

Guía técnica para la instalación y configuración de los equipos y software de C.Nord

Primero que nada nos gustaría agradecerles mucho por haber adquirido nuestro equipo de prueba. Esperamos que nuestros productos les satisfagan.

Contenido

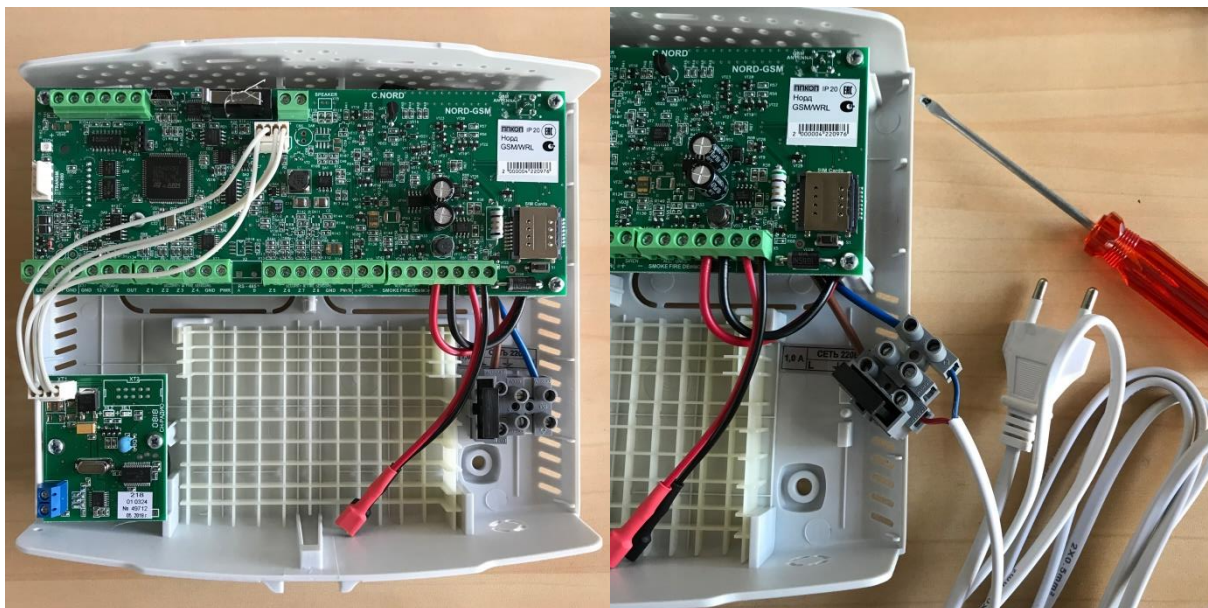
1. Configuración de los paneles y sensores inalámbricos
 - 1.1 Configuración del panel híbrido **Nord GSM WRL** mediante el software **Hubble**
 - 1.1.1 Adición de los sensores inalámbricos al panel

2. Instalación y configuración del software **Security Center**
 - 2.1 Instalación del **Microsoft SQL Server 2017 Express**
 - 2.2 Configuración del **Microsoft SQL Server 2017 Express**
 - 2.3 Configuración del **Firewall de Windows Defender**
 - 2.4 Instalación del **Security Center**
 - 2.5 Configuración y puesta en marcha del **Security Center**
 - 2.5.1 Configuración del **Administrador de eventos**
 - 2.5.2 Adición de nuevos objetos en **Administrador de objetos**
 - 2.5.3 Activación de **MyAlarm** para el nuevo objeto

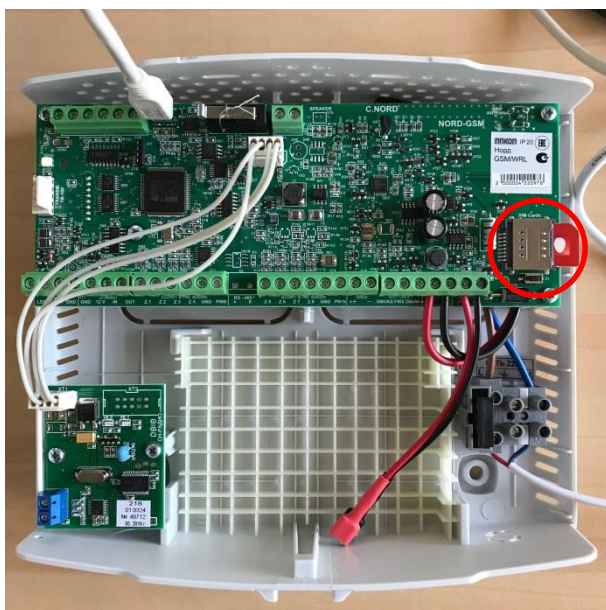
1. Configuración de los paneles y sensores inalámbricos

1.1 Configuración del panel híbrido Nord GSM WRL

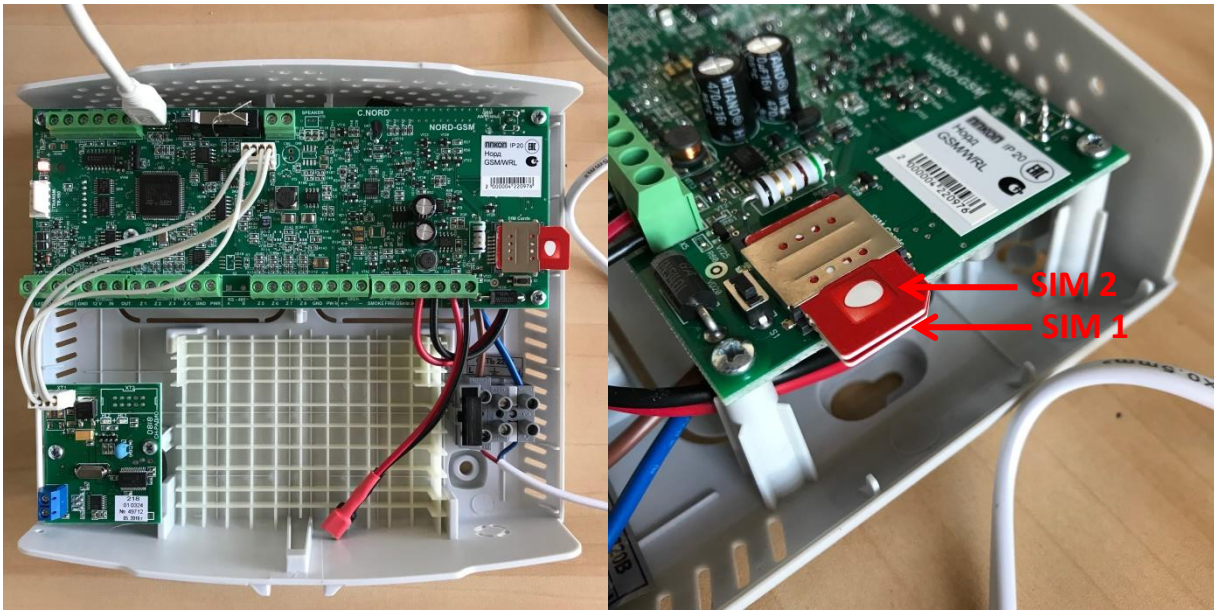
1. Abrir la carcasa del panel y conectar el cable de alimentación a las entradas L y N



2. Insertar el 1-er chip SIM con datos Internet activados en la entrada principal que se encuentra más cerca a la placa

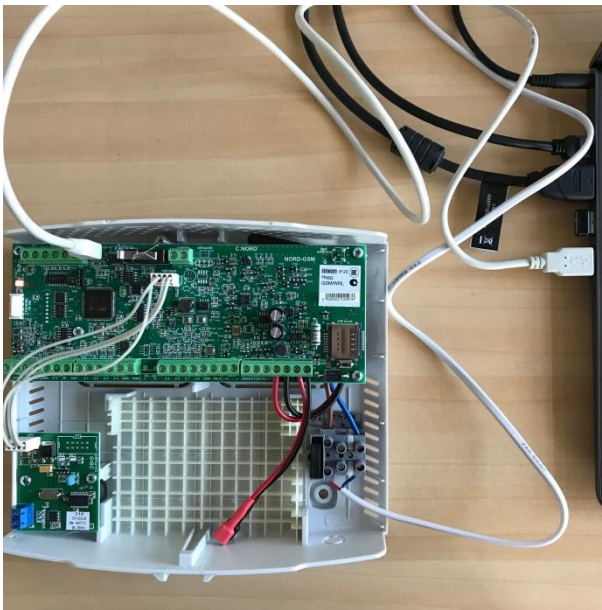


3. Insertar (opcionalmente) el segundo chip SIM con datos Internet activados en la entrada de respaldo que se encuentra por encima de la entrada principal



4. Encender el panel

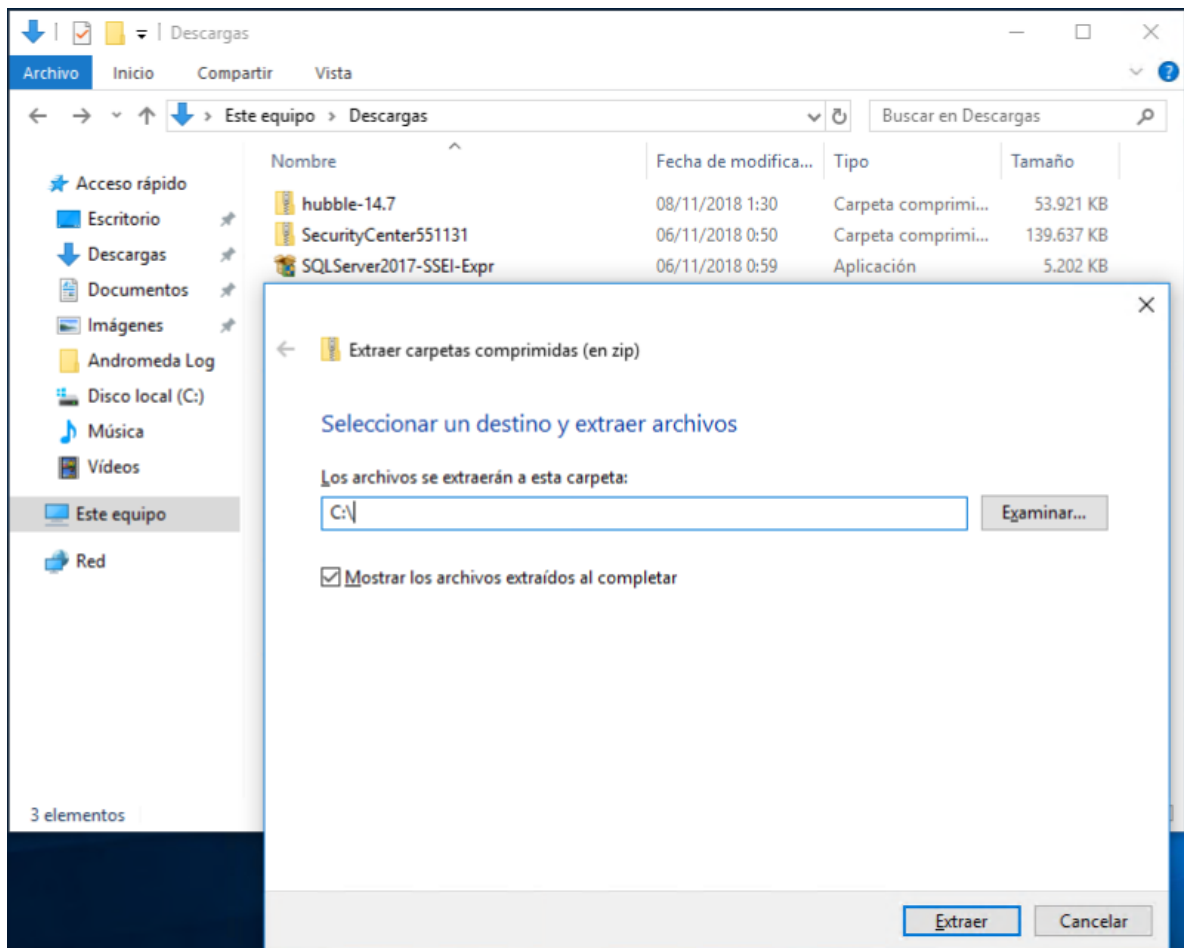
5. Insertar el cable micro-USB en la entrada en la placa del panel y conectarlo al puerto USB de la PC



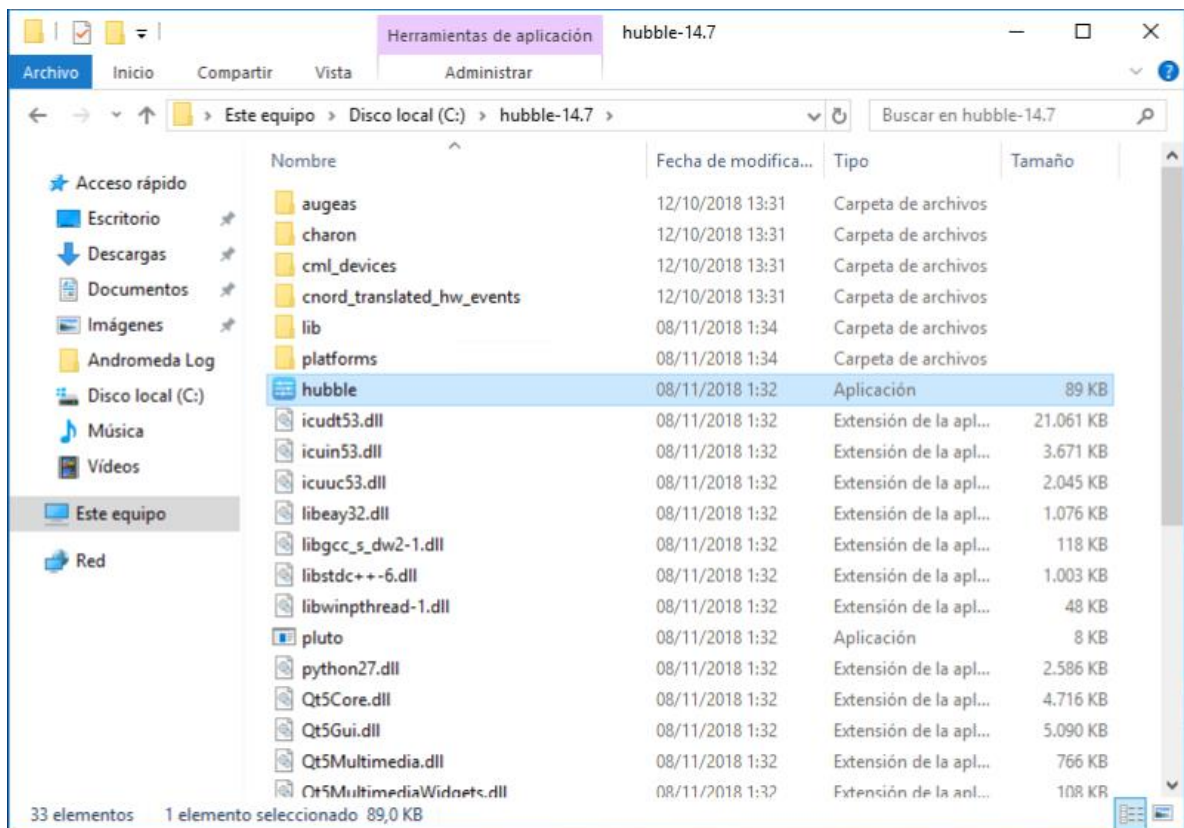
6. Descargar la versión actual del software **Hubble**:

[Descargar aquí](#)

7. Extraer el fichero “hubble-XX.X.zip” en el directorio raíz del disco C:\

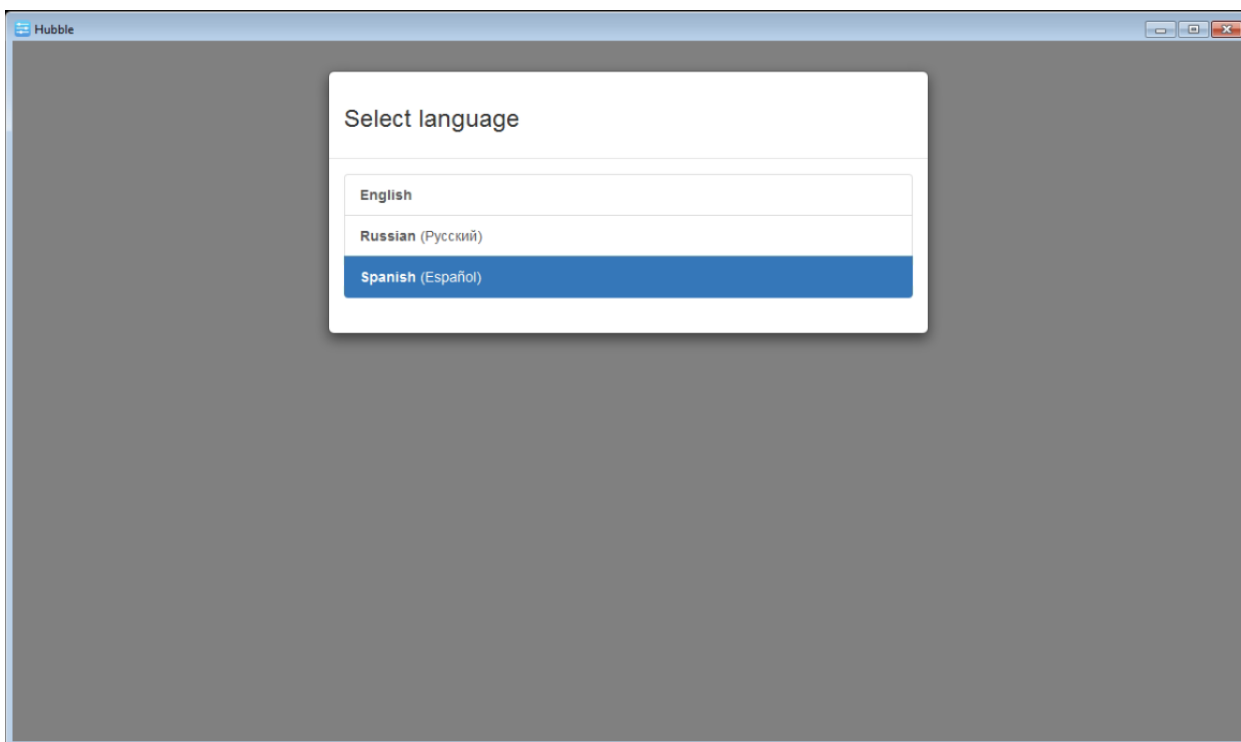


8. Ejecutar el archivo "hubble.exe" del directorio raíz C:\hubble-XX.X

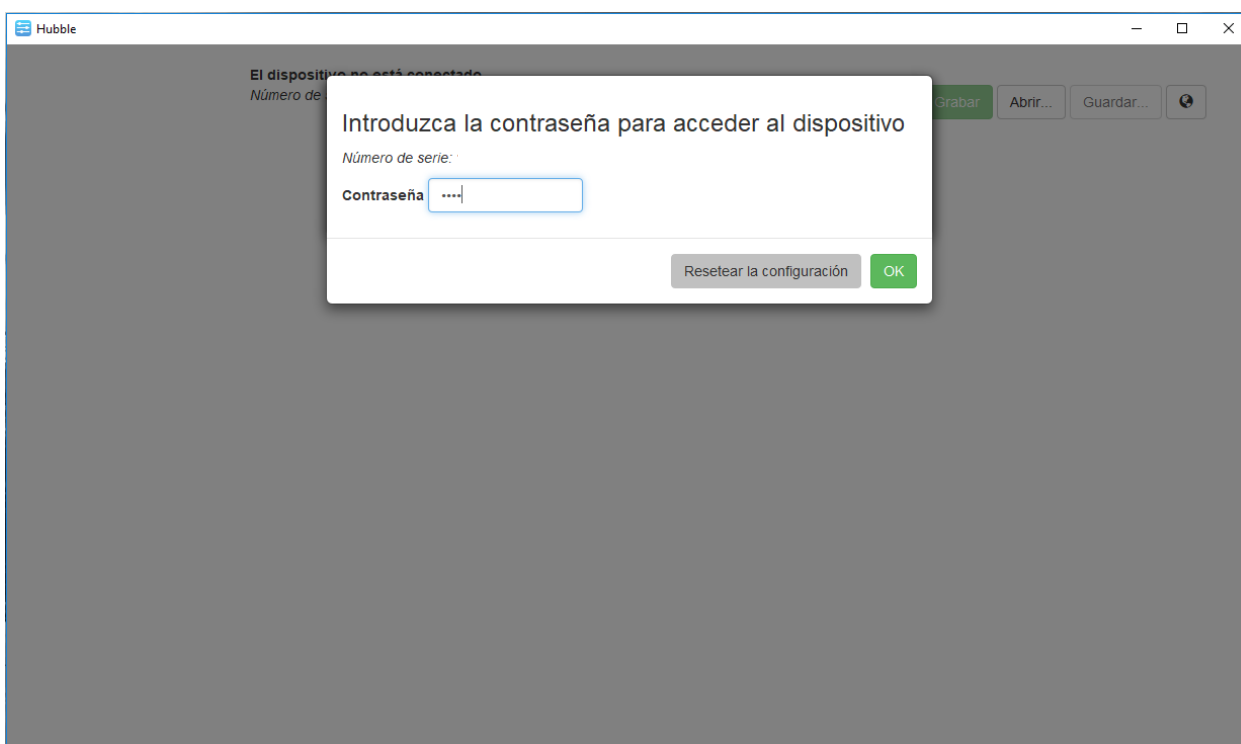


NB! El software Hubble no requiere instalación en la PC.

9. En la ventana emergente seleccionar el idioma

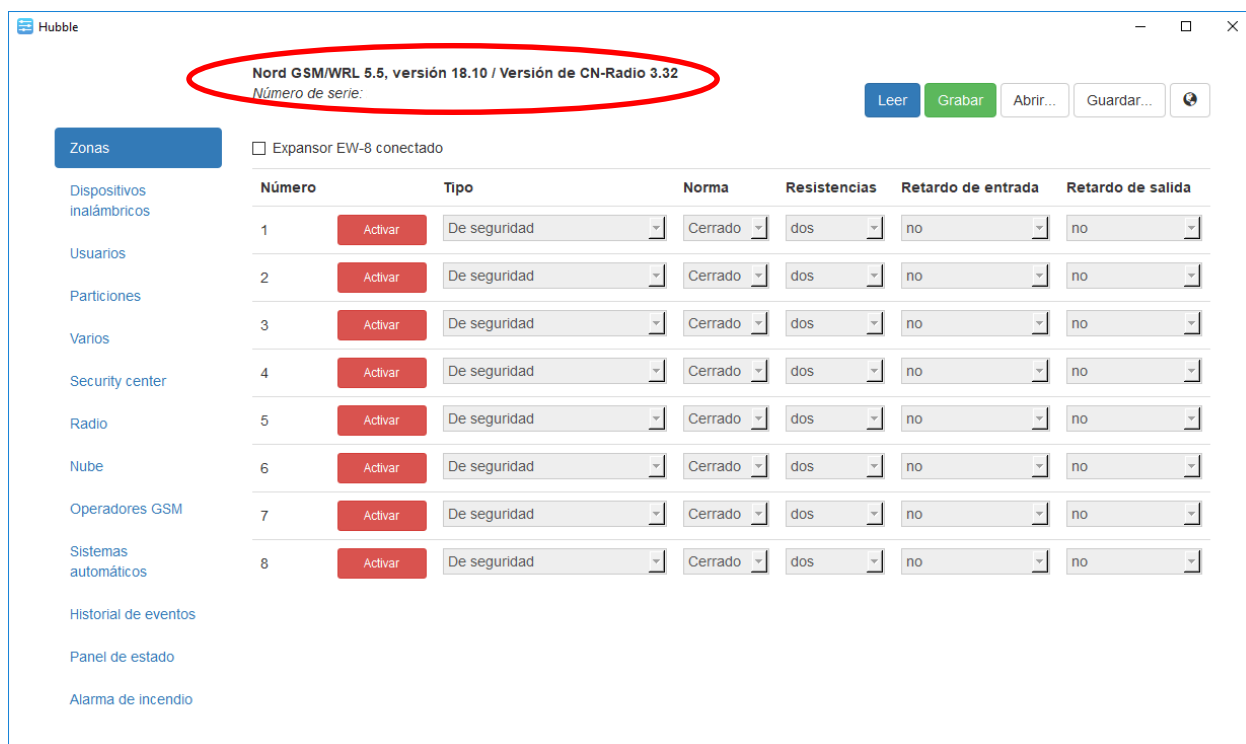


10. Introducir la contraseña para acceder al dispositivo. Por defecto es "0000". Presionar **OK**.

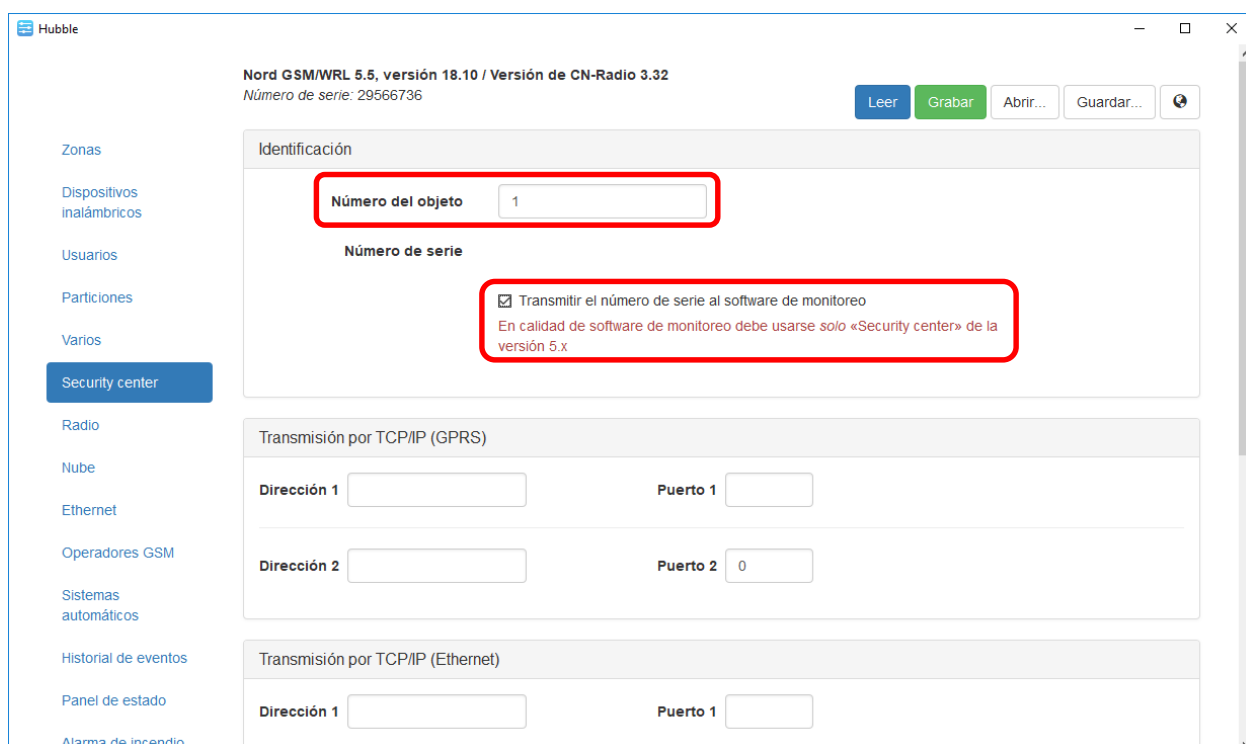


11. Se abrirá la ventana del **Hubble** con toda la información para configuración del panel. En la parte superior izquierda de la ventana se visualiza el modelo del panel, su versión del firmware y la versión del módulo CN-Radio. También aparece el número de serie del panel que es individual y se utiliza como número identificador.

NB! No comparta el Número de serie con terceros.



12. Acceder a la sección **Security center** y en la subsección **Identificación** ingresar el **Número del objeto** que es el número que se asigna al objeto en el módulo Administrador de objetos (Site manager) del software de monitoreo Security Center (véase subsección 2.5.2). Marcar la casilla frente a **Transmitir el número de serie al software de monitoreo**.



13. En la subsección **Transmisión por TCP/IP (GPRS)** ingresar la **Dirección 1** y el **Puerto 1** que son la dirección IP o nombre DNS y puerto externo del servidor dónde se instaló el SC (véase puntos 7-14 de la subsección 2.5.1). Si para la conexión al servidor está utilizado el comunicador de red (*Ethernet Adapter*,

que es opcional) ingresar también la **Dirección 1** y el **Puerto 1** en la subsección **Transmisión por TCP/IP (Ethernet)**

The screenshot shows the 'Security center' configuration page in the Hubble interface. The left sidebar lists various settings categories. The main content area is divided into three sections:

- Identificación:** 'Número del objeto' is set to 1. 'Número de serie' is empty. A checkbox 'Transmitir el número de serie al software de monitoreo' is checked. A note below states: 'En calidad de software de monitoreo debe usarse solo «Security center» de la versión 5.x'.
- Transmisión por TCP/IP (GPRS):** 'Dirección 1' is 'gw.cnord.ru' and 'Puerto 1' is '10006'. 'Dirección 2' and 'Puerto 2' are both set to 0.
- Transmisión por TCP/IP (Ethernet):** 'Dirección 1' is 'gw.cnord.ru' and 'Puerto 1' is '10007'. 'Dirección 2' and 'Puerto 2' are both set to 0.

14. En la sección **Varios** marcar las casillas frente a las opciones **Permitir el arme y desarme remoto desde el «Security center»** y **Activar códigos de desarme bajo obligación**.

The screenshot shows the 'Arme y desarme' configuration page in the Hubble interface. The page contains several checkboxes and a text area:

- Prohibir el arme en caso de alarma en las zonas con retardo de salida
- Prohibir el arme en caso de que no esté disponible la fuente principal de alimentación (AC)
- Prohibir el arme al no haber comunicación IP con «Security center»
- Permitir el arme y desarme remoto desde el «Security center»
- Activar códigos de desarme bajo obligación

Below the checked options, there is a text area explaining the 'Activar códigos de desarme bajo obligación' option:

Se considera código de desarme bajo obligación el código que se diferencia del código del usuario en una unidad en dirección mayor o menor. Por ejemplo, si el código del usuario es «1234», los códigos de desarme bajo obligación serán «1233» y «1235». Teniendo en cuenta:

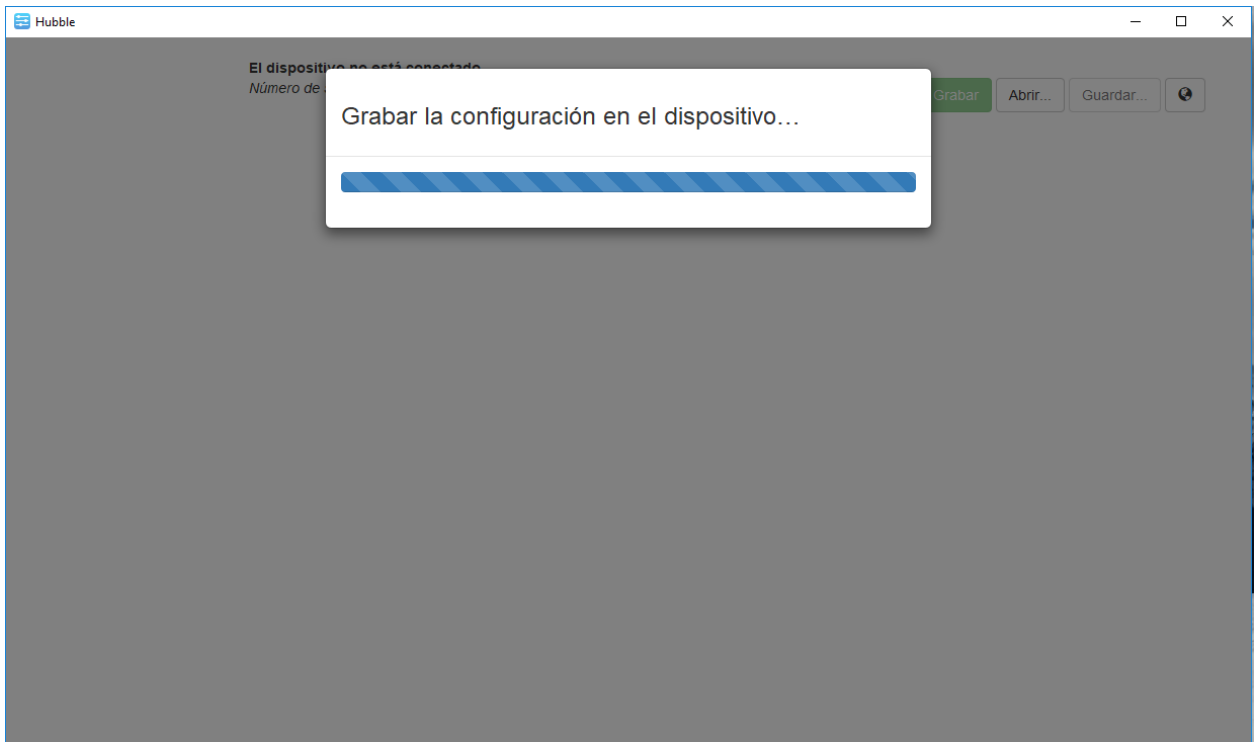
- si el código del usuario termina con el número «0», el código de desarme bajo obligación solo será uno – en una unidad superior. Por ejemplo, si el código del usuario es igual a «5840», el código de desarme bajo obligación solo será el código «5841».
- si el código del usuario termina con el número «9», el código de desarme bajo obligación también será solo uno – en una unidad inferior. Por ejemplo, si el código del usuario es igual a «5849», el código de desarme bajo obligación solo será el código «5848».

Other options include:

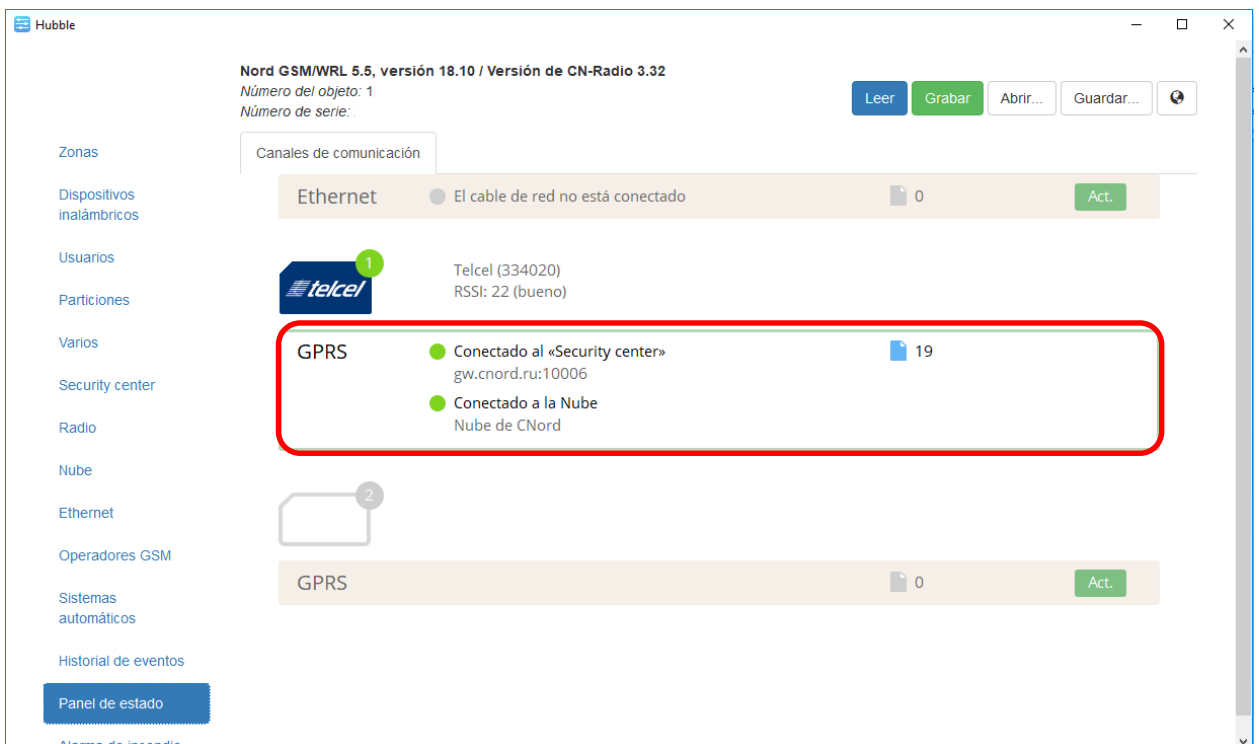
- No indizar el retardo de entrada en CN-Keypad
- Activar el soporte de códigos temporales

At the bottom, there is a field for 'Secreto para la generación de códigos temporales' with the value 'LJ3Tgh4KY2w9QQEDszLV' and a refresh button.

