrado de filtros aparecen activas únicamente cuando se asignan permisos a nivel de nodo.

- **Editar filtro**: concede acceso al Editor SQL para definir filtros de seguridad a nivel de nodo.
- **Editar filtro estándar como avanzado**: edita un filtro estándar como un filtro avanzado.
- **Borrar filtro**: borra un filtro existente definido a nivel de nodo.

Se podrán diseñar filtros de datos para cada uno de los nodos del Meta4Object.

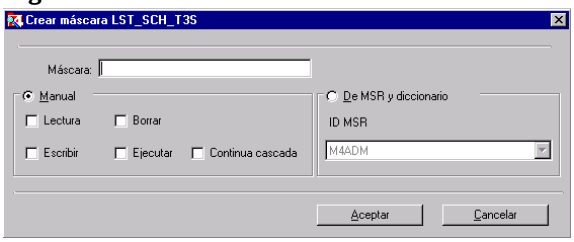
Los filtros permiten limitar los registros que se van a poder leer, borrar, actualizar o agregar al nodo. Definen unas condiciones sobre los elementos de la estructura de nodo, de forma que la máscara únicamente permite trabajar con los registros que cumplen esas condiciones.

Los filtros aplicables a nivel de nodo sólo se pueden definir comparando los valores de los elementos de tipo columna con valores constantes.

En el caso de que exista un filtro de seguridad definido sobre las tablas, a partir de las cuales se ha definido la estructura utilizada por el nodo, el sistema aplicará las condiciones indicadas en los dos filtros; es decir, se aplicarán los filtros definidos a nivel de tabla y de nodo.

Finalmente, desde la barra de herramientas general del **Editor de máscaras**, puede crear una nueva máscara con el botón **Nueva**. De este modo, se tiene acceso a la siguiente ventana:

Figura 19. Crear máscara



Seleccione la opción **Manual** para definir el nombre de la nueva máscara y asigne manualmente los permisos (Lectura, Escribir, Borrar, Ejecutar y Continua cascada) que, por defecto, se aplicarán a todos los componentes del Meta4Object al que está asociada la nueva máscara.

Por otra parte, al seleccionar la opción **De MSR y diccionario**, se puede definir una nueva máscara sobre el Meta4Object seleccionado, aplicando al Meta4Object los mismos permisos existentes sobre las tablas que lo componen. De este modo, es posible asegurar la coherencia en la concesión de permisos sobre tablas y Meta4Objects.

Se puede copiar un perfil de seguridad para un componente determinado del Meta4Object y aplicarlo a otros elementos mediante los botones **Copiar** y **Pegar**.

NOTA:
Los cambios introducidos no tendrán validez hasta que se haga clic en el botón **Guardar** de la barra de herramientas.

Seguridad desde las herramientas de diseño

Desde las herramientas de diseño, también se puede asignar seguridad a los componentes en tiempo de diseño:

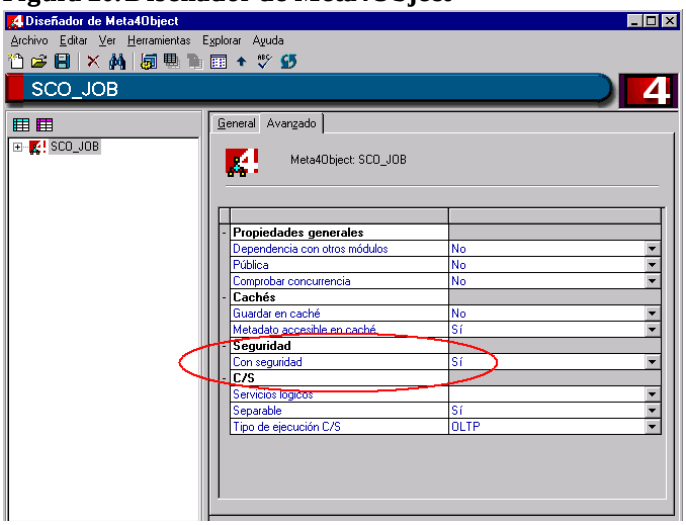
- **Diseñador de Meta4Object**: permite asignar seguridad a los Meta4Objects en tiempo de diseño.
- **Diseñador de modelos de datos**: permite asignar seguridad a tablas en tiempo de diseño.

Las herramientas de diseño son, en principio, independientes de la herramienta de seguridad. Sin embargo, como se verá más adelante, los módulos de diseño y de asignación de seguridad están conectados a un cierto nivel.

Seguridad a nivel de Meta4Objects

Es posible definir la seguridad a nivel de Meta4Objects, nodos, estructuras de nodo y elementos desde el **Diseñador de Meta4Object**, donde existe un apartado dedicado a la seguridad.

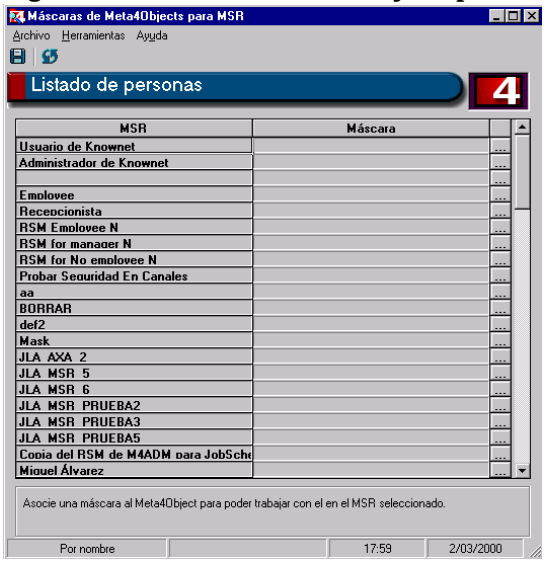
Figura 20. Diseñador de Meta4Object



Para asignar seguridad a un Meta4Object, compruebe primero que en la pestaña **Avanzado** esté activada la opción **Con seguridad**.

