Tot plugin PowerBI Reports integration

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento

Introducción

En Power BI podemos tener 3 tipos de informes:

- Informes que contienen solo el modelo de datos y los datos (datasets)
- Informes que contienen páginas donde se muestra información, pero no tienen datos (hacen consultas a otros informes de Power BI que contienen datasets)
- Informes que contienen el modelo de datos, datos y páginas (los dos anteriores, esto es poco habitual porque se tiende a modularizar y que cada informe tenga una función)

Seguridad física, en el contexto de los informes, es que si un informe tiene varias pestañas o páginas en un contrato se puede parametrizar un subconjunto de ellas y que las personas que lo firmen solo puedan ver ese subconjunto. La manera de implementar esto es que en la creación de un dataset de tipo informe de Power BI hay que informar las pestañas (páginas) que tiene. En el contrato se mostrará la lista de las pantallas del/los informe/s asociado/s al contrato y la lista de páginas registradas para que los data steward seleccionen lo que consideren a qué páginas da acceso ese contrato y se guarde en la BBDD. En base a esto como se puede deducir es que la seguridad física aplica a informes que tienen páginas o mixtos (páginas y datos).

La reducción de datos consiste en que las personas pueden ver aquellos datos que tienen parametrizados, por ejemplo, si una persona se le parametriza que puede ver todos los programas de bachelors en las business units de España y Francia solo podrá ver esos datos cuando abra el informe/s donde se aplica esa parametrización. Esa parametrización se guarda en Anjana en contratos y se implementa en Power BI con una funcionalidad llamada “RLS (Row Level Security)”. Anteriormente hablábamos de los tipos de informe que nos podemos encontrar en Power BI, pues bien, para hacer contratos con reducción de datos se tienen que hacer para informes que contengan el modelo de datos y los datos o que contengan el modelo de datos, los datos y páginas (mixtos).

Cada informe puede tener su propia parametrización, pero esta debe estar en concordancia con el tipo de informe que es. Si un informe es de tipo dataset puramente, cuando se crea en Anjana no se le añadirán páginas, por lo que no se podrá aplicar seguridad física pero sí reducción de datos. A un informe solo con páginas (sin dataset) se le puede aplicar seguridad física pero no reducción de datos. A los informes mixtos se puede aplicar ambos, seguridad lógica y reducción de datos.

Integración de Power BI

Para que la integración Anjana/Power BI se realice correctamente es necesario que desde el diseño del informe se realicen una serie de actuaciones para ello. Los pasos necesarios para conseguirlo se describen a continuación.

Modelo contenedor del Datamart de Seguridad en PBI

Para aplicar seguridad de acceso por páginas y acceso por reducción de datos utilizando la información del Datamart de Seguridad, se ha creado un Informe solo con modelo (conjunto de datos) denominado “Security_Imp.pbix”, es decir, NO contiene visualización de datos.
Solo es necesario crearlo una vez y luego importarlo en los informes que se deseen crear. Este informe , ya creado, sirve como fuente de datos a todos los informes que se deseen crear.
Este Modelo contiene las 4 tablas importadas de seguridad del datamart de seguridad.

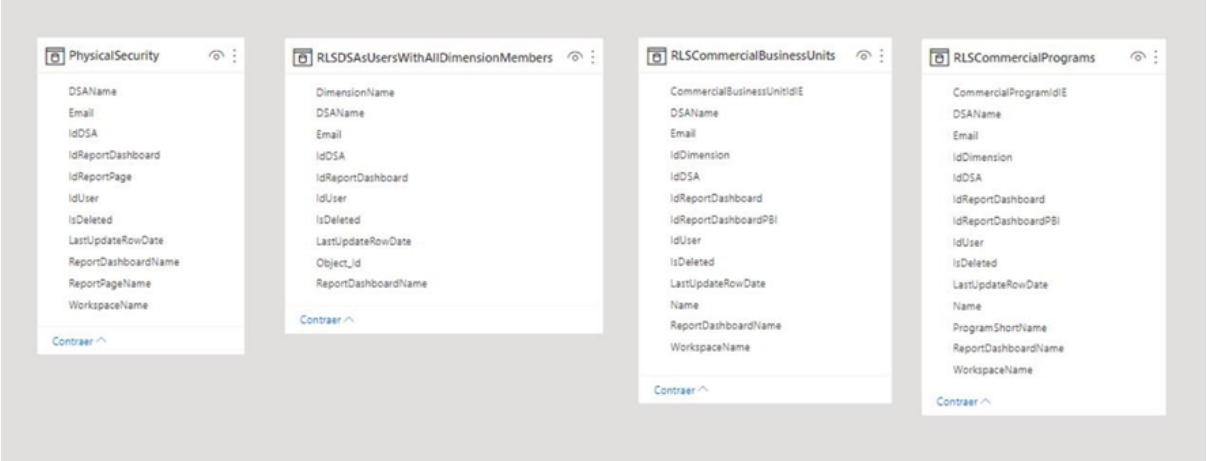


Tabla de acceso por pestañas, Seguridad Física

La vista denominada **PhysicalSecurity** se utiliza en aquellos informes visuales en que los usuarios acceden solo a las pestañas a las que están autorizados (seguridad física).

La tabla PhysicalSecurity se importa de la vista **dm_security.PhysicalSecurity** y contiene la información necesaria para permitir el acceso a páginas del informe ocultas, como se puede ver da información completa para saber a qué y a quién se está dando acceso:

- El email del usuario
- El nombre del contrato, DSAName.
- El nombre del workspace de Power BI, WorkSpaceName.
- El nombre del informe de Power BI, ReportDashboradName.
- El nombre de la página del informe de Power BI, ReportPageName.

Tablas RLS (Row Level Security) de acceso por reducción de datos

Se define una vista por cada dimensión a la que se quiere aplicar el acceso por reducción de datos.

Este informe de Power BI, que actúa como dataset, debe tener tantas dimensiones como se quiera aplicar la reducción de datos. Las dimensiones óptimas para hacer eso son aquellas con menor nivel de granularidad y que tienen una relación directa con las tablas de hechos. Por cada una de esas dimensiones que se quiere hacer reducción de datos hay que aplicar los siguientes pasos:

1. Crear una tabla en el esquema dim que contenga todos los distintos valores que puede tener la dimensión más un registro “Unknown” que tendrá el valor -1. La tabla debe seguir el patrón de diseño de tablas citado en este documento, (pk, campo IsDeleted, fechas creación/última actualización, usuario de creación/última actualización). Estas tablas sirven para alimentar los metadatos de referencia de Anjana que a su vez servirán para parametrizar contratos. Para este caso de uso se han creado las tablas:
    a. dim.CommercialPrograms
    b. dim CommercialBusinessUnits
2. Crear una tabla en el esquema dm_security que recogerá la parametrización asociada a un contrato cuando se selecciona uno o varios valores de esa dimensión (valores de la tabla dim), si se asociará el contrato todos los valores de una dimensión se guardará un registro en la tabla RLSAllDimensions. Como en el punto anterior las tablas deben de seguir el patrón de diseño de tablas citado en este documento, (pk, campo IsDeleted, fechas creación/última actualización, usuario de creación/última actualización). El contenido que almacenan es un valor de dimensión para un informe (el del dataset) y un contrato. Para este caso de uso se han creado las tablas:
    a. RLSCommercialBusinessUnits
    b. RLSCommercialPrograms.
3. Sobre las tablas de dimensiones RLS se crean vistas que son las que se importan en el modelo de datos. Estas vistas tienen por cometido mostrar además de los ids las descripciones asociadas a esos ids. Las vistas importadas en este caso son:
    a. RLSSecurityCommercialBusinessUnits
    b. RLSSecurityCommercialPrograms

Estas 3 tablas son las que se han definido en este modelo para este caso de uso que se importan de las siguientes vistas del esquema **dm_security**.