15. Guardar la configuración presionando el botón verde **Grabar** en la parte superior derecha de la ventana.

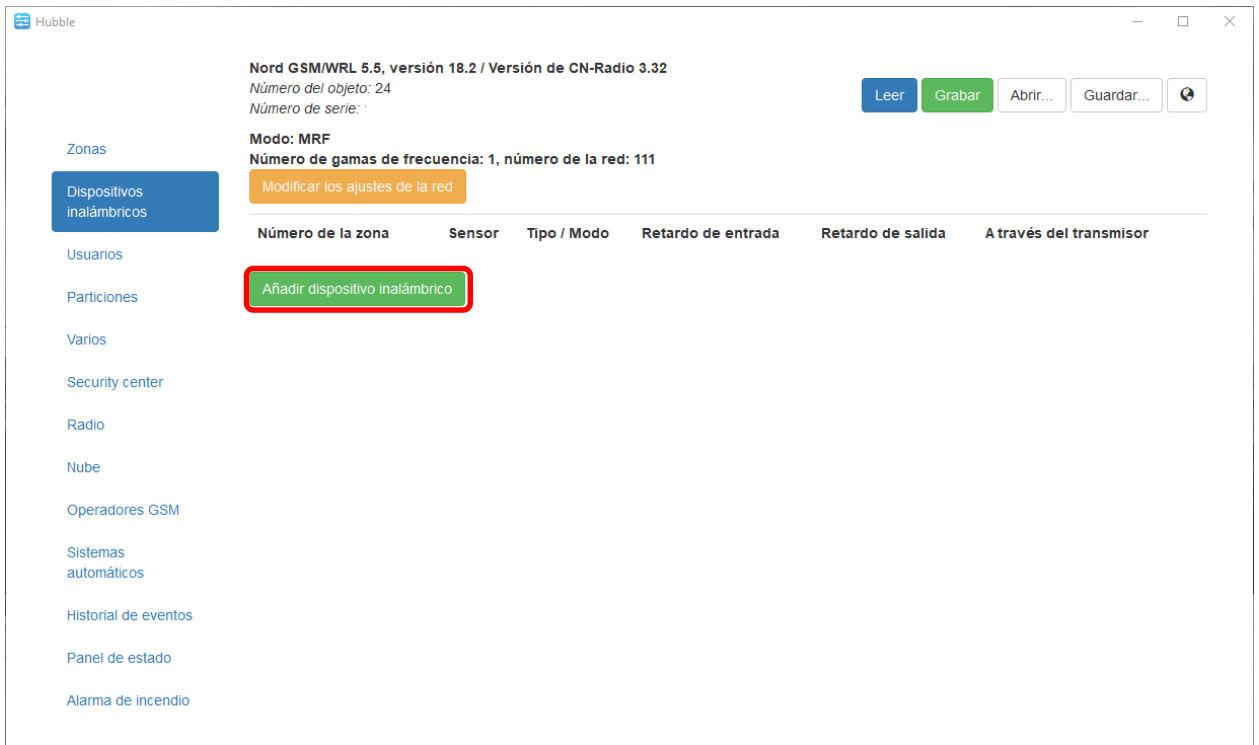


16. Después del reinicio automático del panel acceder a la sección **Panel de estado** y verificar la conexión del panel al **Security Center** y a la **Nube**.

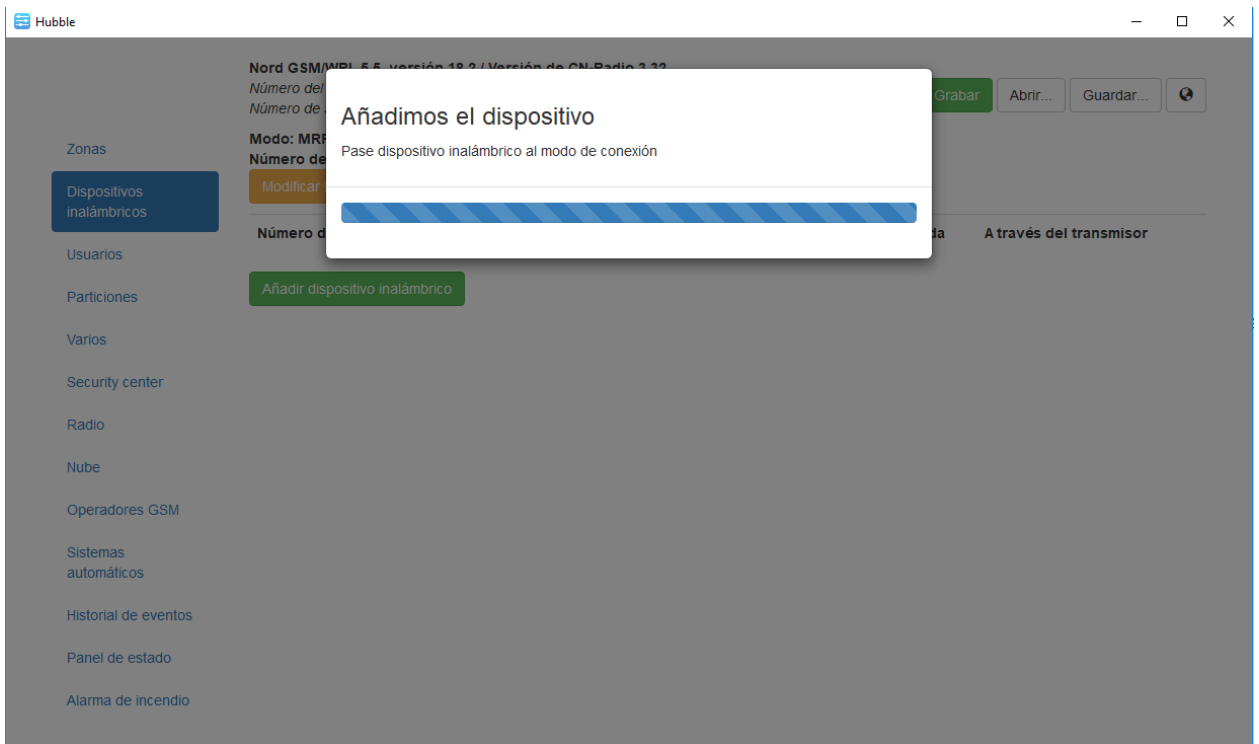


1.1.1 Adición de los sensores inalámbricos al panel

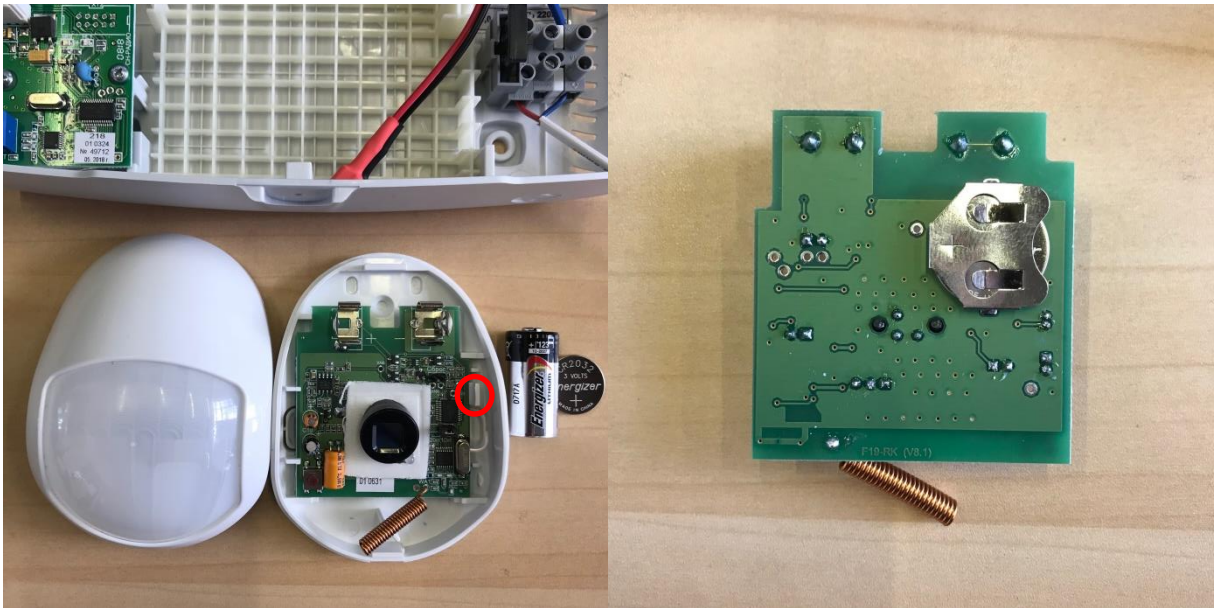
1. Iniciar el **Hubble** y acceder a la sección **Dispositivos inalámbricos**



2. Presionar el botón verde **Añadir dispositivo inalámbrico**



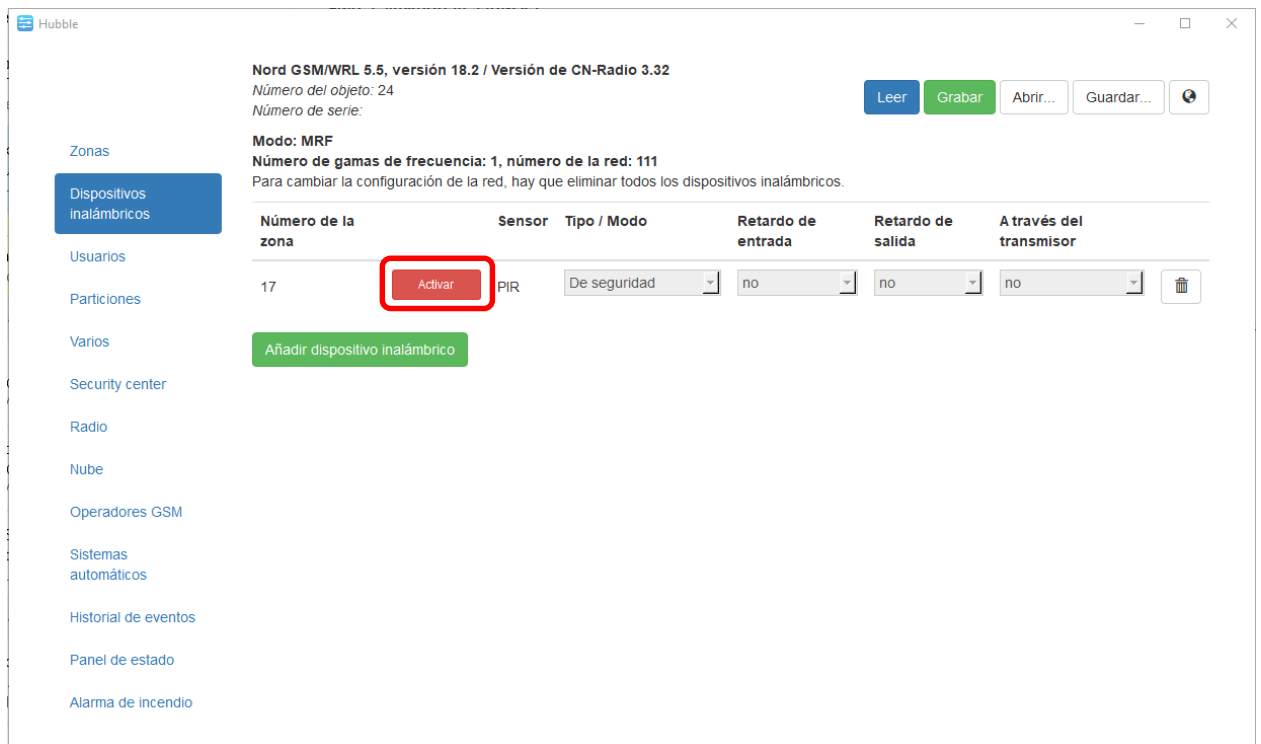
3. Recoger el sensor inalámbrico (en nuestro caso es un sensor infrarrojo de movimiento **CN-PIR**) y abrir la carcasa. Desmontar la placa presionando el sujetador marcado en la foto abajo con un círculo rojo. Insertar la batería de respaldo (CR2032) que se encuentra en la parte lateral de la placa.



4. Volver a montar la placa en la carcasa e insertar la batería principal (CR123A). El parpadeo del indicador verde indica que el dispositivo automáticamente pasó en el modo de conexión con el panel en el cual permanecerá durante 70 seg. Cerrar la carcasa del sensor.



5. Al aparecer el sensor en el listado de los dispositivos inalámbricos con el número de zona asignado presionar el boton **Activar** frente a él.

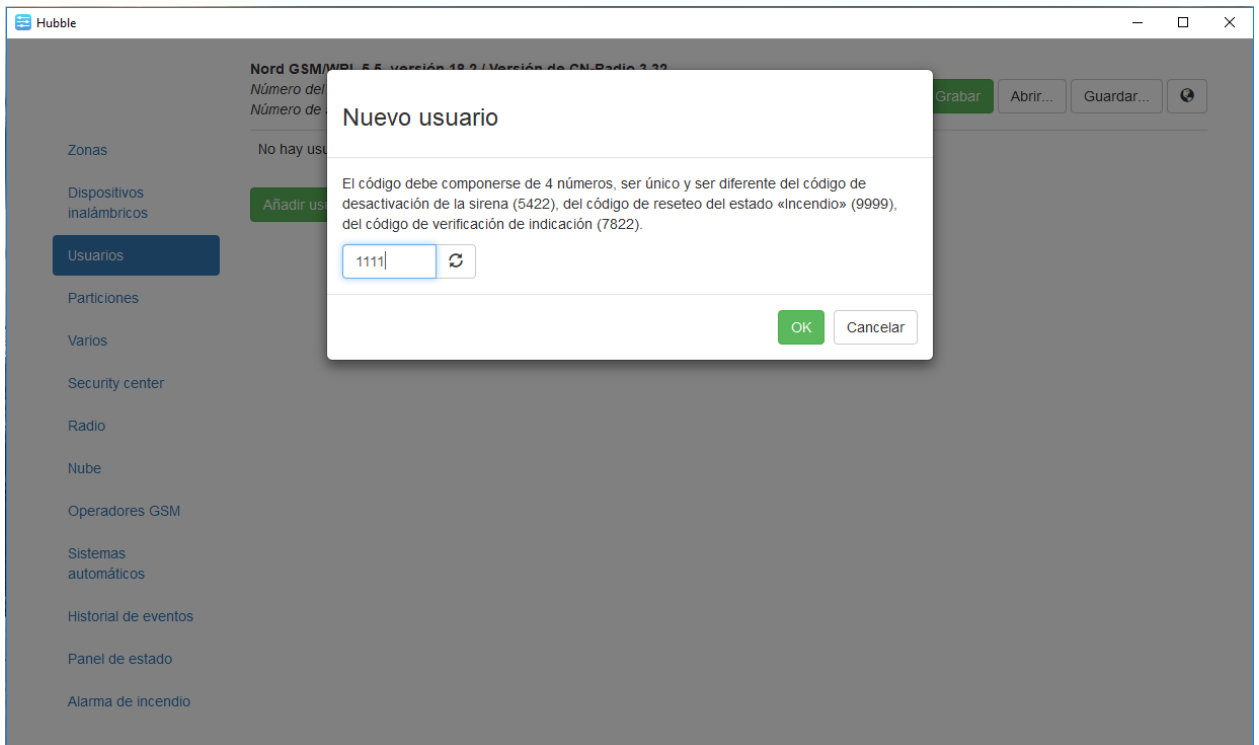


NB! La activación de otros tipos de sensores inalámbricos se realiza de la misma manera

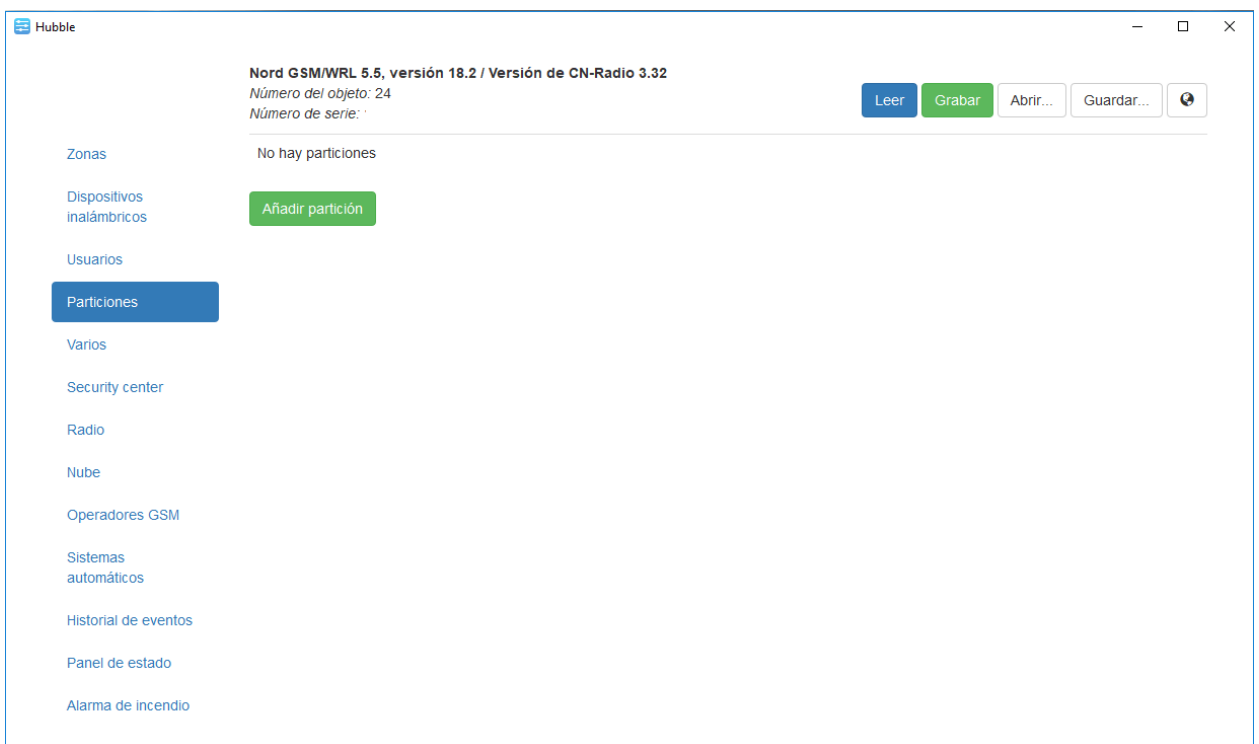
6. Después de que el sensor se activó con éxito se puede asignar **Retardo de entrada** y **Retardo de salida** para esa zona si hay necesidad.



7. Seguir a la sección **Usuarios** y presionar **Añadir usuario**. Ingresar el código de seguridad para el nuevo usuario. Presionar **OK**.



8. Seguir a la sección **Particiones** y presionar **Añadir partición**.



9. En la tabla aparecerá la nueva línea con el número de la partición en el orden ascendente. Para la partición recién creada seleccionar del menú deslizante **Añadir zona** en la columna **Zonas** la zona de seguridad existente.



10. Del menú deslizante **Añadir código** en la columna **Arme y desarme** seleccionar el usuario al que se le asignará derechos de armar y desarmar esa partición.



11. Guardar la configuración presionando el botón verde **Grabar** en la parte superior derecha de la ventana.

12. Después del reinicio automático del panel acceder a la sección **Panel de estado** y en la pestaña **Dispositivos inalámbricos** verificar el estado actual del sensor PIR. El número que aparece en el círculo es el número de la zona inalámbrica que se le asignó al sensor automáticamente después de su adición al panel. El anillo de color verde (rojo, amarillo) demuestra el nivel de la señal entre el panel y el sensor.



13. Haciendo click con el mouse izquierdo sobre el icono del sensor se puede acceder a la información más detallada.

The screenshot shows the Hubble software interface. At the top, it displays 'Nord GSM/WRL 5.5, versión 18.2 / Versión de CN-Radio 3.32', 'Número del objeto: 24', and 'Número de serie:'. There are buttons for 'Leer', 'Grabar', 'Abrir...', 'Guardar...', and a globe icon. A sidebar on the left lists various menu items: Zonas, Dispositivos inalámbricos, Usuarios, Particiones, Varios, Security center, Radio, Nube, Operadores GSM, Sistemas automáticos, Historial de eventos, Panel de estado, and Alarma de incendio. The main content area has two tabs: 'Dispositivos inalámbricos' (selected) and 'Canales de comunicación'. Under the selected tab, there is a circular progress indicator and a text box explaining that the ring's fill level indicates communication quality. Below this, a sensor card for '17, PIR' shows a 'Calidad de comunicación: 92%' and status for 'Carcasa cerrada', 'Batería principal conectada', and 'Batería de reserva conectada'.

Nord GSM/WRL 5.5, versión 18.2 / Versión de CN-Radio 3.32
Número del objeto: 24
Número de serie: :

Leer Grabar Abrir... Guardar...

Dispositivos inalámbricos Canales de comunicación

El anillo alrededor del número y el nombre del sensor actúa en calidad de indicador de la calidad de comunicación con el sensor inalámbrico. El nivel de relleno del anillo en por cientos corresponde a la relación de la señal / ruido en la señal, recibida del dispositivo inalámbrico, medida por el receptor "CN-Radio".
El valor equivalente al 10%, es el mínimo posible para garantizar una comunicación estable con el dispositivo inalámbrico.

17, PIR
Calidad de comunicación:
92%
Carcasa cerrada
Batería principal conectada
Batería de reserva conectada

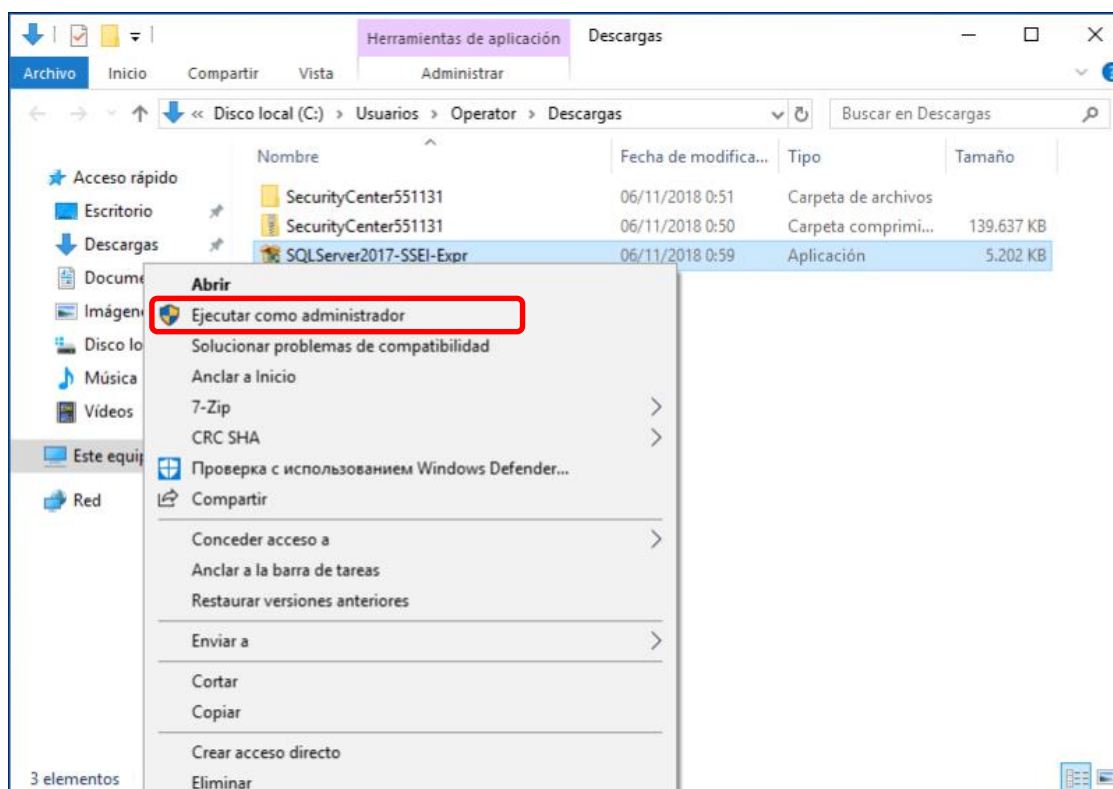
Zonas
Dispositivos inalámbricos
Usuarios
Particiones
Varios
Security center
Radio
Nube
Operadores GSM
Sistemas automáticos
Historial de eventos
Panel de estado
Alarma de incendio

2. Instalación y configuración del software Security Center

NB! Se recomienda hacer la instalación del programa Security Center en la PC con el SO licenciado Windows 7 or 10 con las últimas actualizaciones, 4GB de memoria RAM y disco duro SSD. Sería mejor que el sistema sea vacío, sin programas adicionales como bases de datos SQL, firewall, antivirus.

2.1 Instalación del Microsoft SQL Server 2017 Express

1. Descargar desde el sitio web oficial el programa [Microsoft SQL Server 2017 Express](#)
2. Ejecutar el archivo **SQLServer2017-SSEI-Expr** como Administrador



3. Seleccionar el tipo de la instalación **Básica**

SQL Server 2017 Express Edition



Seleccione un tipo de instalación:

Básica

Seleccione el tipo de instalación Básica para instalar la funcionalidad de motor de base de datos de SQL Server con la configuración predeterminada.

Personalizado

Seleccione el tipo de instalación Personalizada para ejecutar paso a paso el asistente para instalación de SQL Server y elija los elementos que quiera instalar. Este tipo de instalación es detallado y lleva más tiempo que la instalación Básica.

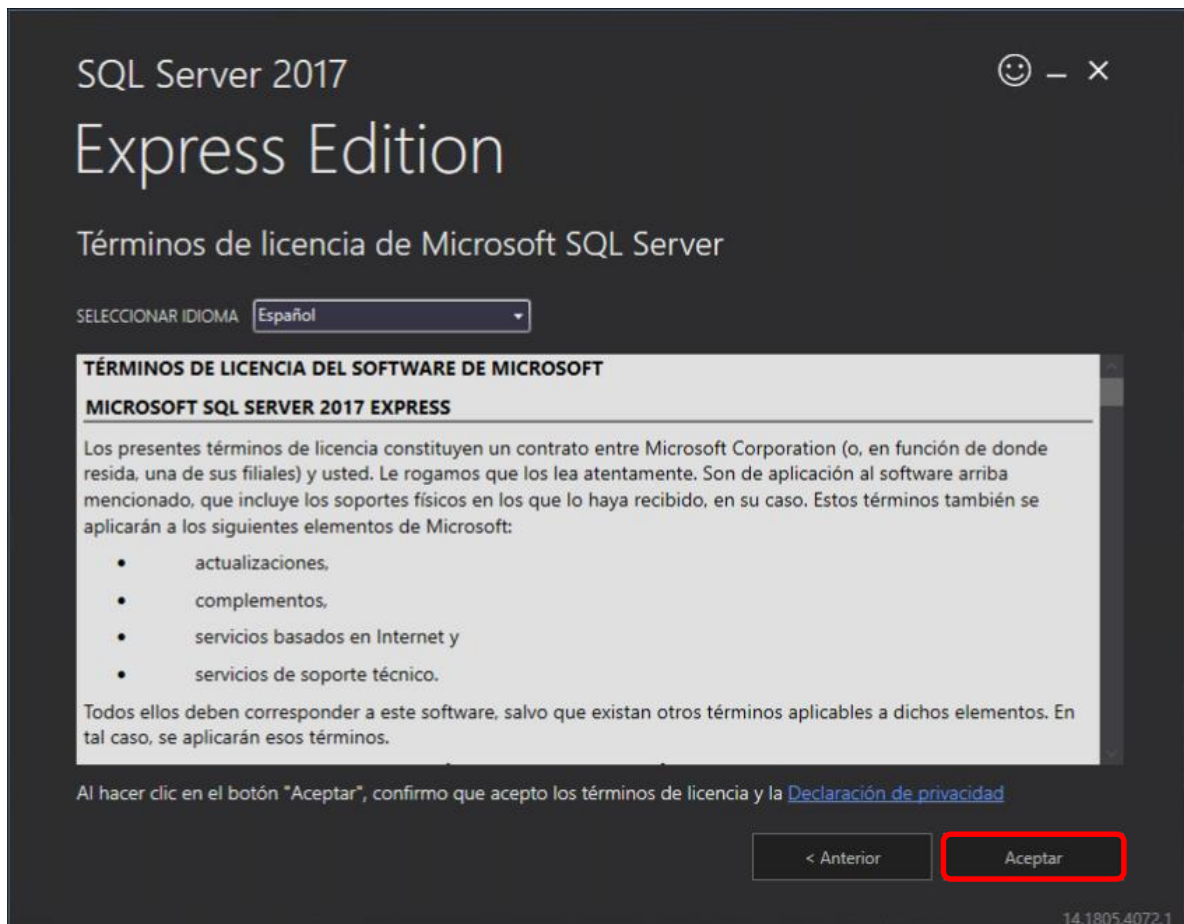
Descargar medios

Descargue los archivos de instalación de SQL Server ahora e instálelos más tarde en una máquina de su elección.

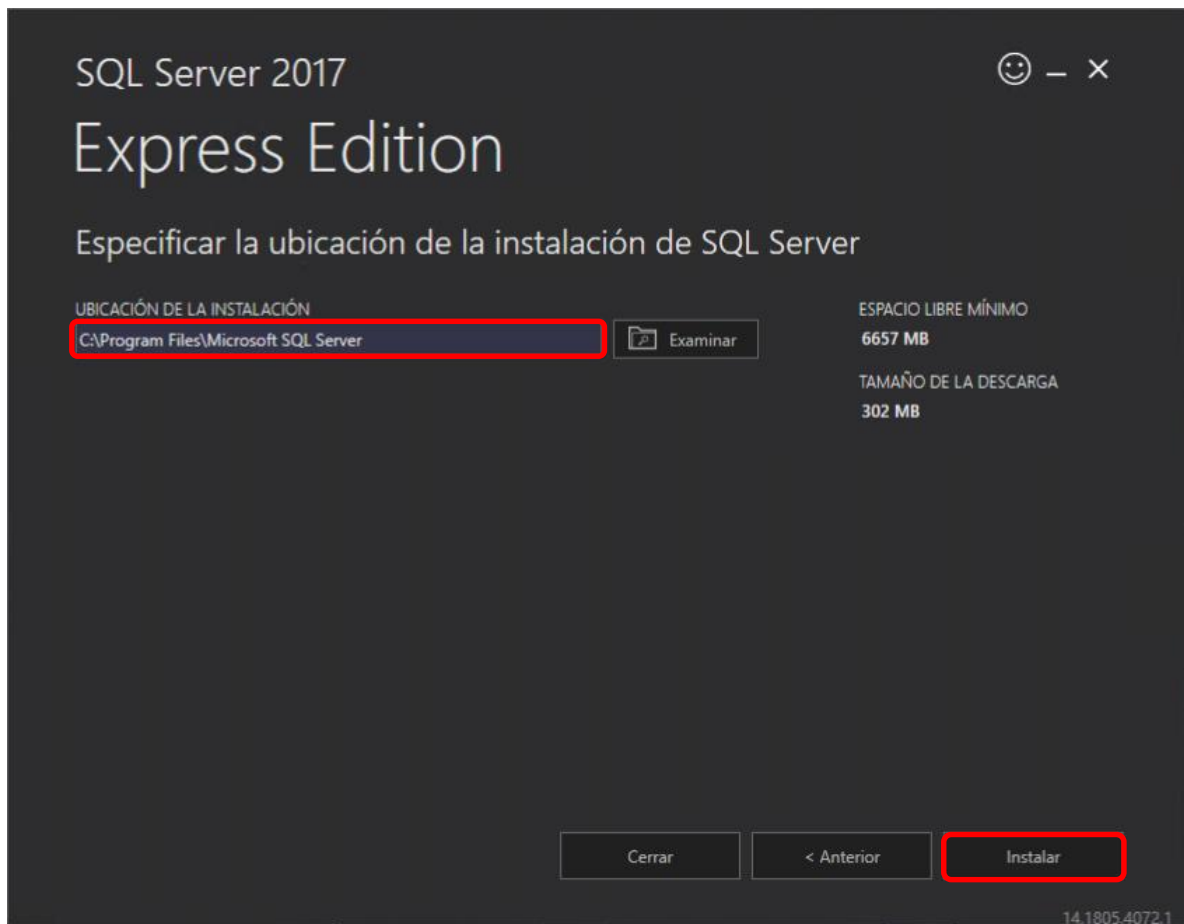
SQL Server transmite a Microsoft información sobre su experiencia de instalación, así como otros datos de uso y rendimiento, con el fin de mejorar el producto. Para obtener más información sobre el procesamiento de datos y los controles de privacidad, y para desactivar la recopilación de esta información después de la instalación, vea [documentación](#)

14.1805.4072.1

4. Seleccionar el idioma del **SQL Server 2017** y presionar **Aceptar**



5. Seleccionar la carpeta para la instalación y presionar **Instalar**



6. Esperar hasta el final de la descarga e instalación

SQL Server 2017 Express Edition



Descargando el paquete de instalación...



Adquiriendo archivos de instalación... 32,819 MB / 294,898 MB 54,117 Mbps

Muestras

Use el repositorio oficial de Microsoft en GitHub, que contiene ejemplos de código para SQL Server (<https://github.com/Microsoft/sql-server-samples/tree/master/samples>), para observar ejemplos de conexión a una base de datos de SQL Server, ejemplos de desarrollo con varias características como OLTP en memoria, R-Services, etc.

También puede utilizar el repositorio de ejemplos de bases de datos de Azure SQL e implementación de referencia (<https://github.com/Azure/azure-sql-database-samples>) para obtener diferentes ejemplos de implementación de referencia para C#, java, node.js, php, python, etc. Tendrá que cambiar el nombre del servidor de forma conveniente en su cadena de conexión cuando utilice estos ejemplos.

Pausar

Cancelar

14.1805.4072.1

SQL Server 2017 Express Edition



La descarga se ha completado correctamente.



Instalando...