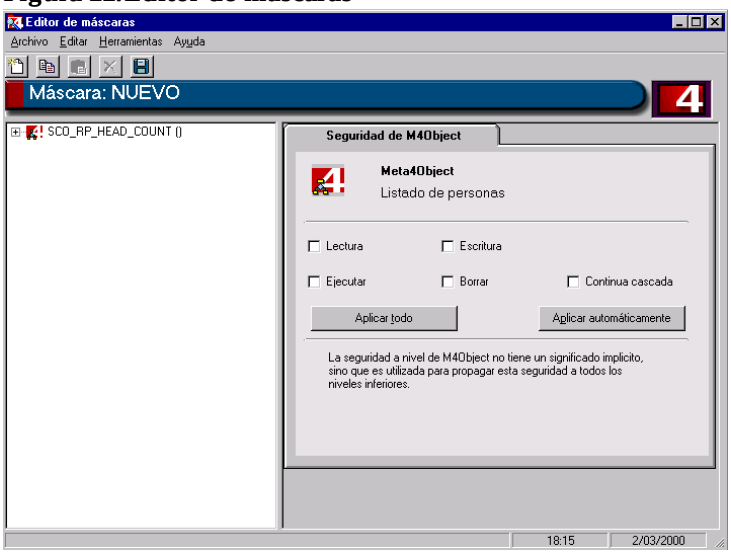
Una vez establecida la opción **Sí** en **Con seguridad** y guardados los cambios, se activa el botón **Ir a editor de seguridad** de la barra de herramientas. Al hacer clic, tendrá acceso a la ventana **Máscaras de Meta4Objects para MSR**. En esta ventana, a través de las correspondientes máscaras de seguridad, se pueden ver todos los MSRs existentes y su relación con el Meta4Object seleccionado.

Figura 21. Máscaras de Meta4Objects para MSR



Al hacer clic en el botón que hay junto a la columna **Máscara,** tendrá acceso a la ventana **Máscaras del Meta4Object**, desde donde puede abrir el **Editor de máscaras**.

Figura 22. Editor de máscaras



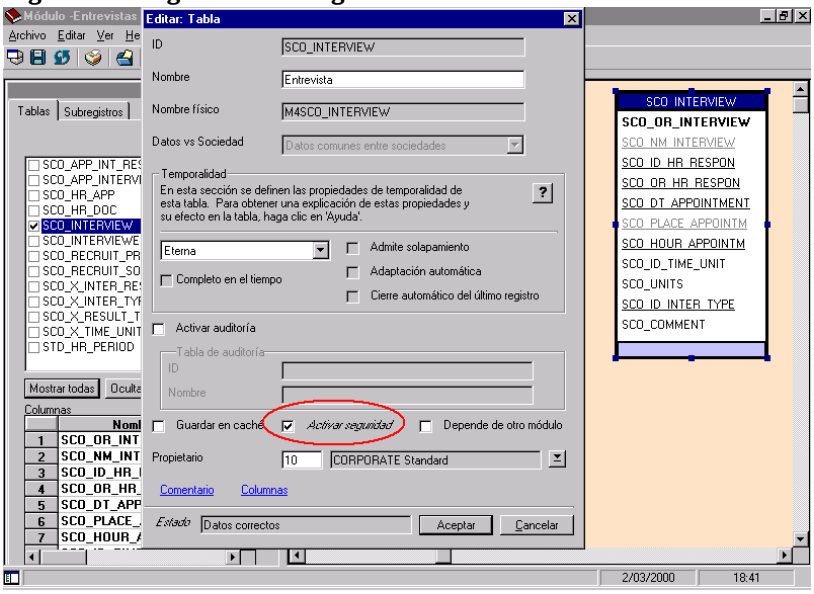
Desde el **Editor de máscaras**, se puede definir un perfil de seguridad para el Meta4Object que se está diseñando, así como para todos los componentes que lo integran, del mismo modo en que se hacía desde el Diseñador MSR.

Desde el **Diseñador de Meta4Object**, también pueden definirse tantas máscaras como se desee sobre un mismo Meta4Object; no obstante, al asignar permisos sobre tareas a un usuario mediante el Diseñador de roles de aplicación, no se podrá asignar más que una máscara a cada Meta4Object.

Seguridad a nivel de tablas

Es posible definir seguridad a nivel de tablas en tiempo de diseño desde la herramienta **Diseñador de modelos de datos**.

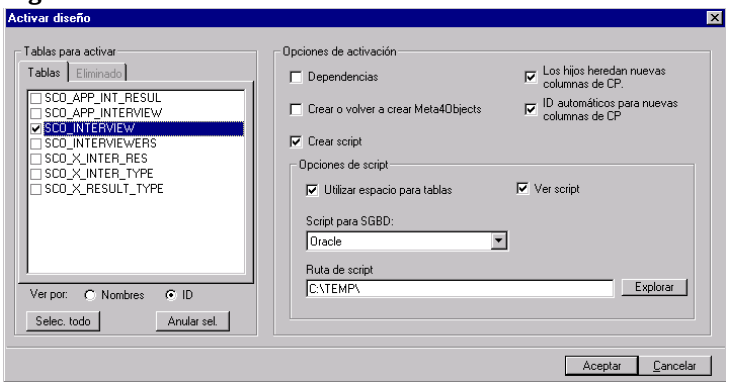
Figura 23. Asignación de seguridad desde el DMD



Una vez cargada o definida sobre el **Diseñador de modelos de datos** la tabla a la que se quiere asignar seguridad, habrá que comprobar que está marcada la propiedad **Activar seguridad** para esa tabla, al igual que se hacía con el Meta4Object en el apartado anterior.