1. RLSDSAsUsersWithAllDimensionMembers → RLSSecurityDSAsUsersWithAllDimensionMembers
2. RLSCommercialBusinessUnits → RLSSecurityCommercialBusinessUnits
3. RLSCommercialPrograms → RLSSecurityCommercialPrograms

La tabla RLSDSAsUsersWithAllDimensionMembers básicamente contiene información de qué contratos tienen asignados todos los valores de una dimensión y los usuarios que tienen asociado ese contrato.

Importación de las 4 tablas (mediante cargas incrementales)

Las 4 tablas se importan definiendo cargas incrementales.
Para configurar las cargas incrementales de estas 4 tablas, se definen 2 parámetros de tipo “Fecha/Hora” denominados RangeStart con valor “01/01/2002” y RangeEnd con un valor futuro, por ejemplo “28/02/2022”.

Para cada una de las 4 vistas se definen los siguientes parámetros para aplicar la carga incremental:

- Establecer intervalos e importación y actualización:
  - Iniciando datos de archivo: 4 años antes de la fecha de actualización.
  - Iniciando actualización de datos: 5 años antes de la fecha de actualización.
- Elegir configuración opcional:
  - Detectar cambios de datos: flag activado.
  - Actualizar solo datos del último período: 5 días si el valor máximo de esta columna datetime cambia: LastUpdateRowDate

Quedando las 4 vistas configuradas del siguiente modo.

Este informe se debe publicar en el workspace que el cliente decida. Para este caso de uso se publica en el workSpace “POC”.

```
PhysicalSecurity = Table.SelectRows(dm_security_PhysicalSecurity, each [LastUpdateRowDate] >=
RangeStart and [LastUpdateRowDate] RangeEnd)

RLSCommercialBusinessUnits = Table.SelectRows(dm_security_RLSCommercialBusinessUnits, each
[LastUpdateRowDate] >= RangeStart and [LastUpdateRowDate] RangeEnd)

RLSCommercialPrograms = Table.SelectRows(dm_security_RLSCommercialPrograms, each [LastUpdateRowDate]
>= RangeStart and [LastUpdateRowDate] RangeEnd)

RLSDSAsUsersWithAllDimensionMembers =
Table.SelectRows(dm_security_RLSDSAsUsersWithAllDimensionMembers, each [LastUpdateRowDate] >=
RangeStart and [LastUpdateRowDate] RangeEnd)
```

Creación modelo de un Informe de Power BI que importa el Modelo de Datos de Seguridad

En cada informe que se cree que tenga que utilizar el modelo de Seguridad de Datos se deben realizar las siguientes tareas, además de importar las tablas del propio informe:

1. Importar las 4 tablas del modelo de seguridad (Security_Imp.pbix).
2. Configurar el acceso físico, si procede.

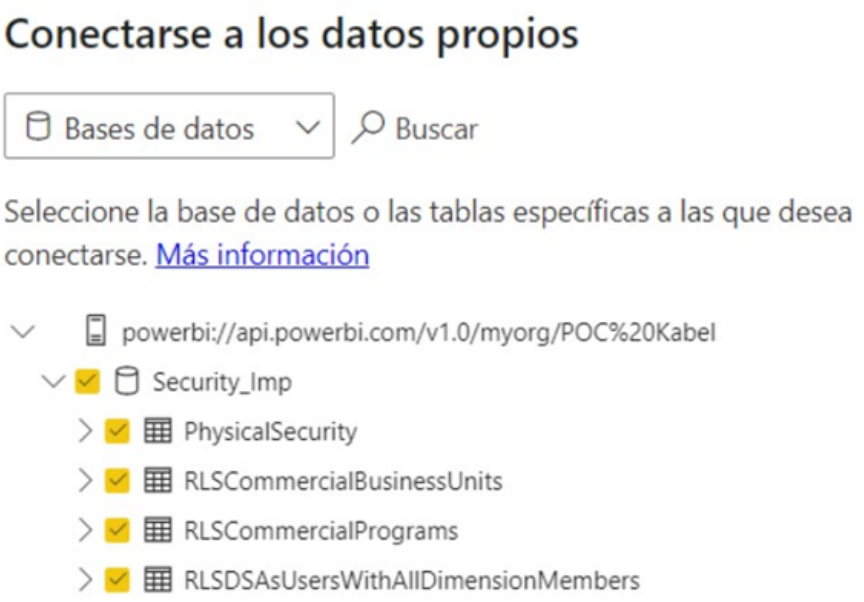
3. Configurar el acceso por reducción de datos, si procede.

Al crear un informe de Power BI se deben importar mediante **Direct Query,** las 4 tablas de datos del modelo de Datos de Seguridad visto en el apartado anterior.

Para este caso de uso se ha creado un modelo (conjunto de datos) denominado "**Commercial_Dashboard_Modelo_Data_and_Security_Imp.pbix**" y un informe de visualización denominado "**Commercial_Dashboard_V2_XXXX.pbix**", que está basado en el informe original del cliente denominado "**Commercial_Dashboard_V2.pbix**".

Importación de las 4 tablas del modelo de Datos de Seguridad.

Seleccionar como origen de datos el tipo "***conjunto de datos de Power BI***" en el modelo del informe "**Security_Imp.pbix**" que está publicado en el workspace.



Una vez importadas las 4 vistas el modo de almacenamiento debe mostrar: "Direct Query"

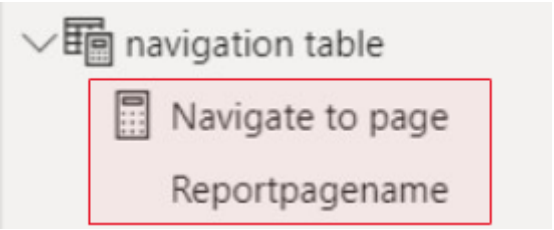
Acceso por páginas, Seguridad física.

Por cada nuevo informe que consuma el dataset "**Secutity_Imp.pbix**, si tiene acceso físico por pestañas, se configura un botón que permite el acceso a páginas ocultas.

