# O3 Security

Manual de uso de O3 Security 7.x


El esquema de seguridad de O3 BI se basa en la definición de roles sobre los cuales se asignan accesos y permisos. A su vez se definen usuarios, los cuales se asignan a los roles, adquiriendo de esta forma los accesos y permisos requeridos. Este esquema de seguridad permite definir el acceso y permisos una vez sola a nivel de roles simplificando la administración del mismo.

***O3 BI*** ofrece dos mecanismos de autenticación: un mecanismo de seguridad propio basado en un repositorio de seguridad incluido en la instalación por defecto, o la posibilidad de integrarse a un esquema LDAP (Lightweight Directory Access Protocol).

En el caso del mecanismo de seguridad propio, la información de seguridad reside en un repositorio que está alojado en una base de datos, permitiendo que los diferentes componentes de ***O3 BI*** compartan el mismo esquema de seguridad. Por ejemplo, las definiciones de seguridad que controlan el acceso a Cubos también se utilizan para controlar el acceso a Tableros de Control, Reportes, ePortal. En este caso para administrar la seguridad se utiliza ***O3 Security*** para definir el esquema en forma integrada.

En el caso de LDAP, las definiciones de seguridad residen en un servidor LDAP. Las definiciones de usuarios y roles se realizan desde un cliente LDAP y ***O3 Security*** se utiliza para configurar los parámetros de acceso al servidor LDAP y definir los accesos y permisos sobre los componentes de ***O3 BI***.

Es importante considerar que para poder utilizar un esquema de seguridad compartido es necesario que todos los componentes de ***O3 BI*** es tén publicados en un ***O3 Server***.

Este manual se divide en las siguientes secciones:



**Acceso a O3 Security**

| **Acceso a O3 Security** |
| --- |
| Interfaz Web para O3 Security 7 |

**Administración de Usuarios**

| **Administrando Usuarios en O3 Security** |
| --- |
| Mantenimiento de Usuarios, asignación de roles, atributos del usuario, password |

**Administración de Roles**

| **Administrando Roles en O3 Security** |
| --- |
| Mantenimiento de Roles de O3BI Server |

**Administración de Grupos**

| Administrando Grupos en O3 Security |
| --- |
| Mantenimiento de Grupos de O3BI Server |

**Administrando Permisos**

| Administrando Permisos en O3 Security |
| --- |
| Mantenimiento de Permisos sobre componentes de O3 BI |

**Usuarios y Roles en LDAP**

| Usuarios y Roles en LDAP |
| --- |
| Las definiciones de usuarios y roles en este caso se realizan con las herramientas de LDAP que se utilizan normalmente. Se detallan las características que deben cumplir los usuarios y roles creados en el servidor LDAP para que puedan ser utilizados por O3 Server. |

# Acceso a O3 Security

Interfaz Web para O3 Security 7

## Cómo acceder a la interfaz Web de segiridad de O3 BI ?

Para acceder al componente O3 Security se deben tener iniciados todos los servidores de O3 BI.

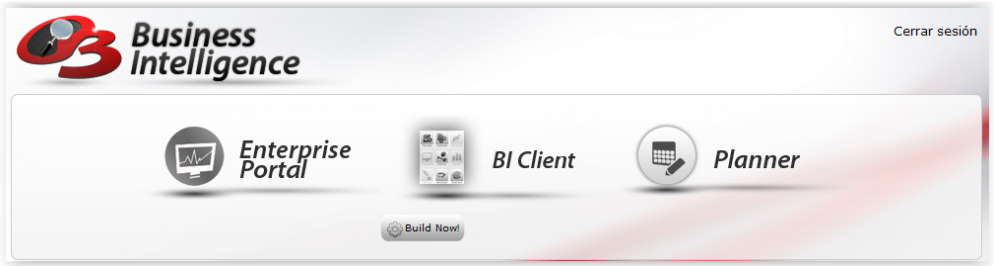
En **BI Client** se encontrará el componente **O3 Security**.

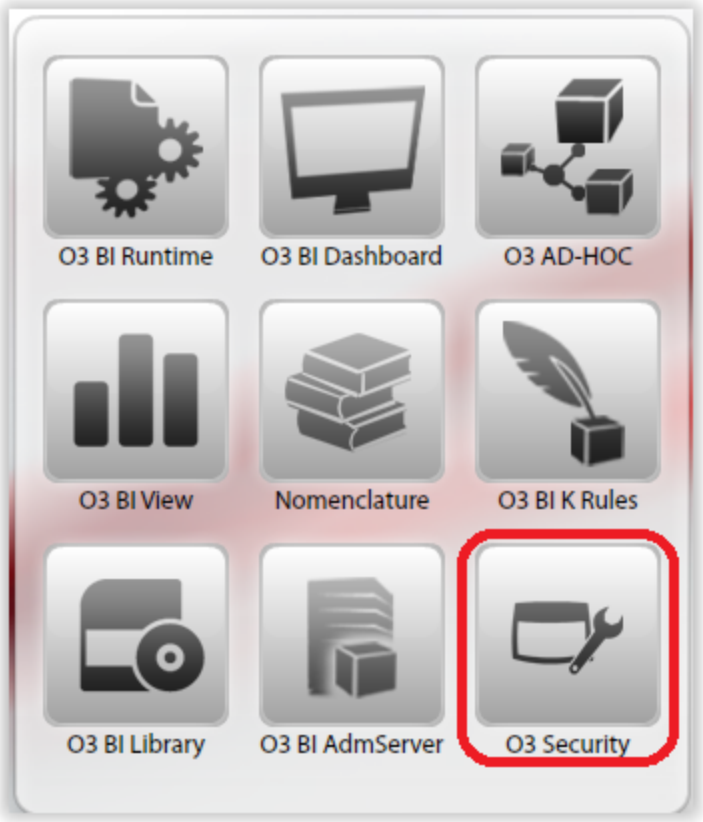
### Acceso a O3 Security

Para acceder a los componentes de seguridad, se debe autenticar con un usuario administrador.  En la instalación original de O3 BI, estos componentes están disponibles para el usuario **admin** de O3 BI.

Paso 1: ingresar a http://<servidorO3>:8080/o3web

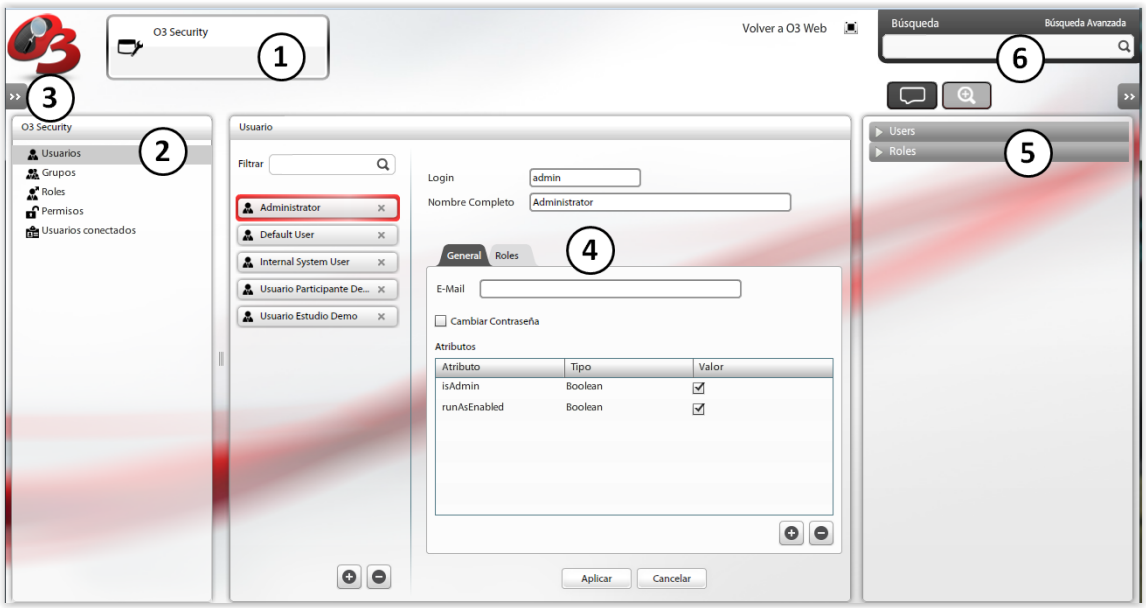
Paso 2: acceder al componente






O3 Security ofrece las funcionalidad de definición de usuarios, roles y permisos de acceso a los distintos componentes de análisis.

**Espacio de trabajo**




1. Ubicación actual. Indica el componente sobre el que se está navegando.
2. Panel de opciones. Presenta los distintos niveles de seguridad y usuarios conectados
3. Volver al menú principal del O3 BI Client. Haciendo click en las flechas  en el ángulo superior izquierdo de la pantalla y debajo del logo de O3 BI, se despliega el menú principal del O3 BI Client. A partir de allí es posible navegar hacia otro componente.
4. Panel central, presenta opciones según el contexto seleccionado en el Panel de Opciones (**2**).
5. Panel de búsquedas. Se puede ocultar con el botón disponible en la parte superior de éste panel. 
6. Búsqueda avanzada.

La forma de uso de la nueva interfaz web requiere la selección de una opción o elemento en el panel de opciones (**2**), la consulta o

modificación de su definición en el panel central (**4**) eventualmente con el uso de búsquedas y ayudas (**5**).

El botón  en el ángulo superior derecho, a la izquierda de la búsqueda avanzada, permite cambiar el modo de visualización a pantalla completa. Este modo desactiva el teclado. Para volver a la pantalla normal, se presiona el botón nuevamente o presionando <*esc*> en su teclado.

# Administrando Grupos en O3 Security

O3 BI Security 7.x
Mantenimiento de Grupos de O3BI Server

Con el objetivo de reflejar en O3 Server un esquema de seguridad similar al utilizado a nivel de sistemas operativos, también es posible definir grupos de usuarios en O3 Server. El uso de grupos aumenta la complejidad del esquema de seguridad y para esquemas de seguridad simples es posible obviar el uso de grupos. Las actividades de administración de grupos incluyen el agregar grupos y agregar usuarios a un grupo.

- Agregar Grupos
- Relacionar Usuarios a Grupos

## Agregar y Eliminar Grupos

Para agregar grupos:

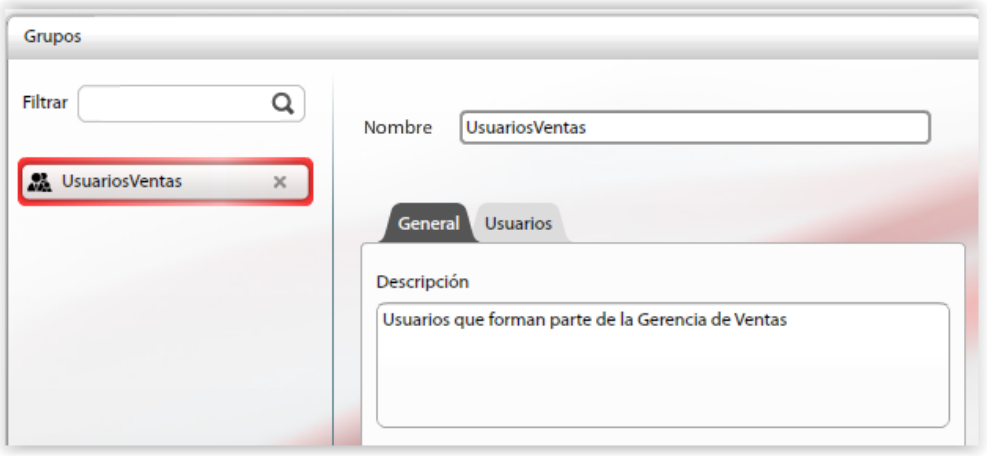
1. Posicionarse en el Panel O3 Security en Grupos 

2. Seleccione el boton del símbolo de más en la parte inferior del panel de Grupos 
3. Ingrese un Nombre, debe ser sin espacios, el mismo sistema no le permite.
4. Puede ingresar una descripción para identificar el Grupo.
5. Haga click en el botón Aplicar.