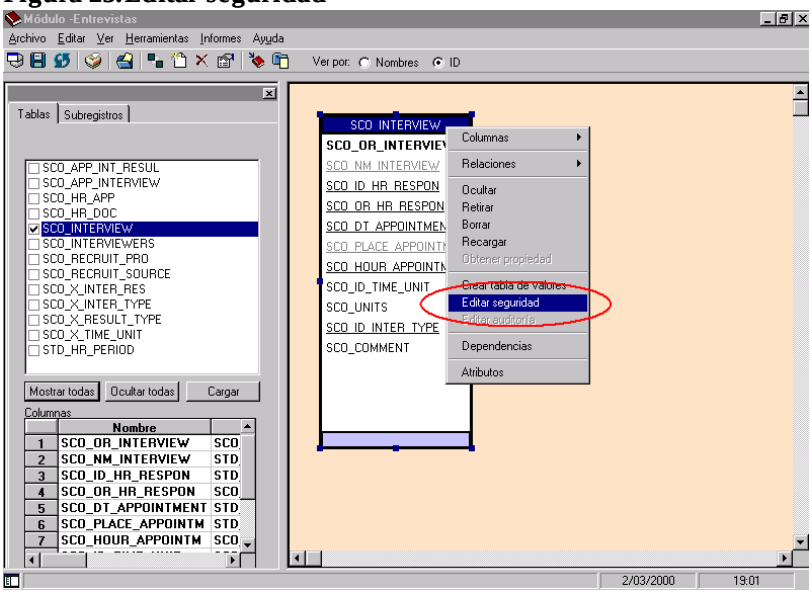
Para que la opción de asignación de seguridad para una tabla se active, es preciso transferirla al diccionario de datos. Para que esta operación se lleve a cabo, seleccione la opción **Herramientas|Activar diseño|Módulo** de la barra de menús, lo que hará que se abra la ventana **Activar diseño**.

Figura 24. Activar diseño



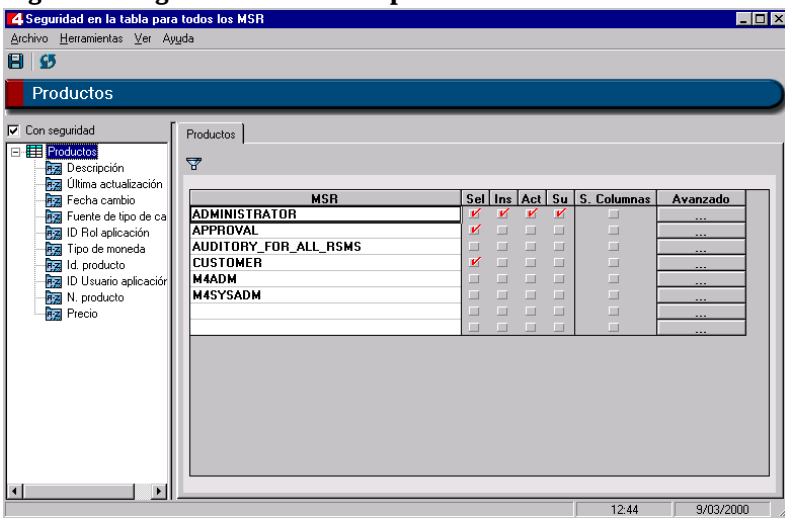
Una vez transferida la tabla al diccionario de datos, ya se está en condiciones de activar la opción de asignación de seguridad sobre ella. Para ello, seleccione la tabla, haga clic con el botón derecho del ratón y escoja la propiedad **Editar seguridad** de la lista que se despliega.

Figura 25. Editar seguridad



Al seleccionar la opción **Editar seguridad** asociada a la tabla a la que se quiere asignar seguridad, aparecerá en pantalla la ventana **Seguridad en la tabla para todos los MSRs**, en la que se muestran los permisos sobre la tabla y las columnas que la componen para todos los MSRs definidos.

Figura 26. Seguridad en la tabla para todos los MSRs



Sobre el formulario **Seguridad en la tabla para todos los MSRs**, similar al que aparece en el Diseñador MSR, es posible asignar permisos de selección, inserción, actualización y borrado sobre la tabla seleccionada y sobre las columnas que la integran, así como permisos a nivel de registro mediante el Diseñador de filtros. Las opciones de asignación de seguridad funcionan de manera similar a las que se describen en el apartado "Seguridad sobre tablas" del capítulo dedicado al Diseñador MSR.

Al igual que en la asignación de seguridad desde el Diseñador MSR, debe tenerse cuidado con la coherencia en la superposición de permisos sobre las entidades de diferente nivel: recuerde que, en caso de conflicto entre permisos, el programa aplicará la opción más restrictiva. Para que los cambios introducidos tengan validez, debe hacer clic en el botón **Guardar** de la barra de herramientas.

Mantenimiento de roles de aplicación

Esta herramienta, por superposición de permisos sobre los Meta4Objects que intervienen en la realización de cada tarea, permite definir roles de aplicación o perfiles de seguridad sobre tareas para determinados usuarios.

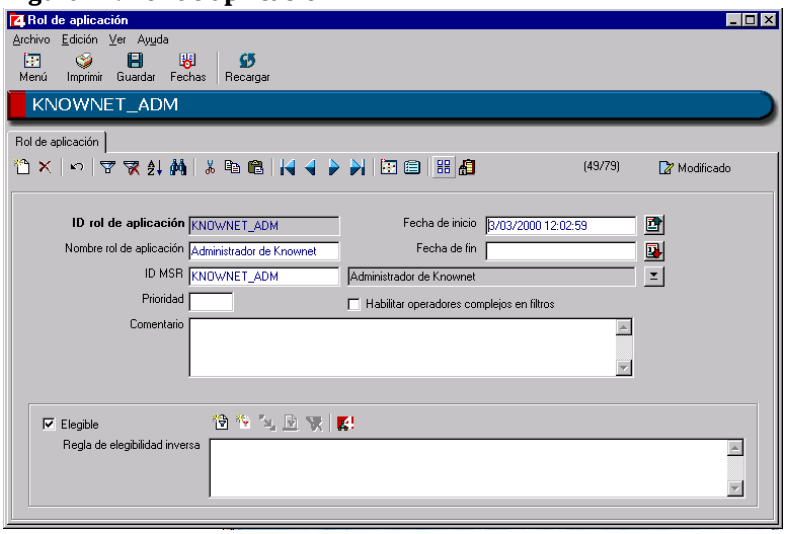
Se distinguen dos tipos de roles de aplicación:

1. Roles de aplicación fijos: se pueden asignar directamente a los usuarios.
2. Roles de aplicación por reglas de elegibilidad: se pueden aplicar por defecto a un usuario; por ejemplo, en función de la posición que ocupe en la empresa.