Para ello, se crea una tabla virtual con el nombre "**navigation table**"en conjunto de datos del informe.

Por ejemplo, en el informe del caso de uso se ha creado en "**Commercial_Dashboard_Modelo_Data_and_Security_Imp.pbix**".

En esta tabla se ha creado una medida denominada "Navigate to page" y una columna denominada "ReportPage".



La métrica "Navigate to page" tiene la siguiente definición DAX, que articula la relación entre el botón que dan acceso a una página con la vista PhysicalSecurity:

```
Navigate to page =
MAXX (
    FILTER (
        PhysicalSecurity,
        PhysicalSecurity[ReportPageName] = SELECTEDVALUE ('navigation table'[Reportpagename] )
            && PhysicalSecurity[Email] = USERPRINCIPALNAME ()
    ),
    PhysicalSecurity[ReportPageName]
)
```

La columna "ReportPageName" selecciona las páginas del del informe activas en la vista del datamart de seguridad PhysicalSecurity.

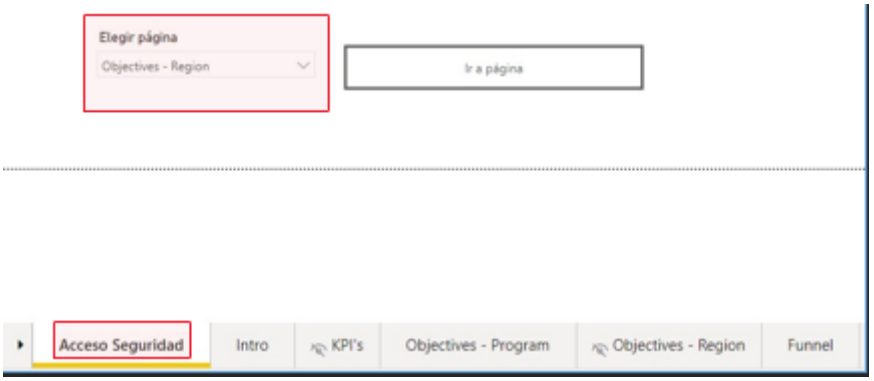
```
navigation table =
VAR nombrereport = "Commercial_Dashboard_V2_Kabel"
RETURN
    SELECTCOLUMNS (
        FILTER (
            PhysicalSecurity,
            PhysicalSecurity[ReportDashboardName] = nombrereport
                && PhysicalSecurity[IsDeleted] = "N"
        ),
        "Reportpagename", PhysicalSecurity[ReportPageName]
    )
```

En la variable "nombrereport" se asigna el nombre del informe PBI que corresponda.

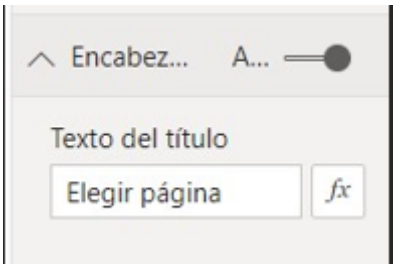
El informe de visualización da acceso a las páginas ocultas a los usuarios que tienen permisos, mediante un selector de páginas y un botón para redirigir a la página seleccionada por el usuario:

1. Vincular el informe al dataset donde tenemos los datos y la seguridad (punto anterior)
2. Crear las páginas del informe con los controles deseados
3. Ocultar las páginas que queremos que tengan un acceso especial, en nuestro caso serán la pestaña "KPI's" y "Objetives – Region".

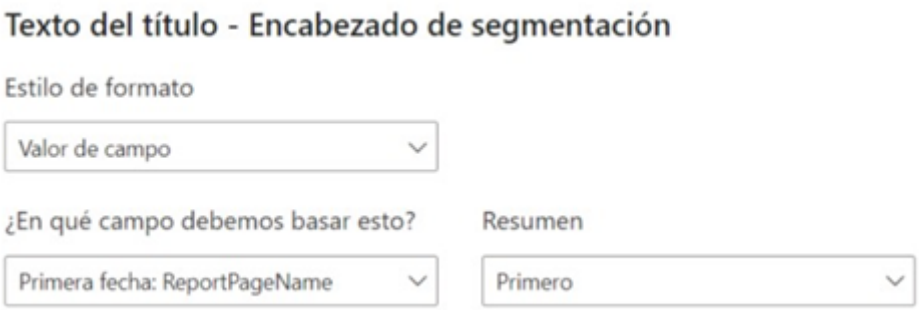
4. En una página que hemos llamado “Acceso Seguridad” añadimos el selector (segmentación de datos) y un botón para acceder a las páginas ocultas:



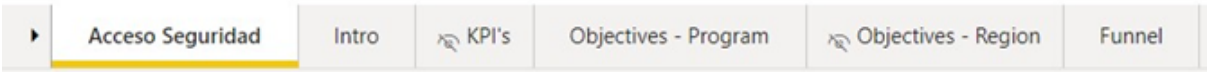
   a. Ir a la propiedad “Encabezamiento” del objeto “segmentación de datos” añadido y seleccionar sobre el botón “fx” para indicarle que el destino depende de un campo:

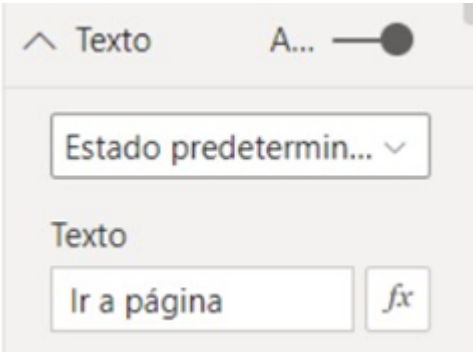


   b. Seleccionar el campo ReportPageName de la tabla PhysicalSecurity

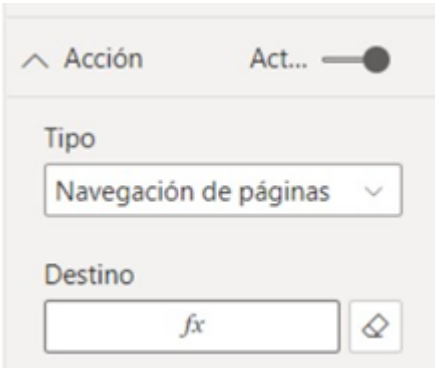


5. Dentro del botón se utiliza la métrica “Navigate to Page” definida en la tabla virtual “navigation table”.

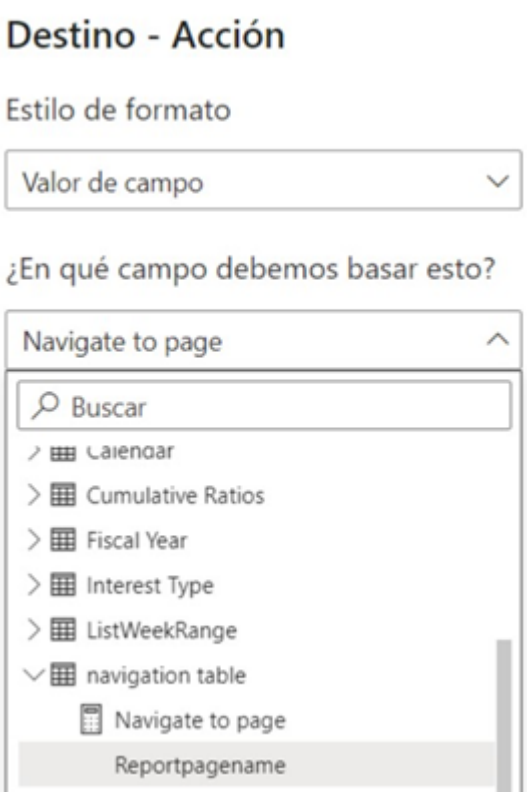




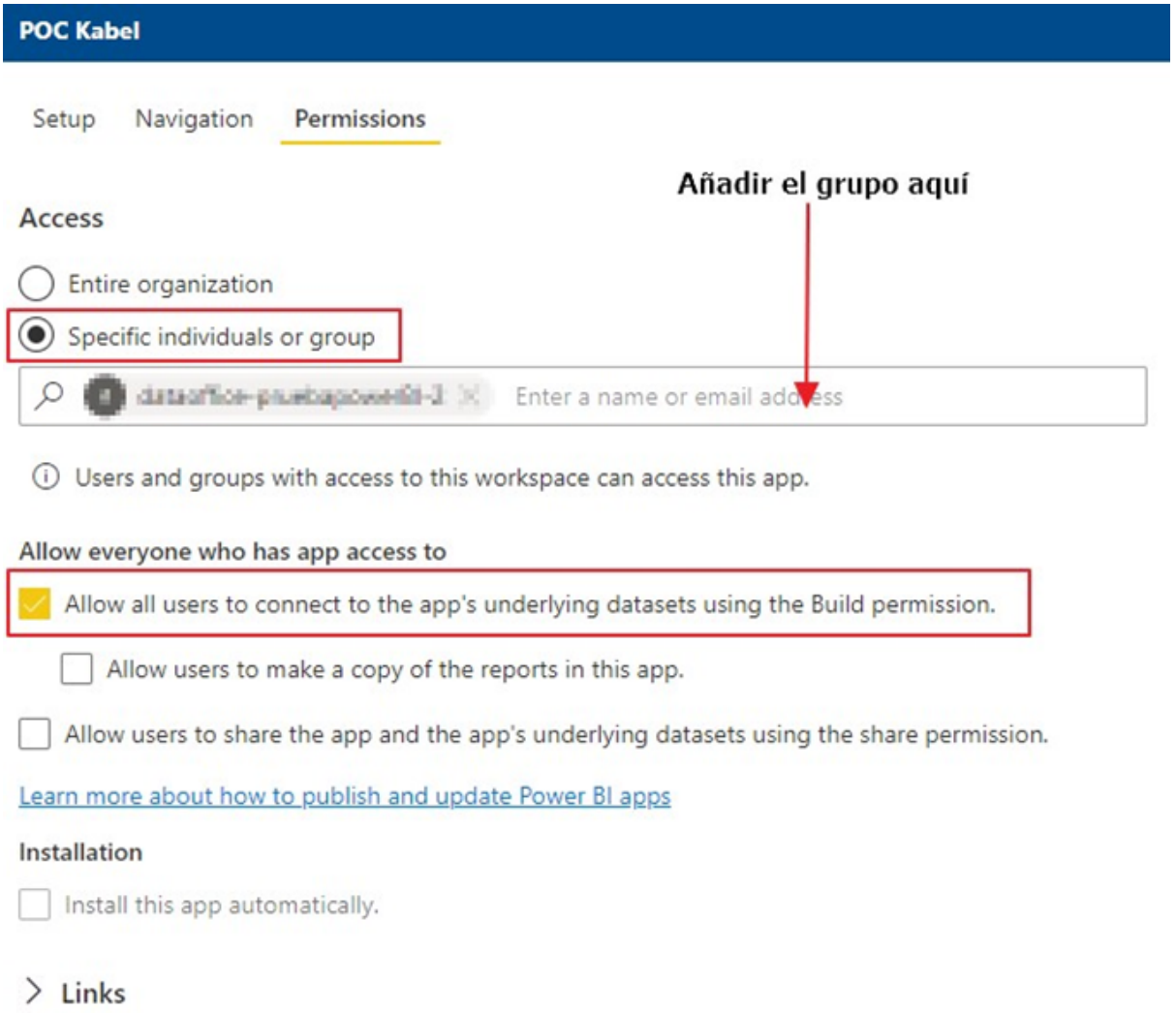
a. En la propiedad “Texto” definir “ir a página”
b. En la propiedad “Acción” del botón elegir tipo “Navegación de páginas” y seleccionar sobre el botón “fx” para indicarle que el destino depende de una métrica



c. Seleccionar la métrica “Navigate to Page” y al pulsar “Aceptar” para guardar:



6. Si todo ha ido bien se sube el informe al workspace que corresponda de Power BI
7. Por último, si es el primer informe que subimos lo añadirá a la App. Tendremos por tanto que asignar el grupo de usuarios XXXXXXXXXXXXXXX a la App de Power BI para que los usuarios que tienen acceso a el informe puedan acceder y marcar el check que permite a los usuarios conectar los datasets subyacentes de los informes.



8. Importante, una App de Power BI puede tener varios informes, al dar acceso a la App se da acceso a todos los informes, hemos parametrizado Anjana para que, aunque se pueda ver esos informes no muestre ningún dato por defecto. Para que pudieran ver datos será necesario que tengan al menos un contrato firmado en Anjana con el dataset subyacente de un informe.
9. Probar que el botón da acceso a la página seleccionada. Si el usuario no tiene permisos de acceso, no le mostrará la página seleccionada.

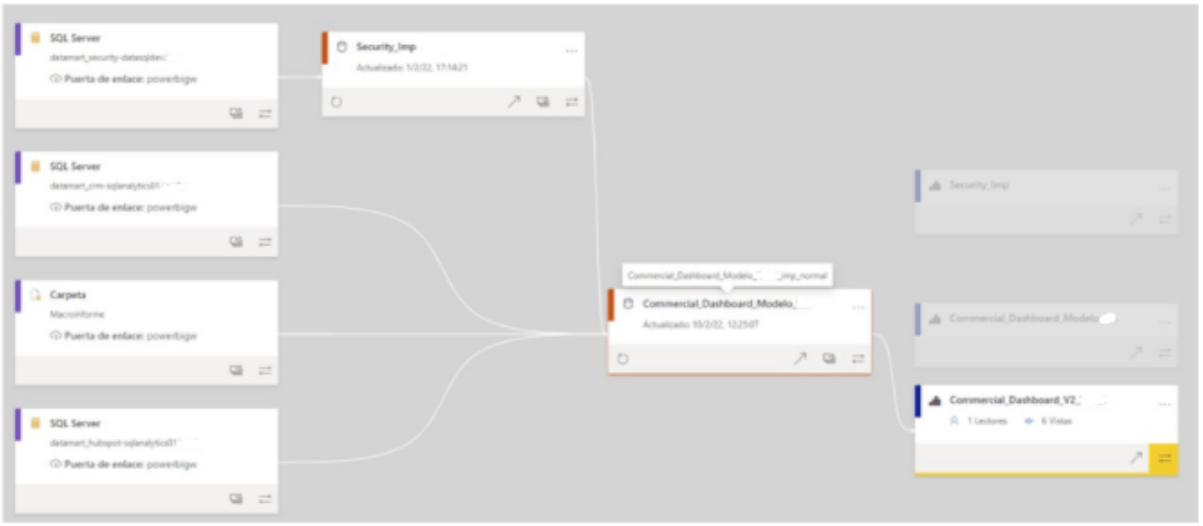
Configuración de acceso por Reducción de Datos (RLS).