Instalando SQL Server... Acción en curso: SaveConfigurationFile

Introducción a SQL Server

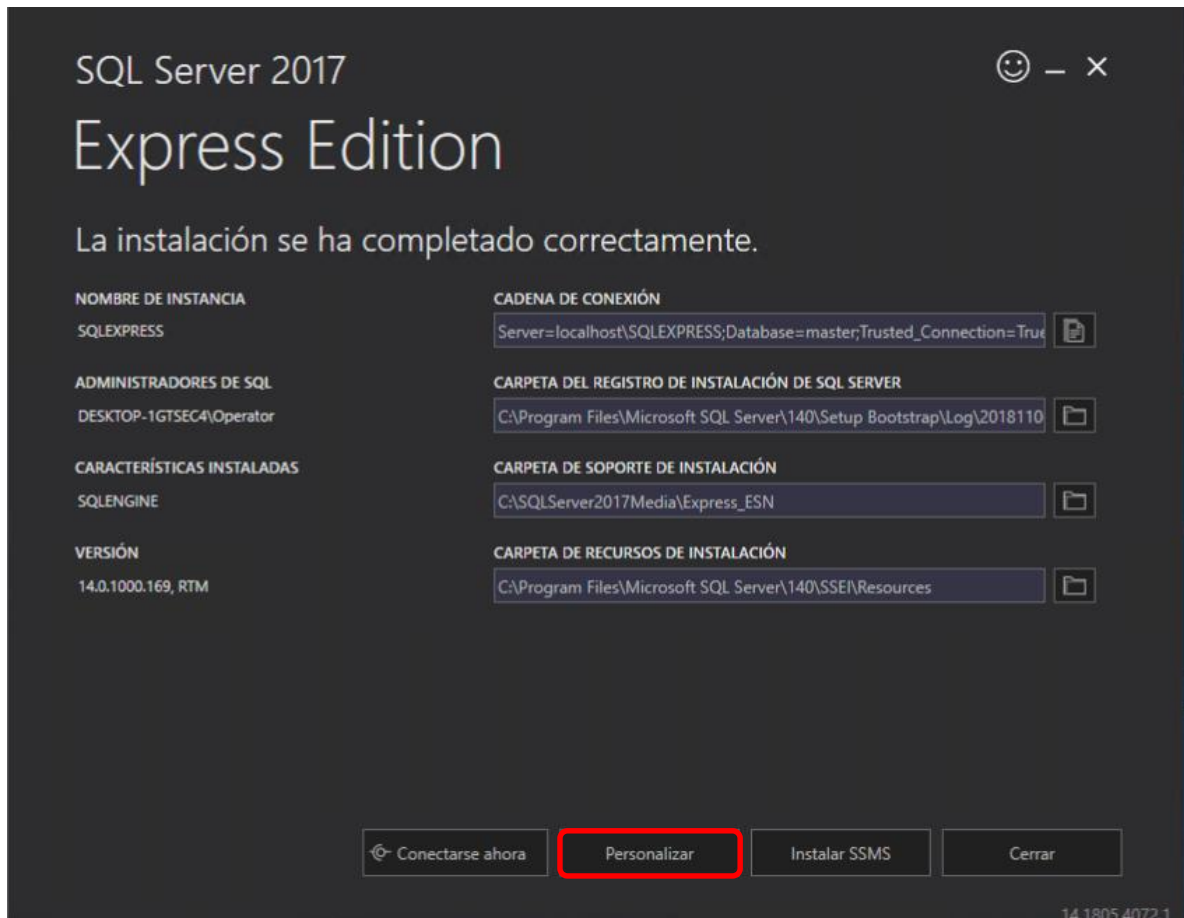
Gracias por instalar Microsoft SQL Server. Si se está conectando a SQL Server desde una máquina remota, necesitará completar los requisitos previos mencionados en "Antes de comenzar", que se encuentra ubicado en la carpeta Recursos.

Pausar

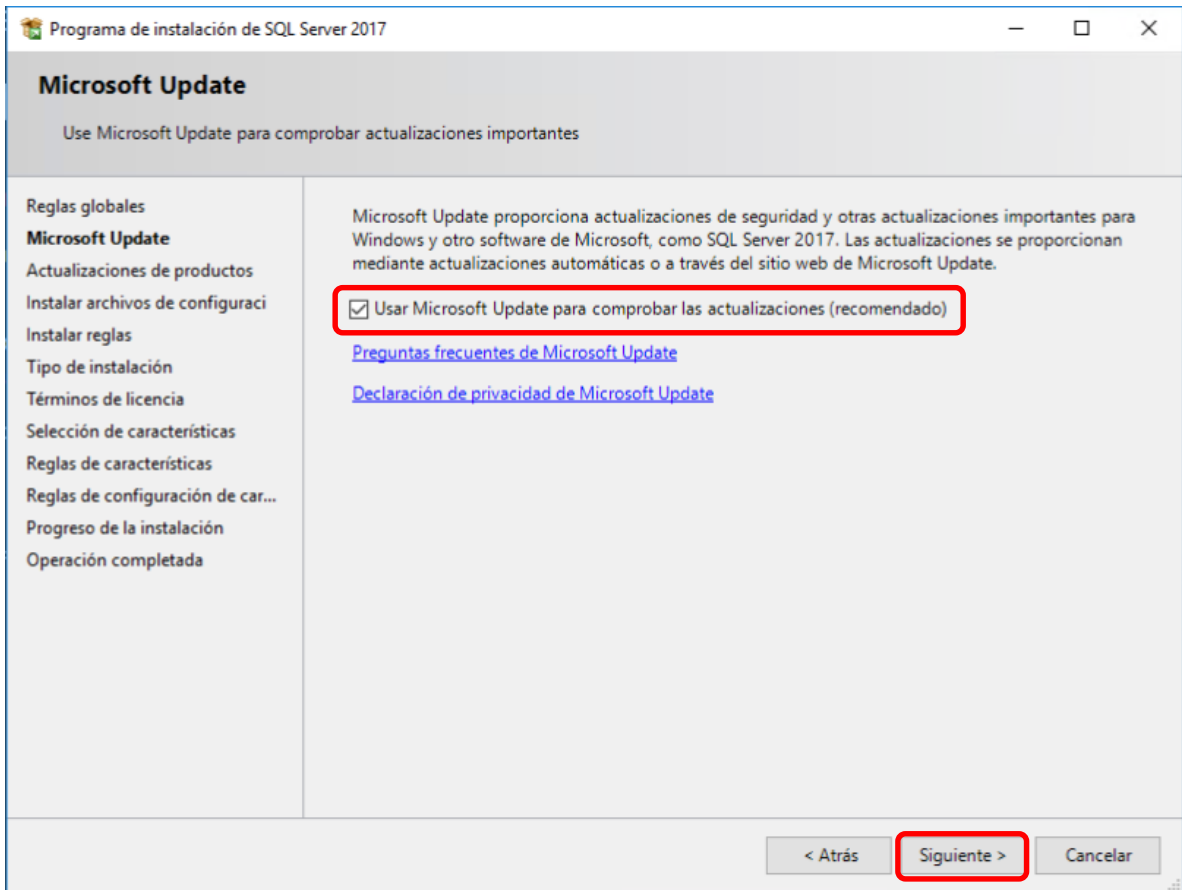
Cancelar

14.1805.4072.1

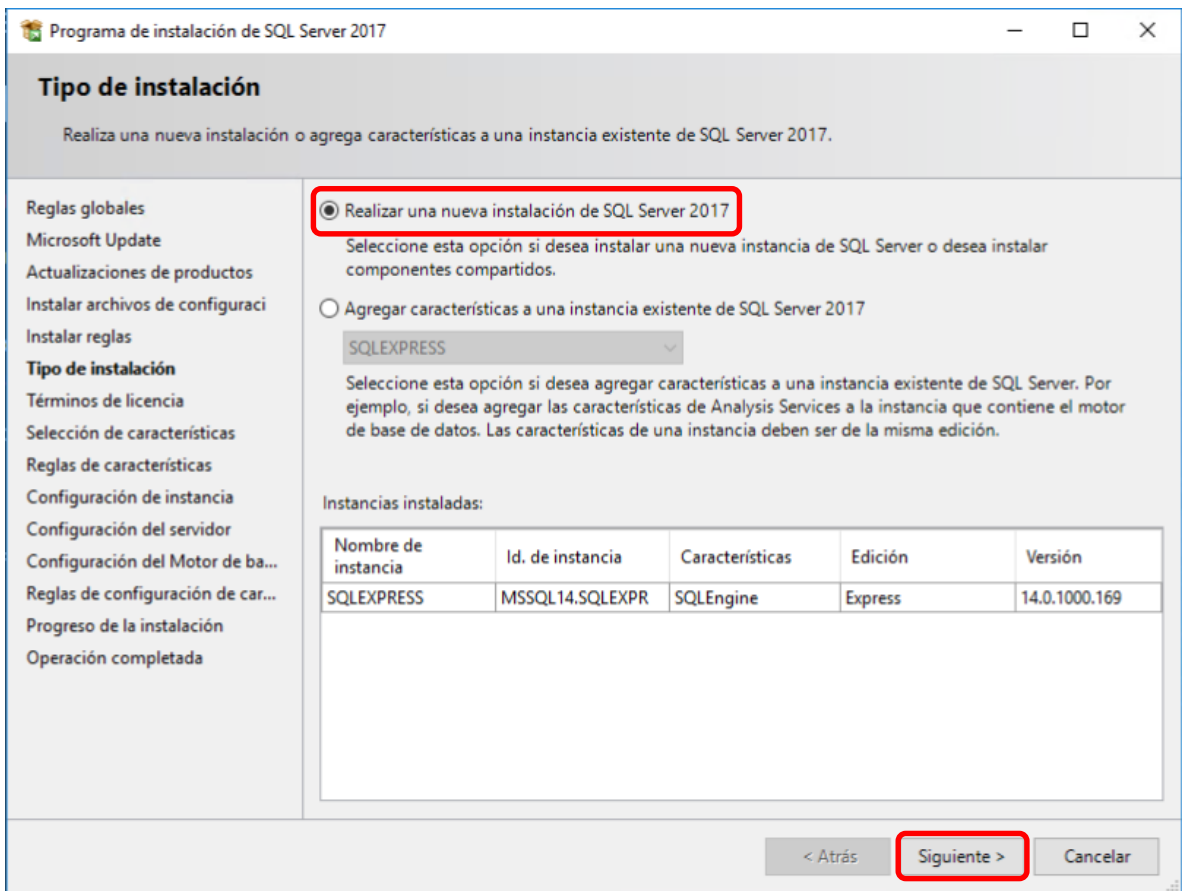
7. Al completar el proceso de la instalación presionar el botón **Personalizar**. Se abrirá la nueva ventana.



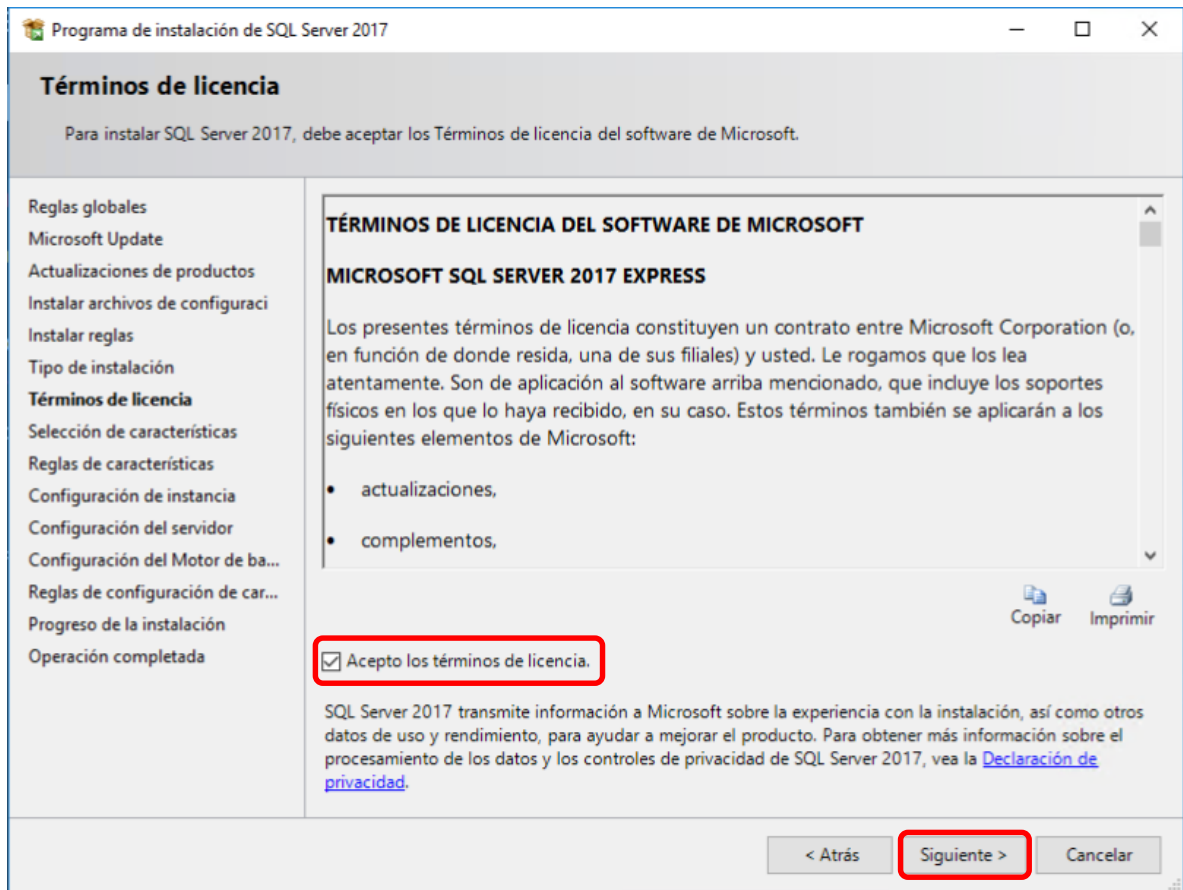
8. Seleccionar la opción **Usar Microsoft Update...** y presionar el botón **Siguiente**



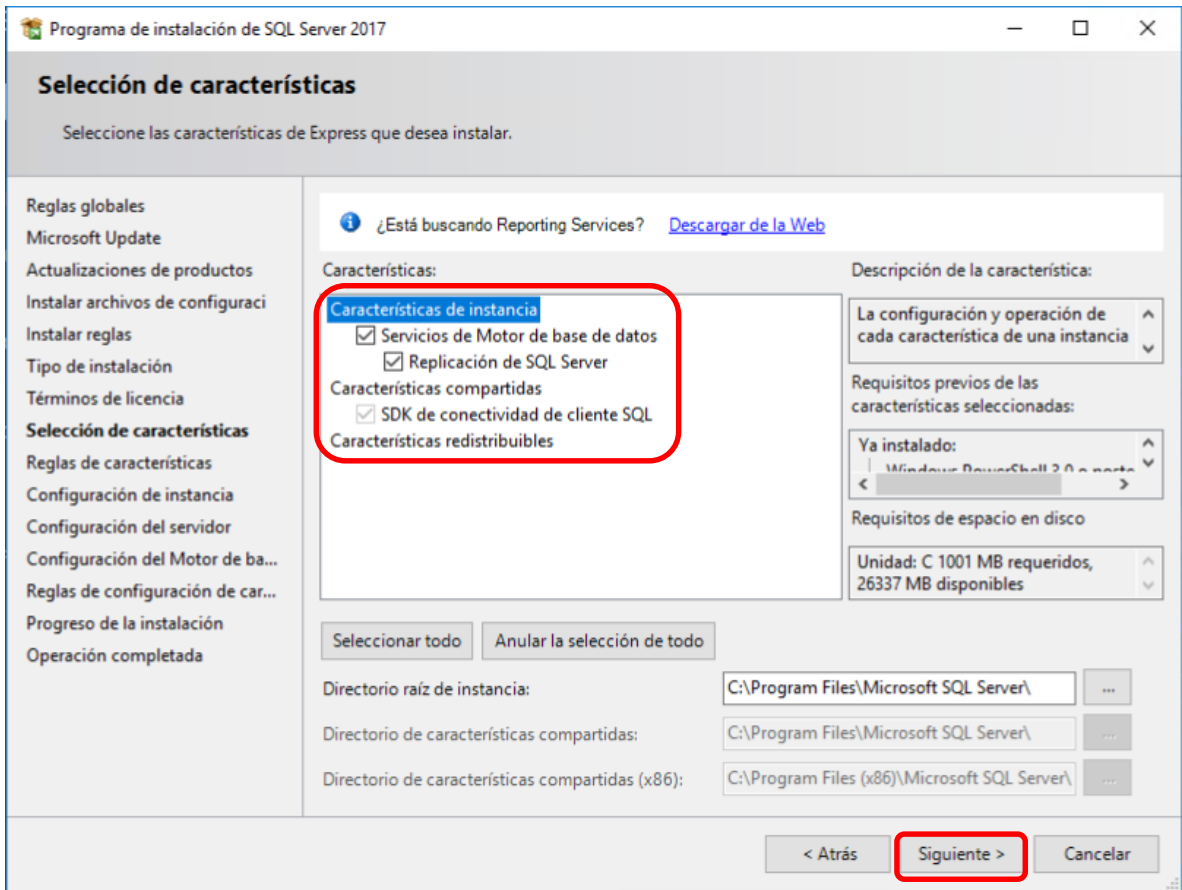
9. Seleccionar la opción **Realizar una nueva instalación del SQL Server 2017** y presionar **Siguiente**



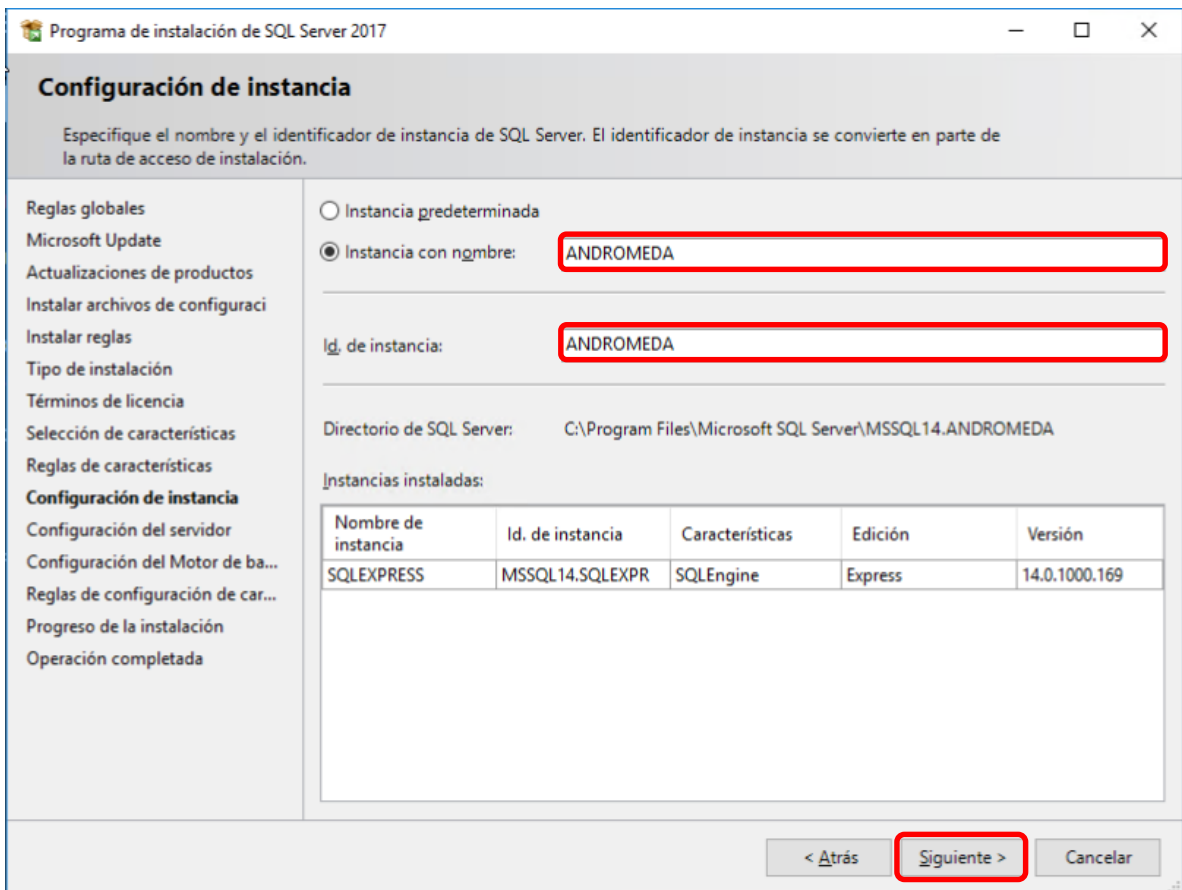
10. Aceptar los términos de la licencia y presionar **Siguiente**



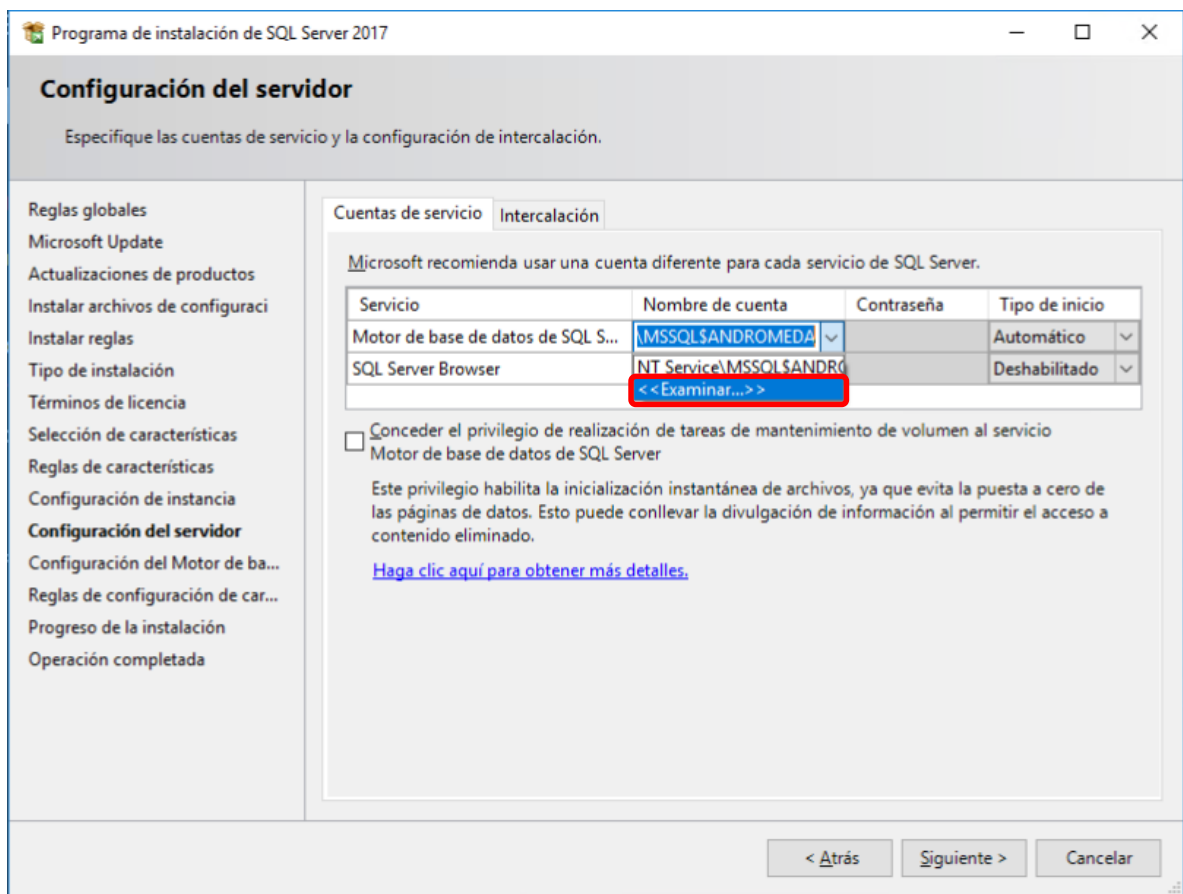
11. Verificar que todas las tres casillas esten marcadas y presionar **Siguiente**



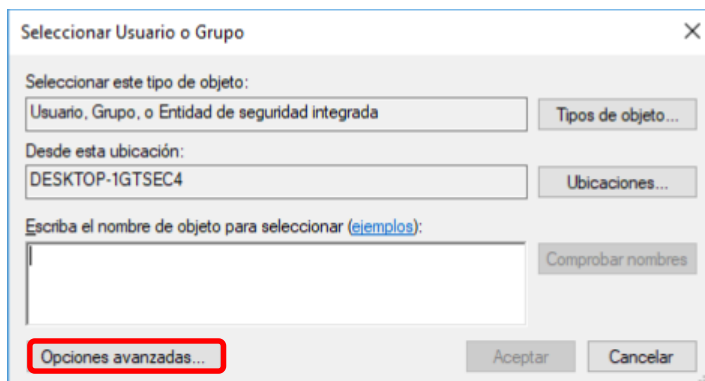
12. Especificar el nombre y el identificador de instancia de SQL Server: **ANDROMEDA**. Presionar el botón **Siguiente**



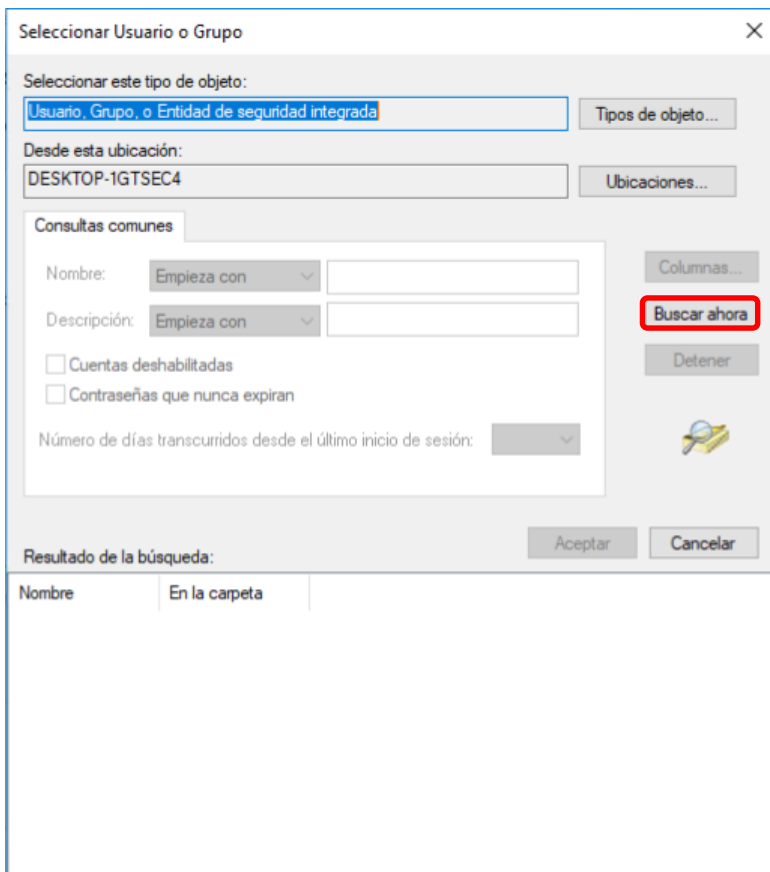
13. Para el servicio **Motor de base de datos de SQL Server** ingresar en los parametros de redacción del nombre de la cuenta. Para eso en el menú deslizable seleccionar **Examinar**



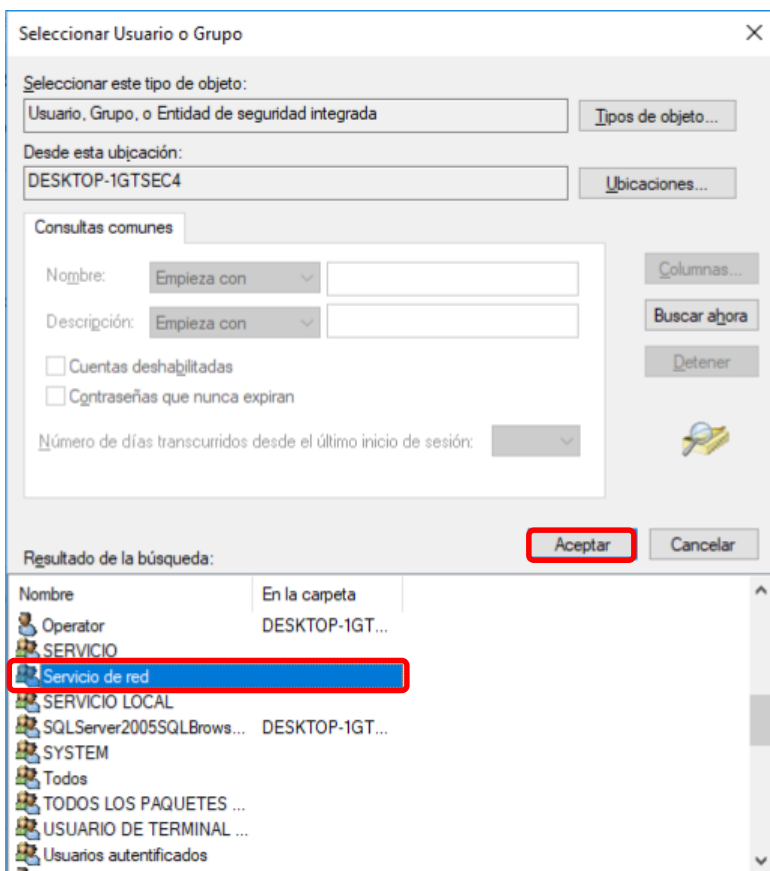
14. En la ventana emergente presionar el botón **Opciones avanzadas...**



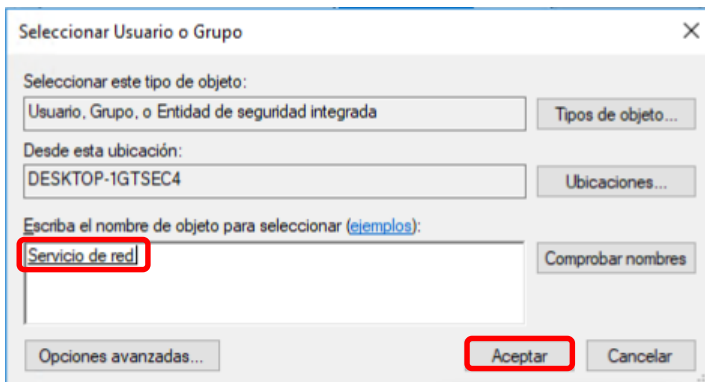
15. En la siguiente ventana presionar el botón **Buscar ahora**



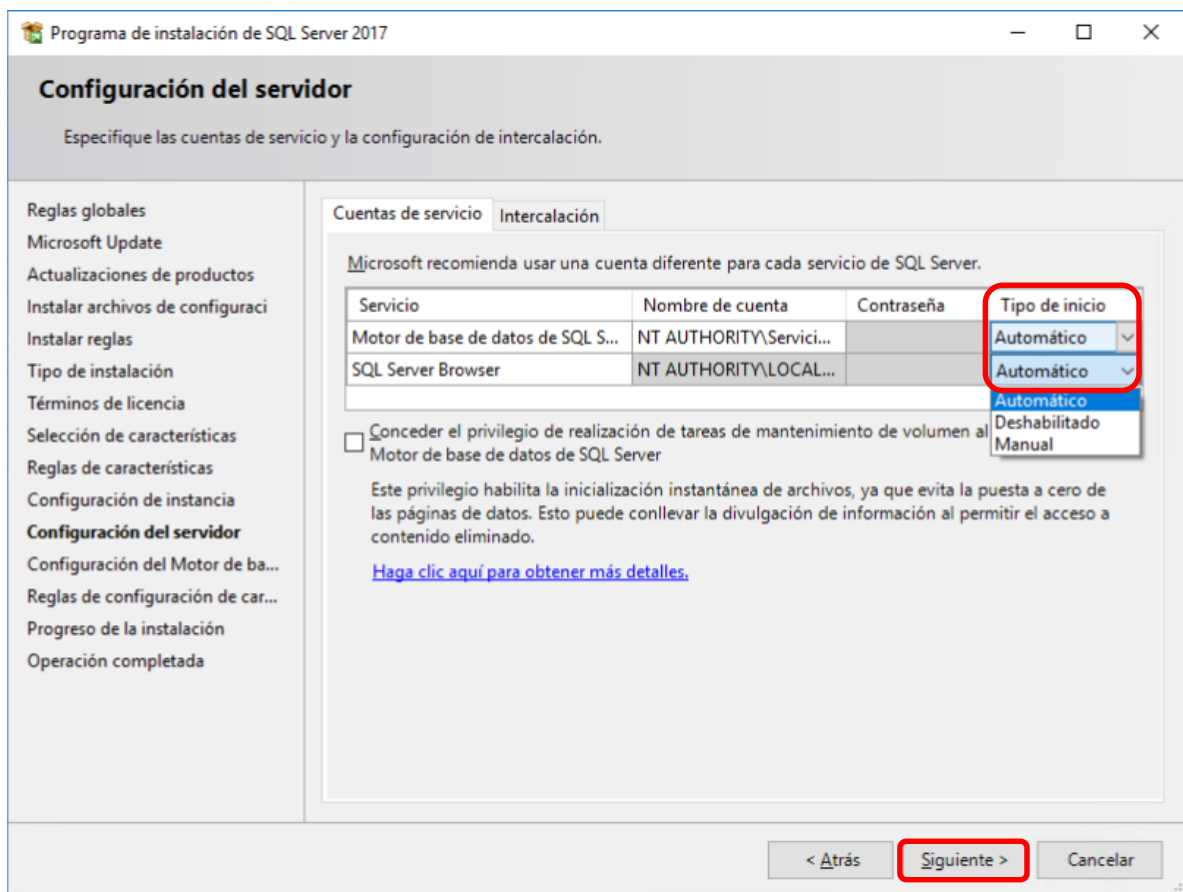
16. En la ventana emergente seleccionar la opción **Servicio de red** y presionar **Aceptar**



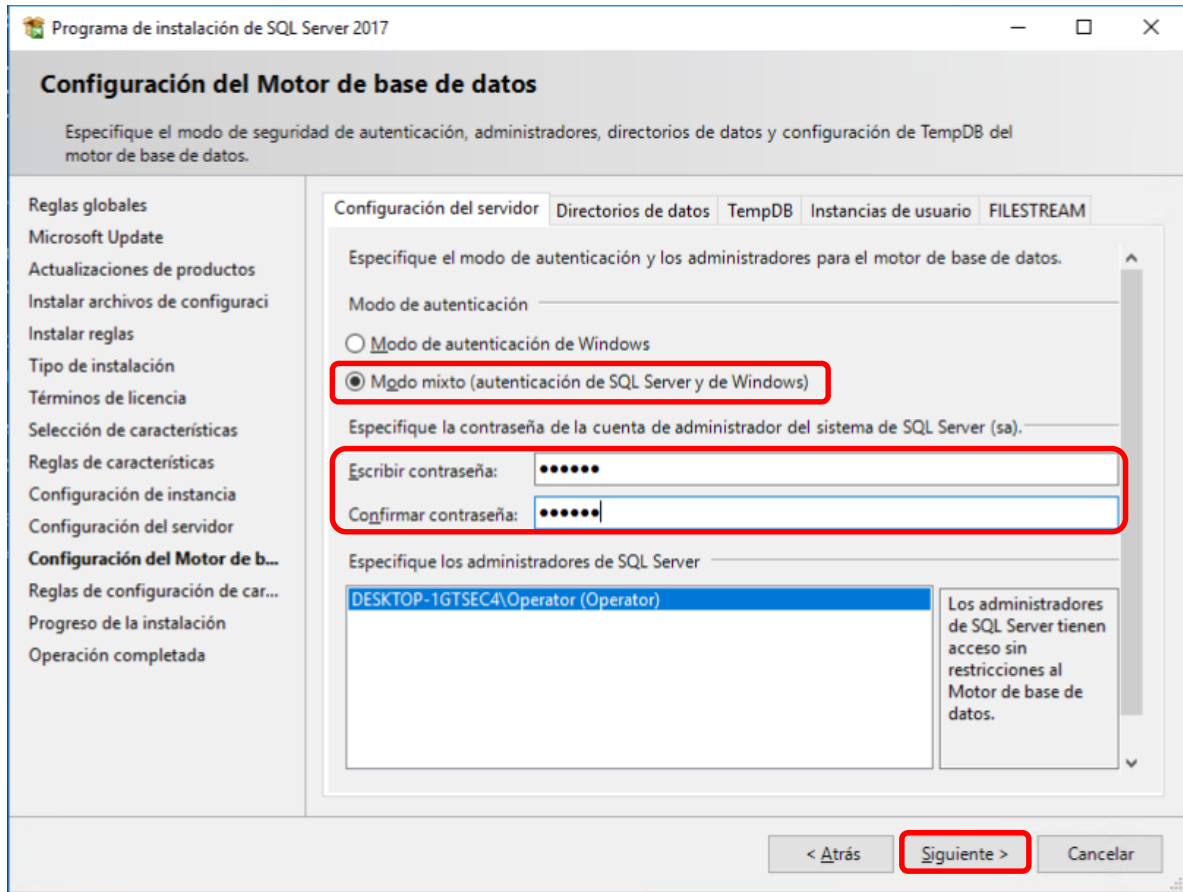
17. Comprobar que en el campo inferior apareció el objeto con el nombre **Servicio de red**. Presionar **Aceptar**.