Este segundo tipo simplifica notablemente la tarea del mantenimiento de la seguridad, puesto que los permisos predefinidos se asignan de manera automática a un usuario con sólo introducir en el sistema sus datos de identificación.

Para tener acceso a esta herramienta, seleccione **Mind|Herramientas de desarrollo|Seguridad|Mantenimiento de roles de aplicación** en el panel de navegación de la aplicación.

Figura 27. Rol de aplicación



Desde esta ventana, se puede realizar el mantenimiento de los roles de aplicación existentes y crear otros nuevos.

Datos de un rol de aplicación

En la pestaña **Rol de aplicación**, se encuentran todos los datos necesarios para definir un rol de aplicación. En los cuadros de texto que contiene, se muestra la información del rol de aplicación seleccionado. Para desplazarse por los diferentes roles de aplicación, utilice la barra de navegación incluida en la barra de herramientas. También se indica el número de orden del rol de aplicación en el que se encuentra.

A continuación, se describen los elementos incluidos en el primer cuadro de grupo que contiene esta pestaña:

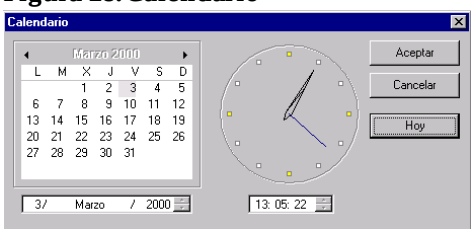
- **ID Rol de aplicación:** código identificativo del rol de aplicación.
- **Nombre rol de aplicación:** nombre del rol de aplicación.

NOTA:
MSR: modelo de sistema de roles.

- **ID MSR:** código identificativo del MSR asociado al rol de aplicación. Para ver la lista de MSRs disponibles, haga clic en el botón de selección que aparece a la derecha del grupo de remonte. Conviene recordar que se está estableciendo la seguridad a nivel de tareas, y que puede que dichas tareas necesiten tener acceso a datos de Meta4Objects. Para poder ejecutar la tarea, deberá disponer de permisos sobre los Meta4Objects a los que está asociada.

  El rol de aplicación recogerá permisos para ejecutar tareas, mientras que el MSR asociado recogerá los permisos sobre los modelos utilizados por la tarea.
- **Fecha de inicio:** fecha y hora de inicio del periodo de validez del rol de aplicación. Utilice el botón de calendario situado a la derecha del cuadro para introducir con mayor facilidad la fecha y hora que desee desde la ventana **Calendario**.
- **Fecha de fin:** fecha y hora de fin del periodo de validez del rol de aplicación. Al igual que en el caso anterior, utilice el botón de calendario que aparece a la derecha del cuadro para introducir con mayor facilidad la fecha y hora que desee.

Figura 28. Calendario



- **Prioridad**: este campo se utiliza para asignar prioridad a la ejecución de una tarea que esté asignada a varios roles; esto sólo tiene sentido cuando se trabaja en entorno JAVA.
- **Habilitar operadores complejos en filtros**: habilita los operadores complejos que aparecen en las ventanas de filtro.
- **Comentario**: comentario acerca del rol de aplicación

El segundo cuadro de grupo que contiene esta pestaña incluye la casilla de verificación **Elegible,** que se activa para asignar los permisos a los usuarios mediante los siguientes filtros y reglas de elegibilidad:

- **Nuevo filtro estándar**: haga clic en este botón para crear un nuevo filtro estándar o documentado.Tendrá acceso al **Editor de sentencias**.

- **Nuevo filtro avanzado**: si, por el contrario, hace clic en este botón, tendrá acceso al **Editor de filtros avanzados**. Al igual que el Editor de sentencias, éste es de gran utilidad para crear la sentencia SQL que determine los usuarios a los que afectará el rol de aplicación. A diferencia del filtro estándar, en el avanzado se escriben las sentencias de forma directa y no se comprueban posteriormente.

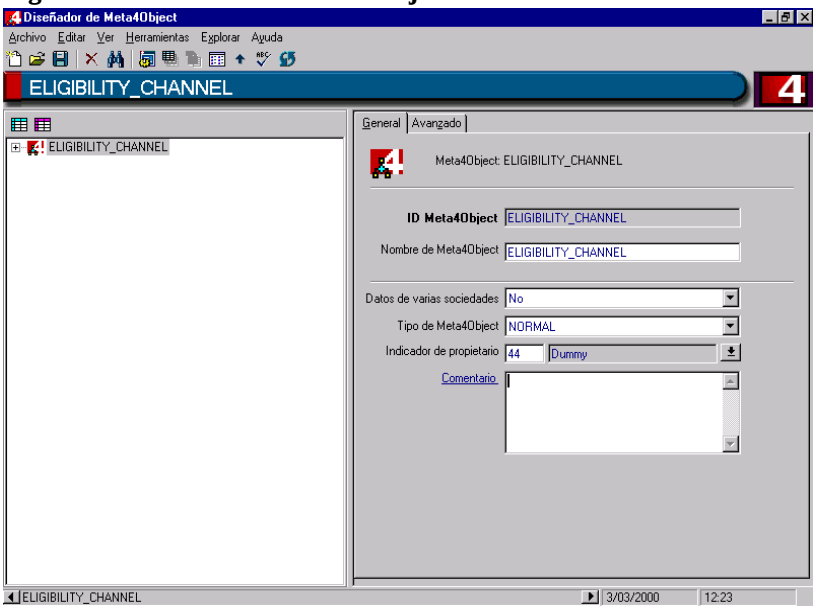
- **Convertir filtro**: haga clic en este botón para convertir un filtro estándar o documentado en un filtro avanzado o semidocumentado.

- **Editar filtro**: este botón permite editar la instrucción SQL que compone el filtro.

- **Borrar filtro**: marca el filtro para borrarlo.Tenga en cuenta que, al hacer clic en este botón, el filtro se borrará sin pedir previamente confirmación.