La configuración de reducción datos en un informe de Power BI que actúa como dataset aplicará la reducción de datos de un data consumer en todos los informes de Power BI que consuman ese dataset.

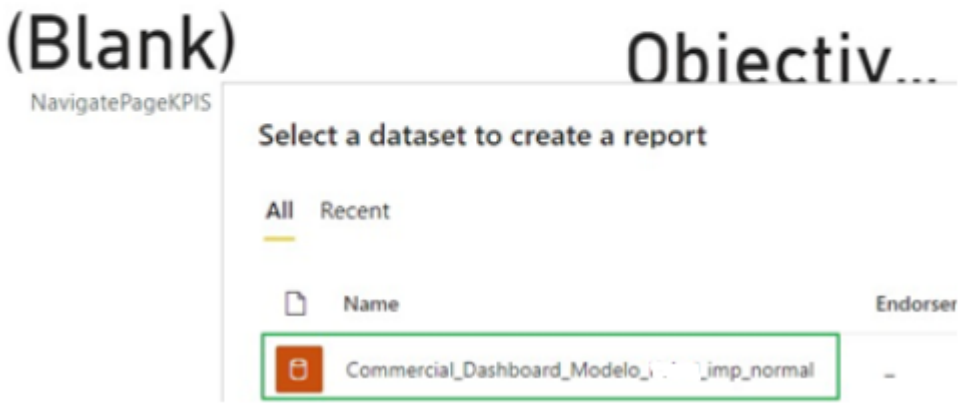
Por ejemplo, si tenemos un dataset y es consumido por los informes I1, I2, I7, la reducción de datos que tenga un usuario basado en los contratos que haya firmado se aplicará en I1, I2 e I7, esto es, si ha firmado contratos que le confieren permisos sobre la business unit XX-Spain y todos los programas en los informes I1, I2 e I7 verá solo esos datos.

Esto es así porque Power BI no permite configurar RLS (Row Level Security) en informes que no tienen datos (datasets).

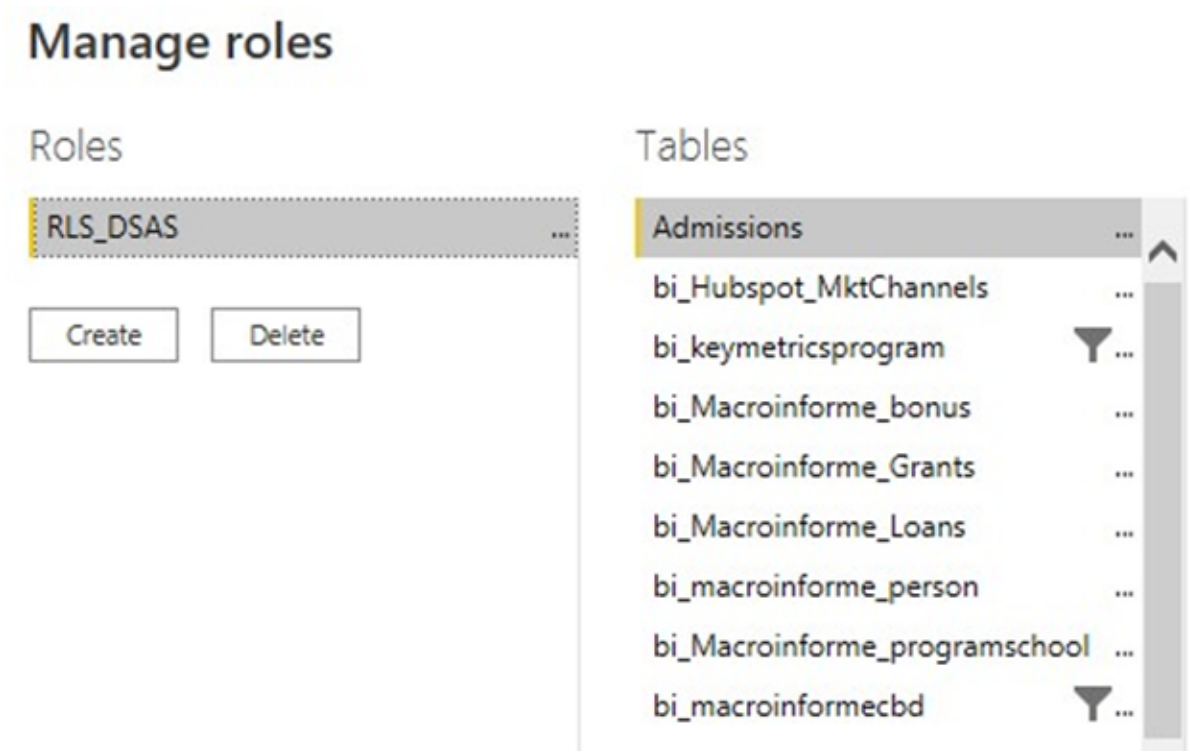
Para este caso, se ha utilizado también el informe denominado “Commercial_Dashboard_V2_XXXX.pbix“, este informe utiliza el dataset “Commercial_Dashboard_Modelo_XXXX_imp_normal.pbix”.