Para eliminar grupos:

1. Posicionarse en el Panel O3 Security en Grupos 

2. Seleccione el grupo a eliminar.
3. Seleccione el boton del símbolo de menos en la parte inferior del panel de Grupos  . También puede realizar la operación haciendo click sobre la **x** a la derecha del nombre del Grupo.
4. Haga click en el botón Aplicar



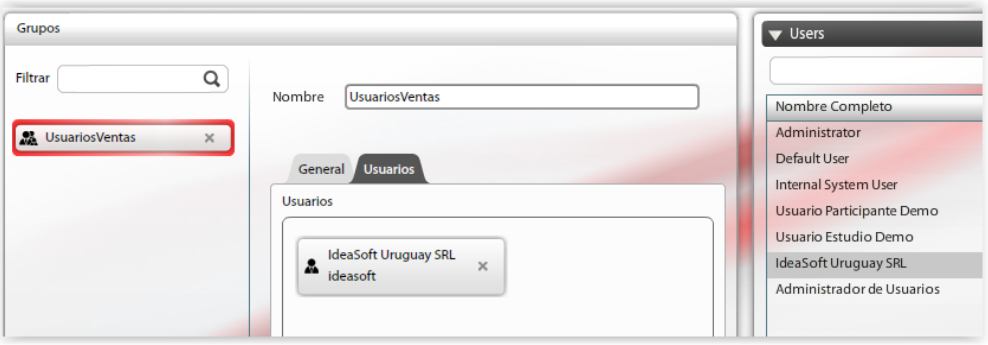

### Relacionar Usuarios a Grupos

**Relacionar Usuarios a un Grupo:**

1. Seleccione el elemento Grupos en el Panel de O3 Security.
2. Seleccione el grupo al cual quiere agregar o actualizar usuarios, en la sección derecha del Panel de Grupos.
3. Seleccione la pestaña de Usuarios.
4. Desde el Panel de Búsqueda (izquierda), seleccionar el usuario a agregar y arrastralo hasta la ventana de Usuarios.
5. Repetir el paso 2 por cada Usuario a agregar
6. Haga click en el botón Aplicar para confirmar los cambios realizados.

**Eliminar Usuarios de un Grupo:**

1. Seleccione el elemento Grupos en el Panel de O3 Security.
2. Seleccione el grupo al cual quiere agregar o actualizar usuarios, en la sección derecha del Panel de Grupos.
3. Seleccione la pestaña de Usuarios.
4. Haga click en la **x** a la derecha del nombre del usuario.
5. Haga click en el botón Aplicar para confirmar los cambios realizados.




# Administrando Permisos en O3 Security

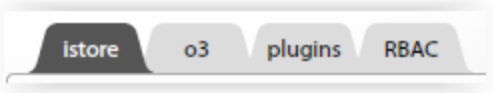
O3 BI Security 7.x
Mantenimiento de Permisos sobre componentes de O3 BI

En forma adicional a la definición de accesos y restricciones sobre cubos, puede ser necesario también definir permisos sobre los diferentes componentes analíticos guardados en el servidor como ser modelos, reglas, expresiones, vistas, etc., así como componentes que ofrecen funcionalidades especificas de la plataforma de BI.

La administración de permisos sobre las vistas difiere a la de los componentes anteriores debido a la integración que se requiere con los cubos y a la forma en que los usuarios pueden ir creando, mejorando y compartiendo las vistas. Así mismo para plugins y RBAC.

La administración de Permiso sobre componentes de O3 BI abarca las siguientes tareas:

- Permisos sobre istore
- Permisos sobre o3
- Permisos sobre plugins
- Permisos sobre RBAC




## Permisos sobre istore

Sobre los Tableros, Modelos, Reglas, Acciones, Escritorios, Consultas, Reportes, Simulaciones y Expresiones se aplican las definiciones de acceso y restricciones sobre los cubos que utilizan, pero puede ser necesario por ejemplo limitar a los usuarios para que no puedan modificar o ver determinados componentes.

Se pueden asignar permisos para *Listar*, *Escribir* y *Leer* sobre estos componentes.

Al igual que con los cubos, la asignación de estos **permisos se realiza sobre roles** y los usuarios actores de cada rol adquieren indirectamente los permisos. Es importante considerar que únicamente se puede asignar permisos a aquellos componentes que están guardados en O3 Server (istore).

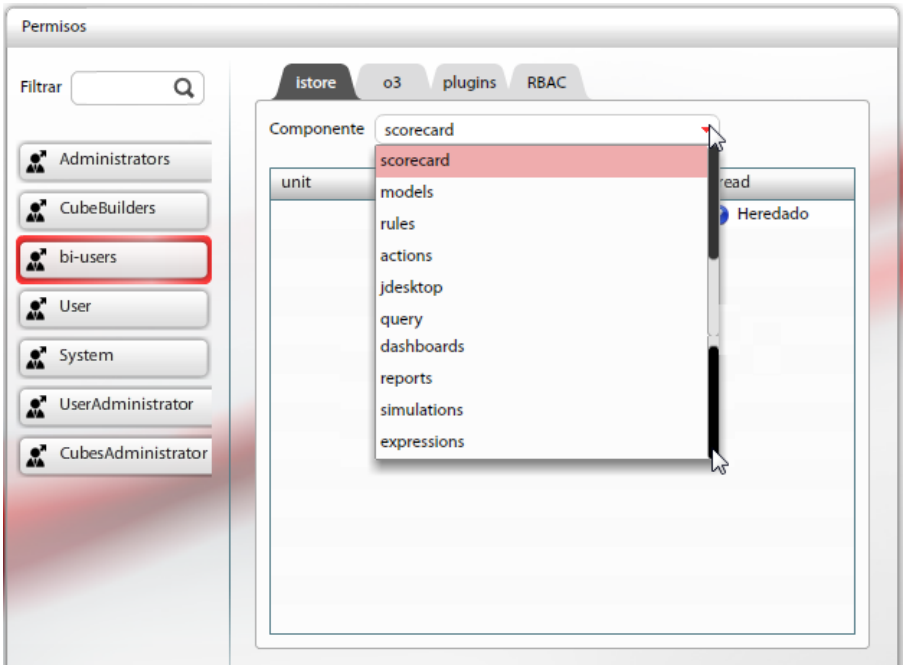
Es posible también asignar permisos sobre componentes a un rol en forma general o particular. Por ejemplo se puede asignar permisos a un rol para *Leer* por defecto todos los reportes definidos y únicamente asignar permisos para *Escribir* sobre un reporte en particular para que los usuarios lo mejoren.

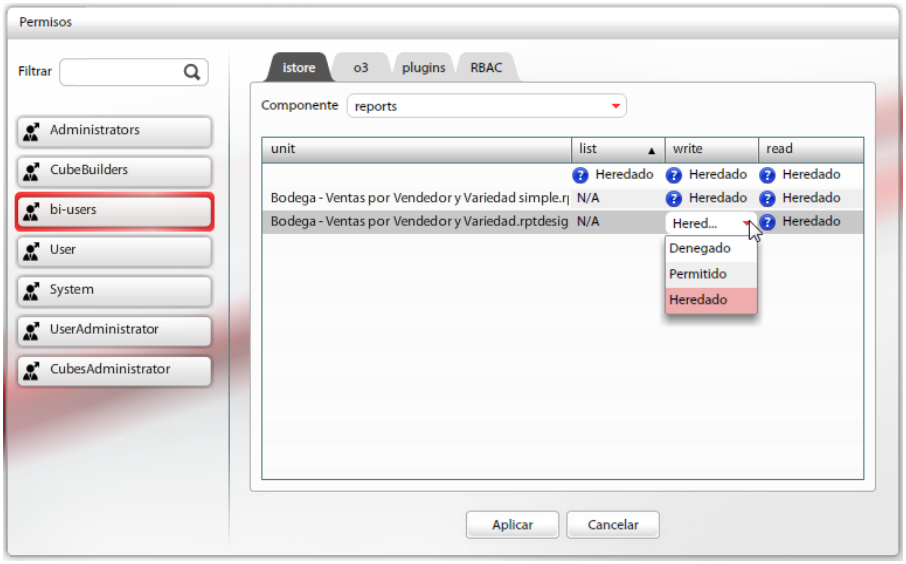
Para asignar permisos en forma general el primer ítem de la lista de componentes siempre es *el Repositorio* (está en blanco), este ítem especial no corresponde a ningún componente específico y se utiliza para asignar los permisos que por defecto heredan los restantes componentes de la lista.

Por defecto cuando se graba por primera vez un componente en O3 Server este hereda los permisos para *Listar*, *Escribir* y *Leer* definidos en el primer ítem *Repositorio* de cada rol. A su vez por defecto este ítem *Repositorio* también queda configurado con el valor *Heredado* e implica que todos los usuarios actores del rol tendrán permisos totales sobre los componentes del tipo seleccionado.


Para asignar permisos sobre componentes a un rol:

1. Seleccione *Permisos* del Panel de Propiedades.
2. Seleccione del Panel de Permisos el rol al cual quiere asignar permisos.
3. Seleccione el Componente de la lista desplegable *Componente* de la pestaña *istore*, por ejemplo *reports*.
4. Seleccione la Unidad a la cual desea asignar y/o modificar permisos, de la lista "unit"
5. Para asignar permisos sobre el componente seleccionado de la lista es necesario cambiar los valores de las columnas *Listar*, *Escribir* y *Leer*. Los valores se indican en forma independiente y por defecto cada componente queda configurado con valores *Heredado*. Los valores posibles para asignar permisos son los siguientes:
    a. **Denegado**, los usuarios actores del rol seleccionado se les denegara el permiso correspondiente a la columna.
    b. **Permitido**, los usuarios tendrá el permiso correspondiente a la columna.
    c. **Heredado**, el permiso quedara determinado por el valor del primer ítem de la lista, *Repositorio*. Asignando el valor *Heredado* es como se asignan permisos a todos los componentes para un rol determinado.
6. Haga click sobre el botón Aplicar para confirmar los cambios.