- **Acceso al Meta4Object de elegibilidad**: mediante este botón obtiene acceso al Meta4Object de reglas de elegibilidad. Gracias a la definición de este tipo de reglas, los usuarios tendrán una serie de privilegios y permisos de acceso en función del tipo de la actividad desarrollada, el grupo de trabajo, las tareas de la unidad, etc.

Figura 29. Diseñador de Meta4Object



Desde la barra de herramientas de la pestaña **Rol de aplicación**, puede crear un nuevo rol de aplicación, editar un rol, borrar uno existente y desplazarse por los diferentes roles de aplicación.

Creación de un rol de aplicación

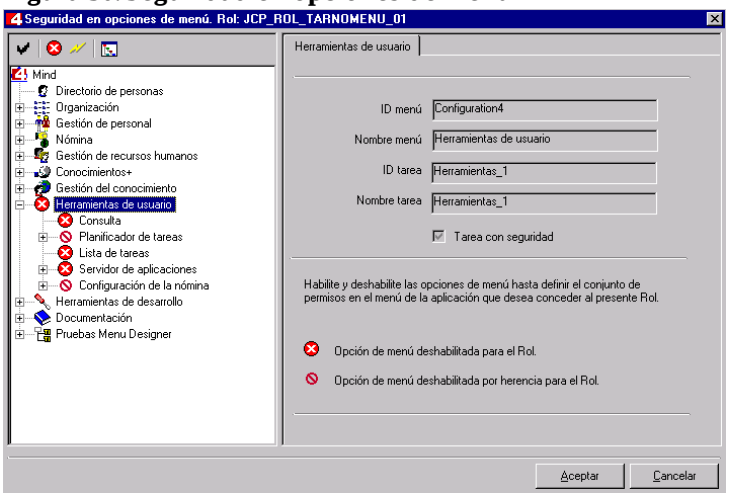
Para crear un rol de aplicación, siga estos pasos:

1. Haga clic en el botón **Nuevo** de la barra de herramientas de la pestaña **Rol aplicación**. Así se agrega un nuevo elemento a la lista de **roles de aplicación** existentes. Todos los datos se quedan en blanco para que se proceda a su definición.
2. Introduzca la información requerida en el cuadro de grupo que tiene la pestaña.
3. Si lo desea, puede hacer clic en los botones Seguridad en tareas de menú, Seguridad en tareas no asociadas al menú, Sociedades del rol u Opciones de programa para establecer seguridad a estos niveles.

Seguridad en opciones de menú

Si desea asignar seguridad en las opciones de menú, haga clic en el botón **Seguridad en tareas de menú** que se muestra al margen.

Figura 30. Seguridad en opciones de menú



Desde aquí puede habilitar o deshabilitar las opciones de menú hasta definir un conjunto de permisos en el menú de la aplicación Meta4Mind Set que desee conceder al rol.

La ventana contiene un árbol de menús, que es el que está asociado a ese rol cuando se inicia la aplicación. Moviéndose a través de ese árbol, puede realizar las siguientes operaciones:

- **Habilitar opción de menú**: habilita la opción de menú en la que se encuentre posicionado dentro del árbol de menús.

- **Deshabilitar opción de menú**: deshabilita la opción de menú en la que se encuentre posicionado dentro del árbol de menús.

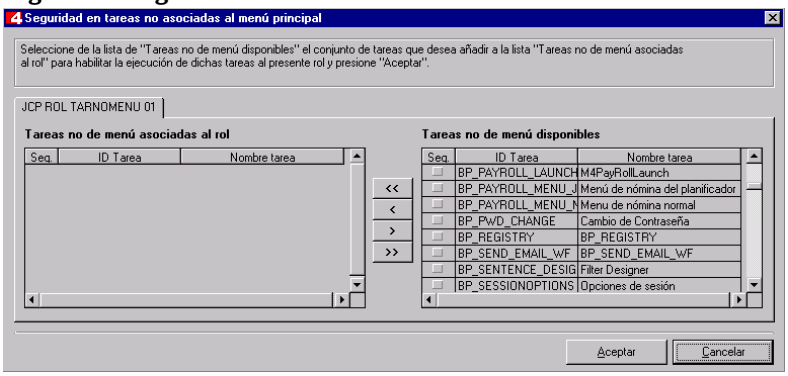
- **Deshabilitar todo el menú**: deshabilita todas las opciones que se encuentran en el árbol de menús.

- **Visualizar opciones de menú habilitadas**: muestra en el árbol de menús sólo las opciones que se encuentren habilitadas.

Seguridad en tareas no asociadas al menú

Para asignar seguridad a tareas que no se encuentren asociadas al menú, haga clic en el botón **Seguridad en tareas no asociadas al menú** que se muestra al margen.

Figura 31. Seguridad en tareas no asociadas al menú



Esta ventana se compone de dos cuadros: en el de la parte derecha se muestra una lista con las tareas disponibles no asociadas al menú, y en el cuadro de la parte izquierda se van mostrando las tareas que se habiliten para que las ejecute el rol. Para realizar esto, dispone de unos botones en la parte central que realizan las siguientes operaciones:

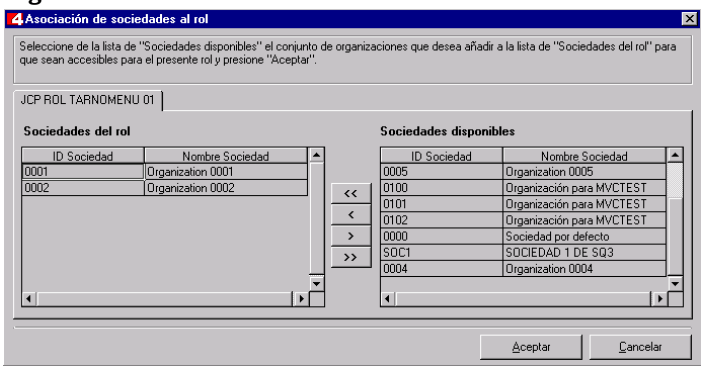
- **<<**: pasa todas las tareas disponibles al rol.
- **<**: pasa la tarea en la que esté posicionado al rol.
- **>**: pasa la tarea en la que esté posicionado del rol a la lista de tareas disponibles.
- **>>**: pasa todas las tareas del rol a la lista de tareas disponibles.