Como se puede ver en la siguiente imagen en el informe Commercial_Dashboard_V2_XXXX no deja crear roles porque no tiene datos, hace direct query al dataset Commercial_Dashboard_Modelo_XXXX_imp_normal:



1. Como comentamos en el apartado esquema dim, para este informe actuaremos filtrando por las dos tablas de dimensiones que tiene:
    a. bi_keymetricsprogram: Programas Comerciales.
    b. bi_macroinformecbd: Business Units



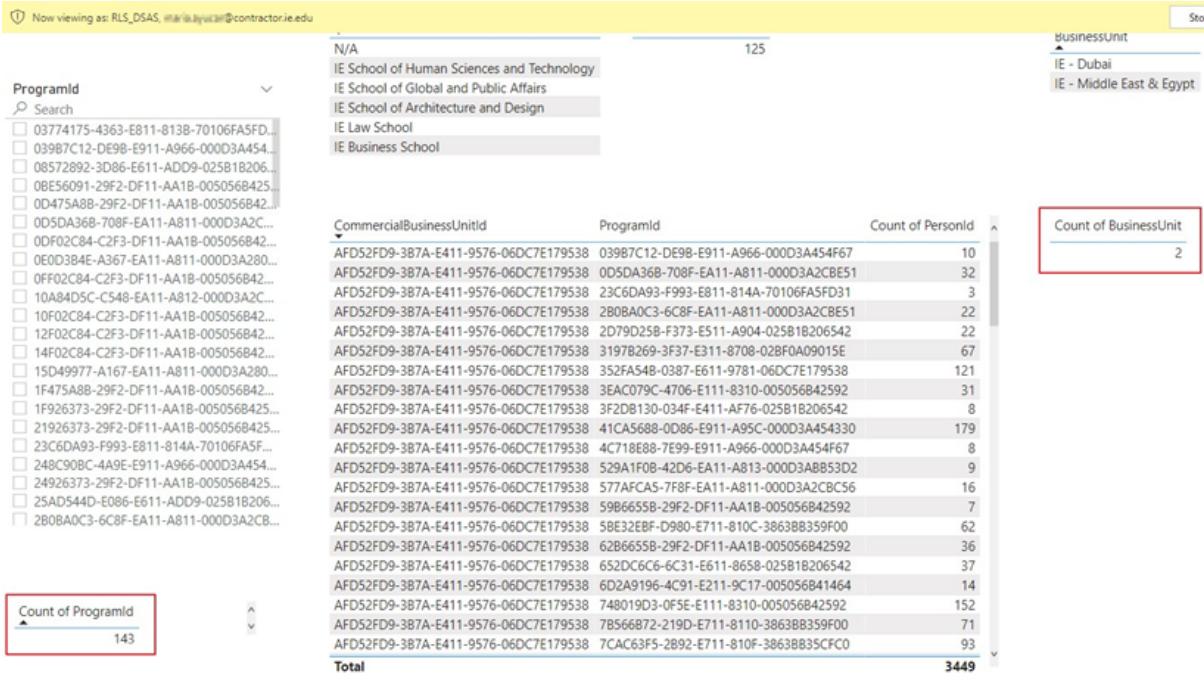
c. Se define la siguiente expresión DAX en la tabla “by_keymetricsprogram” (Programas Comerciales):

```
VAR USR =  USERPRINCIPALNAME ()
VAR dimensionname = "CommercialPrograms"

//SI UN USUARIO TIENE PARAMETRIZADO TODOS LOS PROGRAMAS PUEDE VERLOS TODOS
VAR TODOS_PROGRAMAS =
    SELECTCOLUMNS (
        CROSSJOIN (
            DISTINCT ( bi_keymetricsprogram[ProgramId] ),
            SELECTCOLUMNS (
                FILTER (
                    RLSDSAsUsersWithAllDimensionMembers,
                    RLSDSAsUsersWithAllDimensionMembers[DimensionName] = dimensionname
                        && RLSDSAsUsersWithAllDimensionMembers[email] = USR
                        && RLSDSAsUsersWithAllDimensionMembers[IsDeleted] = "N"
                ),
                "Email", [Email]
            )
        ),
        "ProgramId", [ProgramId]
    )

//LISTA DE PROGRAMAS QUE EL USUARIO TIENE PARAMETRIZADOS (NO SON TODOS)
VAR PROGRAMAS_PARAMETRIZADOS =
    SELECTCOLUMNS (
        FILTER ( RLSCommercialPrograms, RLSCommercialPrograms[Email] = USR
                && RLSCommercialPrograms[IsDeleted]="N"
        ),
        "ProgramId", RLSCommercialPrograms[CommercialProgramIdIE]
    )
RETURN
 [ProgramId] IN    DISTINCT ( UNION ( TODOS_PROGRAMAS, PROGRAMAS_PARAMETRIZADOS ) )
```

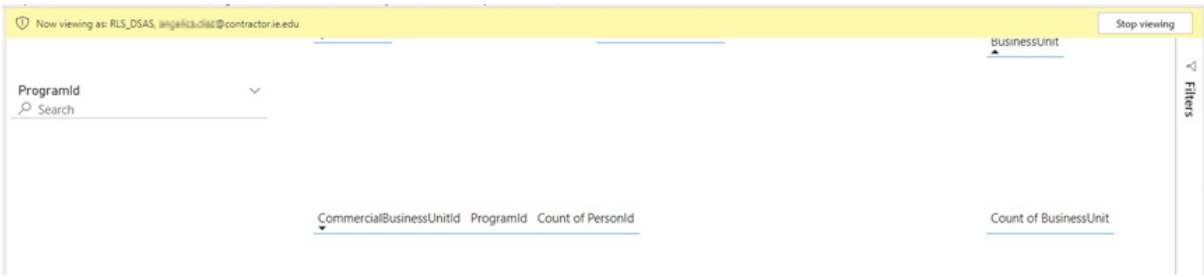
d. Se define la siguiente expresión DAX en la tabla “bi_macroinformecbd” (Business Unit):

```
VAR USR =  USERPRINCIPALNAME ()
VAR dimensionname = "CommercialBusinessUnits"

//SI UN USUARIO TIENE PARAMETRIZADO TODOS LAS BBUU PUEDE VERLAS TODAS
VAR TODAS_BBUU  =
    SELECTCOLUMNS (
        CROSSJOIN (
            DISTINCT ( bi_macroinformecbd[CommercialBusinessUnitId]) ,
            SELECTCOLUMNS (
                FILTER (
                    RLSDSAsUsersWithAllDimensionMembers,
                    RLSDSAsUsersWithAllDimensionMembers[DimensionName] = dimensionname
                        && RLSDSAsUsersWithAllDimensionMembers[email] = USR
                        && RLSDSAsUsersWithAllDimensionMembers[IsDeleted] = "N"
                ),
                "Email", [Email]
            )
        ),
        "CommercialBusinessUnitId", [CommercialBusinessUnitId]
    )

//LISTA DE BBUU QUE EL USUARIO TIENE PARAMETRIZADAS (NO SON TODAS)

VAR BBUU_PARAMETRIZADAS =
SELECTCOLUMNS(
   FILTER(RLSCommercialBusinessUnits,
          RLSCommercialBusinessUnits[Email]=USR
           && RLSCommercialBusinessUnits[IsDeleted]="N"
   )
   ,"CommercialBusinessUnitId"
,RLSCommercialBusinessUnits[CommercialBusinessUnitIdIE]
)

return     [CommercialBusinessUnitId] IN DISTINCT ( UNION ( TODAS_BBUU, BBUU_PARAMETRIZADAS ) )
```