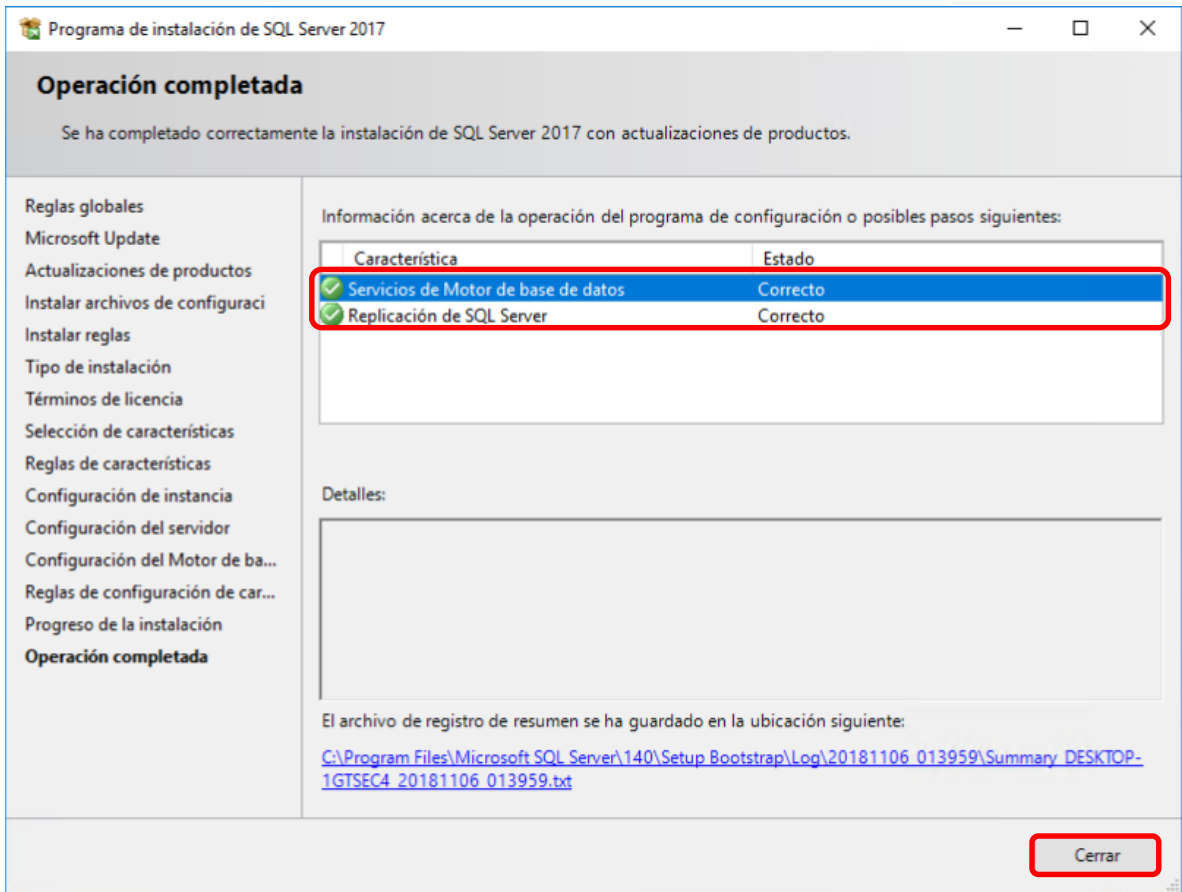
18. Para los servicios **Motor de base de datos SQL Server** y **SQL Server Browser** seleccionar el tipo de inicio **Automático**. Presionar el botón **Siguiente**.



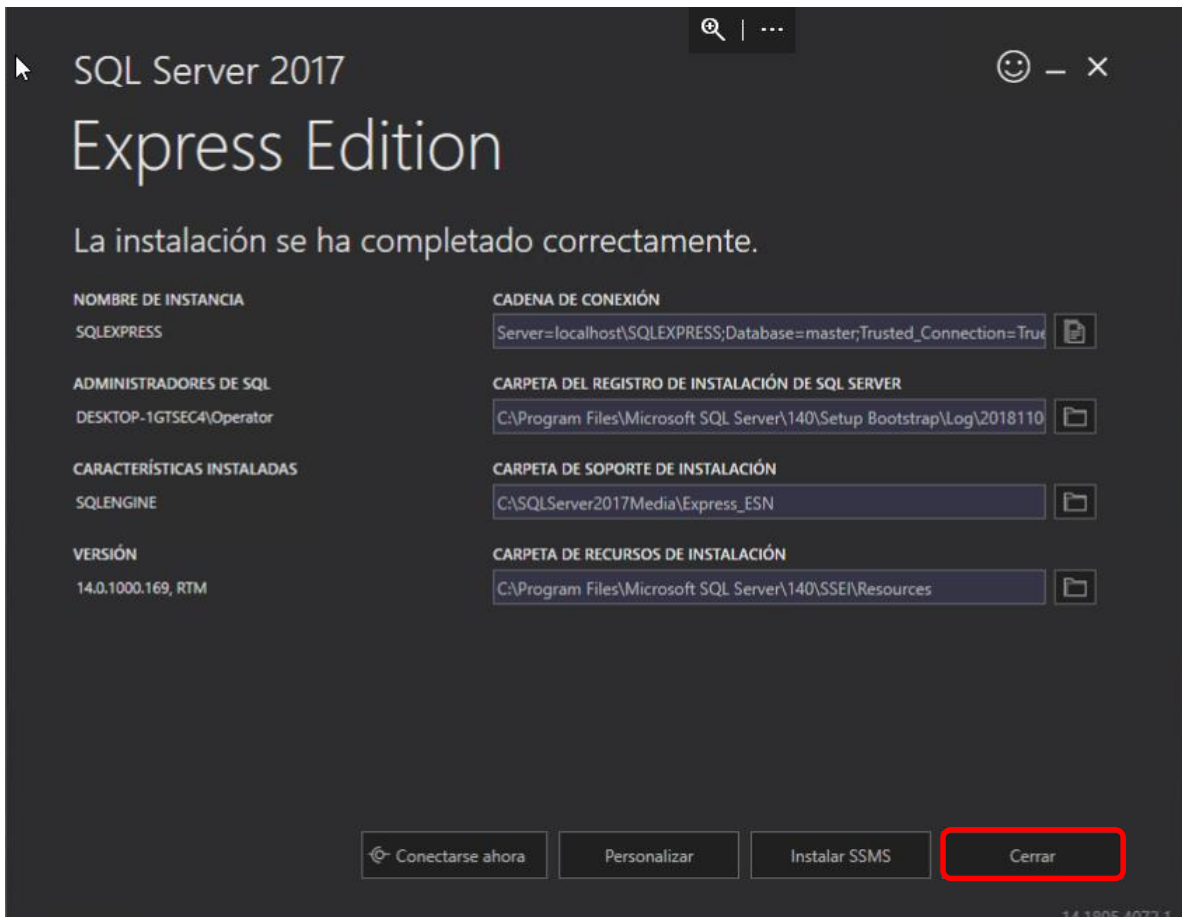
19. Especificar **Modo mixto** para la autenticación e ingresar dos veces la contraseña (puede ser cualquiera).



20. Presionar **Siguiente** y esperar hasta el final del proceso de instalación. Si la instalación se ha completado correctamente presionar **Cerrar**.



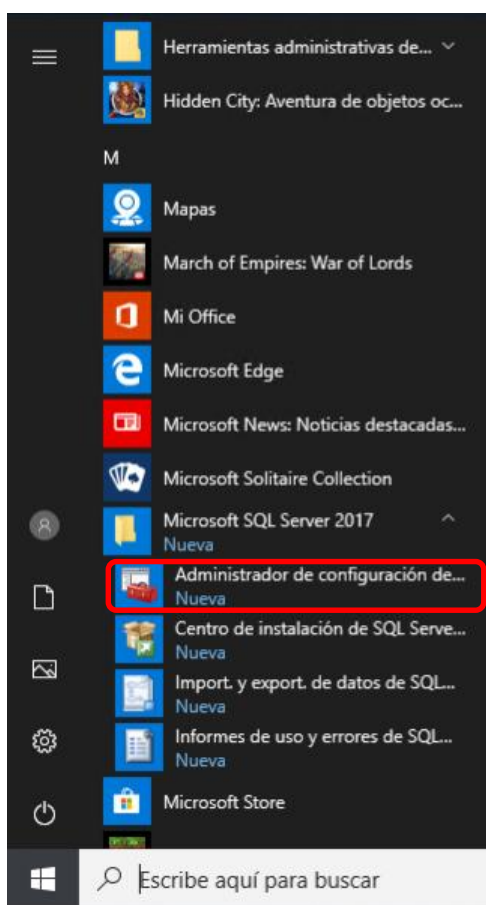
21. Presionar **Cerrar** segunda vez



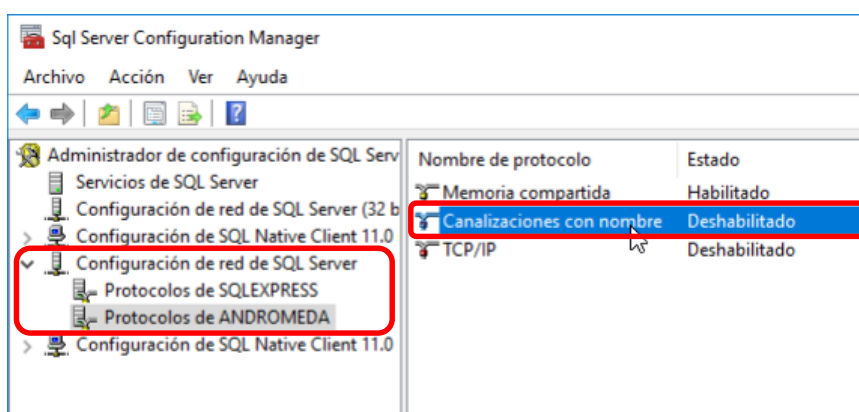
2.2 Configuración del Microsoft SQL Server 2017 Express

Para configurar **SQL Server** realice las siguientes acciones

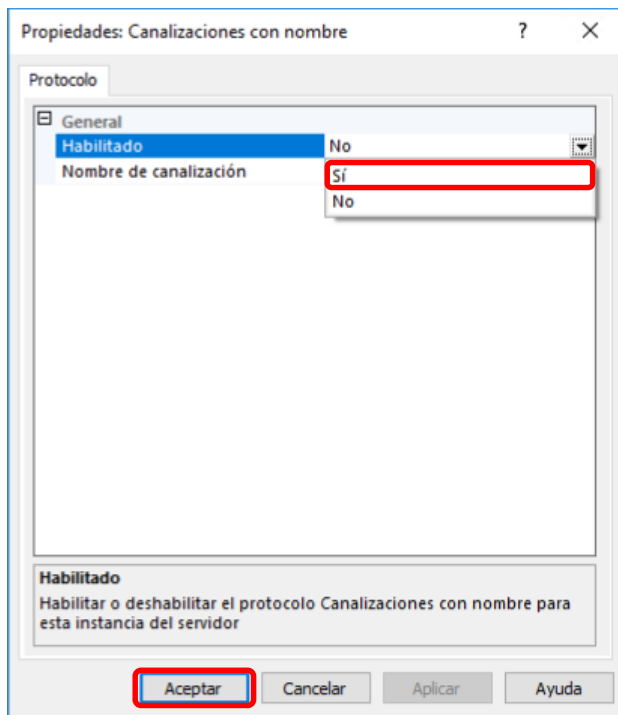
1. Ejecutar **Administrador de configuración de SQL Server 2017**



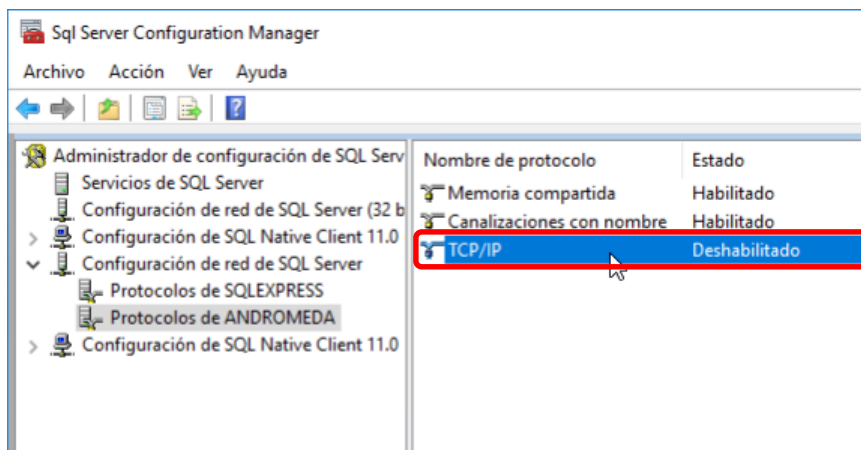
2. En la ventana emergente seleccionar **Configuración de red de SQL Server -> Protocolos de ANDROMEDA**. Hacer el doble click en el protocolo **Canalizaciones con nombre** en la parte derecha.



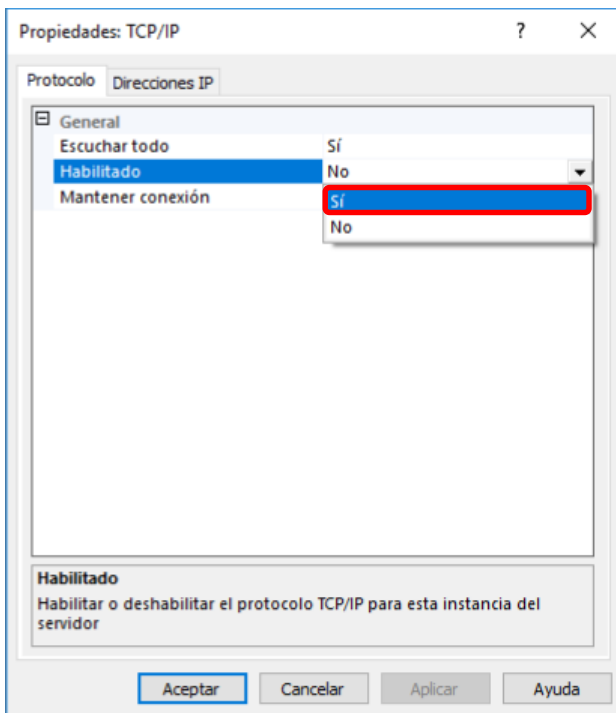
3. En la ventana siguiente seleccionar **Sí** frente a la opción **Habilitado**. Presionar **Aceptar**.



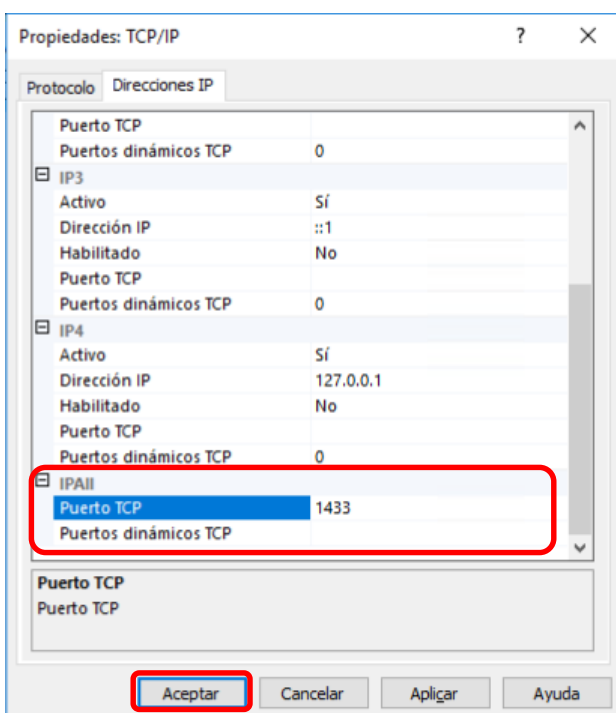
4. Hacer doble click en el protocolo **TCP/IP** para acceder a sus propiedades



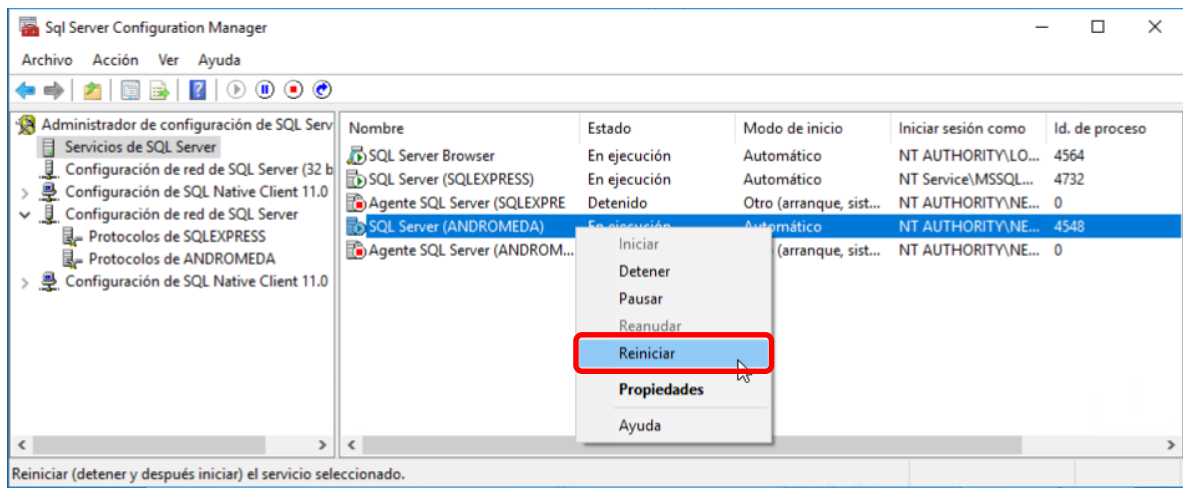
5. En la ventana siguiente seleccionar **Sí** frente a la opción **Habilitado**.



6. En la pestaña **Direcciones IP** pasar a la sección **IPAll**. Eliminar el valor frente a **Puertos dinámicos TCP**. Para el parámetro **Puerto TCP** indicar – 1433. Presionar **Aceptar**.



7. En los **Servicios de SQL Server** reiniciar **SQL Server (ANDROMEDA)** -> presionar el botón derecho del mouse -> **Reiniciar**

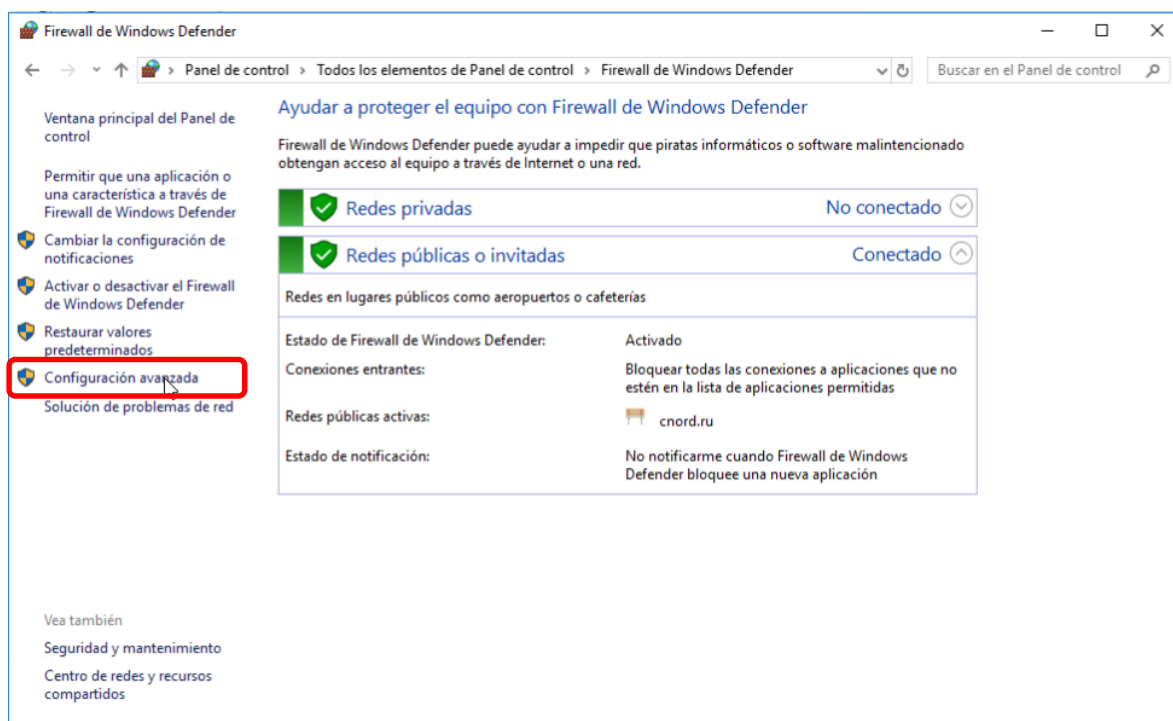


La configuración del **SQL Server** está completada.

2.3 Configuración del Firewall de Windows Defender

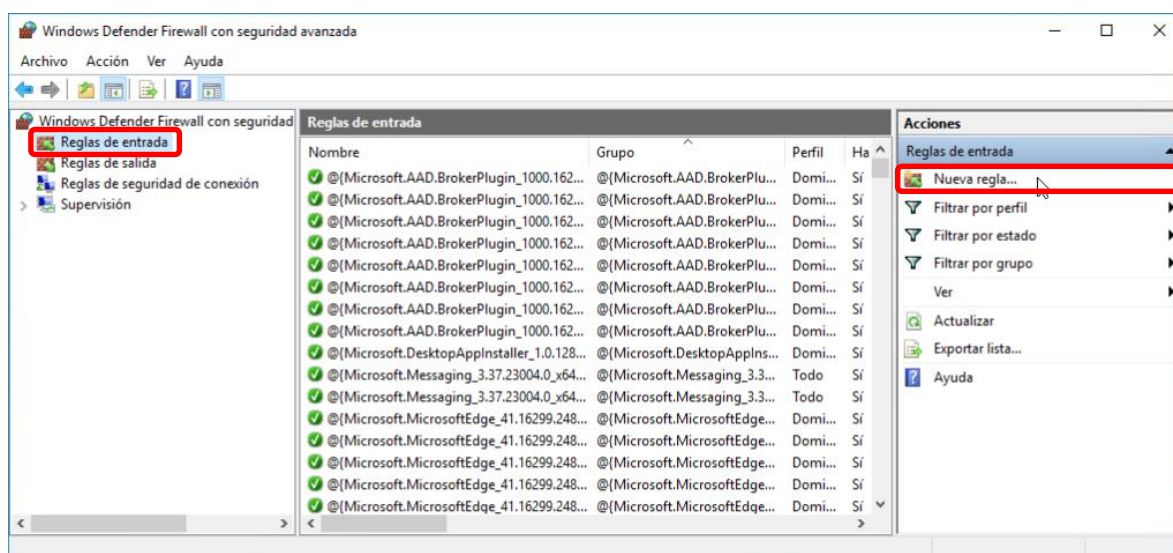
Para configurar **Firewall de Windows Defender** realice las siguientes acciones

1. Seguir al **Panel de control** -> **Firewall de Window Defender** y seleccionar en la parte de izquierda la opción **Configuración avanzada**

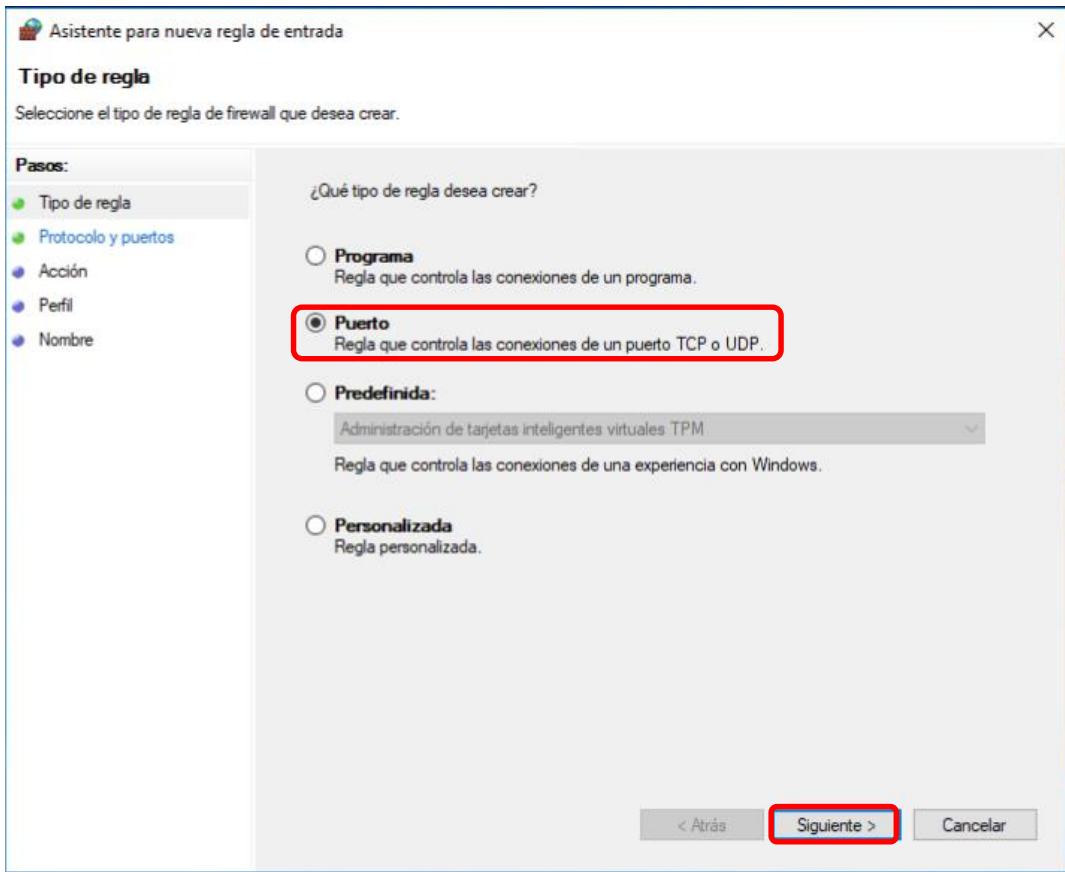


2. Agregar la regla para el puerto TCP/IP

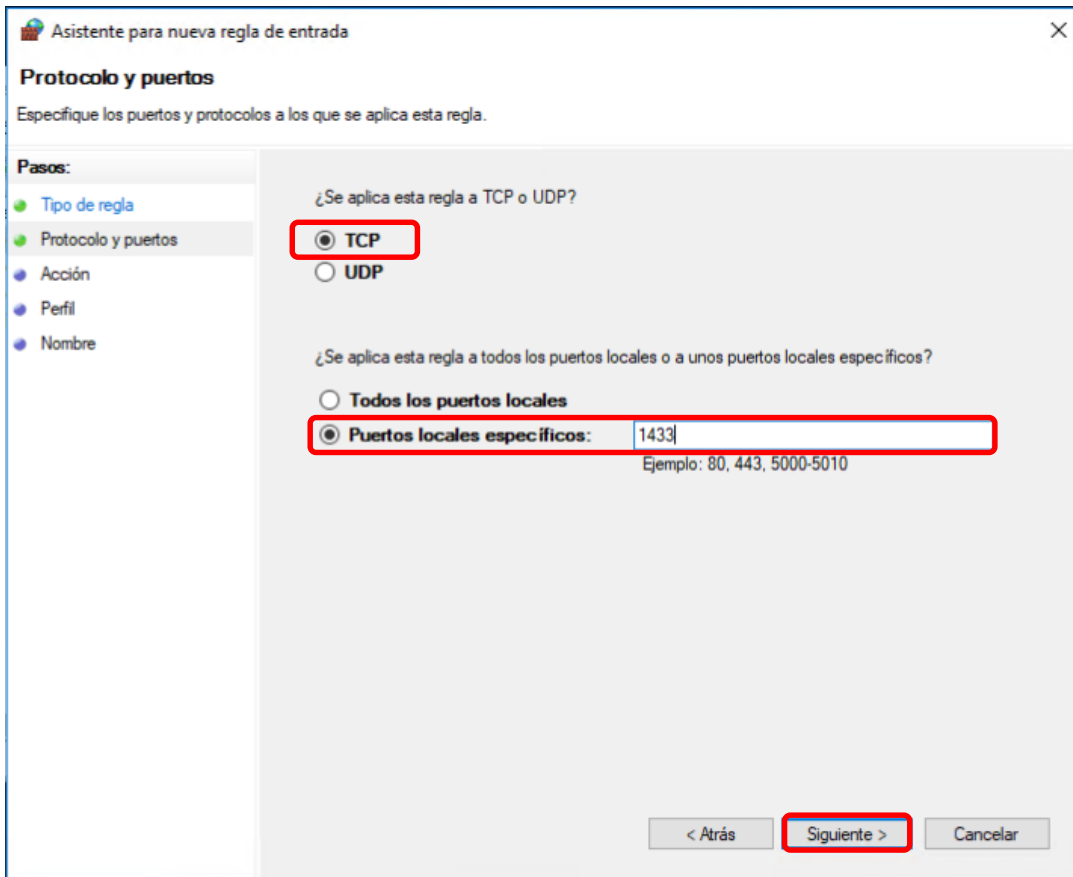
En la nueva ventana seguir a la sección **Reglas de entrada** y en la parte derecha hacer click en **Nueva regla**.



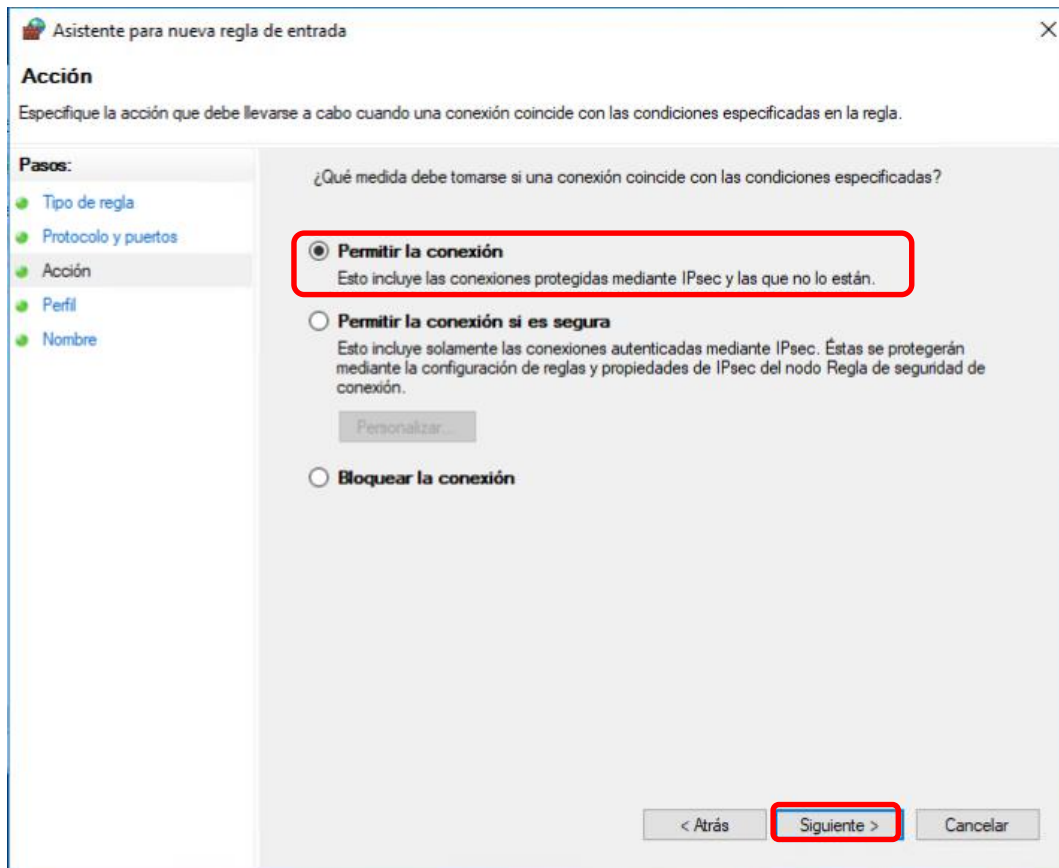
3. En la ventana emergente seleccionar **Puerto** y presionar **Siguiente**



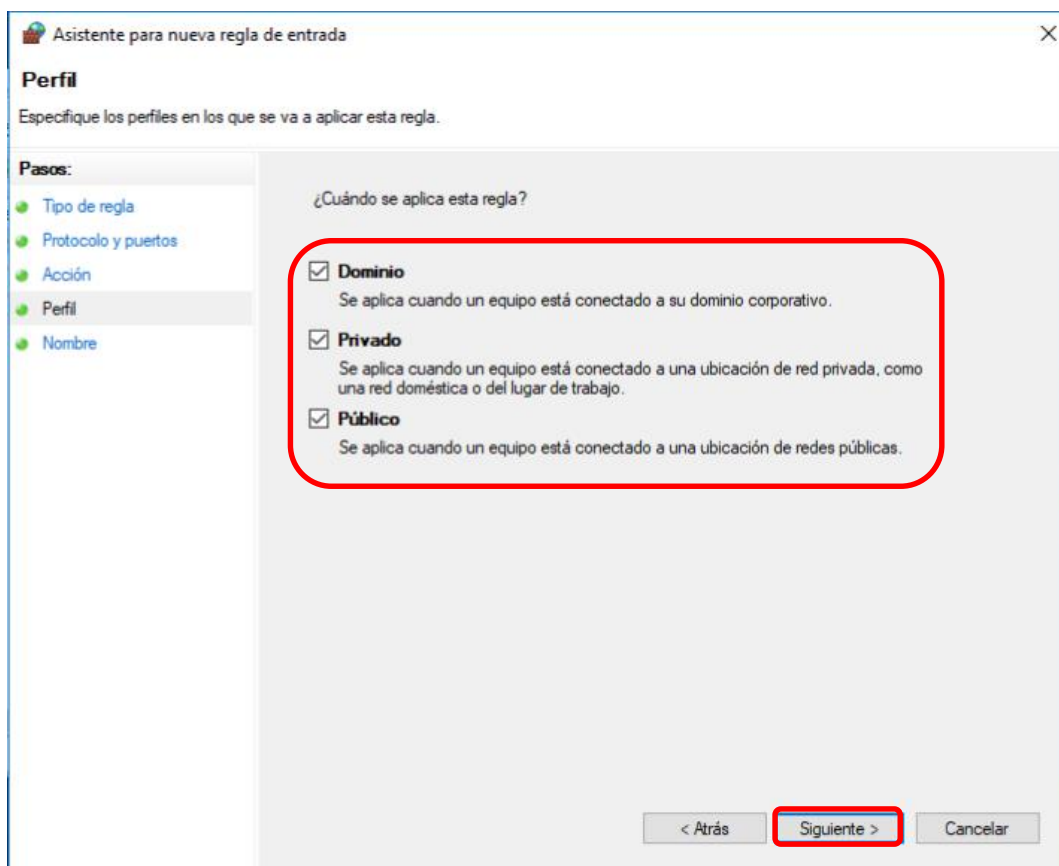
4. Marcar la casilla frente a **TCP** y en el campo **Puertos locales específicos** ingresar el valor **1433**. Presionar **Siguiete**.