Todas las tareas no asociadas al menú poseen una columna **Seg.** que permite asignar seguridad a la tarea que se pasa al rol.

Asociación de sociedades al rol de aplicación

Si trabaja en un entorno societario, puede asignar sociedades a un rol de aplicación; haga clic en el botón **Sociedades del rol** que se muestra al margen.

Figura 32. Asociación de sociedades al rol



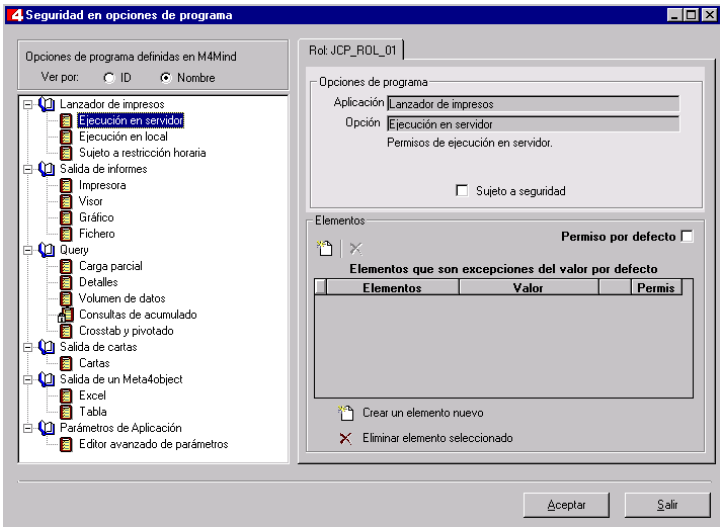
Esta ventana contiene dos cuadros; el de la derecha muestra una lista con las sociedades disponibles y en el otro cuadro se ven las sociedades por defecto que tiene asociadas ese rol. En la parte central aparecen unos botones que realizan las siguientes operaciones:

- **<<**: pasa todas las sociedades disponibles al rol.
- **<**: pasa la sociedad en la que esté posicionado al rol.
- **>**: pasa la sociedad en la que esté posicionado del rol a la lista de sociedades disponibles.
- **>>**: pasa todas las sociedades del rol a la lista de sociedades disponibles.

Seguridad en opciones de programa

Puede asignar o restringir permisos a opciones de programas de otros módulos de la aplicación como *Consulta*, *Informes*, etc. Para esto, haga clic en el botón **Opciones de programa** que se muestra al margen.

Figura 33. Seguridad en opciones de programa



La ventana contiene un árbol de navegación donde se muestran las opciones de programa y sus elementos. Para asignar seguridad, sitúese en la opción de programa y active la casilla de verificación **Sujeto a seguridad**. Para restringir la seguridad a los elementos especificados en el cuadro de texto **Elementos**, active la casilla de verificación **Permiso por defecto**.

Edición de un rol de aplicación existente

Para editar un rol de aplicación existente, siga estos pasos:

1. Utilice la barra de navegación de la barra de herramientas de la pestaña **Rol aplicación** para situarse en el rol de aplicación que desea editar.
2. Realice las modificaciones que considere oportunas, tanto en la definición del rol de aplicación como en la lista de tareas que va a incluir en él.
3. Guarde las modificaciones; para ello, haga clic en el botón **Guardar cambios** de la barra de herramientas o seleccione en el menú **Archivo** la opción **Guardar cambios**.

Borrado de un rol de aplicación existente

Para borrar un rol de aplicación existente, siga estos pasos:

1. Utilice la barra de navegación de la barra de herramientas de la pestaña **Rol aplicación** para situarse en el rol de aplicación que desea borrar.

2. Marque el rol de aplicación seleccionado. Para ello, haga clic en el botón **Borrar** de la barra de herramientas de la pestaña **Rol aplicación**. Aparecerá una ventana de confirmación de borrado.
3. Borre el rol de aplicación seleccionado. Para ello, haga clic en el botón **Guardar** de la barra de herramientas o seleccione la opción **Archivo|Guardar** de la barra de menús.

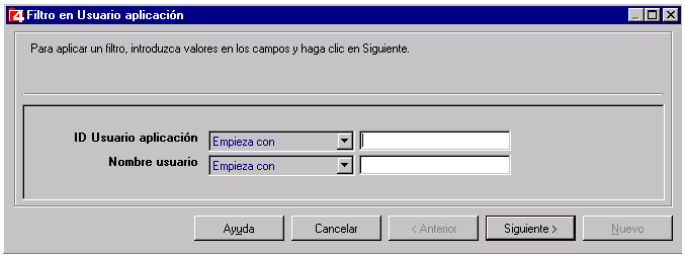
Mantenimiento de usuarios de aplicación

Para tener acceso a esta herramienta, seleccione **Mind | Herramientas de desarrollo | Seguridad | Mantenimiento de usuarios de aplicación** del panel de navegación situado en la parte izquierda de la aplicación Meta4Mind Set.

Aparece un formulario de filtro por usuario que le permite seleccionar el usuario que desea cargar de acuerdo con los siguientes parámetros:

- **ID Usuario aplicación:** código identificativo del usuario de la aplicación.
- **Nombre usuario:** nombre del usuario de la aplicación.