## Permisos sobre o3

Aplicar permisos sobre el repositorio de Vistas, así como permitir el acceso a los componentes de O3 BI Client

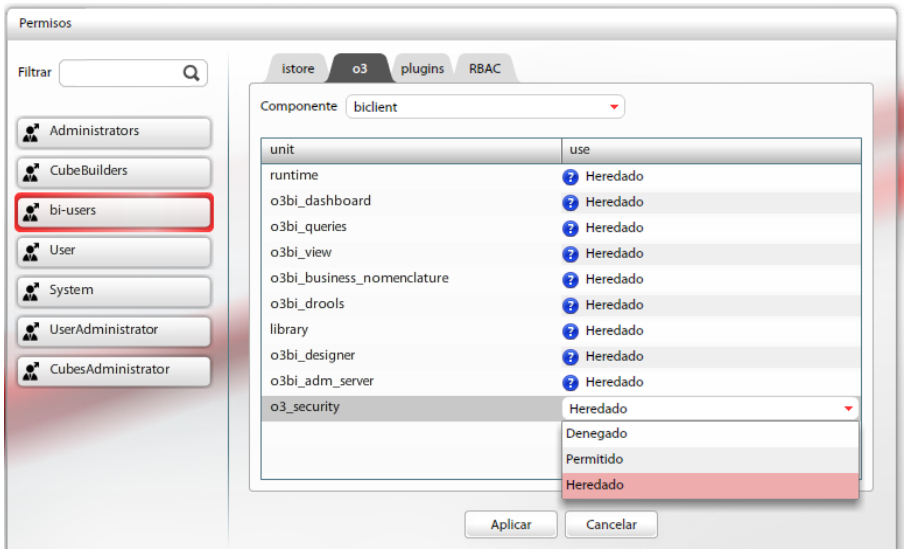

Para asignar permisos sobre el **repositorio de vistas**:

1. Seleccione *Permisos* del Panel de Propiedades.
2. Seleccione del Panel de Permisos el rol al cual quiere asignar permisos.
3. Seleccione la pestaña *o3*.

4. Seleccione el Componente *view* de la lista desplegable de *Componente*.
5. Para asignar o cambiar permisos de escritura es necesario cambiar los valores de las columnas *Public*, *Role* y *Private*, correspondientes a los distintos repositorios de vistas. Los valores se indican en forma independiente y por defecto cada repositorio queda configurado con valores *Heredado*. Los valores posibles para asignar permisos son los siguientes:
    a. **Denegado**, los usuarios actores del rol seleccionado se les denegará el permiso de grabar en el repositorio indicado.
    b. **Permitido**, los usuarios podrán grabar en el repositorio indicado.
    c. **Heredado**, asignando el valor *Heredado* es como se asignan permisos de poder grabar a todos los repositorios de vistas para un rol determinado.
6. Haga click sobre el botón Aplicar para confirmar los cambios.


Para asignar permisos sobre el **componentes del BI Client**:

1. Seleccione *Permisos* del Panel de Propiedades.
2. Seleccione del Panel de Permisos el rol al cual quiere asignar permisos.
3. Seleccione la pestaña *o3*.
4. Seleccione el Componente *biclient* de la lista desplegable de *Componente*.
5. Para asignar o cambiar permisos de acceso es necesario cambiar los valores de la columna *use*. Los valores se indican en forma independiente y por defecto queda configurado con valores *Heredado*. Los valores posibles para asignar permisos son los siguientes:
    a. **Denegado**, los usuarios actores del rol seleccionado se les denegará el permiso de grabar en el repositorio indicado.
    b. **Permitido**, los usuarios podrán grabar en el repositorio indicado.
    c. **Heredado**, asignando el valor *Heredado* es como se asignan permisos de poder grabar a todos los repositorios de vistas para un rol determinado.
6. Haga click sobre el botón Aplicar para confirmar los cambios.

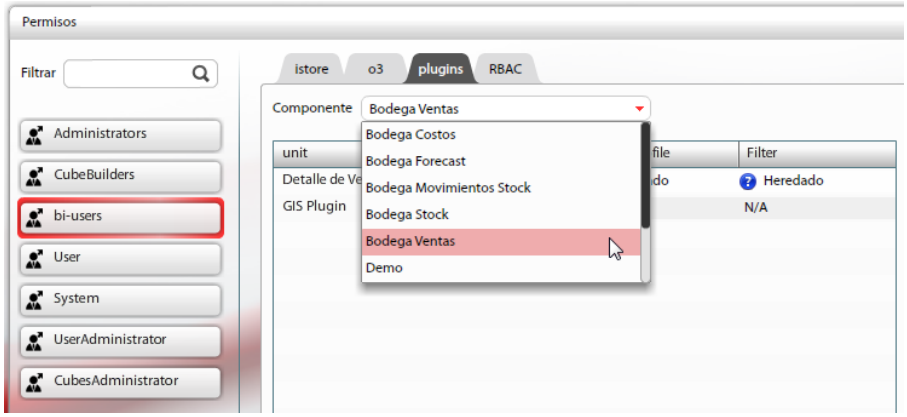


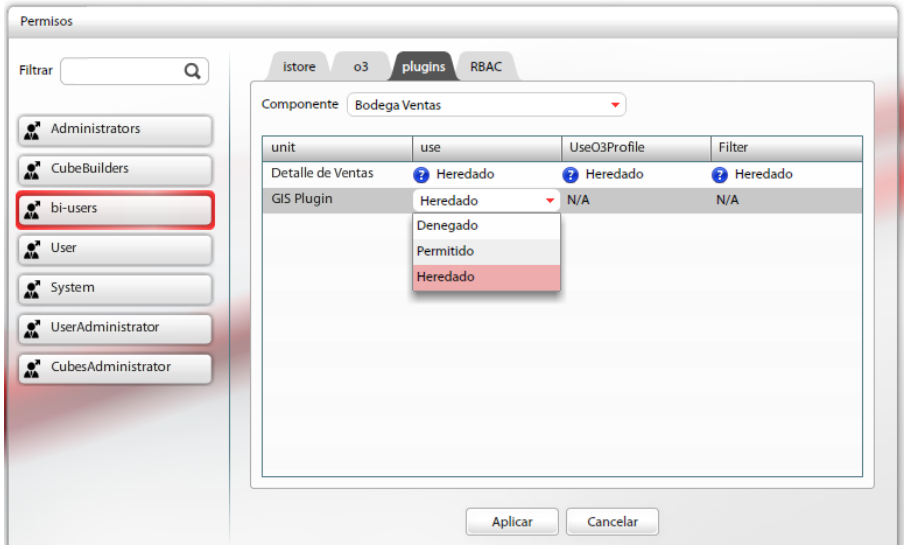

## Permisos sobre plugins

Aplicar permisos sobre los plugins asociados a un cubo.


Para asignar permisos sobre un **plugins de un cubo**:

1. Seleccione *Permisos* del Panel de Propiedades.
2. Seleccione del Panel de Permisos el rol al cual quiere asignar permisos.
3. Seleccione la pestaña *plugins*.
4. Seleccione el *Cubo con plugins asociados* de la lista desplegable de *Componente*.
5. Seleccione el *Plugins* a aplicar los cambios.
6. Para asignar o cambiar permisos es necesario cambiar los valores de las columnas *use, UseO3Profile y Filter*. Los valores se indican en forma independiente y por defecto queda configurado con valores *Heredado*. Los valores posibles para asignar permisos son los siguientes:
    a. **Denegado**, los usuarios actores del rol seleccionado se les denegará el permiso de usar el Plugin.
    b. **Permitido**, los usuarios podrán .
    c. **Heredado**, asignando el valor *Heredar* es como se asignan permisos de poder grabar a todos los repositorios de vistas para un rol determinado.
    d. **N/A,** valor de No Aplica a los plugins asociados a un GIS (Sistema de Información Geográfico) para las columnas de UseO3Profile y Filter.
7. Haga click sobre el botón Aplicar para confirmar los cambios.



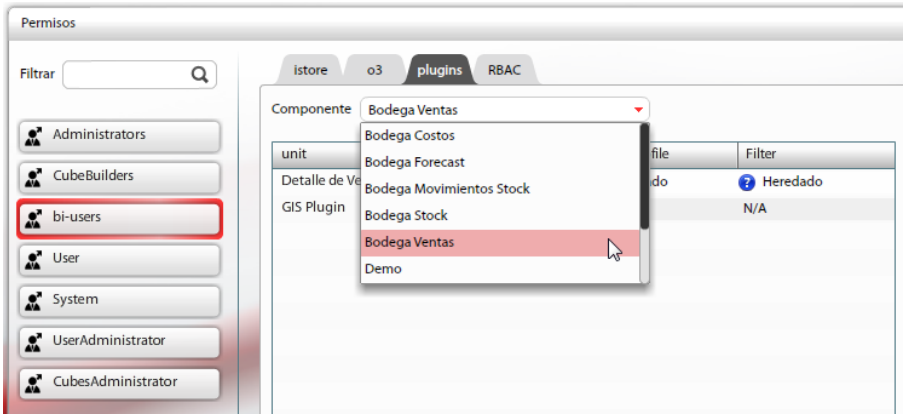



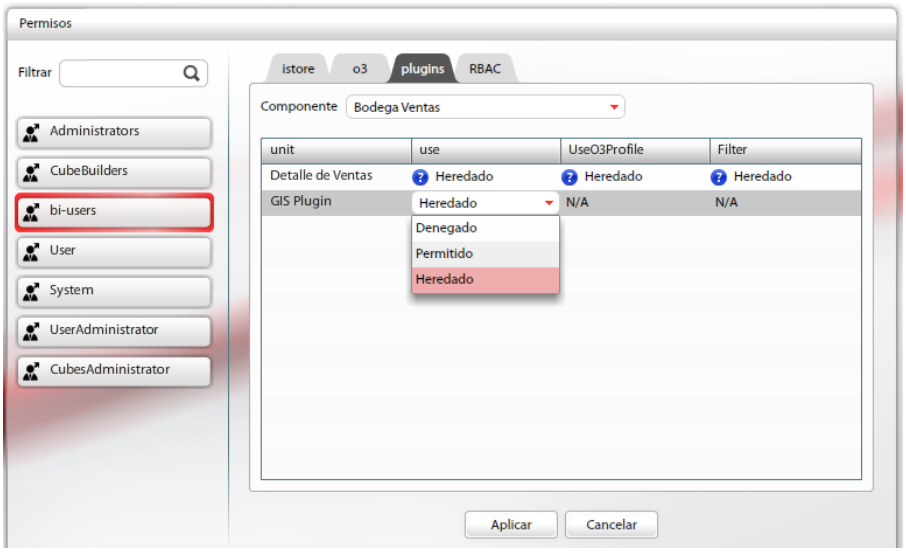

## Permisos sobre RBAC

En esta opción se aplican permisos de administración a nivel de usuarios  (Administrator), y permisos generales (Grants Management).


Para asignar permisos de **RBAC**:

1. Seleccione *Permisos* del Panel de Propiedades.
2. Seleccione del Panel de Permisos el rol al cual quiere asignar permisos.
3. Seleccione la pestaña *RBAC*.
4. Seleccione el *Tipo de Componente de Administración* de la lista desplegable de *Componente*.
    a. **Administrator** para tener permisos sobre los componentes de ***Usuarios, Grupos y Roles*** de *O3 Security***.**
    b. **Grants Management** para tener permisos sobre el componente ***Permisos*** de *O3 Security*.
5. Para asignar o cambiar permisos es necesario cambiar los valores de la columna *Open*. Los valores se indican en forma independiente y por defecto queda configurado con valores *Heredado*. Los valores posibles para asignar permisos son los siguientes:
    a. **Denegado**, los usuarios actores del rol seleccionado se les denegará el permiso.
    b. **Permitido**, los usuarios tendrán permisos de administración de acuerdo al *Componente* seleccionado .
    c. **Heredado**, asignando el valor *Heredado* en este caso, es lo mismo que *Denegado*.
6. Haga click sobre el botón Aplicar para confirmar los cambios.