5. Asegurarse de que se haya seleccionado la opción **Permitir la conexión** y presionar **Siguiente**.



6. Asegurarse que todas las opciones estén seleccionadas y presionar **Siguiente**



7. Ingresar el nombre para la regla, e.g. **SQLServerTCP** y presionar **Finalizar**

Asistente para nueva regla de entrada

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

Nombre:

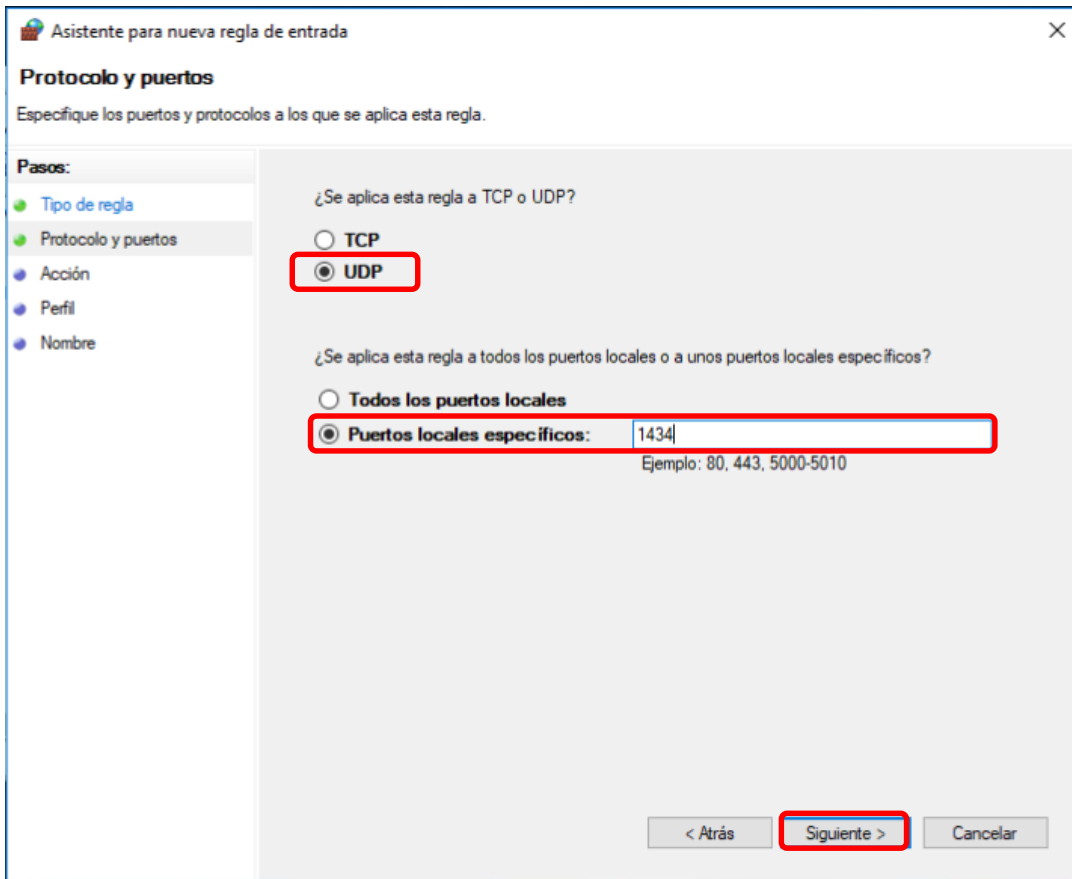
SQLServerTCP

Descripción (opcional):

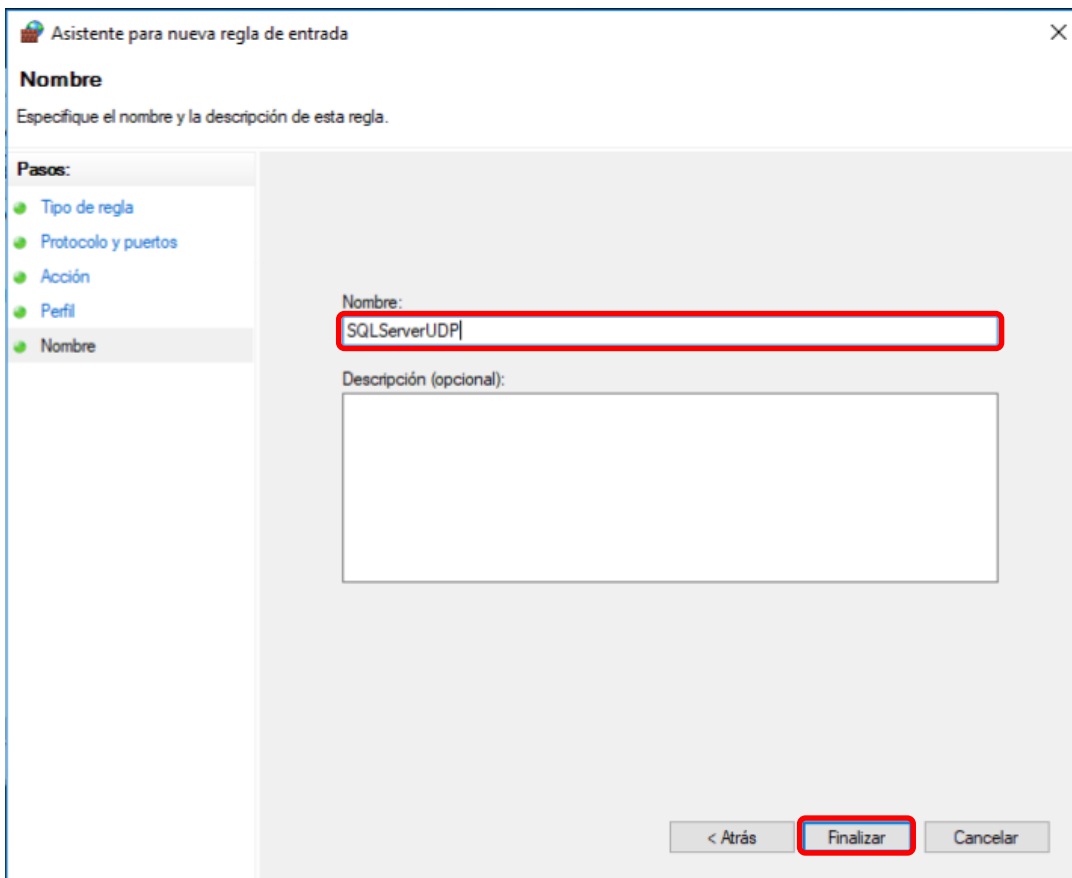
< Atrás Finalizar Cancelar

8. Agregar la regla para el puerto **UDP**

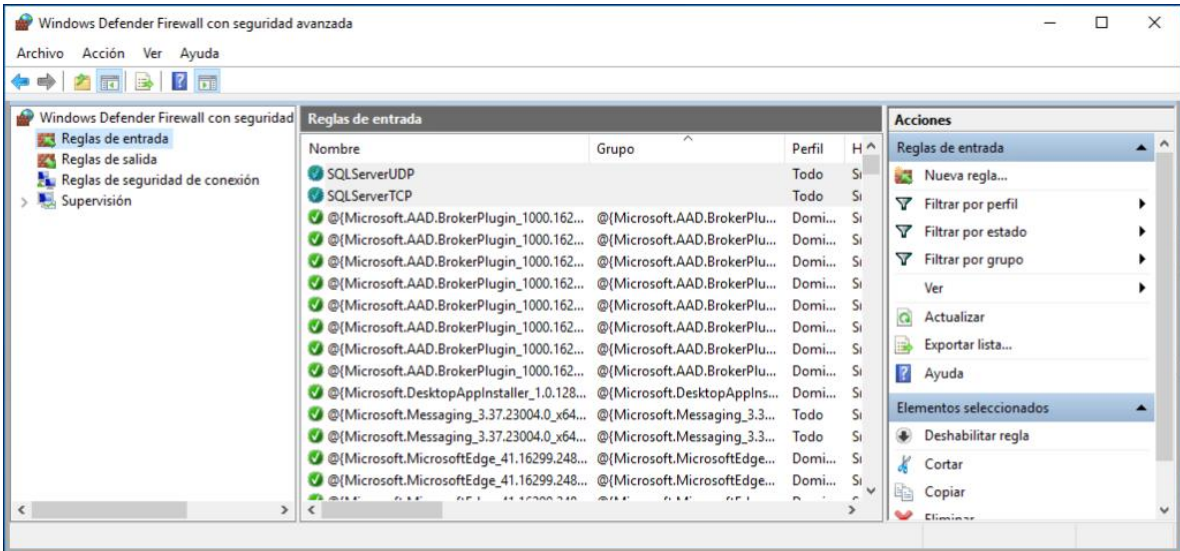
Repetir los pasos 2 y 3. Marcar la casilla frente a **UDP** y en el campo **Puertos locales específicos** ingresar el valor **1434**. Presionar **Siguiente**.



9. Repetir los pasos 5 y 6. Ingresar el nombre para la regla, e.g. **SQLServerUDP** y presionar **Finalizar**

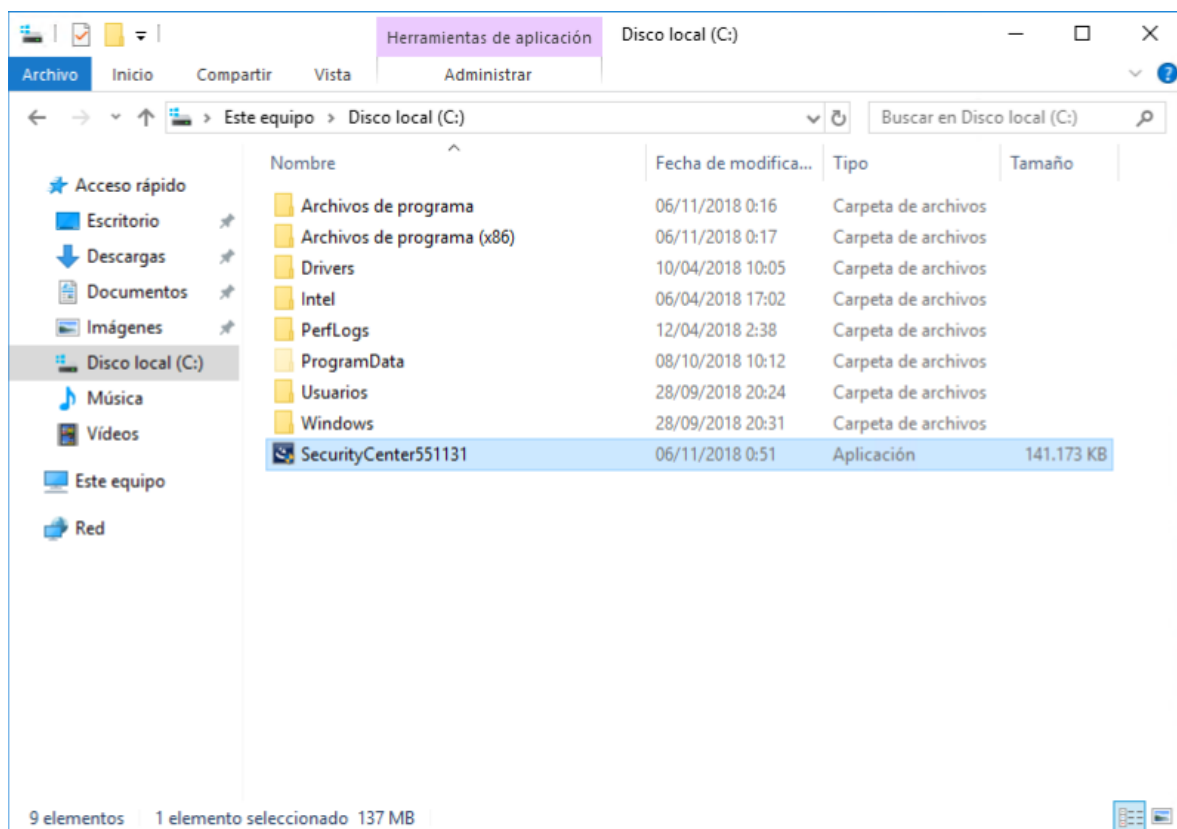


La configuración del **Firewall de Windows Defender** está finalizada.



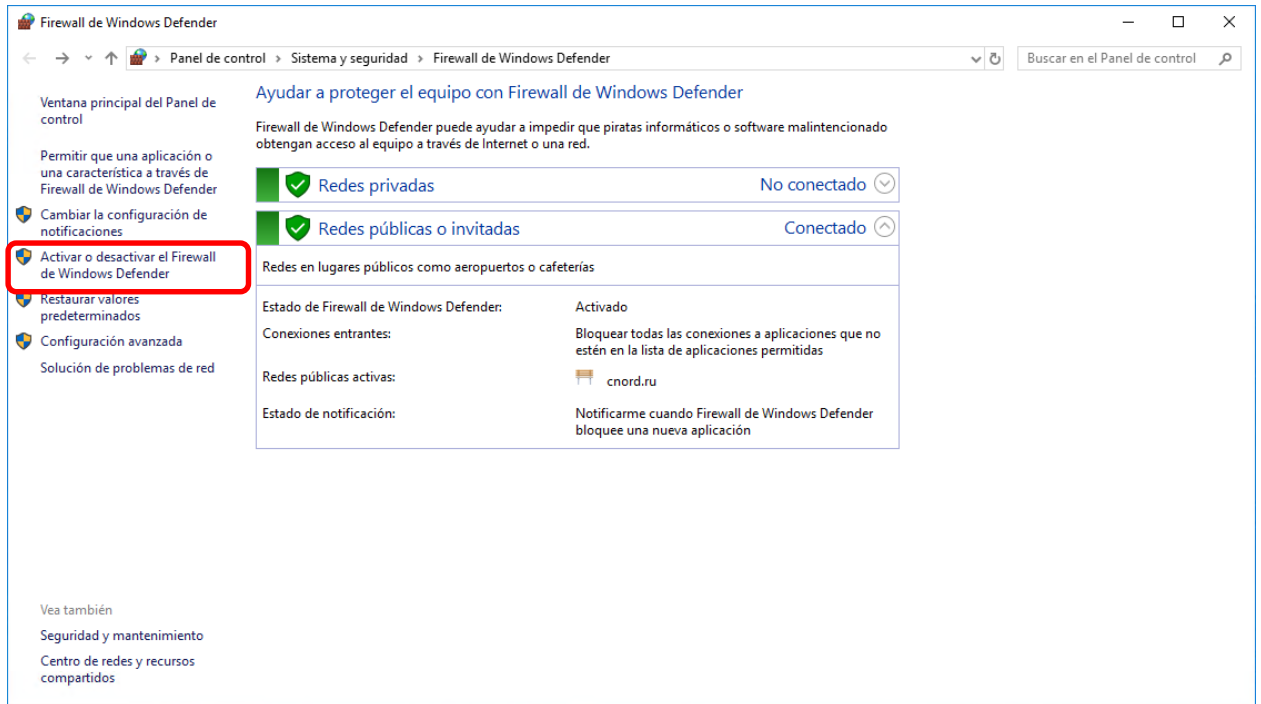
2.4 Instalación del Security Center

1. Descargar directamente la última versión del programa [Security Center](#) o desde nuestro [sitio web](#)
2. Mover el fichero “**SecurityCenterXXXXXX.exe**” en el directorio raíz del disco **C:**

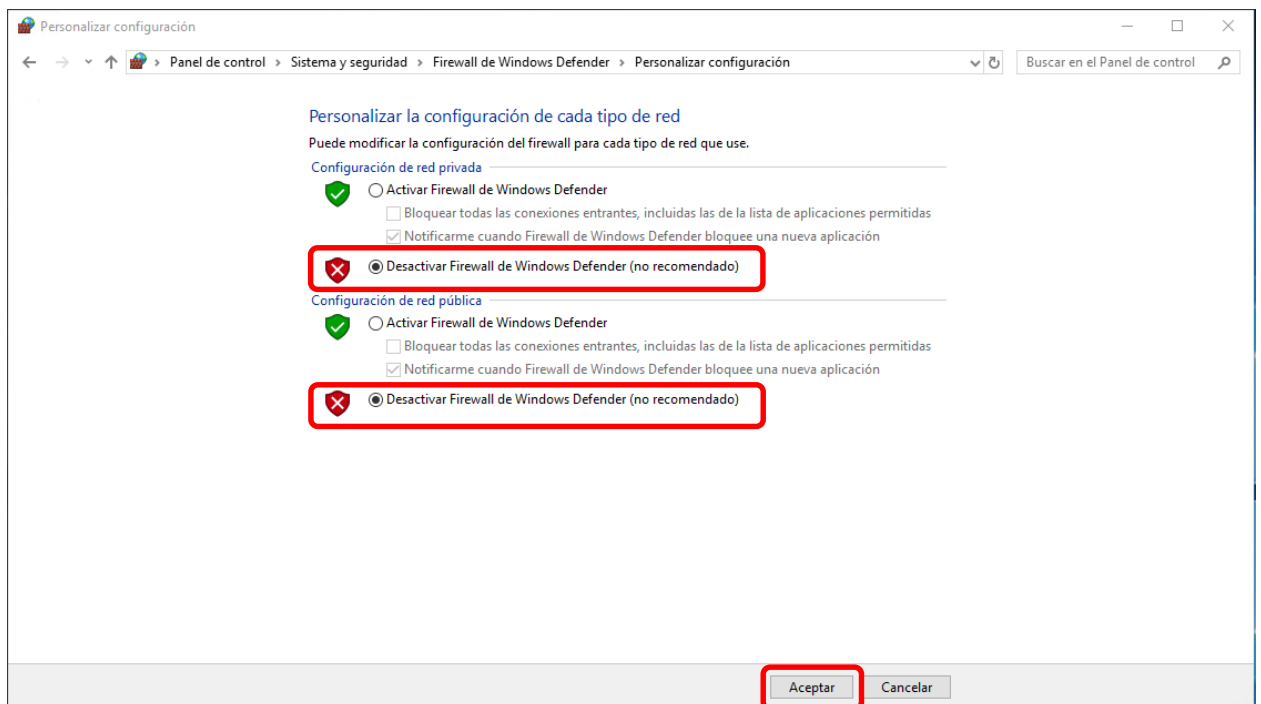


Antes de iniciar la instalación del SC modificar las siguientes configuraciones del SO (en el ejemplo de Win10)

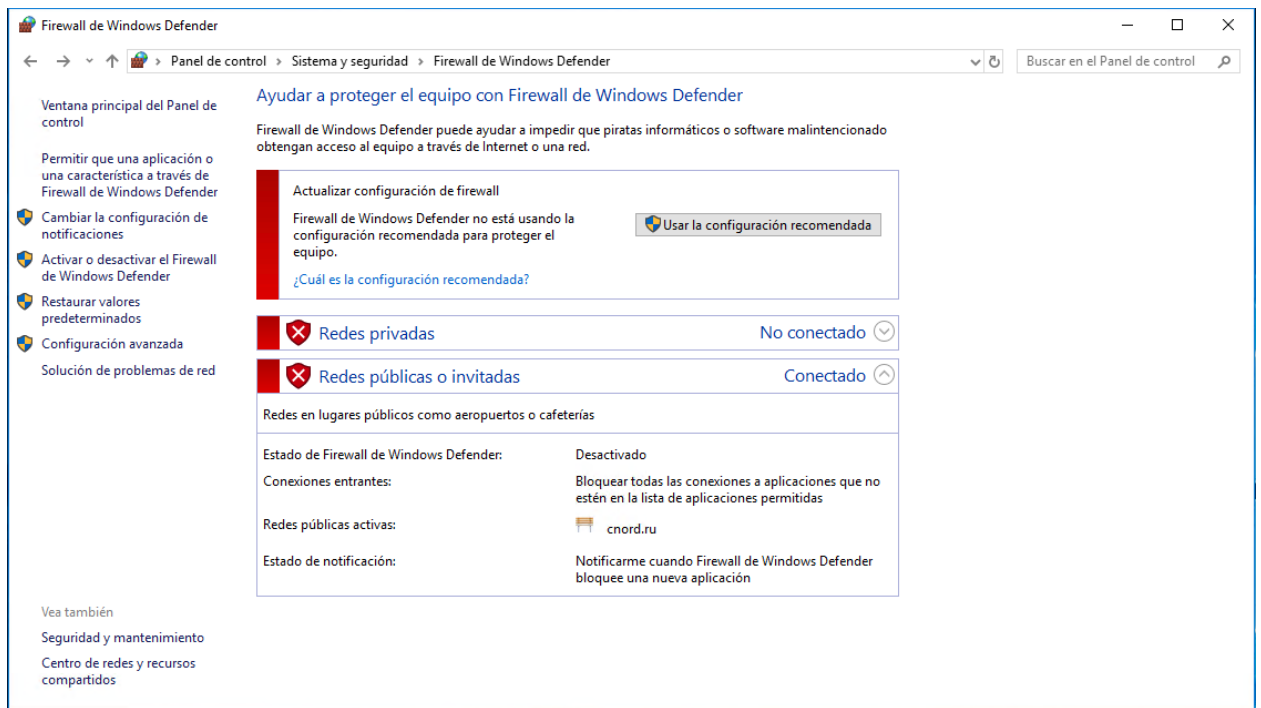
3. Seguir al **Panel de control** -> **Firewall de Window Defender** -> **Activar o desactivar el Firewall de Windows Defender**



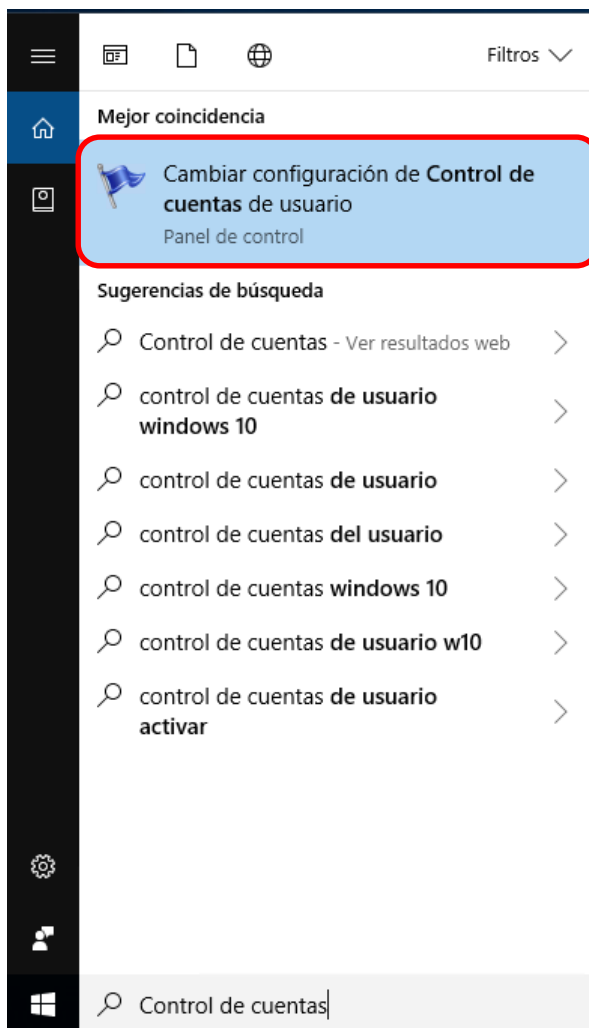
4. Marcar la opción **Desactivar Firewall de Windows Defender** en Configuraciones de red privada y red pública. Presionar **Aceptar**.



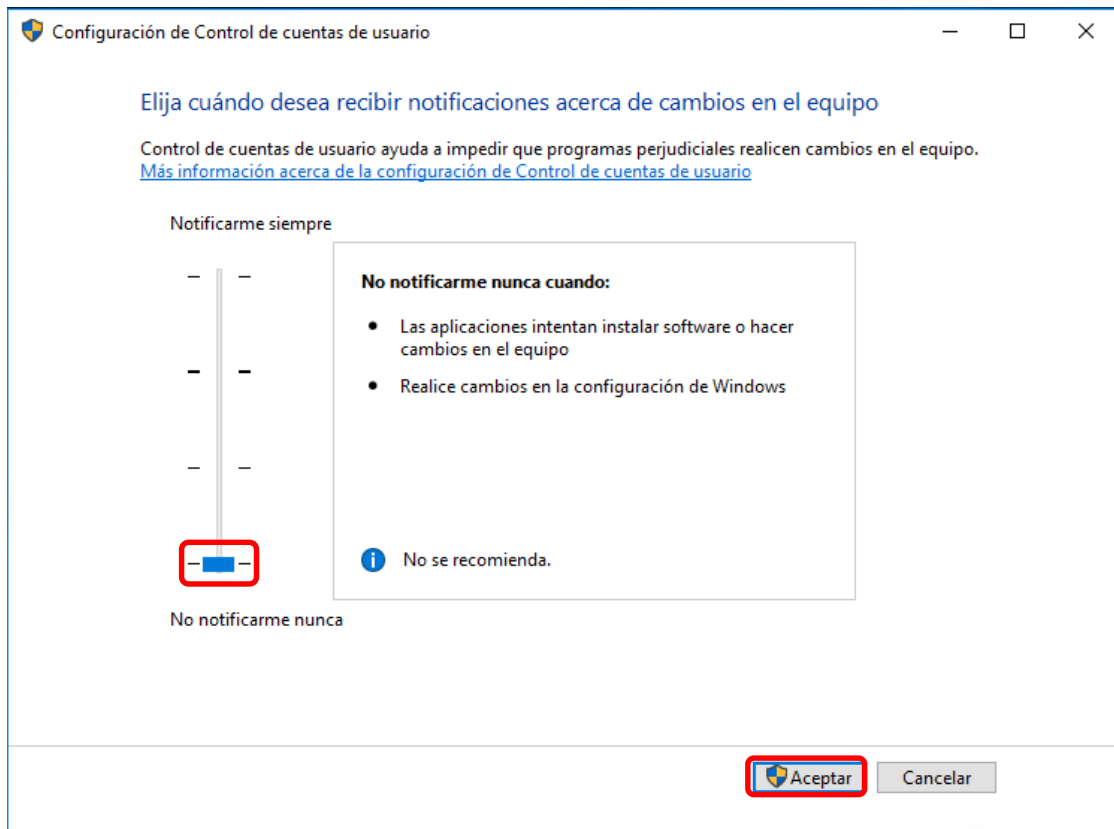
5. La configuración del **Firewall de Windows Defender** está finalizada



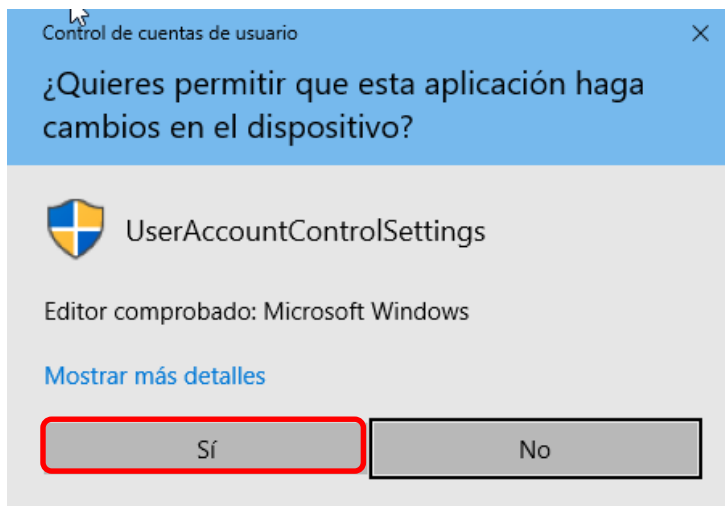
6. En la barra de búsqueda ingresar “Control de cuentas” y en los resultados seleccionar la opción **Cambiar configuración de Control de cuentas de usuario**



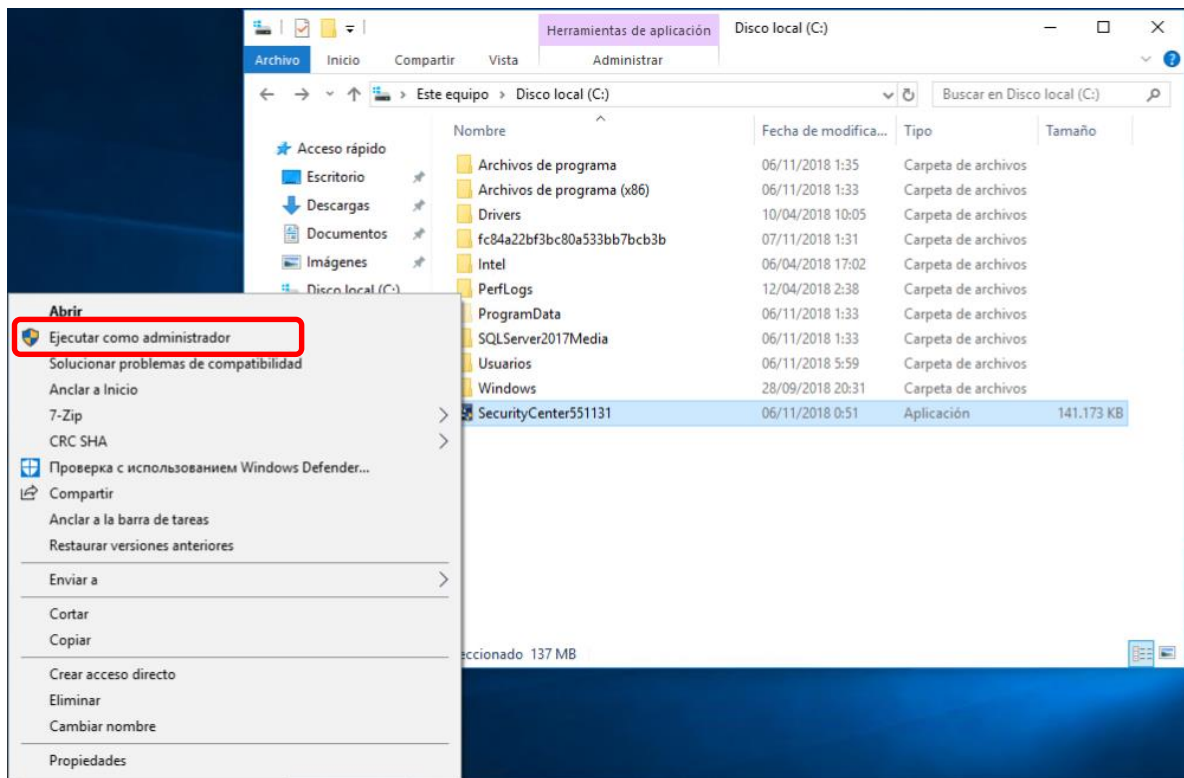
7. Con el control deslizante desactivar el recibo de notificaciones acerca de cambios en el equipo y presionar **Aceptar**



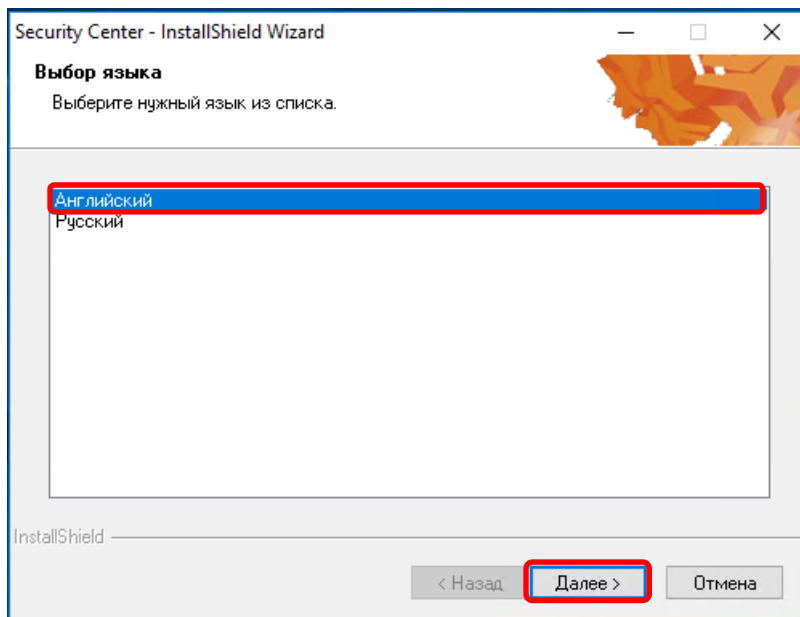
8. Aceptar los cambios en la ventana emergente



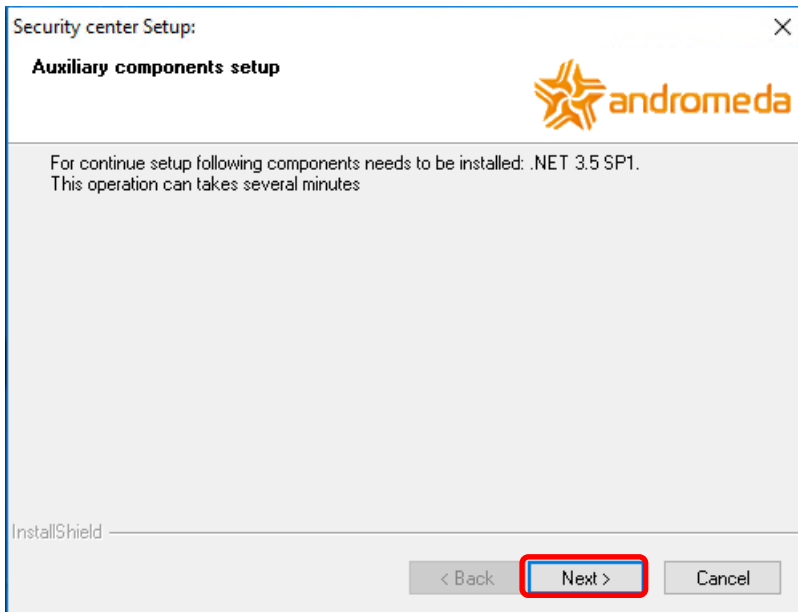
9. Ejecutar el archivo **C:\ SecurityCenterXXXXXX.exe** como administrador