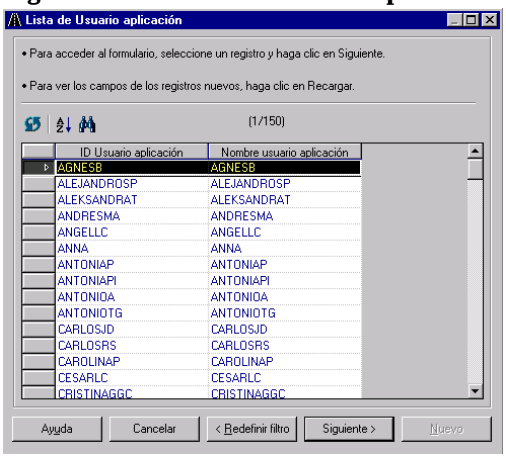
Figura 34.Filtro en usuario aplicación



Una vez completados los campos con el usuario que desea cargar, haga clic en **Siguiente>**. Si no desea realizar un filtrado de usuarios, deje en blanco el formulario y haga clic en **Siguiente>**. Aparecerá la lista de usuarios que cumplen los criterios especificados en el filtro. Si no especifica ningún criterio, incluirá la lista de todos los usuarios de la aplicación. En dicha lista, se especifican el código identificativo y el nombre de los usuarios que van a cargarse.

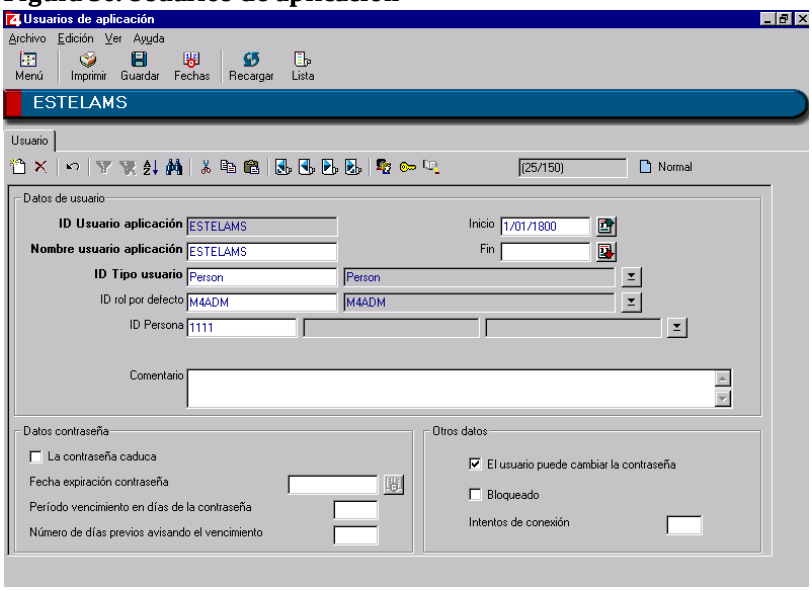
En la lista de usuarios, seleccione aquél que desee ver al abrir la herramienta. Para ello, utilice la barra de desplazamiento vertical que aparece en la parte derecha del formulario, o bien seleccione directamente el usuario haciendo clic en él.

Figura 35. Lista de usuarios de aplicación



A continuación, aparece la ventana principal de Usuarios de aplicación.

Figura 36. Usuarios de aplicación



NOTA:
La asignación de permisos mediante reglas de elegibilidad simplifica enormemente la administración de la seguridad: los permisos de un usuario cambiarán de forma dinámica y transparente para el gestor a medida que varíe la situación del empleado.

Esta herramienta le permite definir parámetros de seguridad a nivel de usuario de la aplicación. Además de una serie de parámetros básicos, como el nombre de usuario y la contraseña de acceso, el administrador del sistema dispone de un conjunto de opciones avanzadas; por ejemplo, la asignación de permisos derivados de las reglas de elegibilidad, que simplifican notablemente la gestión de la seguridad a nivel de usuario.

Desde la barra de herramientas tiene acceso a diferentes botones que le permiten realizar las operaciones que se explican a continuación.

Creación de un usuario de aplicación

Para dar de alta a un usuario determinado, haga clic en el botón **Nuevo**. Para definir un nuevo perfil de usuario, deben determinarse los datos básicos del usuario:

- **ID Usuario aplicación**: código identificativo del usuario del sistema.
- **Nombre usuario aplicación**: nombre con el que el usuario va a tener acceso a la aplicación. Puede coincidir con el anterior.
- **ID Tipo usuario:** código identificativo del tipo de usuario, que puede ser, entre otros, una persona (*Person*) o un usuario de sistema (*System*). Selecciónelo de la lista que se despliega al hacer clic en el botón de selección del grupo de remonte.
- **ID Rol por defecto**: perfil de seguridad de usuario o rol de aplicación por defecto entre los definidos desde el Diseñador de roles de aplicación. Selecciónelo también de la lista que se despliega al hacer clic en el botón de selección del grupo de remonte.
- **ID Persona:** código identificativo del usuario del sistema. Selecciónelo de la lista que se despliega con el nombre y el apellido del usuario al hacer clic en el botón de selección del grupo de remonte.

NOTA:
Mediante los periodos de validez de usuarios, se pueden gestionar las situaciones que surgen al contratar a trabajadores temporales, trabajadores externos, etc., que necesitan utilizar Meta4Mind Set.

- **Inicio:** fecha de inicio de validez del perfil de usuario definido, que generalmente coincide con la fecha de alta de dicho usuario en el sistema.
- **Fin:** fecha de fin de validez del perfil de usuario definido. Por defecto, el sistema asigna a este campo la fecha 1/1/4000, pero es posible modificarla (por ejemplo, para usuarios temporales del sistema).
- **Comentario**: puede escribir un breve comentario acerca del usuario.

Una vez determinados los datos básicos del usuario, defina desde el cuadro de grupo **Datos contraseña** los parámetros de seguridad propiamente dichos, con información relativa a la contraseña de acceso y otras propiedades de la sesión:

- **La contraseña caduca**: casilla de verificación que se activa si la contraseña establecida tiene un periodo de validez limitado.
- **Fecha expiración contraseña**: fecha de finalización del periodo de validez de la contraseña.
- **Periodo vencimiento en días de la contraseña**: indica cada cuántos días debe actualizar la contraseña el usuario.

- **Número de días previos avisando el vencimiento**: número de días con antelación a la fecha de vencimiento de la contraseña en la que se avisa al usuario de la finalización del periodo de validez de la misma.