### Permisos por defecto en cada nueva instalación de O3

Los permisos presentados anteriormente tienen distintos valores por defecto en cada instalación de O3. Estos valores pueden ser modificados según las necesidades presentadas en cada instalación.

Estos valores se definen en el archivo de configuración O3Server_custom.properties ubicado en la raíz de la instalación de O3

Existen facilidades para definir permisos por producto, componente y unidad. A continuación se describe cómo identificar cada permiso y cuáles son los elementos disponibles.

#### *Formato para definir / identificar las properties existentes:*

rbac.appPermissions.default.<producto>[.<componente>[.<unidad>]] = <boolean_value>

| producto | componente | unidad |
|---|---|---|
| **istore** | • models<br>• rules<br>• actions<br>• reports<br>• query<br>• expressions | |
| **o3** | views | |
| | biclient | • O3 Security<br>• O3 BI AdmServer<br>• O3 BI Views<br>• O3 BI Runtime<br>• O3 AD-HOC<br>• O3 BI Dashboards<br>• Nomenclature<br>• O3 BI Library<br>• O3 BI K Rules |
| **plugins** | Los componentes son los cubos a los que se asocian distintas funcionalidades a través de la técnica de plugins | Ejemplos de unidades son:<br>• GIS plugins<br>• Query (drill throguh) |
| **RBAC** | Administration | Administrator |
| | Grants Management | Grants Management |

# Administrando Roles en O3 Security

O3 BI Security 7.x
Mantenimiento de Roles de O3BI Server

En O3 BI la asignación de accesos se realiza sobre los roles en lugar de asignarlos directamente a los usuario. Agregando a los usuarios como actores de cada rol es como el usuario adquiere los accesos requeridos. Esta práctica simplifica el esquema de seguridad y facilita su administración.

En forma adicional para soportar esquemas de seguridad complejos es posible definir roles de tipo *Paramétrico* e *Instancia* en los cuales los usuarios actores quedan definidos automáticamente a partir de sus atributos.

- Agregar Roles
- Relacionar Usuarios a Roles
- Agregar y/o actualizar atributos de un Rol

A continuación se describen las funcionalidades existentes para llevar adelante estas tareas.

### Agregar y Eliminar Roles


Para agregar roles:

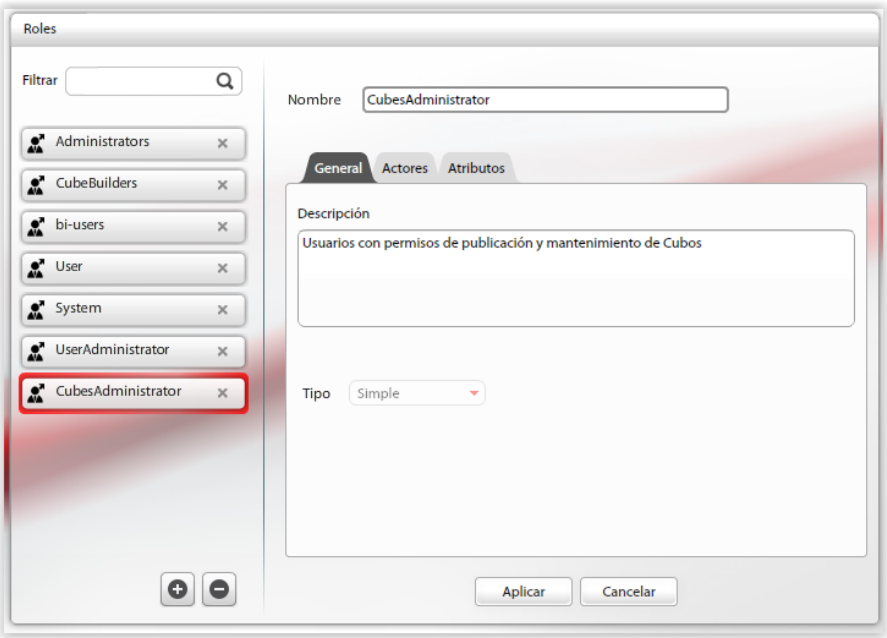
1. Posicionarse en el Panel O3 Security en Roles 

2. Seleccione el boton del símbolo de más en la parte inferior del panel de Roles 
3. Ingrese un Nombre, debe ser sin espacios, el mismo sistema no le permite.
4. Puede ingresar una descripción para identificar el rol.
5. Haga click en el botón Aplicar.

Para eliminar roles:

1. Posicionarse en el Panel O3 Security en Roles 

2. Seleccione el rol a eliminar.
3. Seleccione el boton del símbolo de menos en la parte inferior del panel de Usuario  .También puede realizar la operación haciendo click sobre la **x** a la derecha del nombre del Rol.
4. Haga click en el botón Aplicar



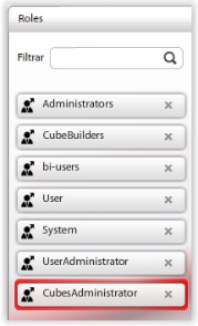

## Relacionar Usuarios a Roles

Para que un usuario adquiera accesos es necesario agregarlo como actor de un rol de licenciamiento.

Los Roles de Licenciamiento son aquellos que nos permiten ingresar al o3web y/o eportal. Algunos de ellos son:

- bi-users - Usuarios Analistas Nominados
- bi-users-vwr - Usuarios ePortal Viewer Nominados
- bi-conc-std - Usuario Studio

Debido a que los accesos se realizan sobre roles y no directamente sobre los usuarios es necesario que todos los usuarios pertenezcan como mínimo a un rol.

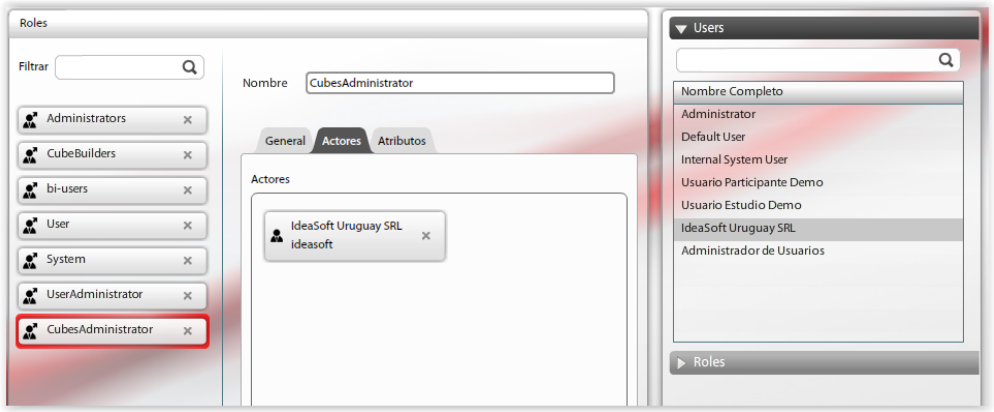

Para relacionar usuarios a roles hay dos opciones:

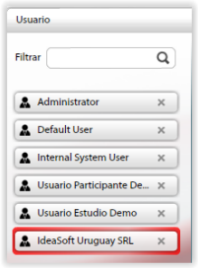
**Relacionar Usuarios a un Rol:**

1. Seleccione el elemento Roles en el Panel de O3 Security.
2. Seleccione el rol al cual quiere agregar o actualizar usuarios, en la sección derecha del Panel de Roles.
3. Selecciones la pestaña de Actores del Panel de Roles.
4. Desde el Panel de Búsqueda (izquierda), seleccionar el usuario a agregar y arrastralo hasta la ventana de Actores.
5. Repetir el paso 4 por cada Usuario a agregar
6. Haga click en el botón Aplicar para confirmar los cambios realizados.

**Relacionar Roles a un Usuario:**

1. Seleccione el elemento Usuarios en el Panel de O3 Security
2. Seleccione el usuario al cual quiere agregar o actualizar roles, en la sección derecha del Panel de Usuarios.
3. Seleccione la pestaña de Roles del Panel de Usuarios.
4. Desde el Panel de Búsqueda (izquierda), seleccionar el rol a agregar y arrastralo hasta la ventana de Roles.
5. Repetir el paso 4 por cada Rol a agregar
6. Haga click en el botón Aplicar para confirmar los cambios realizados.



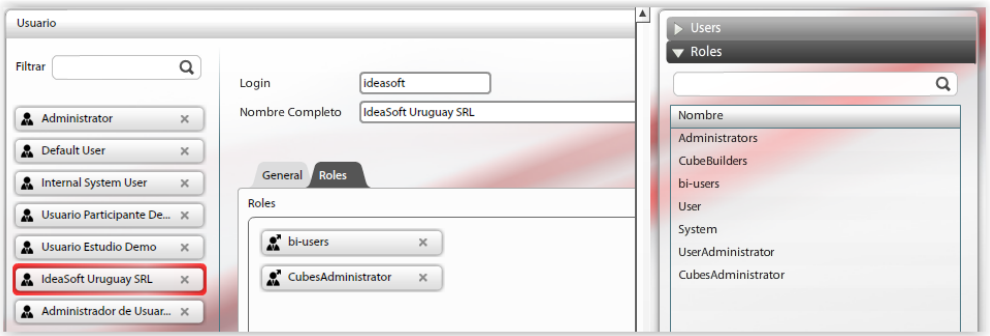




**Eliminar Usuarios de un Rol:**

1. Seleccione el elemento Roles en el Panel de O3 Security.
2. Seleccione el rol al cual quiere eliminar usuarios, en la sección derecha del Panel de Roles.
3. Selecciones la pestaña de Actores del Panel de Roles.
4. Haga click sobre la **x** a la derecha del nombre del Usuario.
5. Repetir el paso 4 por cada Usuario a eliminar.
6. Haga click en el botón Aplicar para confirmar los cambios realizados.

**Eliminar Roles de un Usuario:**

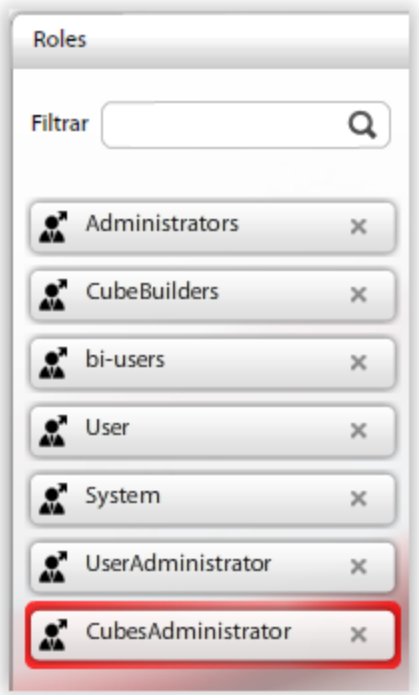
1. Seleccione el elemento Usuarios en el Panel de O3 Security
2. Seleccione el usuario al cual quiere eliminar roles, en la sección derecha del Panel de Usuarios.
3. Seleccione la pestaña de Roles del Panel de Usuarios.
4. Haga click sobre la **x** a la derecha del nombre del rol.
5. Repetir el paso 4 por cada Rol a eliminar.
6. Haga clikc en el botón Aplicar para confirmar los cambios realizados.