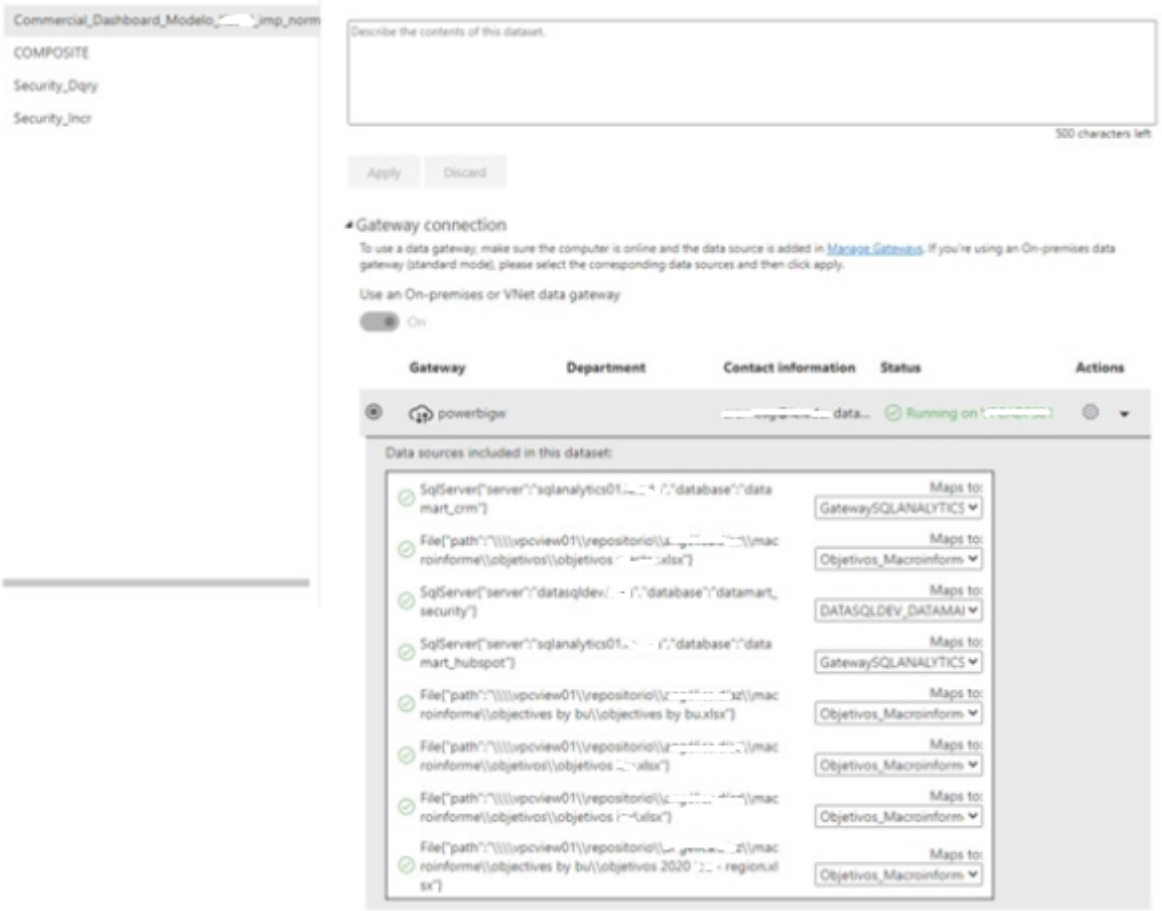
2. Probamos los roles, en nuestro caso vamos a comprobar un par de usuarios:
   a. El primero tiene firmado un contrato donde le da acceso a las business units de Dubai, Oriente Medio, Egipto y todos los Programas de Bachelors, esto es, 2 business units y 143 programas.



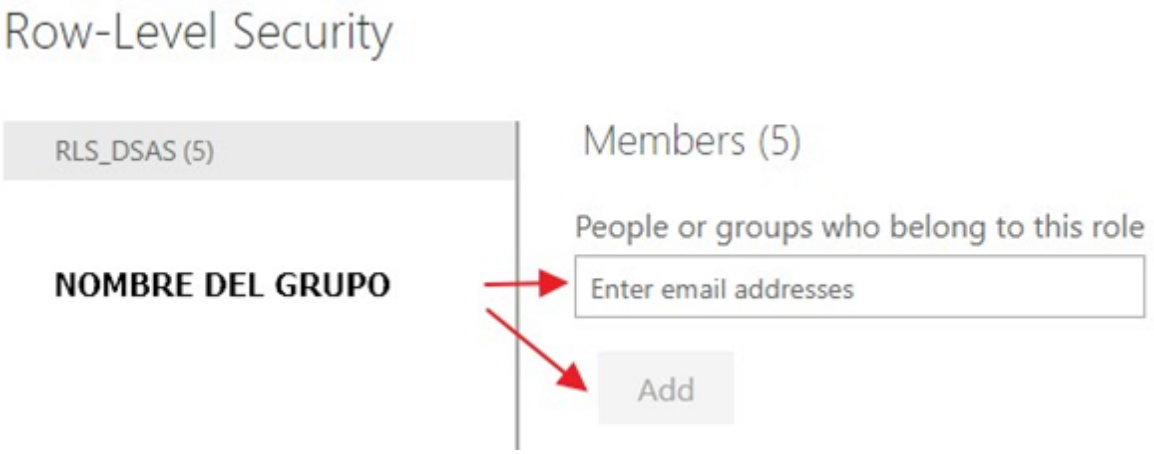
   b. El segundo no puede ver ningún dato.



3. Una vez montado el modelo de datos, la seguridad y probados los roles subimos el informe al servicio de Power BI
4. Configuramos proxies y cadenas de conexión



5. En la pestaña Security añadiremos únicamente al grupo de usuarios XXXXXXXXXXXXXXXXXX. Este grupo también se añadirá a las Apps de Power BI que dan acceso a los usuarios a las aplicaciones donde se meterán a todos los usuarios de Anjana. El cliente debe añadir a este grupo todos los usuarios que vayan a usar Anjana.



6. El cliente deberá por cada usuario que vaya a usar Anjana además de meterlo en el grupo anterior insertar un registro en la tabla “Users” del datamart de seguridad, para que se le pueda asociar parametrización posteriormente
7. Por último, establecemos programaciones para que se actualicen los datos

Cambios que afectan a la Seguridad Después de Implantar un Informe en el servicio de Power BI

Los cambios que afectan a la seguridad después de implantar un informe son 4

Reducción de Datos

Añadir Nueva Dimensión a un Informe

Añadir una nueva dimensión a un informe consiste en:

1. Tablas RLS de dimensiones. Cada informe de Power BI que actúa como dataset puede tener una o varias dimensiones por las que interese hacer reducción de datos. Las dimensiones óptimas para hacer eso son aquellas con menor nivel de granularidad y que tienen una relación directa con las tablas de hechos. Por cada una de esas dimensiones que se quiere hacer reducción de datos habrá que:
    a. Crear una tabla en el esquema dim que contenga todos los distintos valores que puede tener la dimensión más un registro "Unknown" que tendrá el valor -1. La tabla debe seguir el patrón de diseño de tablas citado en este documento, (pk, campo IsDeleted, fechas creación/última actualización, usuario de creación/última actualización). Estas tablas sirven para alimentar los metadatos de referencia de Anjana que a su vez servirán para parametrizar contratos. Ejemplos de ellos son dim.CommercialPrograms y dim.CommercialBusinessUnits
    b. Crear una tabla en el esquema dm_security que recogerá la parametrización asociada a un contrato cuando se selecciona uno o varios valores de esa dimensión (valores de la tabla dim), si se asociará el contrato todos los valores de una dimensión se guardará un registro en la tabla RLSAllDimensions. Como en el ejemplo anterior las tablas deben de seguir el patrón de diseño de tablas citado en este documento, (pk, campo IsDeleted, fechas creación/última actualización, usuario de creación/última actualización). El contenido que almacenan suele ser un valor de dimensión para un informe (el del dataset) y un contrato. Ejemplos de estas tablas son RLSCommercialBusinessUnits y RLSCommercialPrograms.
    c. Sobre las tablas de dimensiones RLS se crean vistas que son las que se importan en el modelo de datos. Estas vistas tienen por cometido mostrar además de los ids las descripciones asociadas a esos ids. Las vistas importadas en este caso son:
        i. RLSSecurityCommercialBusinessUnits se ha importado como RLSCommercialBusinessUnits
        ii. RLSSecurityCommercialPrograms se ha importado como RLSCommercialPrograms
2. En el rol del informe de Power BI que actúa como dataset configuramos la expresión para realizar el filtrado. Ejemplo by_keymetricsprogram

Añadir una Nueva Página Oculta a un Informe

Para añadir una nueva página oculta a un Informe de Power BI:

1. Para el informe que se va a añadir la nueva página ir al Dataset de Anjana y añadir una nueva página a la lista de páginas
2. Creamos o modificamos un contrato en Anjana para dar acceso a esa página en el informe seleccionado
3. Vamos al informe de Power BI que contiene el dataset de datos que consume el informe con la nueva página y refrescamos los datos (para coger la nueva parametrización de Anjana)

4. Seguir los mismos pasos que en el apartado “3.3.2.2 Acceso por páginas, Seguridad física”.

Cambiar una Página Oculta de un Informe a Visible

Para visibilizar una página oculta de un informe:

1. Los data steward y business translator versionaron todos los contratos que tengan esa página oculta en Anjana para que se depreque la versión anterior poniendo una fecha de expiración que les interese (vale fechas a pasado)
2. El equipo de Data Office irá al informe de Power BI que contiene la página oculta y la visibiliza
    a. Subir el informe al servicio de Power BI

Modificación de un Dataset quitándole una/varias Página/s a un Informe

Para quitar una o varias páginas a un dataset que estén en contratos y hayan sido parametrizados, el data steward o el business translator debe:

1. Versionar los contratos que usen ese dataset y página/s para que se depreque la versión anterior poniendo una fecha de expiración que les interese (vale fechas a pasado)
2. Versionar el dataset que tenga esa/s página/s para desligar la dimensión de ellos. Ver punto modificación de un dataset, ello provocará que el registro donde se vincula ese informe y la página el plugin lo marque como borrado (IsDeleted = "Y")
3. Si lo que se desea además de quitarla es borrar la página/s el equipo de Data Offices debe hacer lo siguiente:
    a. a. Borrar la página del informe de Power BI
    b. b. Subir el informe al servicio de Power BI

Modificación de un Dataset quitándole una/varias Dimensión/es a un Informe

Para quitar una o varias dimensiones a un informe de tipo dataset que estén en contratos y hayan sido parametrizados, el data steward o el business translator debe:

1. Versionar los contratos que usen ese dataset y dimensión/es para que se depreque la versión anterior poniendo una fecha de expiración que les interese (vale fechas a pasado)
2. Versionar el dataset que tenga esa/s dimensión/es para desligar la dimensión de ellos. Ver punto modificación de un dataset, ello provocará que el registro donde se vincula ese informe y la dimensión el plugin lo marque como borrado (IsDeleted = "Y"). La tabla es ReportsDimensions

Borrado de una Dimensión

Si una dimensión va a dejar de existir, el data steward o el business translator debe:

1. Versionar los contratos que usen ese dataset y dimensión/es para que se depreque la versión anterior poniendo una fecha de expiración que les interese (vale fechas a pasado)
2. Versionar los dataset que tengan esa dimensión para desligar la dimensión de ellos. Ver punto modificación de un dataset, ello provocará que el registro donde se vincula ese informe y la dimensión el plugin lo marque como borrado (IsDeleted = "Y"). La tabla es ReportsDimensions
3. Modificar la plantilla del DSA para que no se pueda utilizar esa dimensión en el futuro
4. Indicar a alguien del equipo de arquitectura hacer un update en la tabla Dimensions (IsDeleted = "Y") para la dimensión borrada
5. Indicar a alguien del equipo de arquitectura que puede borrar tabla de la dimensión dim

Modificado de una Dimensión

Una dimensión puede ser modificada de dos formas, añadiendo nuevos valores o eliminando los valores existentes.

Añadir nuevos valores a una dimensión

Se requiere actualizar el campo que represente a la dimensión en Anjana añadiendo los nuevos valores.

Y, por supuesto, añadir el registro al esquema de seguridad, en la tabla de datos maestros de la dimensión que corresponda.

Eliminar en una dimensión

Del mismo modo que al añadir valores, es necesario eliminar los valores en el campo que represente la dimensión.
Sin embargo, si dicho valor se está usando en algún objeto de Anjana y como los objetos en Anjana no se borran (excepto por la API administrativa), será necesario editar dichos objetos quitándoles dicho valor antes de eliminar el valor en el campo. Según el estado del objeto es posible que se requiera que la acción se realice por la api administrativa.

En el esquema de seguridad está la opción Eliminar tanto el registro de la tabla de datos maestros de la dimensión como eliminar los registros asociados en la tabla RLS correspondiente.

Otra opción es, en vez de hacer un borrado físico, aprovechar la conexión con Anjana para hacer un borrado lógico, expirando todos los DSAs que están haciendo reducción de datos sobre ese valor que se quiere eliminar, por lo que una vez desaparecido en Anjana y borrado lógicamente en el esquema ya no se aplica ni aplicará a ningún contrato.

Contrato por defecto

En el caso de que se quiera incluir algún tipo de contrato por defecto a los usuarios que se aplique el gobierno activo es necesario hacerlo de manera manual en el esquema.

Primero crear un DSA en la tabla DSAs y añadir los permisos que se quieran asignar de la manera que Power BI interprete (esto varía según el script que se cree), para ello asignar al DSA los registros en las tablas de ReportsPagesDSAs, RLSX y RLSAllDimensions.

Para asignar usuarios a este DSA ficticio se tiene que crear el registro correspondiente en la tabla UsersDSAs.