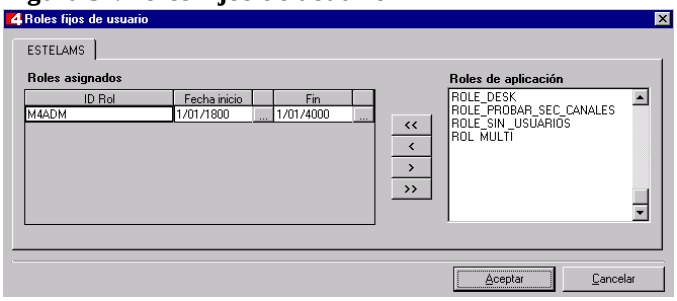
El cuadro de grupo **Otros datos** contiene la información relativa a otras propiedades de la sesión:

- **El usuario puede cambiar la contraseña:** casilla de verificación que se activa si el usuario tiene la posibilidad de cambiar su contraseña de acceso.
- **Bloqueado:** casilla de verificación que se activa cuando se supera el límite de intentos de conexión. Sólo la puede desactivar el administrador del sistema.
- **Intentos de conexión:** número de intentos de conexión consecutivos que el usuario puede realizar, en caso de introducir una contraseña errónea, hasta bloquear la aplicación, lo que impedirá su acceso. En caso de bloqueo, se activará la casilla de verificación **Bloqueado** y sólo el administrador podrá dar acceso a ese usuario.

Asignación de roles fijos a un usuario

El botón **Roles fijos** es la herramienta de asignación de perfiles fijos de seguridad a un usuario concreto.

Figura 37.Roles fijos de usuario



En la ventana **Roles fijos de usuario**, aparecen dos cuadros:

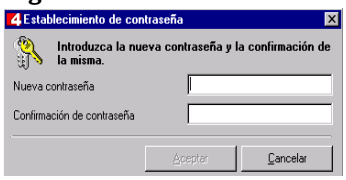
- **Roles asignados**: perfiles fijos asignados al usuario.
- **Roles de aplicación**: perfiles de usuario o roles de aplicación predefinidos que pueden asignarse a un usuario concreto.

Los botones de flecha centrales permiten pasar los roles de aplicación hacia el cuadro de roles asignados y viceversa.

Establecimiento de una nueva contraseña

El botón **Nueva contraseña** permite establecer un nuevo código de acceso a la aplicación para el usuario.

Figura 38. Establecimiento de contraseña



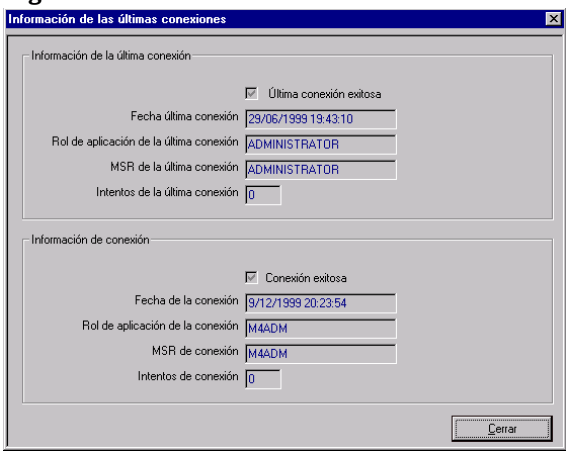
En el formulario **Establecimiento de contraseña**, aparecen dos campos:

- **Nueva contraseña:** escriba su nueva clave de acceso.
- **Confirmación de contraseña:** repita la clave introducida anteriormente; si coincide con la anterior, se activará el botón **Aceptar**. En caso contrario, borre lo escrito y repítalo.

Información de la conexión del usuario

El botón **Información de conexión** le ofrece la posibilidad de revisar toda la información referente a las últimas conexiones del usuario.

Figura 39. Información de conexión



En este formulario, aparecen dos nuevos cuadros de grupo:

- **Información de la última conexión**: datos correspondientes a la última vez que se tuvo acceso.
  - **Última conexión exitosa**: casilla de verificación que se activa si se pudo realizar la conexión.
  - **Fecha última conexión**: fecha de la última vez que se tuvo acceso.
  - **Rol de aplicación de la última conexión**: tipo de rol con el que se pudo conectar.
  - **MSR de la última conexión:** modelo de sistema de roles con el que se tuvo acceso en la última conexión.
  - **Intentos de conexión de la última conexión:** número de intentos que fueron necesarios para entrar la última vez.
- **Información de la conexión**: información sobre la conexión actual.
  - **Conexión exitosa**: casilla de verificación que está activa si la conexión se realizó correctamente.
  - **Fecha de la conexión**: fecha del acceso actual.
  - **Rol de aplicación de la conexión**: tipo de rol con el que se ha tenido acceso.
  - **MSR de conexión:** modelo de sistema de roles con el que se ha tenido acceso.
  - **Intentos de conexión:** número de intentos necesarios hasta que se consiguió conectar satisfactoriamente.

Borrado de un usuario de aplicación

Para borrar un usuario de aplicación existente, siga estos pasos:

1. Utilice la barra de navegación de la barra de herramientas para situarse en el usuario de aplicación que desee borrar.

2. Marque el usuario de aplicación seleccionado. Para ello, haga clic en el botón **Borrar** de la barra de herramientas de la pestaña **Usuario**.
3. Para borrar el usuario de aplicación marcado, haga clic en el botón **Guardar** de la barra de herramientas o seleccione la opción **Archivo|Guardar** de la barra de menús.

Rol de aplicación por defecto

Al iniciar Meta4Mind Set, aparece en primer lugar un formulario de acceso, junto a los campos para el nombre de usuario y la contraseña de acceso. También aparece la casilla de verificación **Rol de aplicación por defecto**, que se activa para asignar dicho perfil de seguridad al usuario cuando éste obtiene acceso a la aplicación.

Figura 40. Formulario de acceso

Si no se activa dicha casilla de verificación, se obtendrá acceso a un segundo formulario de conexión.

Figura 41. Selección del rol de aplicación

Este formulario permite seleccionar el perfil de usuario de una lista en la que aparecen los perfiles de usuario o roles de aplicación fijos, definidos para un usuario determinado, junto a los perfiles asignados al mismo como consecuencia de las reglas de elegibilidad.