## Agregar y/o actualizar atributos de un Rol

Al igual que con los usuarios, la definición de atributos a nivel de roles permite un refinamiento aún mayor de la configuración de seguridad.

Por ejemplo utilizando la función *getRoleValue()* se puede obtener el valor asignado a un atributo de un rol del cual el usuario es actor.

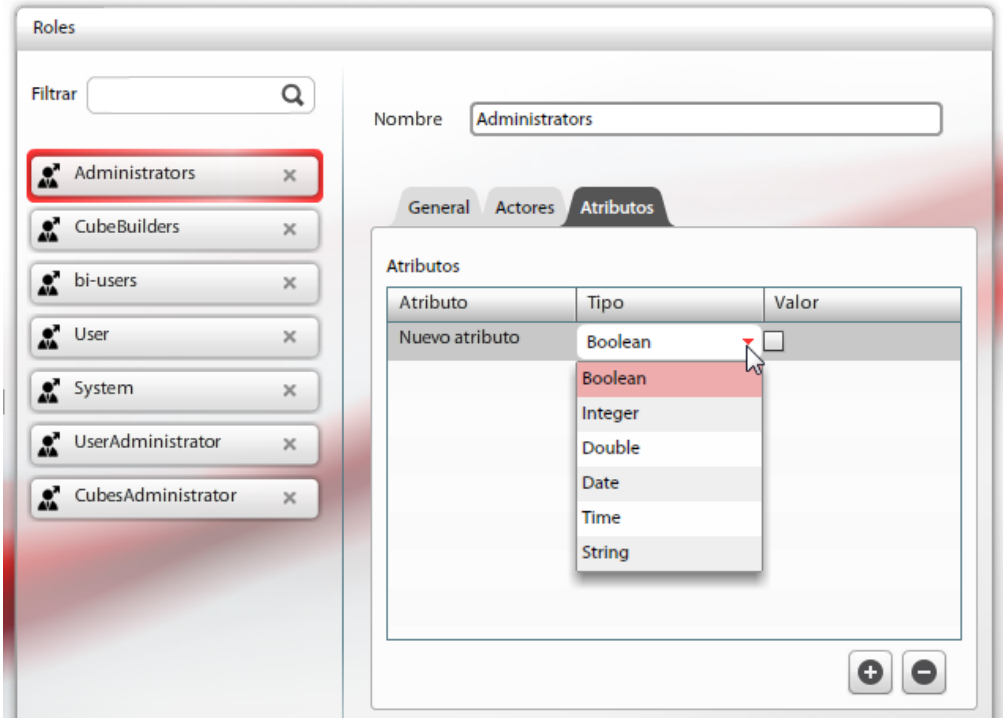



Para agregar o actualizar los atributos de un usuario:

1. Seleccione el rol al cual quiere agregar o actualizar atributos, en la sección derecha del Panel de Roles.
2. Para agregar un nuevo atributo, presione el botón del signo de más para debajo del panel de *Atributos*. Debe completar la siguiente informacion para el nuevo atributo:
    a. ***Atributo***, es el nombre del atributo que se utilizará para referenciar el valor asignado al Rol. Este nombre se utiliza por ejemplo como parámetro de la función *getRolValue()*.
    b. ***Tipo***, es el tipo del atributo el cual puede ser: Boolean, Integer, Double, Date, Time o String.
    c. ***Valor***, el valor asignado al nuevo atributo para el Rol. Por ejemplo este valor es devuelto por la función *getRolValue()*.
3. Para actualizar un atributo se debe seleccionar el atributo de la lista y modificar el nombre, tipo o valor del mismo.
4. Haga clic en el botón Aplicar para confirmar los cambios realizados.

También existen un conjunto de atributos del usuario predefindos, que se utilizan para definir distintos comportamientos, por ejemplo para indicar si un usuario es administrador (Permisos en O3 Security).

Para eliminar un atributo solo debe presionar el botón de menos que está abajo a la derecha del panel de Atributos y presionar el botón de Aplicar para confirmar los cambios realizados.




## Usuario y roles especiales

Existen en O3 BI un usuario y un conjunto de roles predefinidos con funciones especiales que no se recomienda eliminar, aunque pueden ser modificados (sólo su nombre):

- Usuario internal. Usuario para comunicación interna entre servidores de O3 BI. En caso de instalaciones con uso de LDAP para obtener usuarios de repositorios como Active Directory, puede modificarse.
- Rol Administrator.
- Rol System.
- Roles de licenciamiento, por ejemplo bi-users.
- Rol BuildNow. Rol utilizado para construcción de cubos a demanda.

# Administrando Usuarios en O3 Security

O3 BI Security 7.x
Mantenimiento de Usuarios, asignación de roles, atributos del usuario, password

La administración de usuarios abarca las siguientes tareas:

- Agregar Usuarios
- Asignar Atributos a Usuarios
- Restablecer Contraseñas de Usuarios
- Generación de un Usuario administrador de Cubos
- Generación de un Usuario que administra Usuarios

A continuación se describen las funcionalidades existentes para llevar adelante estas tareas, la mayoría disponibles a partir del Catálogo de Seguridad.

### Agregar Usuarios

El esquema de seguridad de O3 BI se basa en la definición de usuarios, los cuales están relacionados con una persona. Para acceder a O3 Server una persona debe tener al menos un usuario definido y conocer su contraseña.

Para agregar usuarios:

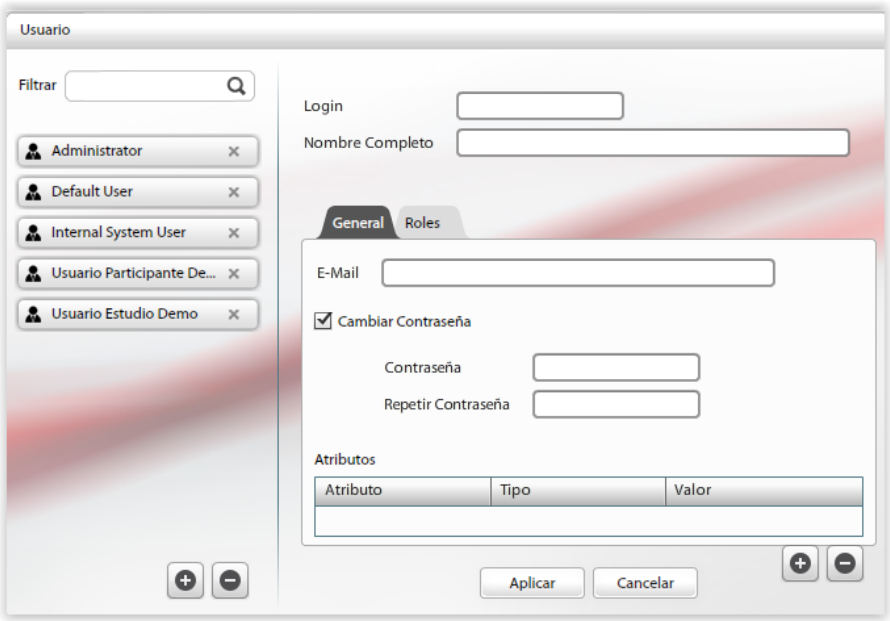
1. Posicionarse en el Panel O3 Security en Usuarios 

2. Seleccione el boton del símbolo de más en la parte inferior del panel de Usuario 
3. Complete las siguientes propiedades en el área derecha del Panel de Usuario:
    a. Login, identificador del usuario para ingresar a O3 Server.
    b. Nombre de la persona, por defecto esta propiedad contiene el texto *Nuevo Usuario*.
    c. e-mail de la persona.
    d. Active la Casilla de *Cambiar Contraseña* para ingresar Contraseña y Repetir Contraseña.
4. Haga click en el botón Aplicar.

Para eliminar usuarios:

1. Posicionarse en el Panel O3 Security en Usuarios 

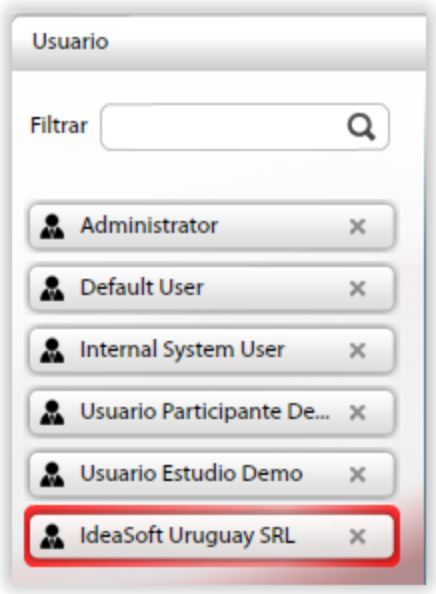
2. Seleccione el usuario a eliminar.
3. Seleccione el boton del símbolo de menos en la parte inferior del panel de Usuario  . También puede realizar la operación haciendo click sobre la **x** a la derecha del nombre del Usuario.
4. Haga click en el botón Aplicar




## Asignar Atributos a Usuarios

La definición de atributos a nivel de usuarios permite realizar un refinamiento mayor de la configuración de seguridad. Por ejemplo se puede restringir el acceso a una dimensión para los usuarios que poseen un atributo en particular, simplificando de esta forma la complejidad del esquema de seguridad. Utilizando luego la funcion *getUserValue()* se puede obtener el valor asignado a un atributo de un usuario.

Otros objetivos pueden ser el de atribuir permisos de administrador general o administrador particular de la instalación.