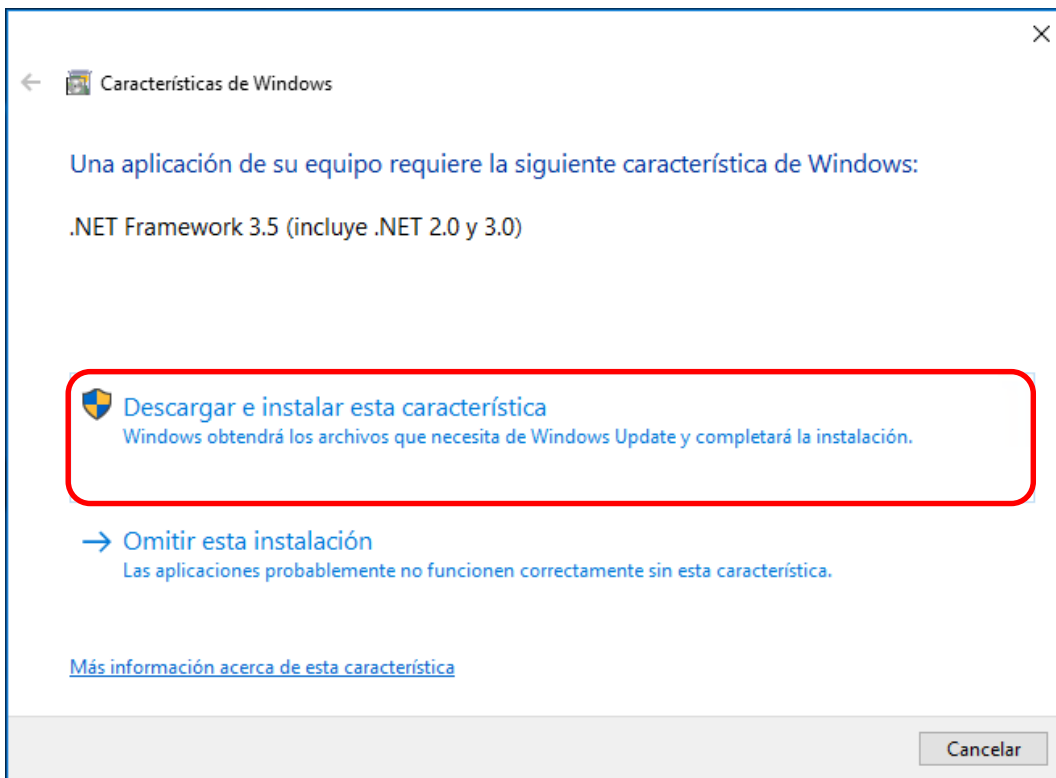
10. En la siguiente ventana seleccionar **inglés** como el idioma del instalador y presionar **Siguiente**



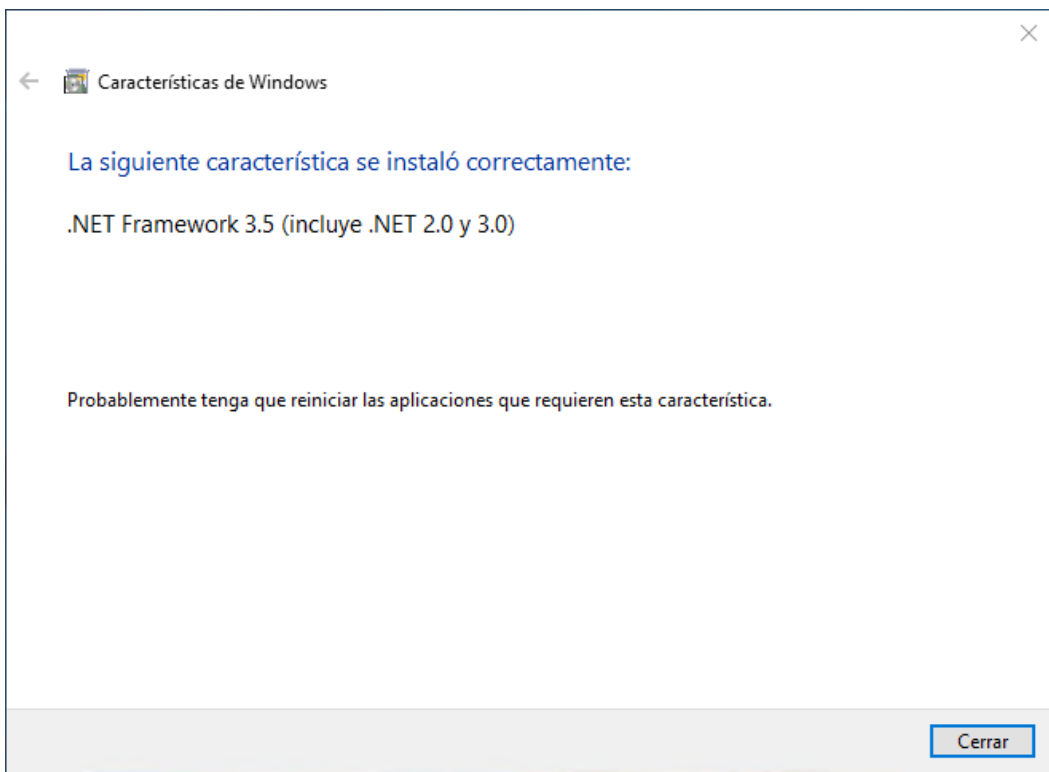
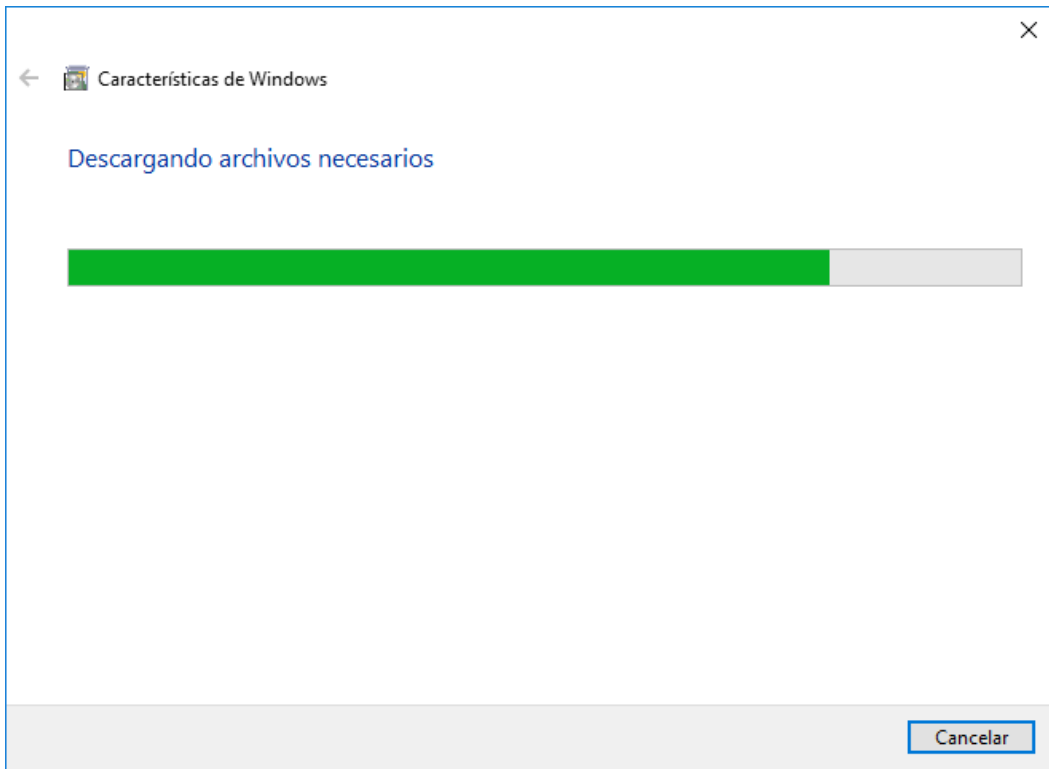
11. Presionar **Next** para instalar **.NET Framework 3.5**



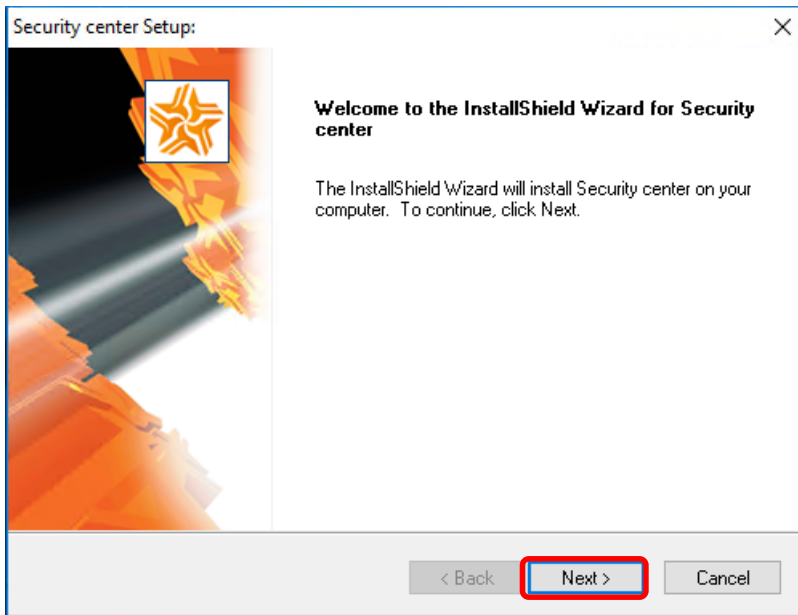
12. Presionar **Descargar e instalar esta característica**



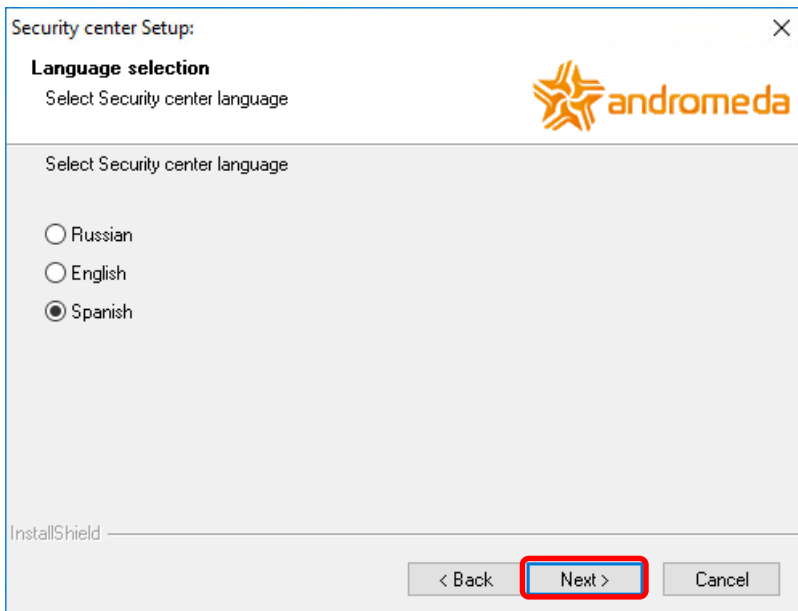
13. Espere mientras se descarguen e instalen los archivos necesarios



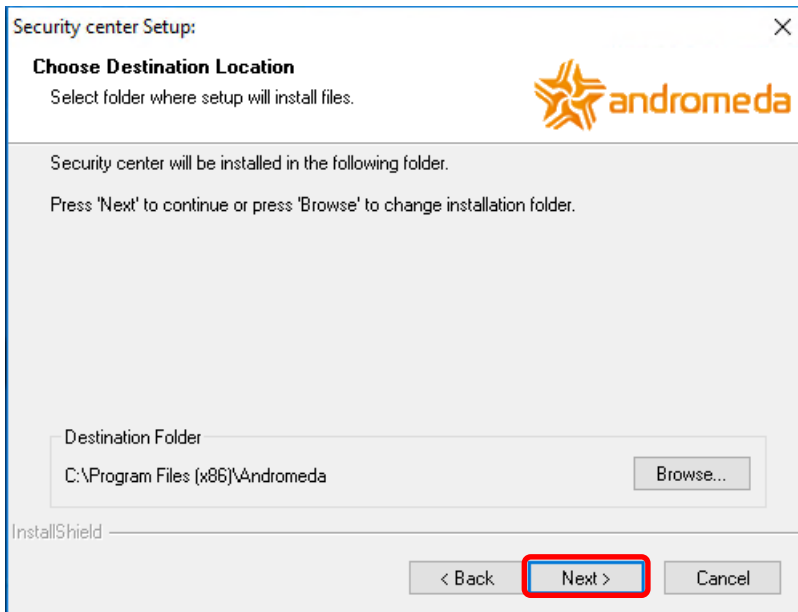
14. En la siguiente ventana presionar **Next**



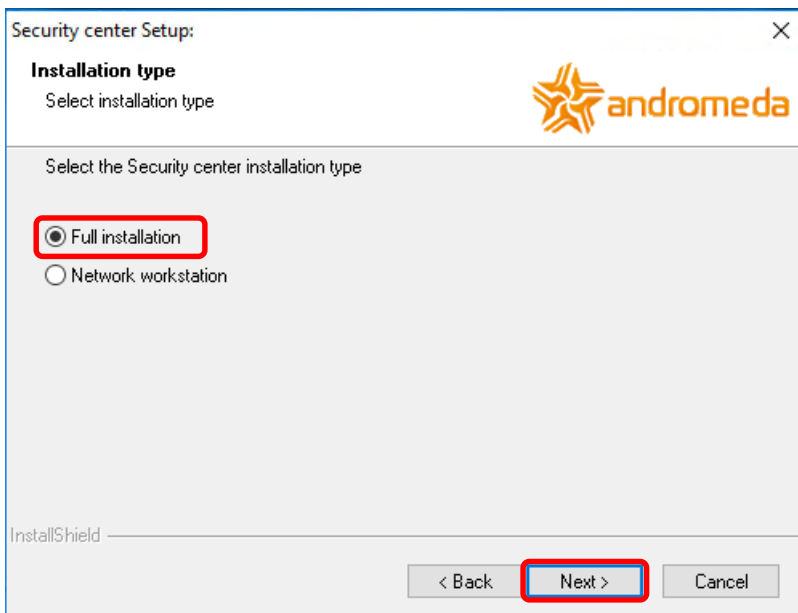
15. Elidir el idioma del Security Center y presionar **Next**



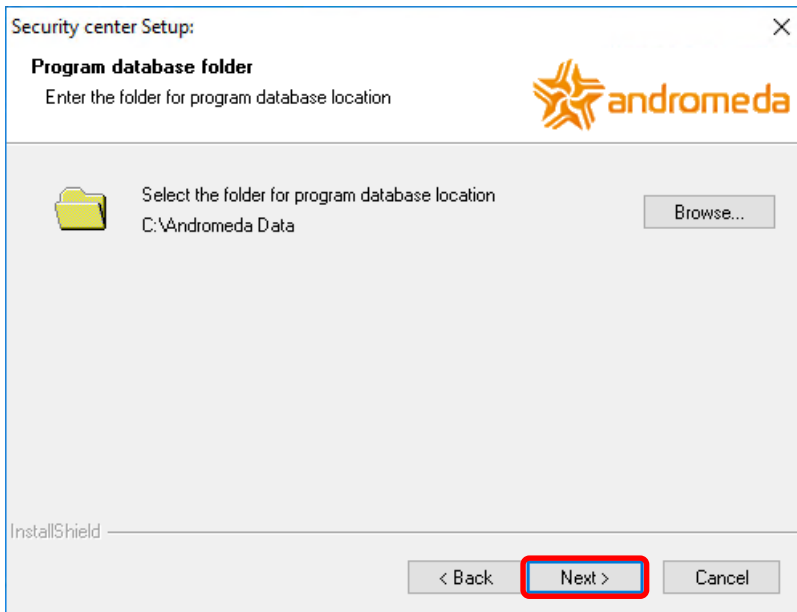
16. Confirmar la carpeta de destino presionando **Next**



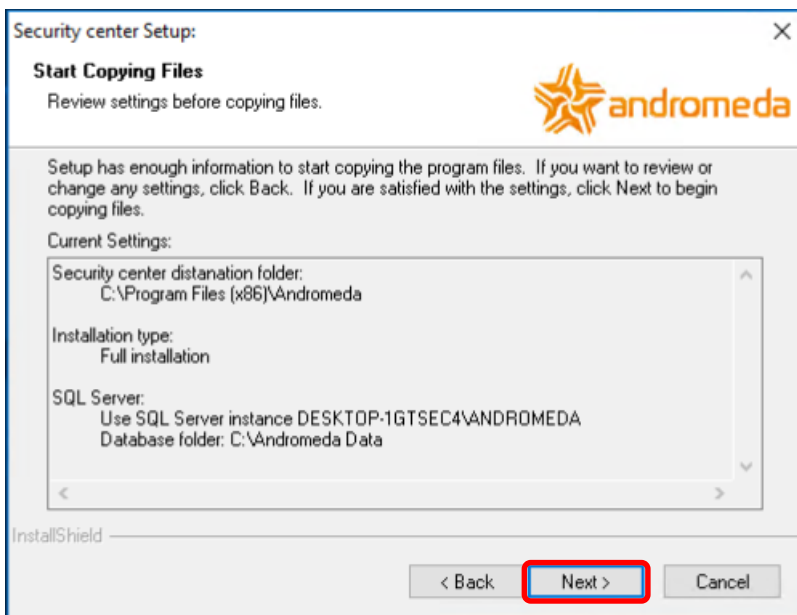
17. Seleccionar **Instalación completa** y oprimir **Next**



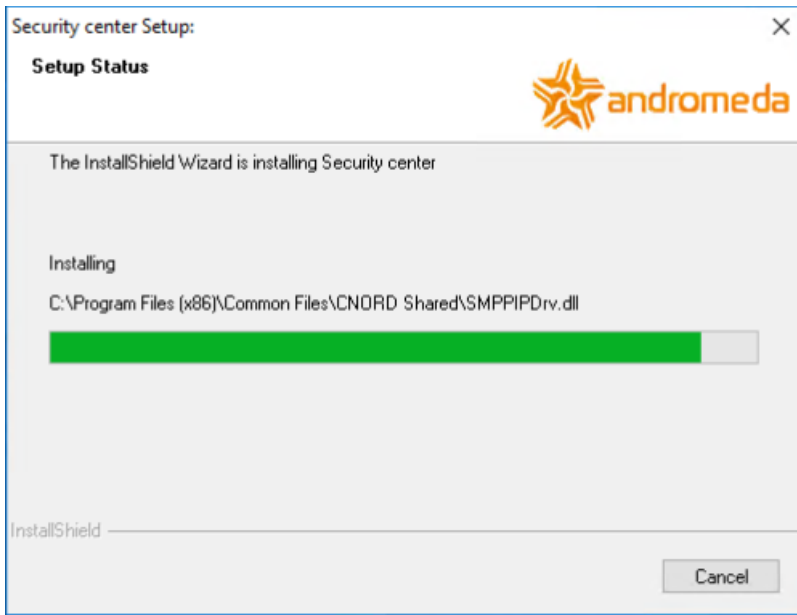
18. Confirmar la carpeta para instalación de la base de datos SQL oprimiendo **Next**



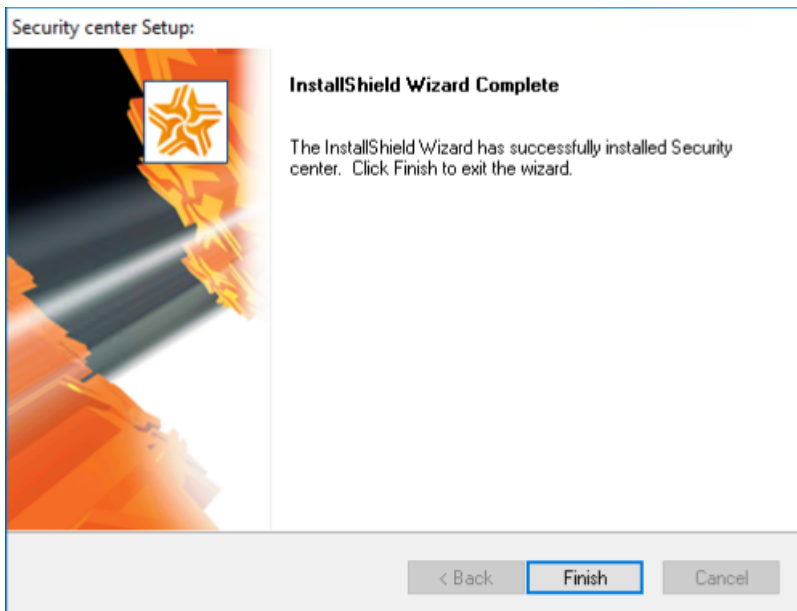
19. Verificar la información en la siguiente ventana y presionar **Next**



20. Esperar hasta el final de la instalación.



La instalación del **Security Center** está finalizada.

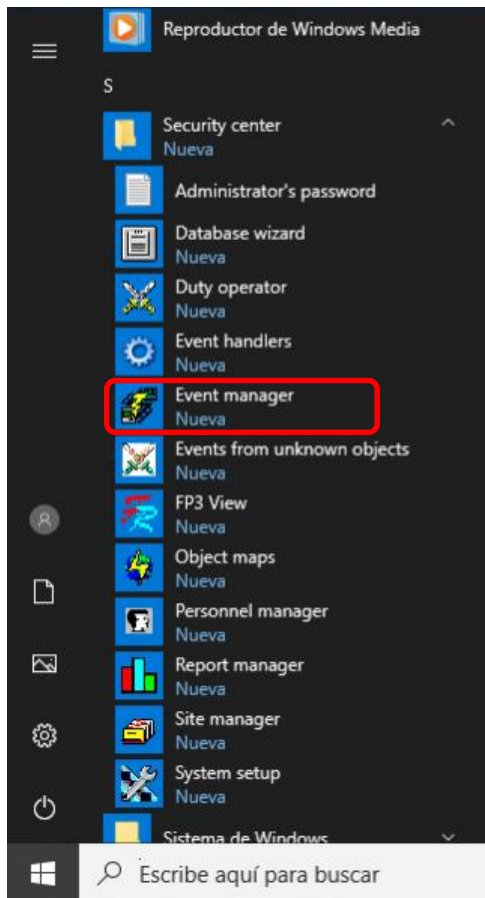


Ahora se puede volver a activar el **Firewall de Windows Defender**.

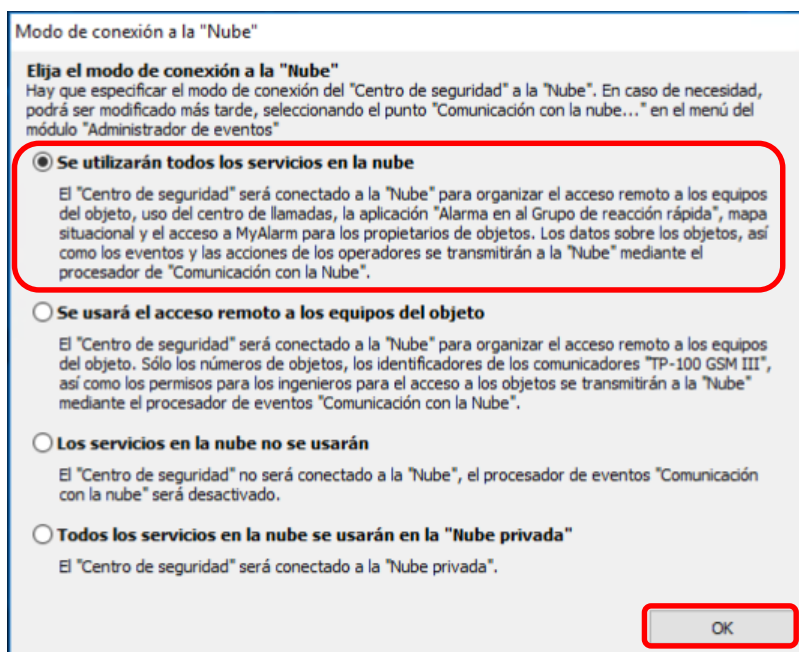
2.5 Configuración y puesta en marcha del Security Center

2.5.1 Configuración del Administrador de eventos

1. Ejecutar el **Event manager** (Administrador de eventos)



2. En la ventana emergente seleccionar el modo de la conexión a la **Nube C.Nord** – **Se utilizarán todos los servicios en la nube**. Presionar **OK**.



3. Ingresar los datos de su empresa y de la persona de contacto. Presionar **Continuar**.

Registro del "Centro de seguridad" en la "Nube" X

¡Atención! Para continuar el trabajo del "Centro de seguridad" hay que registrarlo en la "Nube". Esto le dará la posibilidad de usar el Centro de llamadas, la tarjeta del objeto en el Grupo de reacción rápida. Por favor, rellene todos los campos del formulario:

¿Cómo se llama? *

Apellido Nombre

Teléfono celular + *

Código del país y número de teléfono. Por ejemplo, +7 9211234567.

Correo electrónico *

Nombre de la organización *

Ciudad *


Dirección *

Pueblo, calle, edificio, bloque, edificación, número de oficina.
Por ejemplo, calle Sadovaya, ed. 21, oficina 64.
Otro ejemplo, p. Pontonniy, av. Lenina, ed. 4\2, ap. 5, lit. A, oficina 13.

4. El proceso de registro está finalizado. Presionar **Cerrar**.

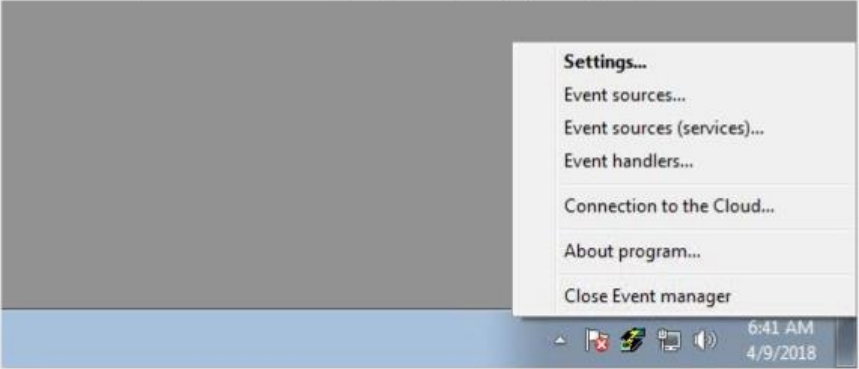
Registro del "Centro de seguridad" en la "Nube" X

¡Gracias por registrar el "Centro de seguridad" en la "Nube"!

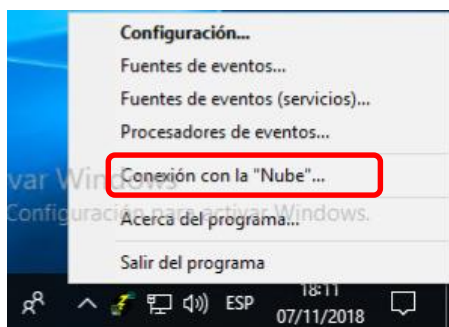
 Por favor, no olvide registrarse en la "Nube", como socio de "Cnord", o vincular este "Centro de seguridad" a la cuenta de usuario existente del socio.

Nueva ventana "Comunicación con la nube"

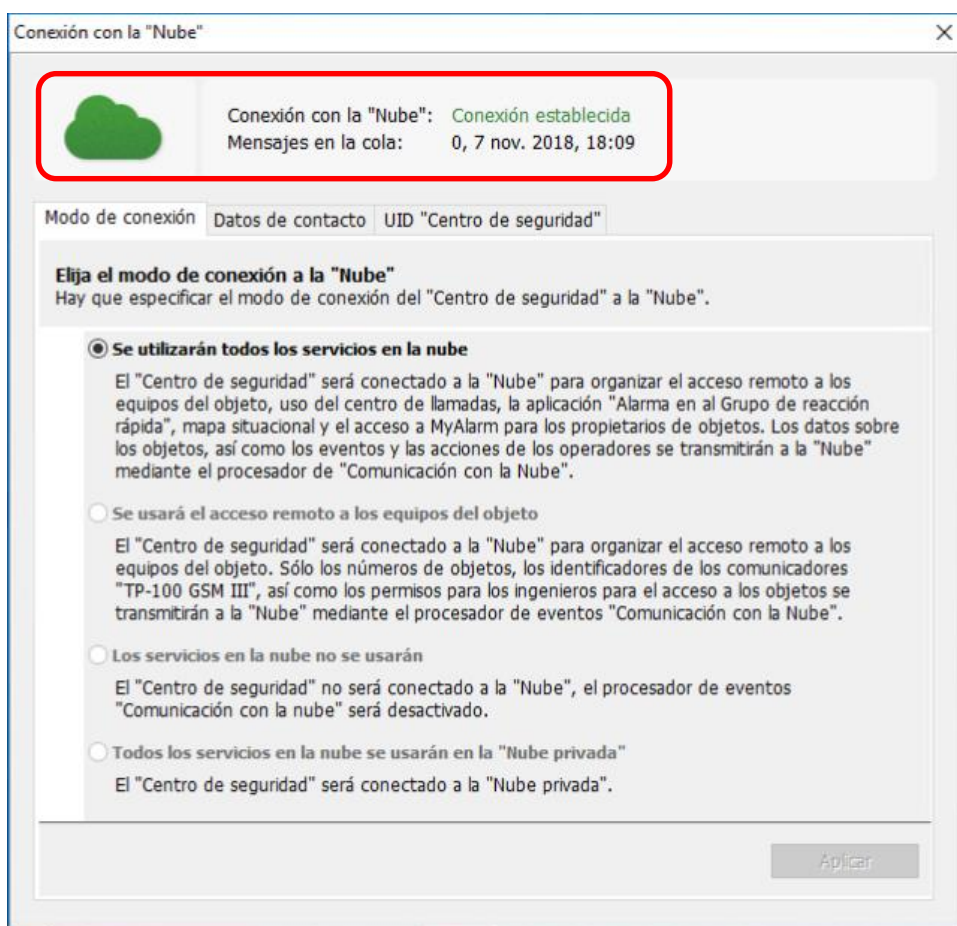
Pulse con un botón derecho del ratón en el "Administrador de eventos" - en el menú emergente aparecerá un nuevo punto "Comunicación con la nube". Allí podrá saber si se estableció la conexión "Centro de seguridad" con la "Nube" y los pasos que hay que dar para que el software funcione con



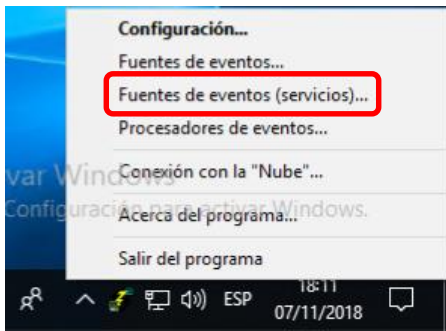
5. Para verificar que el Security Center se conectó a la Nube C.Nord hacer click derecho en el icono del **Administrador de eventos** que se encuentra en la parte derecha de la barra de tareas y elegir **Conexión con la "Nube"** desde el menú deslizante.



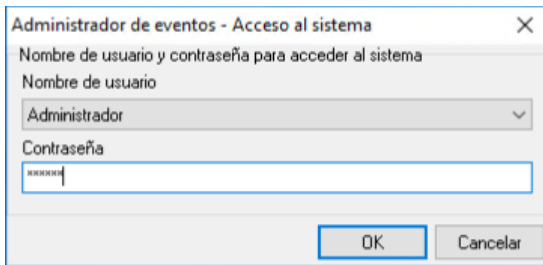
En la ventana emergente aparecerá el estado de la conexión con la **Nube C.Nord**. Se puede cerrar la ventana.



6. Ejecutar la opción **Fuentes de eventos (servicios)** del **Administrador de eventos**

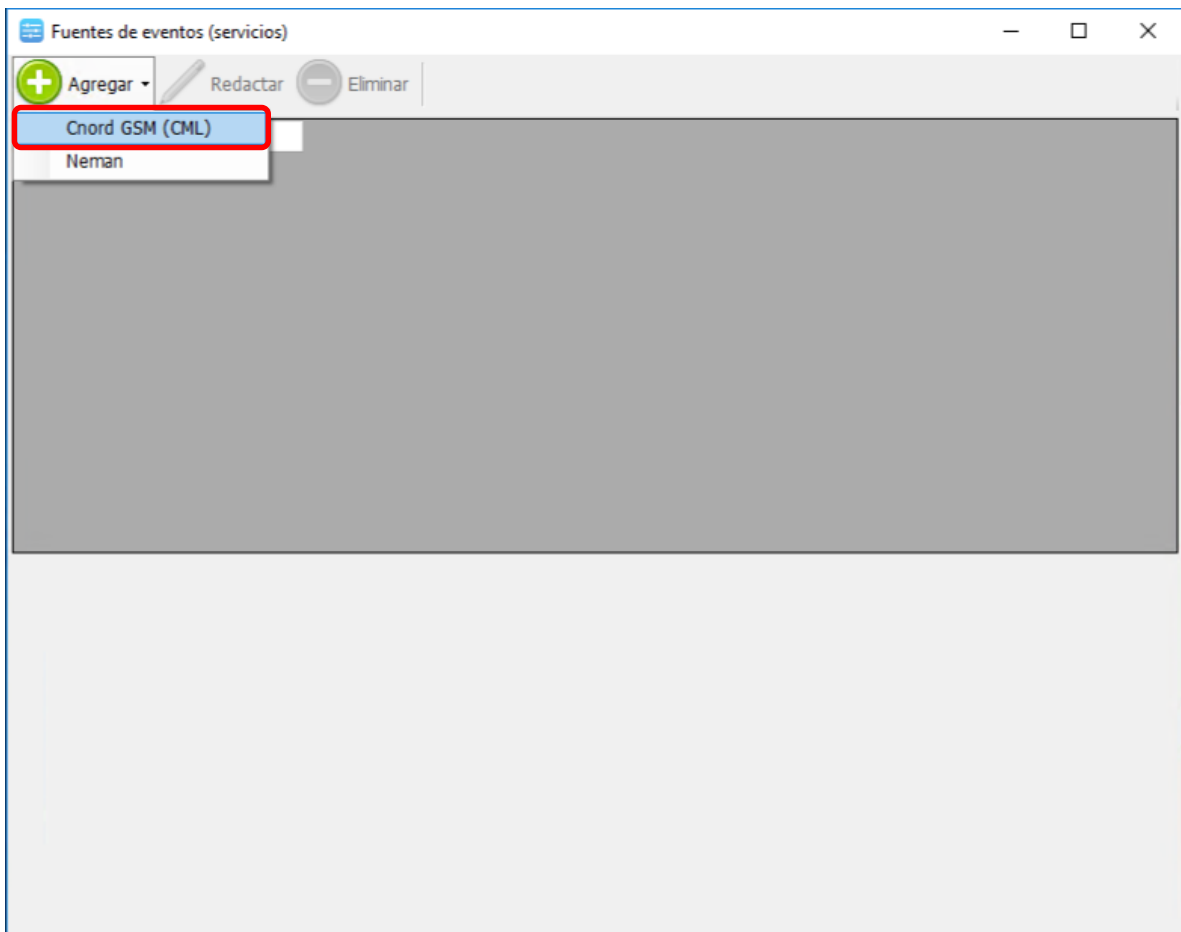


7. En la siguiente ventana ingresar el código del Administrador que por defecto es “222222”.



NB! Para poder configurar el SC para la recepción de los eventos directamente desde los paneles mediante el canal GSM-GPRS o Ethernet el servidor (PC) donde se instaló el SC debe tener la conexión al Internet con la IP pública (en vez de IP se recomienda usar el nombre DNS). Además de la IP habrá que abrir (en la configuración del router) uno o dos puertos para las conexiones entrantes TCP mediante canales GPRS y/o Ethernet.