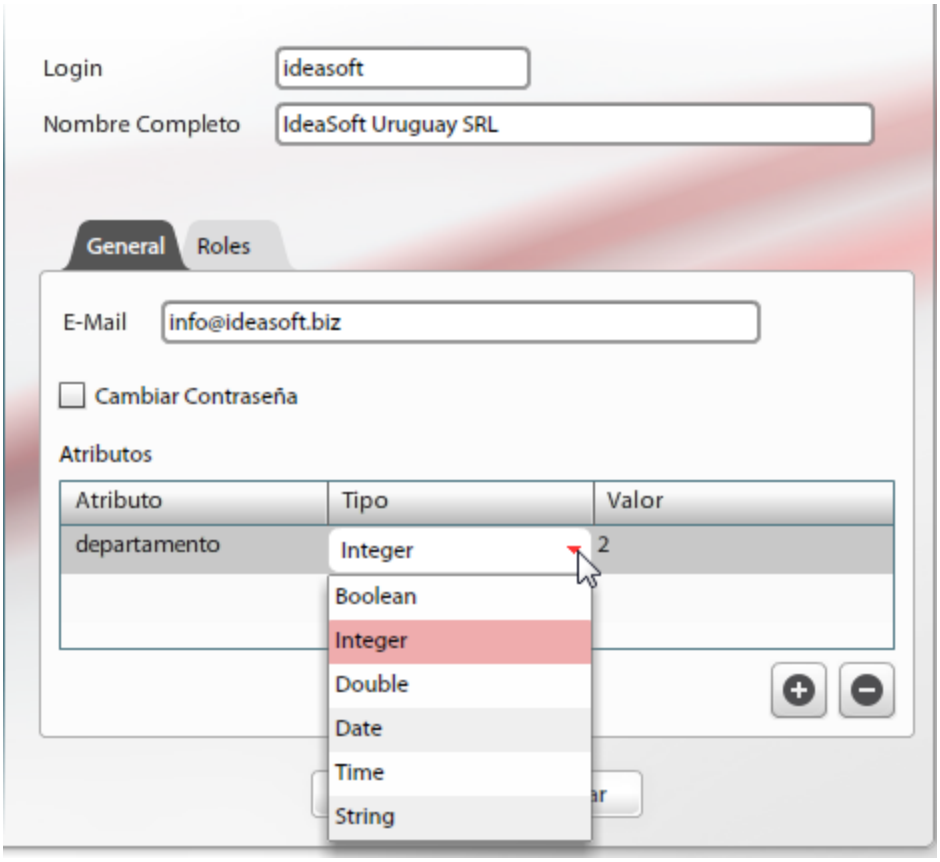



Para agregar o actualizar los atributos de un usuario:

1. Seleccione el usuario al cual quiere agregar o actualizar atributos, en la sección derecha del Panel de Usuarios.
2. Para agregar un nuevo atributo, presione el botón del signo de más para debajo del panel de *Atributos*. Debe completar la siguiente informacion para el nuevo atributo:
    a. Atributo, es el nombre del atributo que se utilizará para referenciar el valor asignado al usuario. Este nombre se utiliza por ejemplo como parámetro de la función *getUserValue()*.
    b. Tipo, es el tipo del atributo el cual puede ser: Boolean, Integer, Double, Date, Time o String.
    c. Valor, el valor asignado al nuevo atributo para el usuario. Por ejemplo este valor es devuelto por la función *getUserValue()*.
3. Para actualizar un atributo se debe seleccionar el atributo de la lista y modificar el nombre, tipo o valor del mismo.
4. Haga clic en el botón Aplicar para confirmar los cambios realizados.

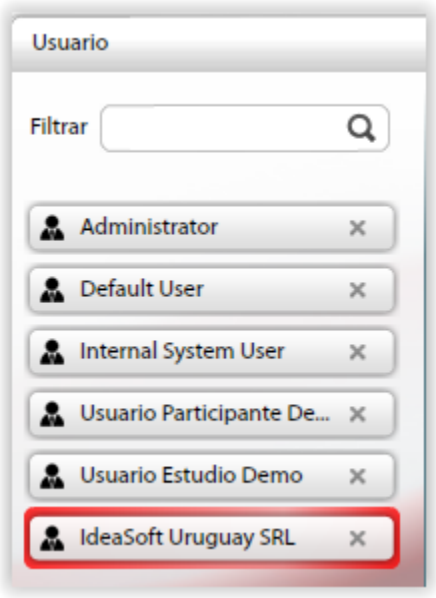
También existen un conjunto de atributos del usuario predefindos, que se utilizan para definir distintos comportamientos, por ejemplo para indicar si un usuario es administrador.

Se puede ver el conjunto completo de estos atributos y su descripción detallada en Definición y Permisos de Usuarios - Atributos



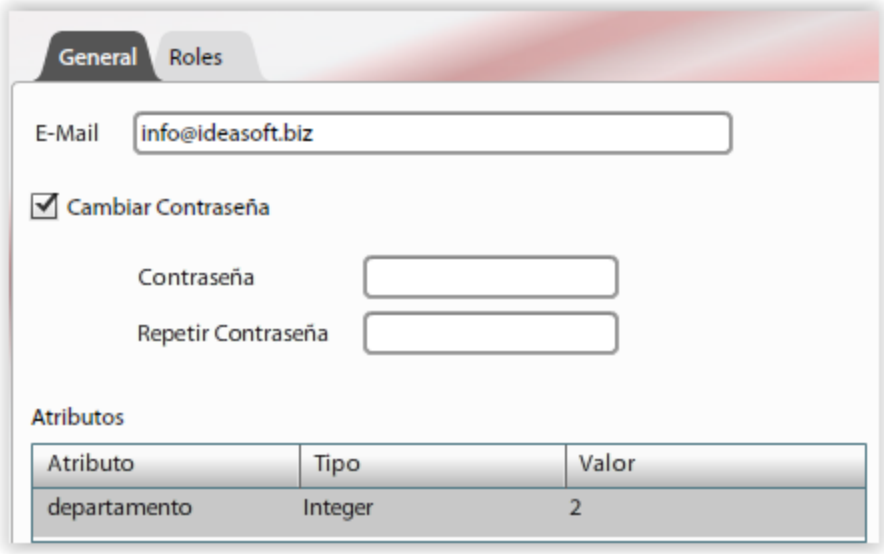

## Restablecer Contraseñas de Usuarios

En los casos en que los usuarios no recuerden su contraseña debemos restablecer la misma con una nueva, ya que la misma no es visible, se guarda encriptada.



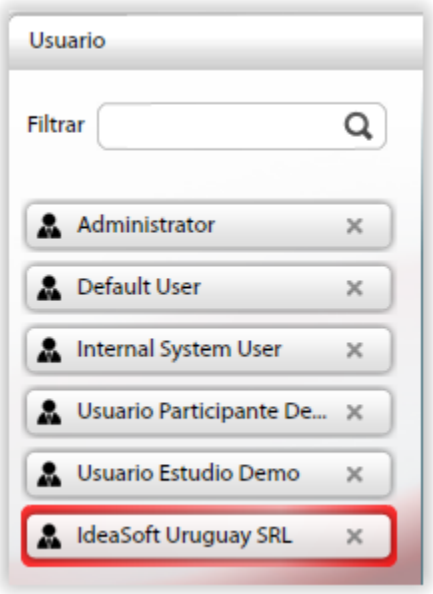

Para agregar o actualizar los atributos de un usuario:

1. Seleccione el usuario al cual quiere agregar o actualizar atributos, en la sección derecha del Panel de Usuarios.
2. Activar la casilla de Cambiar Contraseña
3. Ingresar la nueva contraseña en los dos campos de Contraseña y Repetir Contraseña.
4. Haga clic en el botón Aplicar para confirmar los cambios realizados.



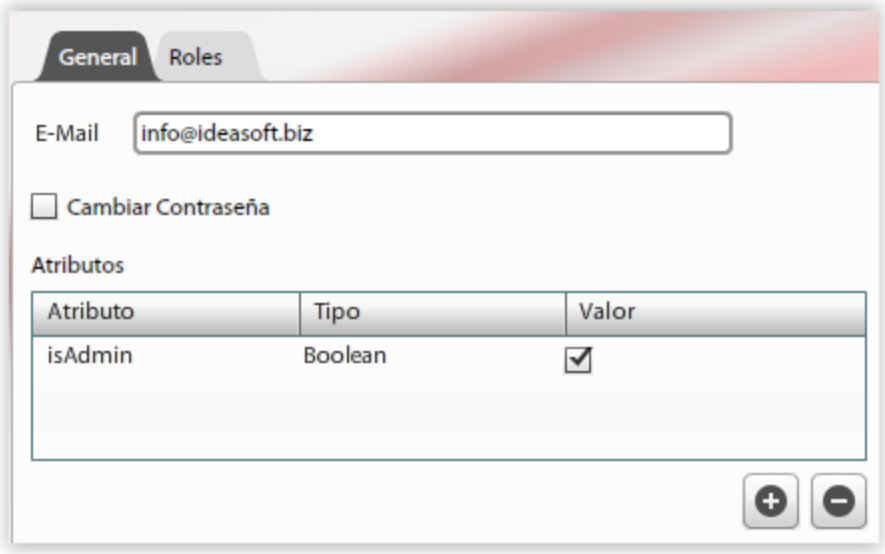

## Generación de un Usuario administrador de Cubos

La definición de un usuario que solo posea acceso a los cubos, nos permite una mejora sustancial del entorno de seguridad, en materia de la administración de los usuarios y sus restricciones.

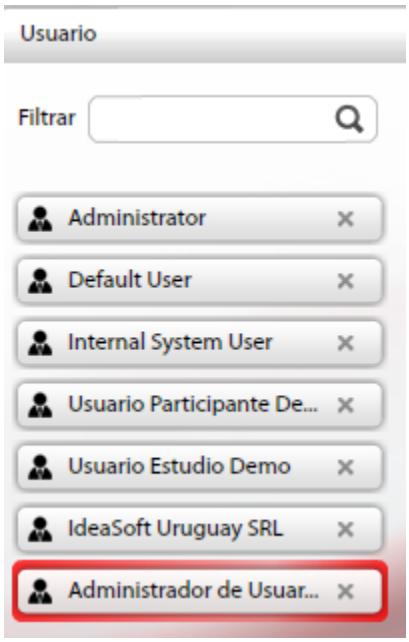



Para agregar o actualizar los atributos de un usuario:

1. Seleccione el usuario al cual quiere agregar o actualizar en la sección derecha del Panel de Usuarios.
2. Agregar un nuevo atributo para que pueda ingresar en O3 BI Server Administrator con la siguiente información:
    a. Nombre: isAdmin
    b. Tipo: Boolean
    c. Activar la Casilla para que tome el valor TRUE
3. Asignar un rol de licenciamiento al Usuario (por ejemplo: bi-users)
4. Haga clic en el botón Aplicar para confirmar los cambios realizados.

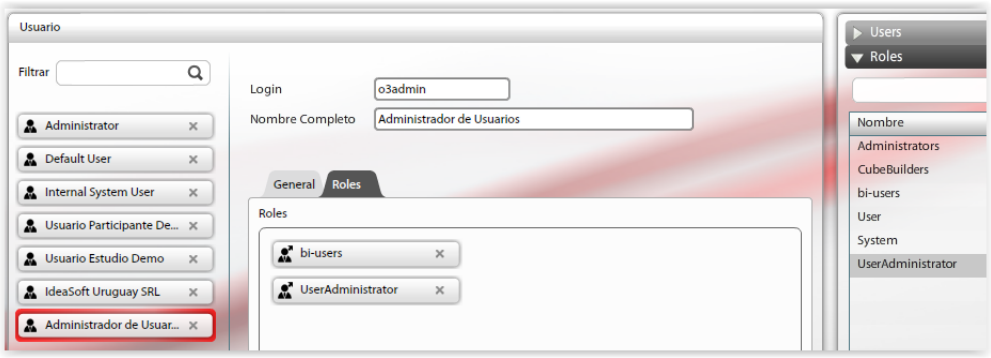


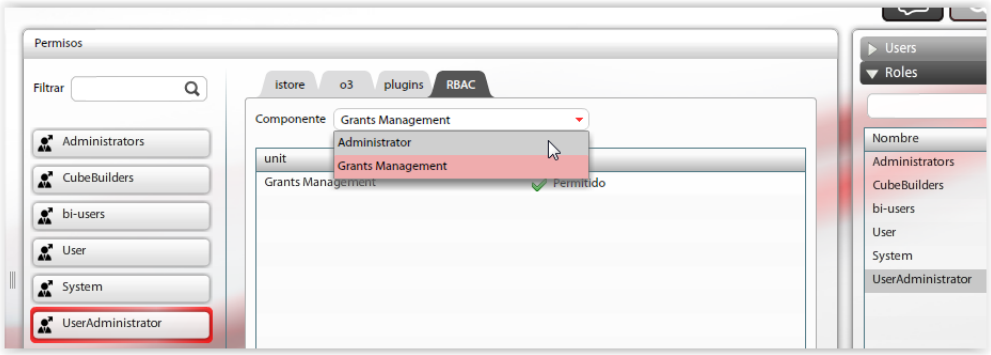

## Generación de un Usuario que administra Usuarios




Para agregar o actualizar los atributos de un usuario:

1. Seleccione el usuario al cual quiere agregar o actualizar atributos, en la sección derecha del Panel de Usuarios.
2. Agregue el Usuario a un Rol de Licenciamiento (por ejemplo: bi-users)
3. Agregue el Usuario a un Rol que tenga Permitidos los Permisos de RBAC para Administrator y/o Grants Management.
    a. Puede generar un rol especifico, por ejemplo UserAdministrator, para este objetivo.
4. Haga clic en el botón Aplicar para confirmar los cambios realizados.






# Definición y Permisos de Usuarios - Atributos

### Atributos que determinan el comportamiento de los usuarios

La definición de usuarios se realiza desde el componente O3 Security.

Para cada usuario pueden definirse distintos atributos que determinan el comportamiento del mismo.

Existe un conjunto de atributos predefinidos, los cuales deben definirse teniendo en cuenta uso de mayúsculas y minúsculas.

A continuación se enumeran los atributos más utilizados:

| Atributo | Significado | Valores posibles | Rol o Usuario | Comportamiento por Defecto |
|---|---|---|---|---|
| **canAddViews** | Si puede grabar vistas en el servidor | booleano | usuario | Si el attr. no existe, el usuario puede grabar vistas |
| **isAdmin** | Indica que el usuario es administrador de O3 | booleano | usuario | Si el attr. no existe, el usuario no es administrador |
| **runAsEnabled** | Responde a requerimientos de configuración cuando el servidor envía notificaciones a los usuarios, por ejemplo a través del servicio de envío de reglas. Permite que el usuario tome momentáneamente los permisos requeridos por el servicio en cuestión. No tiene ningún efecto sobre los permisos que el usuario utiliza al loguearse explícitamente al servidor | booleano | usuario | falso |

### Atributos que determinan el comportamiento de grupos de usuarios

El atributo *CanAddViews* indica si se permite o se niega la posibilidad de salvar vistas en el servidor.

En ocasiones, es necesario definir el comportamiento para un grupo de usuarios más que para cada usuario en particular. En este caso es ventajoso poder definir el comportamiento para los distintos roles del sistema y no solo para cada usuario.

Esta Acción se realiza en Administrando Permisos en O3 Security.

### Controles más específicos

Si bien los atributos presentados anteriormente definen algunas características generales del comportamiento de los usuarios, puede ser insuficiente para modelar ciertos comportamientos que se requieren con frecuencia.

Algunos ejemplos de los comportamientos se detallan a continuación.

***Cada usuario mantiene control de eliminación sobre las vistas creadas por él mismo.***

La situación se presenta en la condición estándar de instalación donde se permite a los usuarios almacenar vistas en el servidor y además tienen acceso al botón de Modo Edición donde pueden eliminar vistas.

En un esquema seguro de trabajo, es recomendable que en este escenario se agregue la restricción de que cada vista solo puede ser eliminada por el usuario que la creó. Para ello se debe agregar la siguiente cláusula en el archivo O3Server_custom.properties

```
o3.views.defaultRestriction=owner
```

El archivo O3Server_custom.properties se debe ubicar en el directorio raíz de la instalación.
Tener en cuenta que dicho archivo no es creado por la instalación del producto, por lo que debe ser creado por el administrador de la instalación

# Usuarios y Roles en LDAP

O3 BI Security 7.x

Las definiciones de usuarios y roles en este caso se realizan con las herramientas de LDAP que se utilizan normalmente. Se detallan las características que deben cumplir los usuarios y roles creados en el servidor LDAP para que puedan ser utilizados por O3 Server.

⚠ Más detalles sobre la configuración sobre LDAP se puede encontrar en la siguiente sección.

## Requisitos de los Usuarios

Para garantizar un correcto funcionamiento de O3 Server sobre un repositorio LDAP es necesario que los usuarios creados en éste cumplan con las siguientes condiciones.

- Los usuarios deben crearse en el contexto o directorio identificado por el parámetro **Ruta base de Búsqueda**.
- A todos los usuarios deberán asignársele el atributo **objectclass** con el valor **humanParticipant** además de otros valores que este atributo pueda tener
- Todos los usuarios deberán tener asignado el atributo **uid** cuyo valor será el login para conectarse a O3 Server.
- Todos los usuarios deberán tener asignado el atributo **cn** cuyo valor será el nombre real del usuario. Esto implica que no tiene por qué coincidir con el valor asignado a **uid**
- Cada usuario deberá tener un conjunto de roles asignados. Esto se realiza mediante la especificación del atributo **assignedRoles** cuyo valor deberá ser la lista de roles. Esta lista contendrá los nombres de los roles involucrados separados por ":" (dos puntos). Esta lista además debe terminar con ":" (dos puntos)
- Para que un usuario tenga privilegios de administrador en el Servidor de O3, deberá tener asignado el rol especificado por el parámetro **Rol del Administrador**.

## Requisitos de los Roles

Para garantizar un correcto funcionamiento de O3 sobre un repositorio LDAP es necesario que los roles creados en éste cumplan con las siguientes condiciones.

- Los roles deben crearse en el contexto o directorio identificado por el parámetro **Ruta base de Búsqueda** (referirse a la sección "Parámetros LDAP" para un detalle de los parámetros)
- A todos los usuarios deberán asignársele el atributo **objectclass** con el valor **ftorganizationalrole** además de otros valores que este atributo pueda tener
- Todos los usuarios deberán tener asignado el atributo **cn** cuyo valor será el nombre del rol
- Todos los usuarios deberán tener asignado el atributo **description** cuyo valor será el nombre del rol

## Ejemplo de una base de datos LDAP para ser utilizada por O3

El siguiente es un ejemplo de una estructura de entradas de directorio en un LDAP utilizado por O3:

```
c=uy
  o=IdeaSoft
    cn=Directory Administrators
    ou=Groups
    ou=People
      uid=admin
      uid=user
      uid=o3user
```

Adicionalmente se sabe que las entradas existentes dentro del contexto o directorio **ou=People**, tienen los siguientes atributos:

uid=user
  cn=Usuario estándar de O3
  objectClass=humanparticipant
  assignedRoles=o3user

uid=admin
  cn=Usuario Administrador de O3
  objectClass=humanparticipant
  assignedRoles=o3admin

uid=o3admin
  cn=o3admin
  description=Rol de Administradores de O3
  objectClass=ftorganizationalrole

uid=o3user
  cn=o3user
  description=Rol de Usuarios de O3
  objectClass=humanparticipant

Especificando como **Ruta base de Búsqueda** el contexto o directorio "**ou=People, o=IdeaSoft, c=uy**", el Servidor de O3 interpretará las entrada "**uid=user**" como un usuario de login "**user**" y nombre "Usuario estándar de O3" que tiene asociado rol "**o3user**".

De la misma manera interpretará la entrada "**uid=admin**" como un usuario de login "**admin**" y nombre "Usuario Administrador de O3" que tiene asociado rol "**o3admin**". Dado que "o3admin" se declaró en el parámetro **Rol del Administrador**, éste usuario contará con privilegios de administrador.

De forma similar se interpretan las entradas "**uid=o3admin**" y "**uid=o3user**" como roles.

# Seguridad de O3 en LDAP y Active Directory

Esta página explica cómo configurar el Servidor de O3 BI para utilizar un servidor LDAP o Active Directory como soporte para la definición de usuarios y roles, así como manejar la autenticación al sistema.

Se asume que se tienen conocimientos básicos del protocolo LDAP, así como conocimientos de cómo configurar el servidor LDAP o Active Directory que se desea utilizar.

Se presentan algunos ejemplos que deben tomarse simplemente como guía ya que las estructuras de directorios presentadas pueden variar dependiendo del servidor LDAP utilizado.



### La seguridad del O3 Server

La seguridad del Servidor de O3 se basa sobre un módulo comúnmente conocido como RBAC (Role Based Access Control).

Este módulo define un conjunto de **repositorios** que son los encargados de almacenar los diferentes elementos involucrados en la seguridad del servidor - usuarios, roles, atributos, asociaciones entre ellos, etc.

Es posible elegir diferentes implementaciones de estos repositorios de modo que los datos puedan ser leídos desde diferentes servidores y utilizando tecnologías diferentes.

O3 BI incluye una implementación de este módulo para poder conectarse a servidores de directorio tales como LDAP y Active Directory.

### Configurando el Servidor de O3

La elección de qué implementación de los repositorios de RBAC usar, se realiza en el archivo **O3Server_custom.properties** que se encuentra

en la raíz de la instalación de O3 BI. En caso de no existir, crear uno respetando las mayúsculas y minúsculas del nombre.

En este archivo se deben definir un conjunto de properties que permiten indicar el repositorio que debe utilizarse.

```
#RBAC Repositories Configuration
#rbac.roleRepository         =
com.ideasoft.rbac.repository.impl.jndi.JndiRoleRepository
#rbac.userRepository         =
com.ideasoft.rbac.repository.impl.jndi.JndiUserRepository
#rbac.raAssignmentRepository =
com.ideasoft.rbac.repository.impl.jndi.JndiRAAssignmentRepository
#rbac.loginService           = com.ideasoft.rbac.repository.impl.jndi.JndiLoginService
```

La distribución de O3 incluye estas properties comentadas en O3Server.properties, tal como puede verse por los caracteres "#" al principio de cada línea. Para poder activar el uso de LDAP o Active Directory es necesario quitar esos caracteres del principio de cada línea de modo que queden de la siguiente forma (es recomendable mantener comentadas estas líneas en el archivo O3Server.properties y agregarlas en el O3Server_custom.properties para una mayor comprensión del manejo de los cambios realizados a la instalación personalizada):

```
#RBAC Repositories Configuration
rbac.roleRepository         =
com.ideasoft.rbac.repository.impl.jndi.JndiRoleRepository
rbac.userRepository         =
com.ideasoft.rbac.repository.impl.jndi.JndiUserRepository
rbac.raAssignmentRepository =
com.ideasoft.rbac.repository.impl.jndi.JndiRAAssignmentRepository
rbac.loginService           = com.ideasoft.rbac.repository.impl.jndi.JndiLoginService
```

⚠ Si lo único que se desea es validar los usuarios contra LDAP o Active Directory, teniendo los roles definidos en la base de datos de O3, sólo deberá descomentarse las líneas que especifican el **rbac.loginService** y **rbac.userRepository**. Si no se habilita el rbac.userRepository todos los usuarios deberán existir tanto en LDAP como en la base de datos de O3.

⚠ Tener en cuenta bien el rbac.userRepository que sea **com.ideasoft.rbac.repository.impl.jndi.JndiUserRepository** ya que hay otra que es para lectura/escritura

Además de habilitar el uso de implementaciones alternativas de los repositorios de RBAC, es necesario configurar una serie de parámetros que cada mecanismo (LDAP o Active Directory) requieren para su correcto funcionamiento.