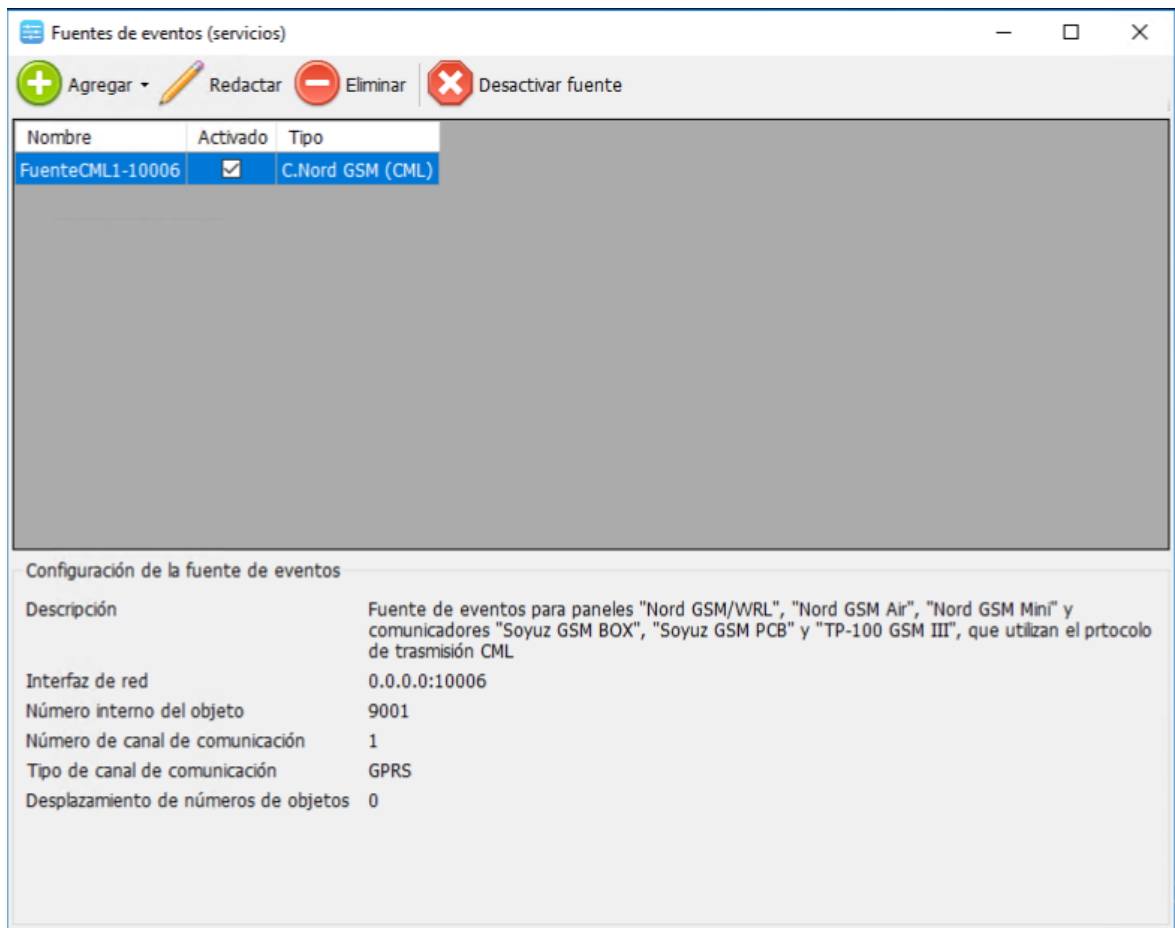
8. En la ventana emergente presionar el botón **Agregar** y seleccionar la fuente **Cnord GSM (CML)**



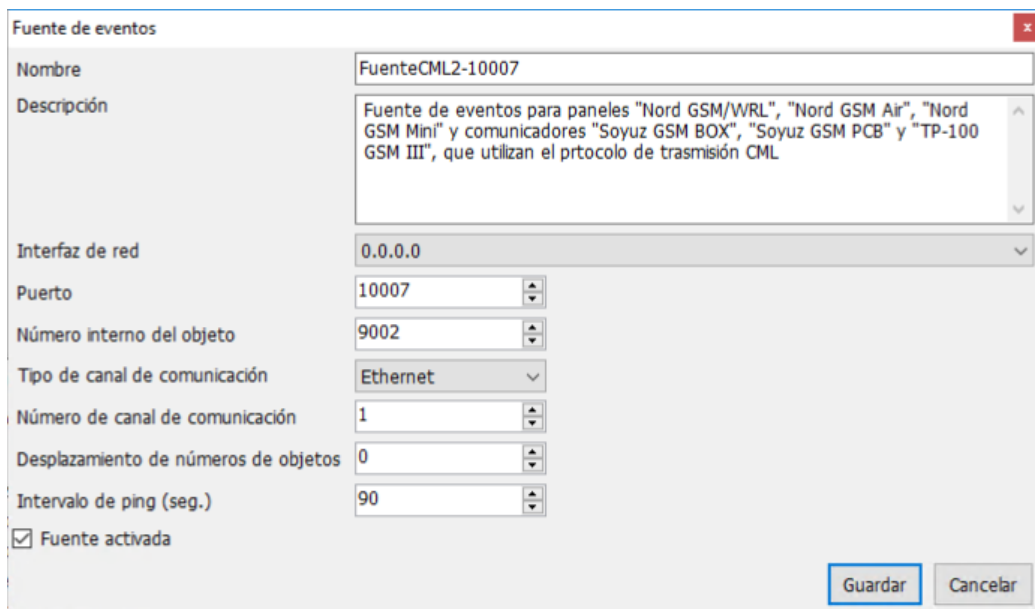
9. En la ventana que aparecerá ingresar el **Nombre** de la fuente, el **Puerto** (para evitar conflictos con los puertos usados en el SO Windows se recomienda usar el valor del puerto que sea superior a 10000), **Número interno del objeto** (que es el numero del objeto en la base de datos del SC) y seleccionar **Tipo de canal de comunicación** (GPRS o Ethernet). Marcar la casilla frente al **Fuente activada** y presionar **Guardar**.

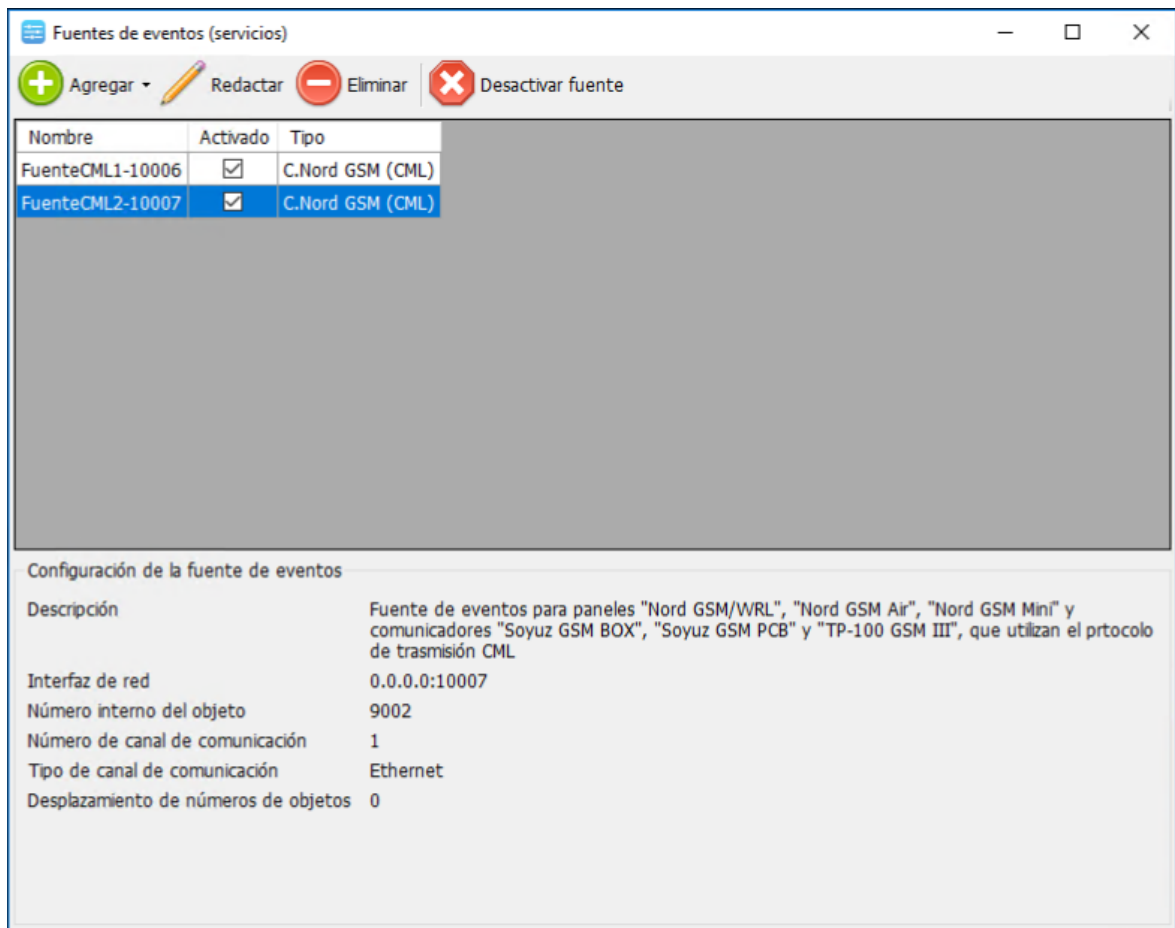
| | |
|---|--|
| Nombre | FuenteCML1-10006 |
| Descripción | Fuente de eventos para paneles "Nord GSM/WRL", "Nord GSM Air", "Nord GSM Mini" y comunicadores "Soyuz GSM BOX", "Soyuz GSM PCB" y "TP-100 GSM III", que utilizan el protocolo de transmisión CML |
| Interfaz de red | 0.0.0.0 |
| Puerto | 10006 |
| Número interno del objeto | 9001 |
| Tipo de canal de comunicación | GPRS |
| Número de canal de comunicación | 1 |
| Desplazamiento de números de objetos | 0 |
| Intervalo de ping (seg.) | 90 |
| <input checked="" type="checkbox"/> Fuente activada | |

En la ventana **Fuentes de eventos (sericios)** aparecerá la fuente nueva



10. Vamos a agregar la segunda fuente para el canal Ethernet. Para eso repetimos los pasos 8 y 9.





11. Crear una nueva regla de entrada en el **Firewall de Window Defender** para dos puertos que fueron seleccionados para las fuentes de eventos. Para eso repetir los pasos 1-3 descritos en la sección **2.3**. Luego marcar la casilla frente a **TCP** y en el campo **Puertos locales específicos** ingresar el valor **10006-10007**. Presionar **Siguiente**

Asistente para nueva regla de entrada

Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

TCP

UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

Todos los puertos locales

Puertos locales específicos: 10006-10007

Ejemplo: 80, 443, 5000-5010

< Atrás **Siguiente >** Cancelar

12. Repetir los pasos 5-6 descritos en la sección 2.3. Luego ingresar el nombre para la regla, e.g. **SecurityCenterTCP** y presionar **Finalizar**

Asistente para nueva regla de entrada

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

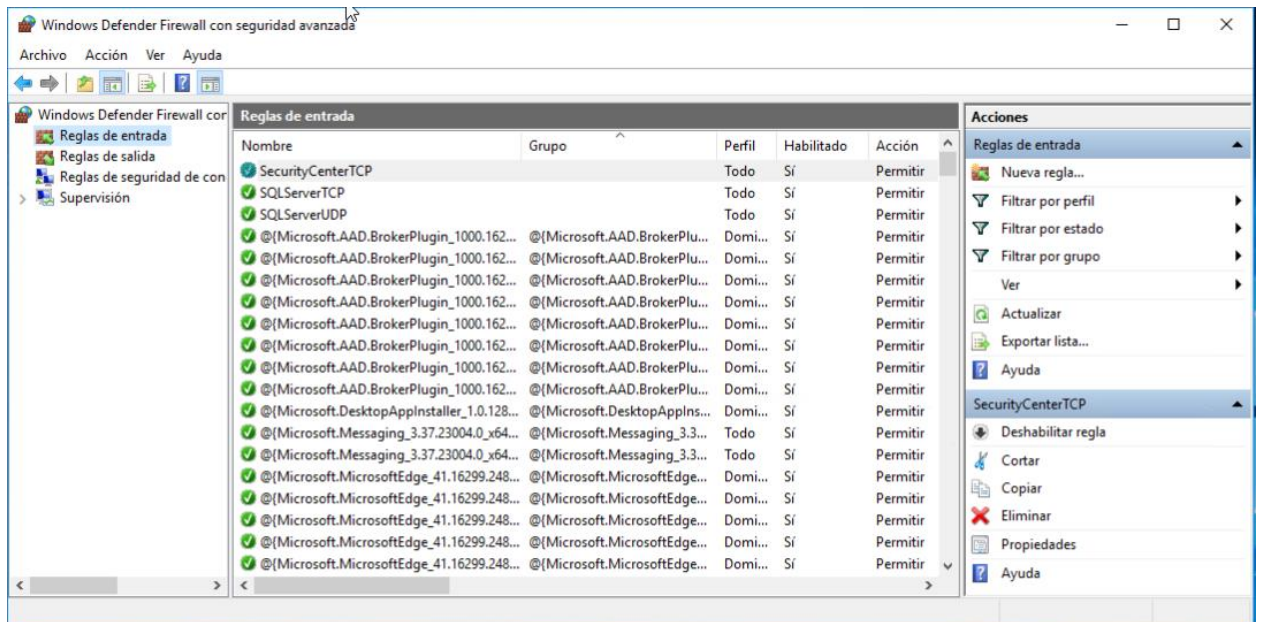
Nombre:

SecurityCenterTCP

Descripción (opcional):

< Atrás **Finalizar** Cancelar

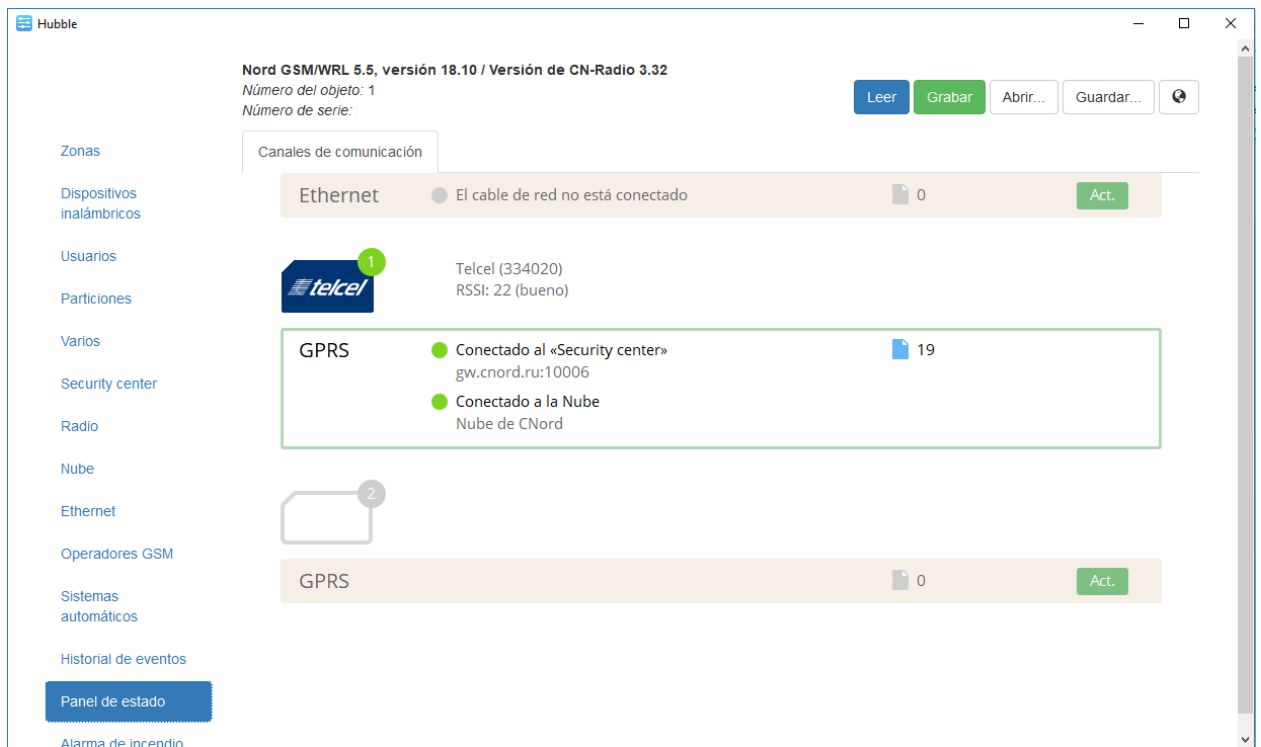
La configuración del **Firewall de Window Defender** está finalizada



13. Para verificar que su servidor tiene la IP pública y los puertosTCP están abiertos para las conexiones entrantes se puede utilizar la [pagina especial](#) en nuestro sitio web

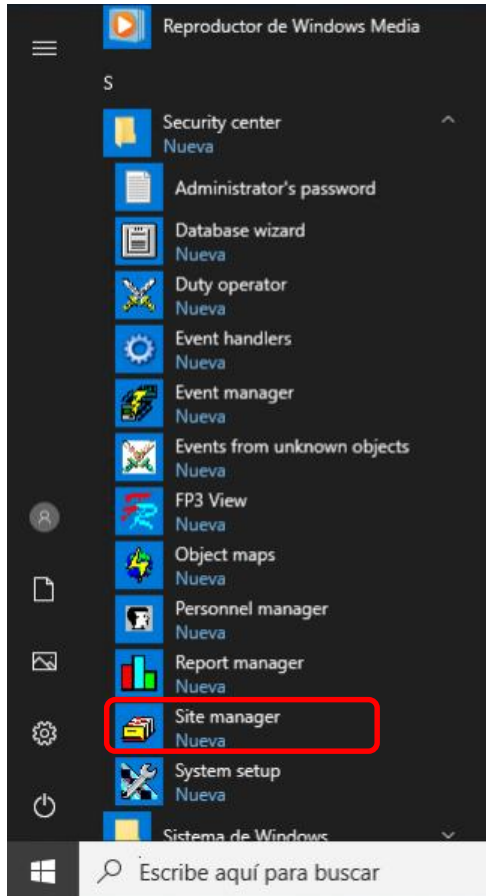


14. Si todo está configurado correctamente los paneles se conectarán automáticamente al **Security Center** y en el Panel de estado en **Hubble** se visualizará el estado de la conexión

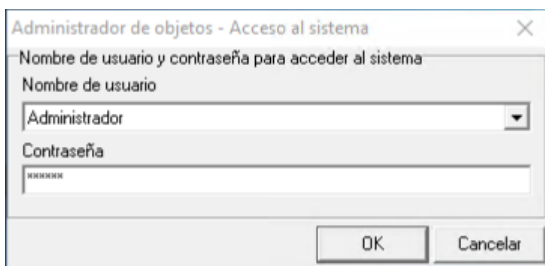


2.5.2 Adición de nuevos objetos en Administrador de objetos

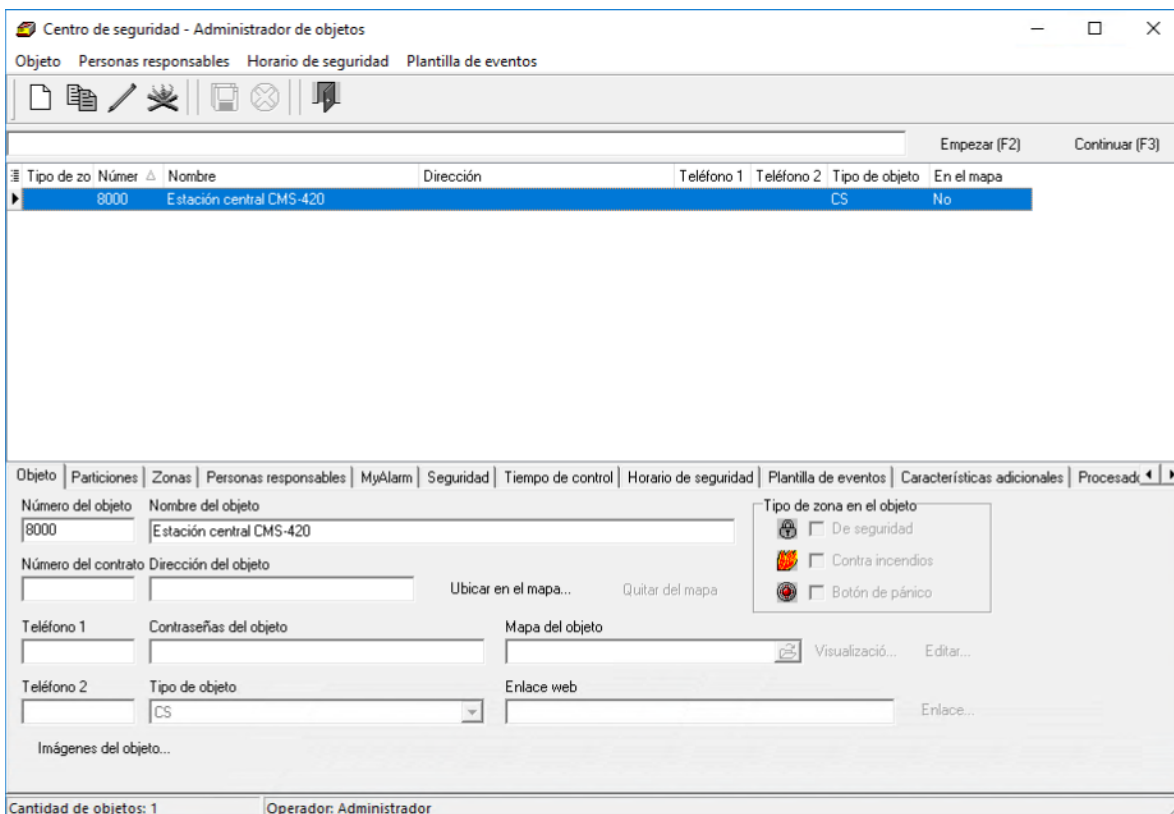
1. Ejecutar el **Site manager** (Administrador de objetos)



2. En la ventana emergente ingresar la contraseña (222222 – por defecto)

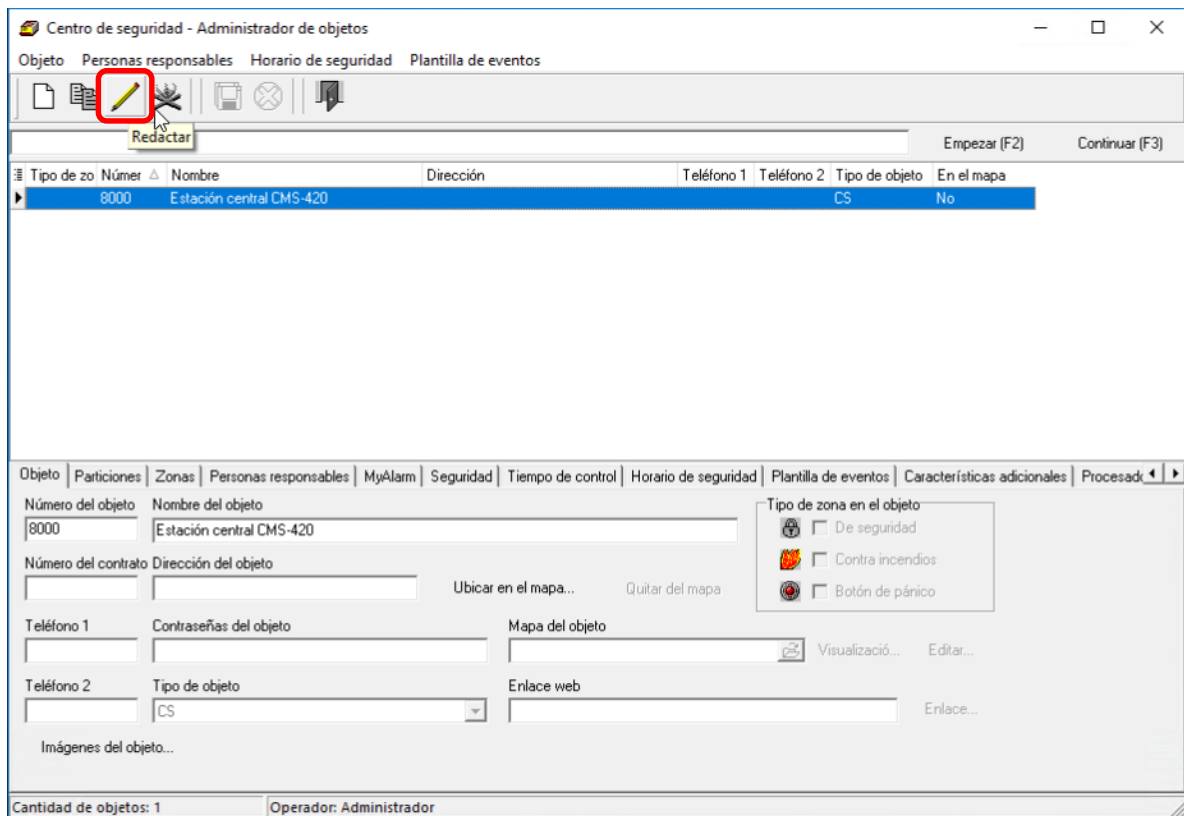


3. Se abrirá la ventana principal del módulo **Administrador de objetos**

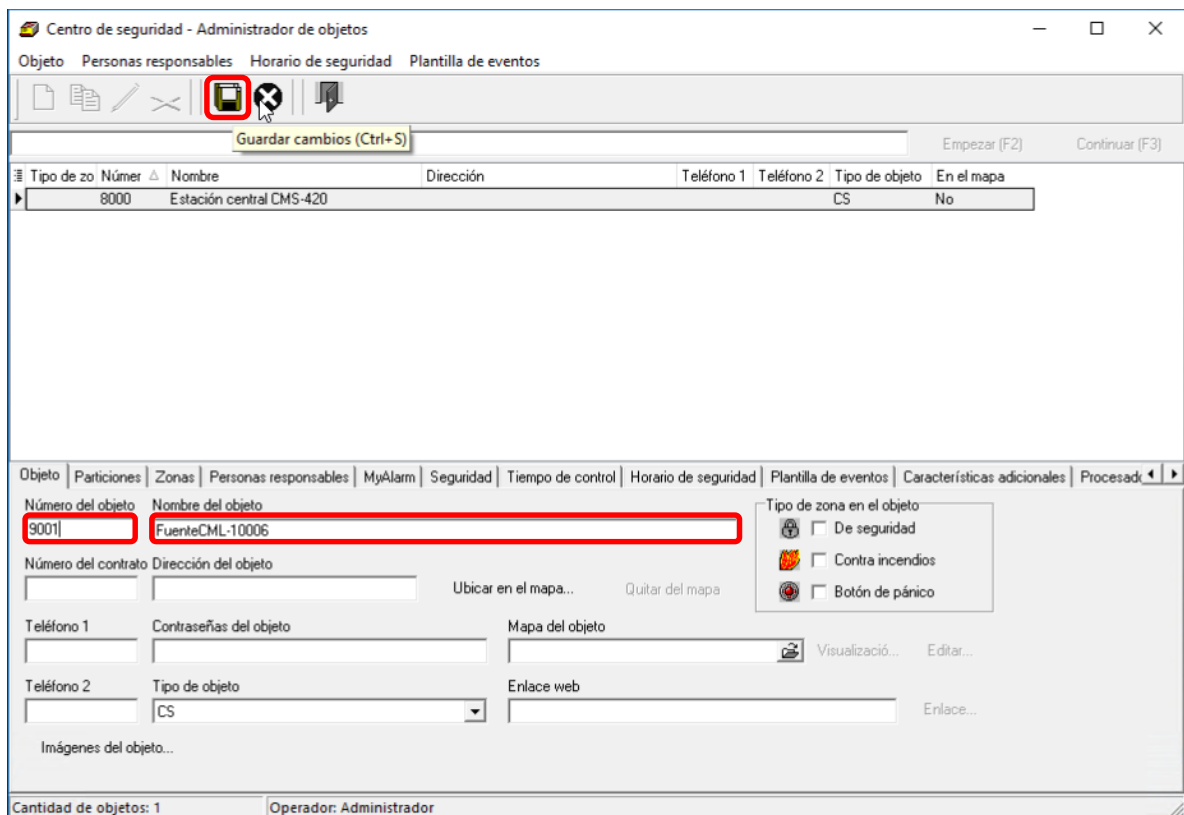


4. Para poder identificar los paneles que no están registrados en la base de datos primero tendremos que crear dos objetos virtuales para los fuentes de eventos – GPRS y Ethernet

Para ello seleccionar el objeto existente en la base de datos con el nombre **Estación central CMS-420** y presionar el botón **Redactar** en la barra de instrumentos de arriba.

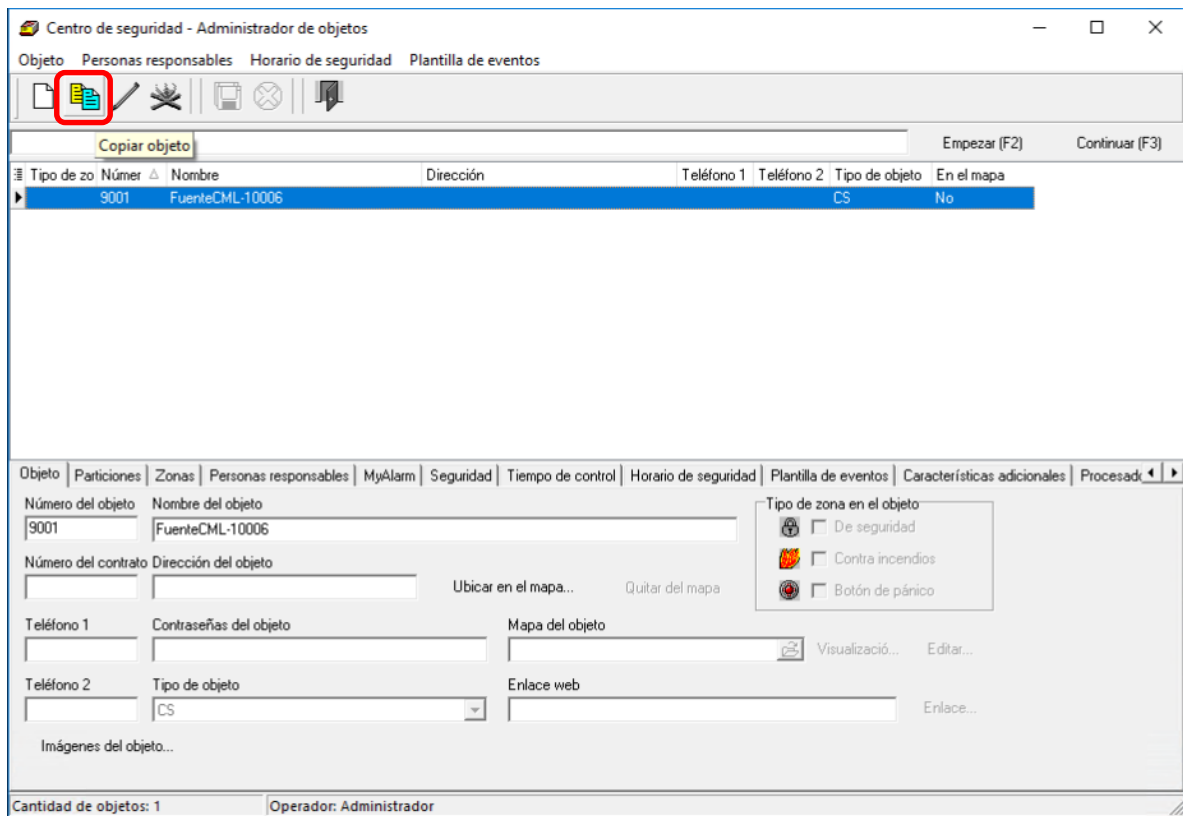


5. Cambiar el **Número del objeto** por “9001” y el **Nombre del objeto** por “FuenteCML-10006” y presionar el botón **Guardar cambios**

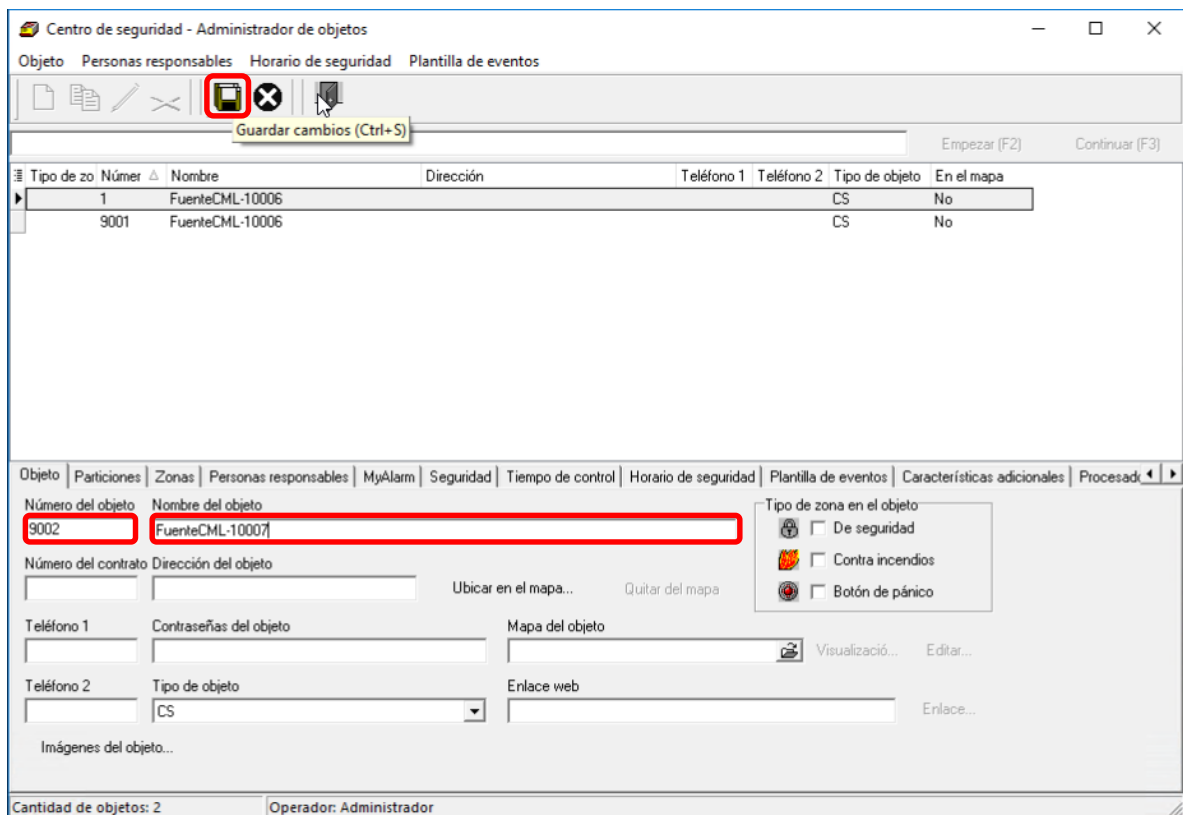


6. El segundo objeto tendrá los mismos parámetros con el objeto **FuenteCML-10006**.

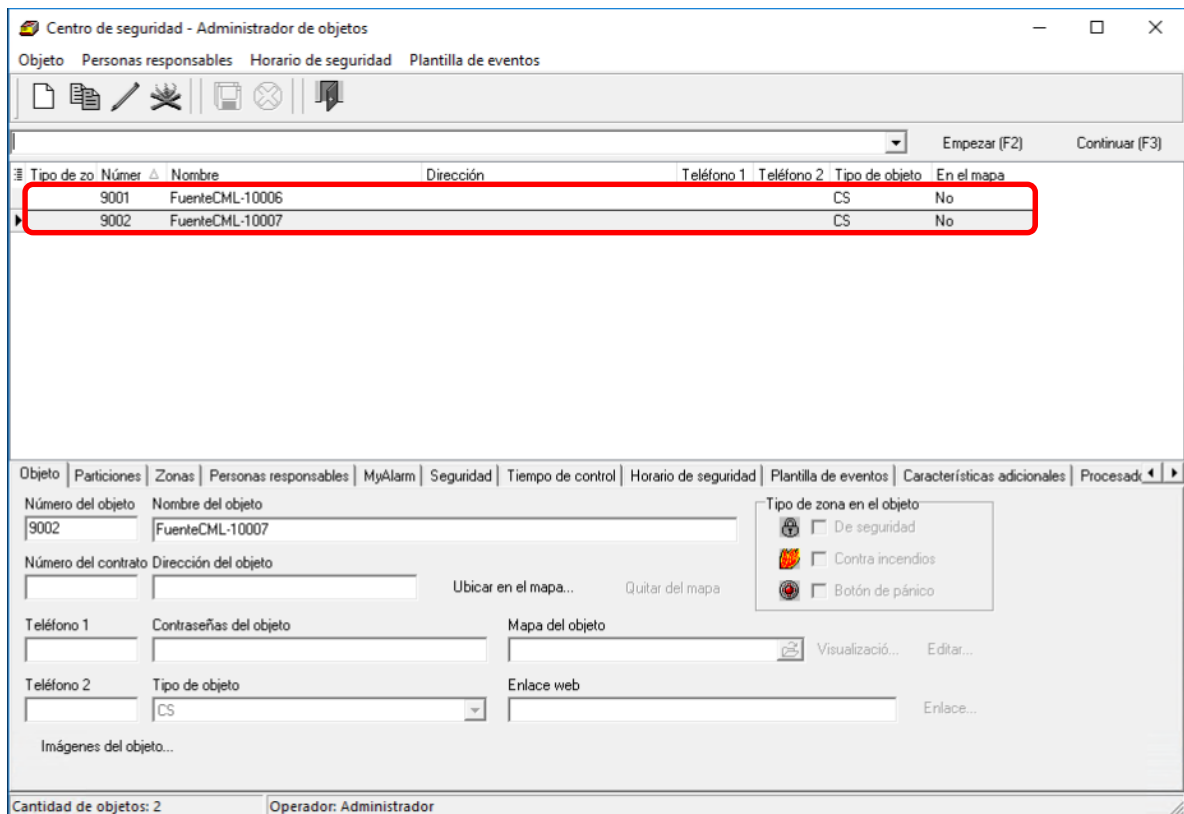
Seleccionar el objeto con el nombre **FuenteCML-10006** y presionar el botón **Copiar objeto**