Estas configuraciones específicas para cada servidor se indican en un archivo adicional que se encuentra en la carpeta <O3>/config/rbac

El nombre del archivo de configuración a utilizar se indica también en el O3Server_custom.properties que puede encontrarse en la raíz de la instalación de O3

```
jndi.cfg.filename = JndiConfiguration-SunONE.properties
```

La distribución de O3 incluye dos archivos de ejemplo **JndiConfiguration-MS.properties** y **JndiConfiguration-SunONE.properties** para Microsoft Active Directory y SunONE Directory Server respectivamente. Al final de este documento se pueden ver estos ejemplos.

Estos archivos definen los siguientes parámetros:

| Parámetro | Descripción |
|---|---|
| **java.naming.provider.url** | Indica la ruta al servidor donde se encuentran los repositorios. Esta ruta es de la forma ldap://<host>:<port> |

| | |
|---|---|
| **java.naming.factory.initial** | Indica el nombre de la clase java que implementa el Contexto Inicial. Este es un parámetro del sistema que no debe cambiarse a menos que se indique lo contrario. El valor por defecto de esta property es "com.sun.jndi.ldap.LdapCtxFactory" |
| **java.naming.security.authentication** | Indica el mecanismo de autenticación. Este es un parámetro del sistema que no debe cambiarse a menos que se indique lo contrario. El valor por defecto de esta property es "simple" |
| **browseUserDN** | Distinguished Name del usuario que utiliza el sistema para obtener las listas de usuarios, roles, etc. |
| **browseUserPassword.plain** | Contraseña del usuario indicado en el parámetro browseUserDN. El valor de esta property se ingresa como texto plano y una vez que el servidor se reinicia ésta es cambiada por la property browseUserPassword cuyo valor será encriptado en forma automática por el servidor |
| **roleDefAttributeID** | Nombre del atributo que deben tener las entradas en el directorio que representan roles |
| **roleDefValueAttributeID** | Valor que debe tener el atributo roleDefAttributeID para ser considerado un rol |
| **roleNameAttributeID** | Atributo que se va a utilizar para recuperar el nombre del rol |
| **roleSearchBaseDN** | DN a partir del cual se buscarán los roles |
| **userDefAttributeID** | Nombre del atributo que deben tener las entradas en el directorio que representan usuarios |
| **userDefValueAttributeID** | Valor que debe tener el atributo userDefAttributeID para ser considerado un usuario |
| **userNameAttributeID** | Atributo que se va a utilizar para recuperar el nombre del usuario |
| **userSearchBaseDN** | DN a partir del cual se buscarán los usuarios |
| **userRolesAttributeID** | Nombre del atributo multivaluado que contiene la lista de los roles que tiene asignado el usuario |

> *Nota*
> *Para el caso en que la lista de roles indicada por la property userRolesAttributeID sea una lista de DN (Distinguished Name) en lugar de los nombres de los roles directamente, es necesario especificar el atributo dereferenceRoleAttribute, el cual indica el atributo a partir del cual se va a obtener el nombre del rol. En este caso, el valor de dereferenceRoleAttribute y el de roleNameAttributeID deben coincidir para que funcione correctamente la asignación de roles a usuarios.*

> *Nota*
> *Para que la validación de usuarios sea exitosa es necesario que éstos tengan definidos el atributo "dn"*

> *Nota*
>
> *En caso de que se tenga mas de un path para buscar los usuarios se debe declarar:*
>
> *userSearchBaseDN_0 = .....*
> *userSearchBaseDN_1 = ....*

## Ejemplos de Archivos de Configuración

**Ejemplo de Archivo de configuración para Microsoft Active Directory**

```
#Microsoft - Active Directoy Configuation file

allowEmptyPasswords       = false

java.naming.provider.url  = ldap://dataserver:389
userRolesAttributeID      = memberOf
dereferenceRoleAttribute  = cn

#Browse user's  DN (used to bind to the Directory)

#Option 1: User Principal Name (username@domain)
#browseUserDN             = o3user@radiusserver.ideasoft.com
#browseUserPassword.plain = ????????

#Option 2: DN (Distinguished Name) asumiendo en AD un usuario O3 User
browseUserDN              = CN=O3 User, CN=Users, DC=xxxxxxx,DC=xxx
browseUserPassword.plain  = ????????

#Roles's Entry definition
roleDefAttributeID        = objectclass
roleDefValueAttributeID   = group
roleNameAttributeID       = cn
roleSearchBaseDN          = ou=Roles, dc=radiusserver, dc=ideasoft, dc=com

#User's Entry definition
userDefAttributeID        = objectclass
userDefValueAttributeID   = user
userNameAttributeID       = sAMAccountName
userSearchBaseDN          = cn=Users, dc=xxxxxxxx, dc=xxx
```

**Ejemplo de Archivo de configuración para SunONE Directory Server**

```
#Sun ONE Directory Server Configuation file

java.naming.provider.url  = ldap://dataserver:51685
userRolesAttributeID      = nsrole
dereferenceRoleAttribute  = cn

#Browse user's  DN (used to bind to the Directory)
browseUserDN              = uid=admin, cn=directory administrators, dc=ideasoft
browseUserPassword.plain  = ????????

#Roles's Entry definition
roleDefAttributeID        = objectclass
roleDefValueAttributeID   = ldapsubentry
roleNameAttributeID       = cn
roleSearchBaseDN          = ou=People, dc=ideasoft

#User's Entry definition
userDefAttributeID        = objectclass
userDefValueAttributeID   = person
userNameAttributeID       = uid
userSearchBaseDN          = ou=People, dc=ideasoft
```

**Ejemplo de Archivo de configuración para Apache DS**

```
java.naming.provider.url    = ldap://localhost:10389
userRolesAttributeID        = memberOf

#Browse user's  DN (used to bind to the Directory)
browseUserDN                = uid=admin,ou=users,o=ideasoft,dc=ideasoft,dc=com
browseUserPassword.plain    = ????????

#Role's Entry definition
roleDefAttributeID          = objectclass
roleDefValueAttributeID     = group
roleNameAttributeID         = cn
roleSearchBaseDN            = ou=Roles, o=ideasoft, dc=ideasoft, dc=com

#User's Entry definition
userDefAttributeID          = objectClass
userDefValueAttributeID     = person
uderNameAttributeIs         = uid
userSearchBaseDN            = ou=users,o=ideasoft,dc=ideasoft,dc=com
```

**Ejemplo de Archivo de configuración para Open Ldap**

```
java.naming.provider.url              = ldap://localhost:389
#userRolesAttributeID                 = nsrole
#dereferenceRoleAttribute             = cn

#Browse user's  DN (used to bind to the Directory)
browseUserDN          = cn=o3,ou=usuarios,dc=ids,dc=com,dc=uy
browseUserPassword.plain      = ????????

#Roles's Entry definition
roleDefAttributeID                    = objectclass
roleDefValueAttributeID               = ldapsubentry
roleNameAttributeID                   = cn
roleSearchBaseDN                      = ou=grupos,dc=ids,dc=com,dc=uy

#User's Entry definition
userDefAttributeID                    = objectclass
userDefValueAttributeID               = person
userNameAttributeID                   = uid
userSearchBaseDN                      = ou=usuarios,dc=ids,dc=com,dc=uy
```

### Modificar usuario internal

El nuevo usuario deberá estar asociado al rol System y tener definido cómo atributo runAsEnabled de tipo Boolean.

En <o3>\O3Server.properties modificar:

```
rest.user=internal
rest.pass=internal
```

En <o3>\Portlets.properties, modificar:

```
gclient.runas.user = internal
gclient.runas.password = internal
```

En <o3>\liferay\tomcat\webapps\o3-parts-web\WEB-INF\classes\portlets-config\portlets-config.properties, modificar:

```
adminUser=internal
adminPass=internal
```

En <o3>\jboss\standalone\deployments\o3report.war\WEB-INF\webapp.properties, modificar:

```
gclient.runas.user = internal
gclient.runas.password = internal
```

## Configuración de Liferay con LDAP y CAS

Por defecto Liferay viene configurado para autentificar con CAS. Si configuramos O3 para que autentifique contra un LDAP o AD, puede interesarnos que los datos de los usuario se importen del LDAP en forma automática, o que todo usuario autorizado por O3 se le cree la cuenta en forma automática en Liferay

#### Hacer que Liferay tome los datos del LDAP

Debemos ir a Panel de Control, seleccionar la opción Configuraciones y luego Autenticación.

En el tab General configurar para que el **método de autenticación de usuarios** sea **Por nombre de usuario**

Luego seleccionamos el tab LDAP, esto es para todo tipo de LDAP incluso Activi Directory.

Verificar que Habilitado y Requerido no estén chequeados.

Elegir en Valores por defecto el LDAP de nuestra preferencia. y luego apretar el botón Restaurar valores, esto hará que se precarguen valores en los campos siguientes.

Debemos completar los datos de conexión, si todo está correcto al apretar el botón de Probar la conexión a LDAP deberia mostrarnos una pantalla diciendo que se ha establecido la conexión con éxito con el servidor LDAP.

#### *Configuración de usuarios*

Esta es la parte más delicada de la configuración, se debe configurar correctamente el **Filtro de búsqueda para autenticación** para que Liferay encuentre el usuario que se quiere loguear. Por defecto el filtro queda configurado con **@user_id@** que deberá ser sustituid por **@screen_name** @, el resto del filtro se debe dejar tal como está. Los demás campos en general queda bien, revisar el campo **Nombre de usuario**, debería coincidir con lo que igualamos @screen_name@

Probamos con el botón de Probar la configuración de usuarios LDAP, si todo está bien nos mostrara una pantalla con los primeros usuarios del LDAP

Atención: ver bien esta pantalla no implica que el **Filtro de búsqueda para autenticación** haya sido bien configurado. Si el filtro quedó mal sucederá que no importara los usuarios.

#### Configuración de CAS

En el tab CAS le diremos a Liferay como autenticarse.

Es **obligatorio** que el checkbox Habilitado este chequeado.

Si queremos que los datos de los usuarios se importen del LDAP debemos chequear **Importación de LDAP**.

El resto de los campos deben dejarse tal como están. Atención, cambios en estos campos pueden llevar a no poder loguearse a liferay, se recomienda consultar antes de modificarlos.

#### Últimos pasos

Luego que configuramos todo solo resta apretar el botón de salvar para persistir los cambios.

Podemos ir al link de **Asociaciones por defecto de los usuarios** y hacer que todo usuario que se crea por defecto pertenezca  a una comunidad y que tenga determinados roles.

**Ejemplo de configuración para Microsoft Active Directory**


## Problemas

1. ***O3 no autentica contra el LDAP***
   Se puede revisar el log del servidor y ver se hay algún error inmediatamente de habernos intentado loguear. Estudiar si es problema de credenciales del usuario, del usuario que accede al ldap para obtener datos, mal el DN base.
2. ***Liferay no auntentica contra el LDAP***
   Revisar que el filtro sea correcto, usualmente en el log se ve que no encuentra al usuario.
3. ***No importa los datos de los usuario***
   Esto se pude deber a que el filtro está mal y no lo encuentra.
   También se pude deber a que faltan datos obligatorios en el LDAP, por ejemplo la casilla de correo, o el apellido, etc. Ver datos necesarios en la parte de usuarios.