7. Cambiar el **Número del objeto** por “9002” y el **Nombre del objeto** por “FuenteCML-10007”. Presionar el botón **Guardar cambios** o **Ctrl+S**

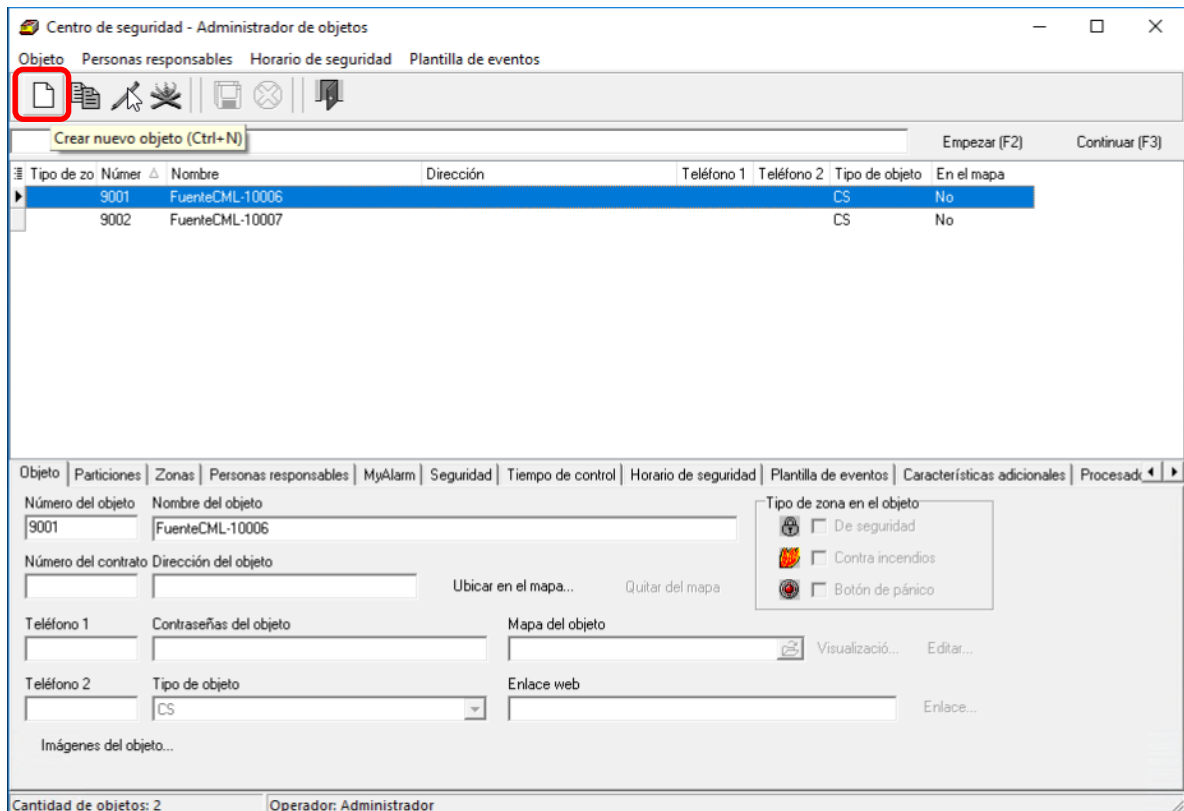


8. Como resultado en la base de datos deben aparecer dos objetos

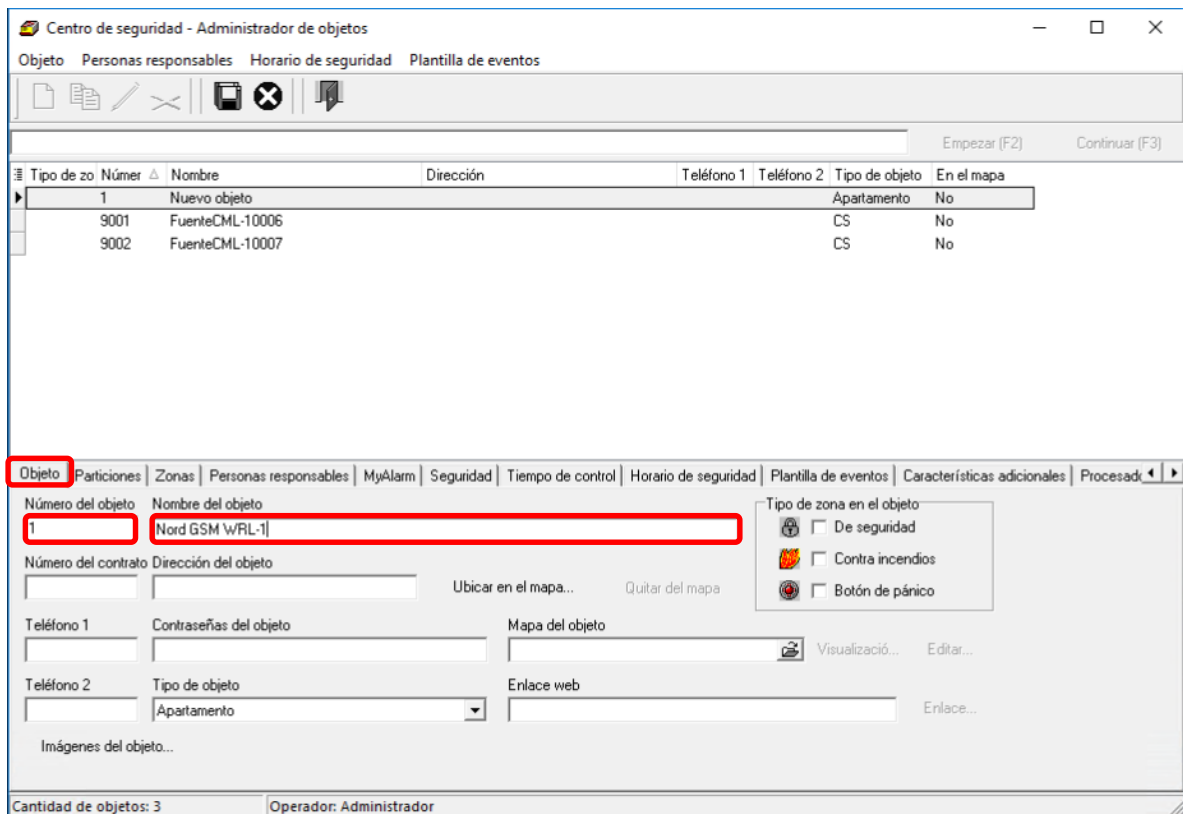


9. Vamos a crear un objeto físico para el panel que ya configuramos anteriormente (vease subsección 1.1)

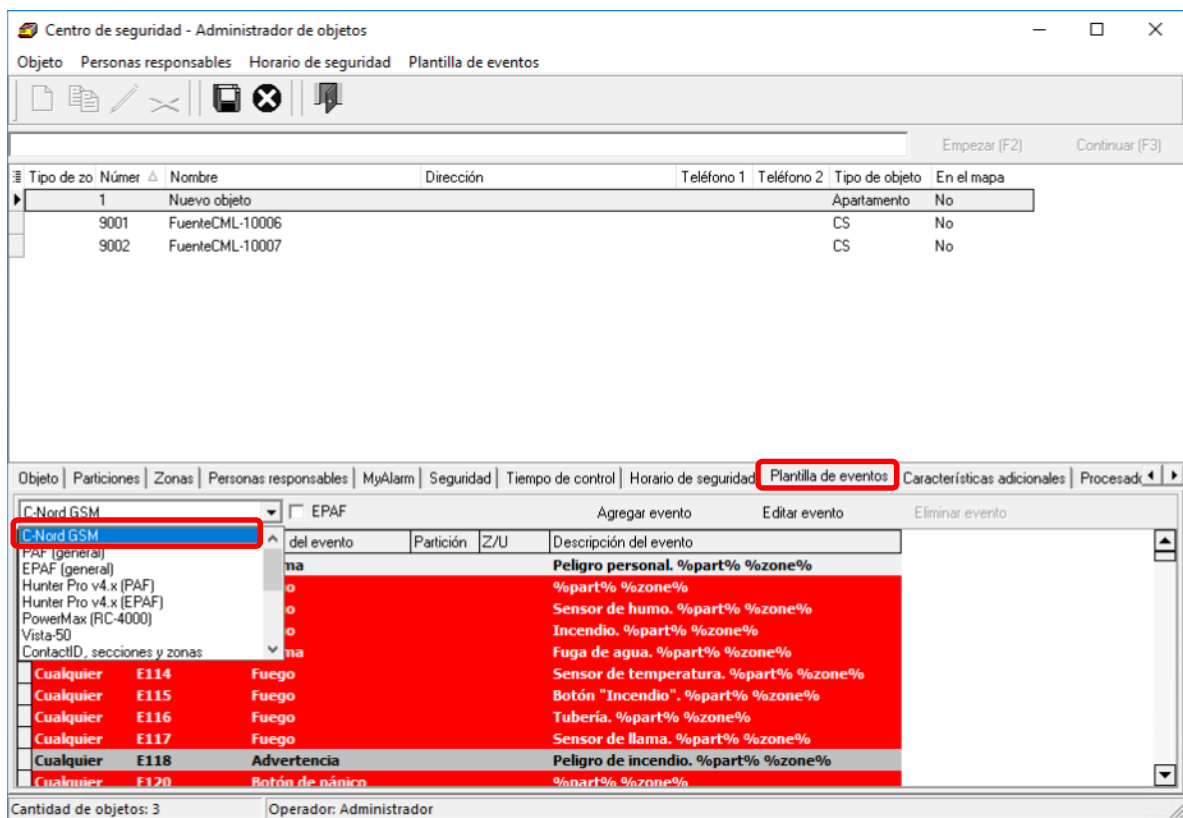
Presionar el botón **Crear nuevo objeto** o **Ctrl+N**



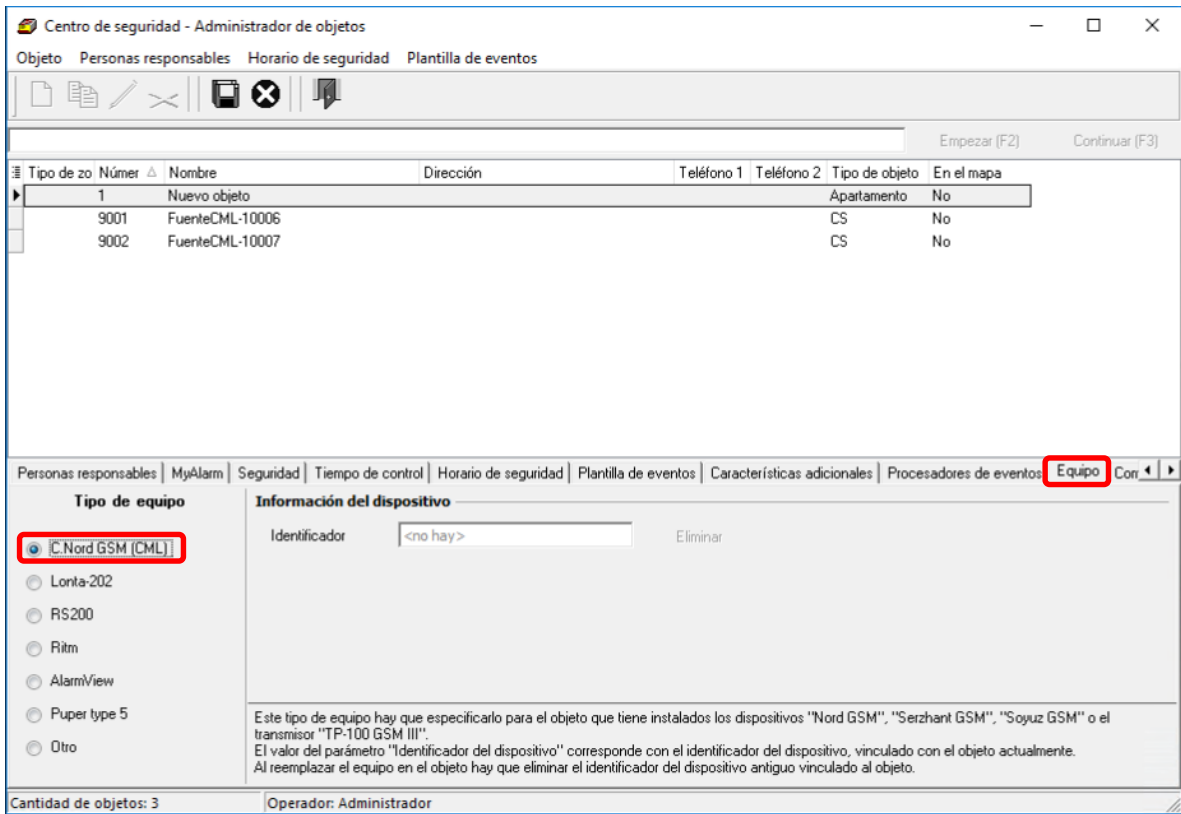
10. En la pestaña **Objeto** ingresar el Número del objeto **"1"** y el Nombre del objeto **"Nord GSM WRL-1"**



11. En la pestaña **Plantilla de eventos** seleccionar **C-Nord GSM** del menú deslizante en la parte superior derecha

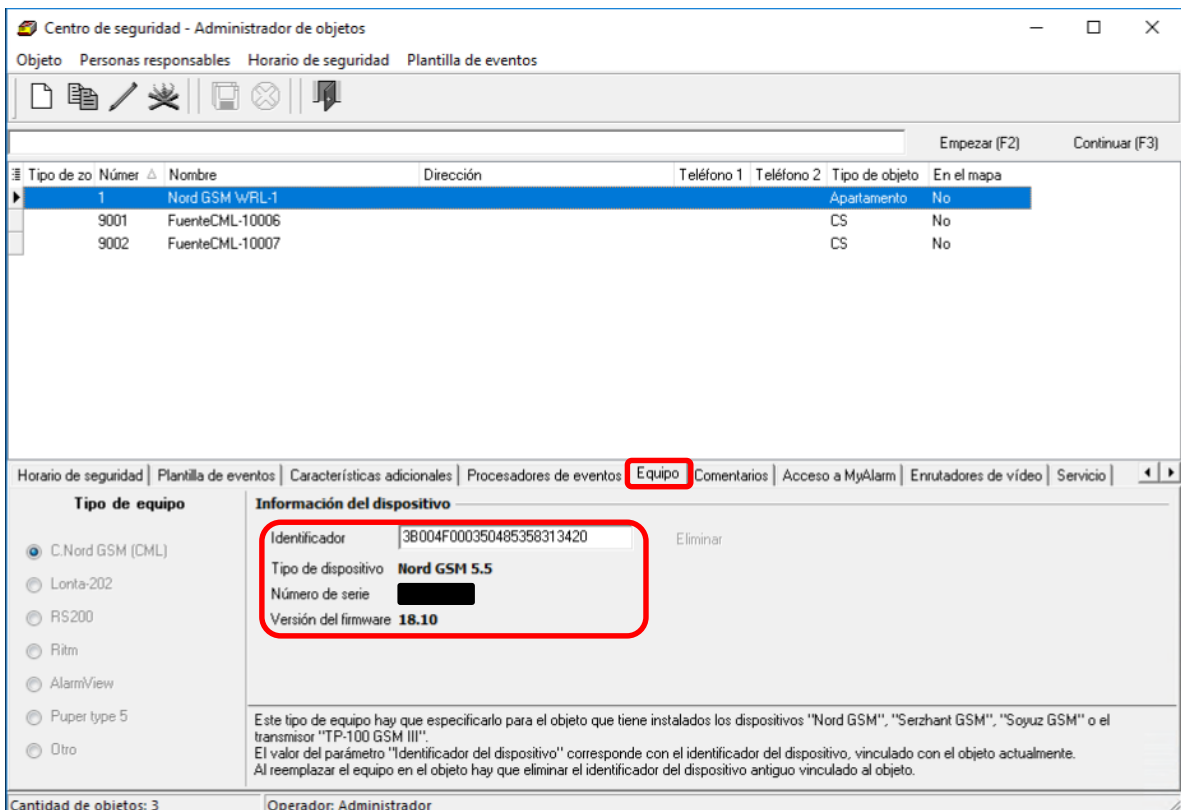


12. En la pestaña **Equipo** seleccionar **C.Nord GSM (CML)** entre las opciones del **Tipo de equipo** disponibles

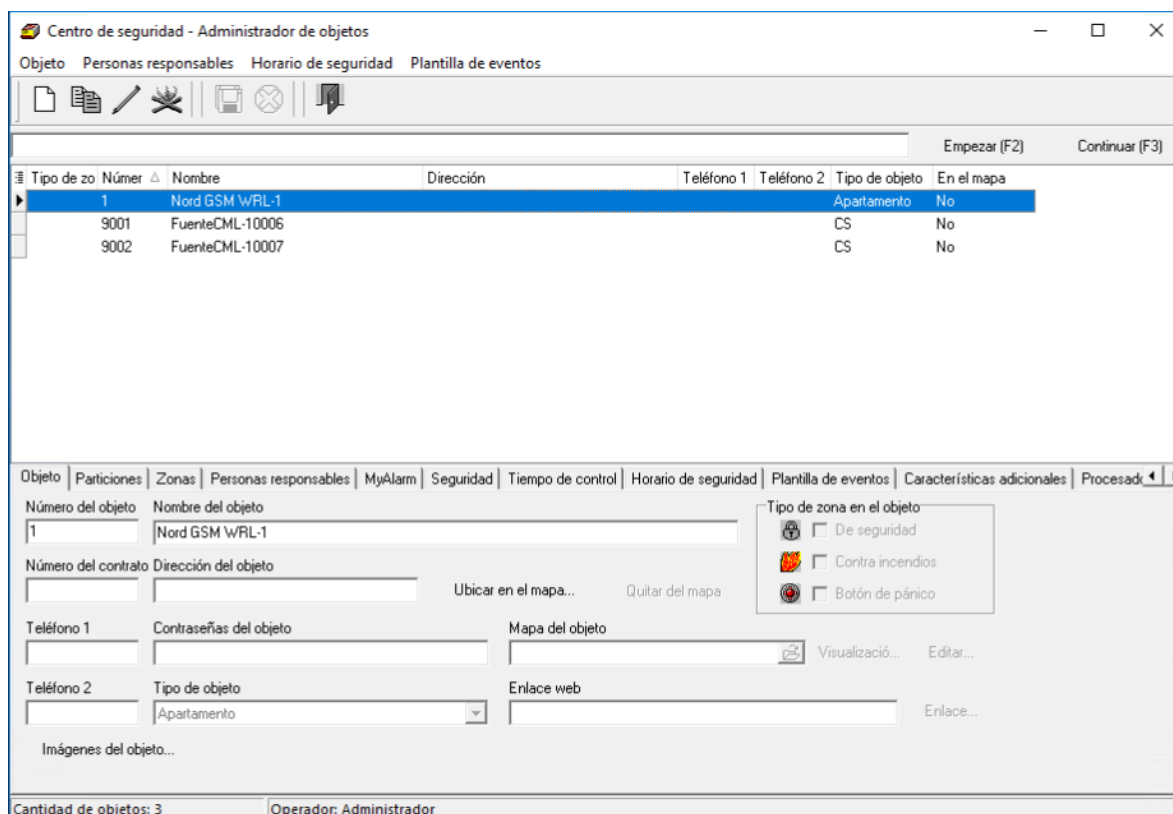


13. Presionar **Guardar cambios**

Para comprobar que el panel se intercambiaron los datos con el SC con éxito verificar los valores de los parámetros **Identificador**, **Tipo de dispositivo**, **Número de serie**, **Versión de firmware** que deberán aparecer en la pestaña **Equipo**



14. La subida del nuevo objeto (panel) a la base de datos está finalizada



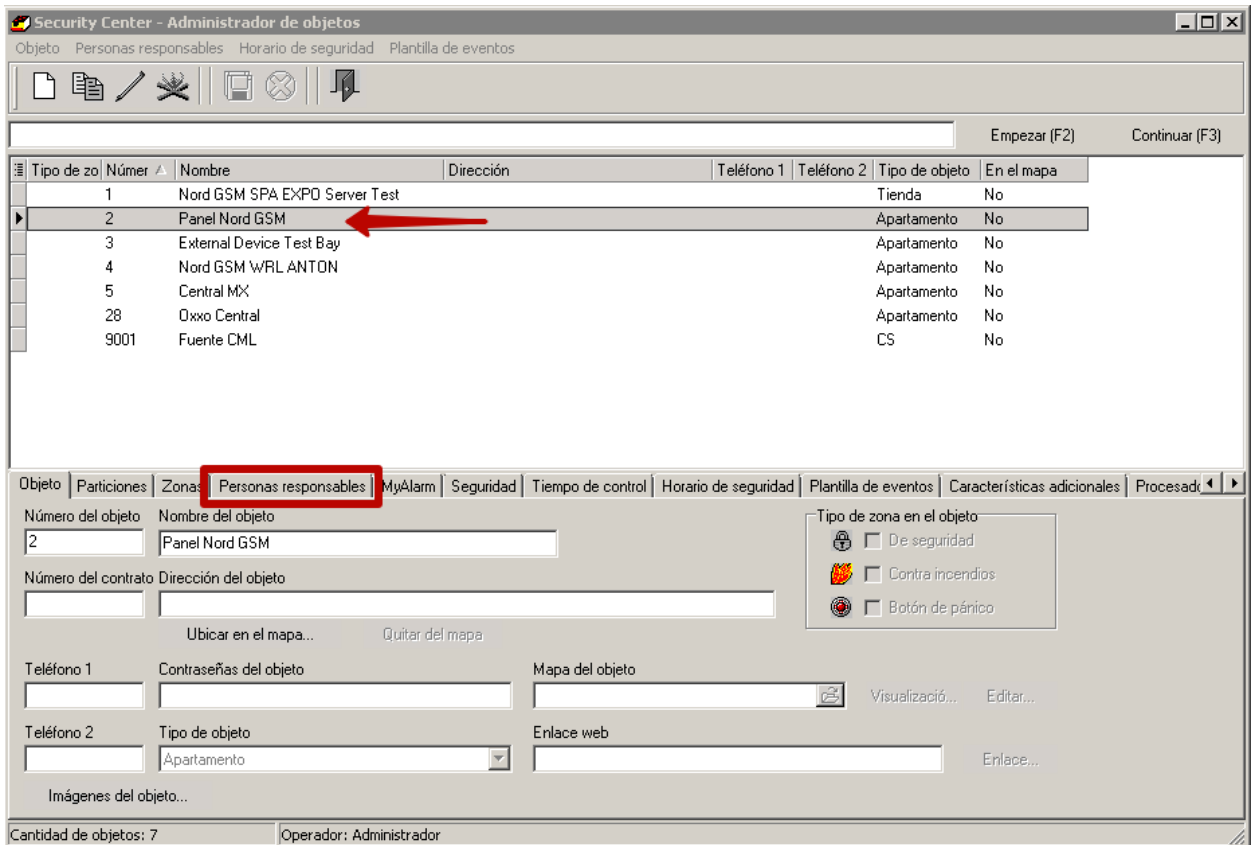
2.5.3 Activación de MyAlarm para el nuevo objeto

La aplicación MyAlarm está disponible en AppStore y Google Play.

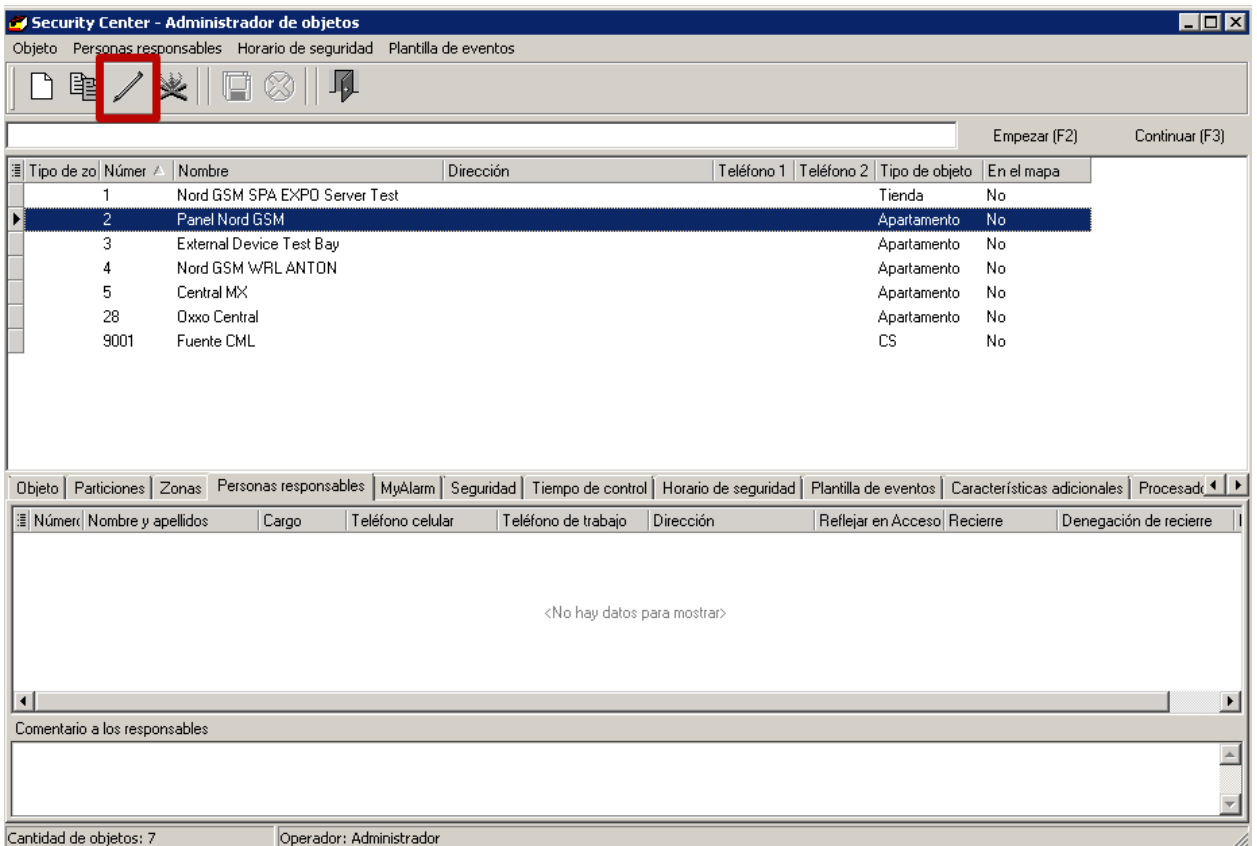


1. Descargue la aplicación en su teléfono, ábrala e ingrese su número de teléfono para registrarse. En breve recibirá un código en SMS para proceder con el registro. Por defecto, el escritorio la aplicación estará vacío, ya que no tiene objetos agregados.

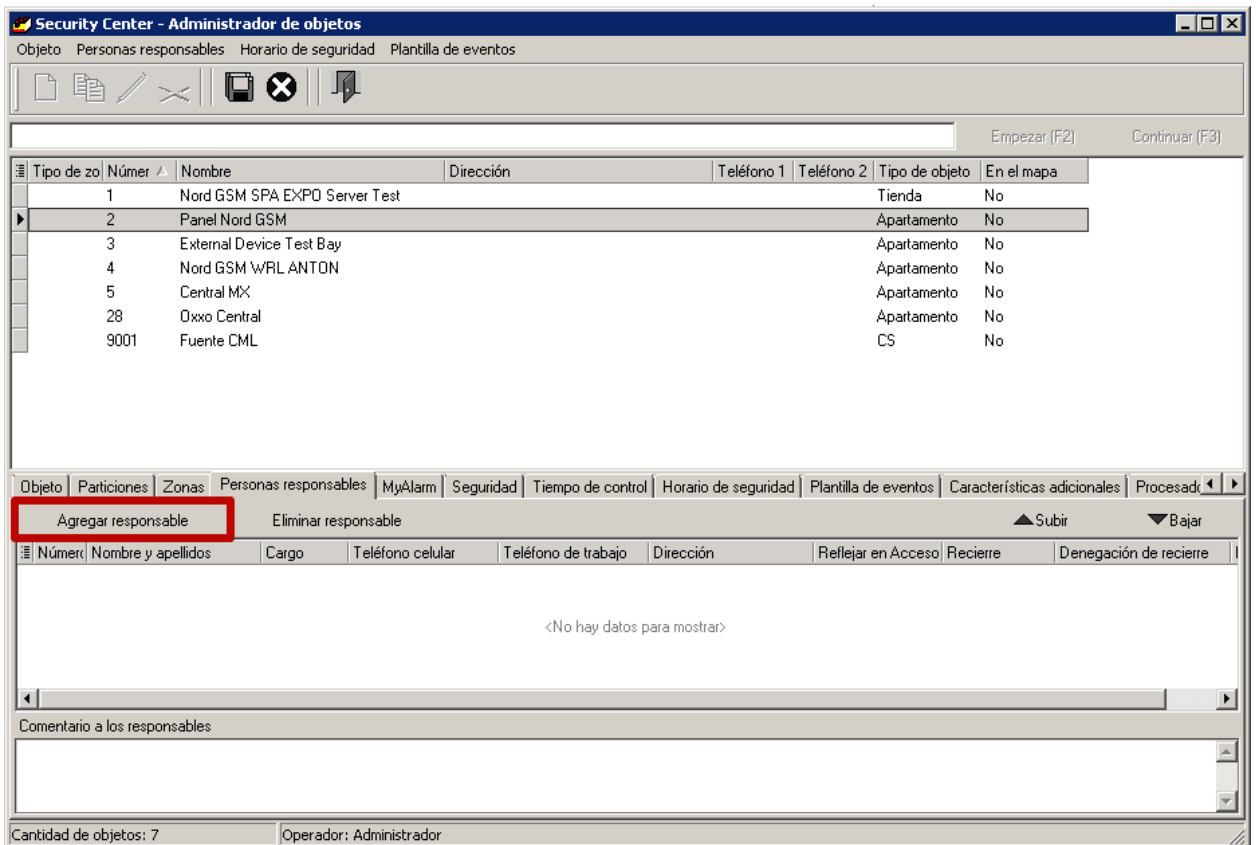
2. Ejecute el **Administrador de recintos**. Seleccione el sitio (Objeto) que desea controlar a través de MyAlarm. Abra la pestaña *Personas Responsables*.



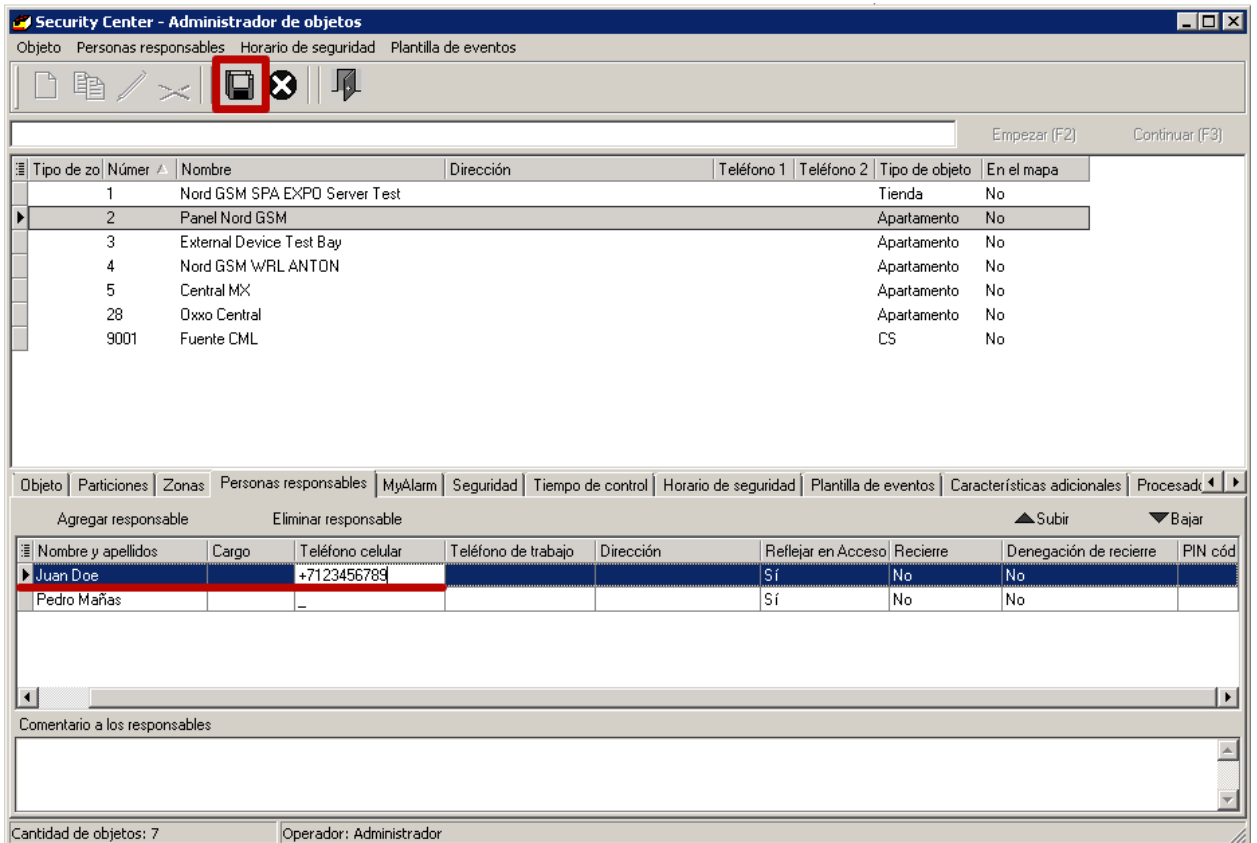
3. Haga clic en el botón **Editar**



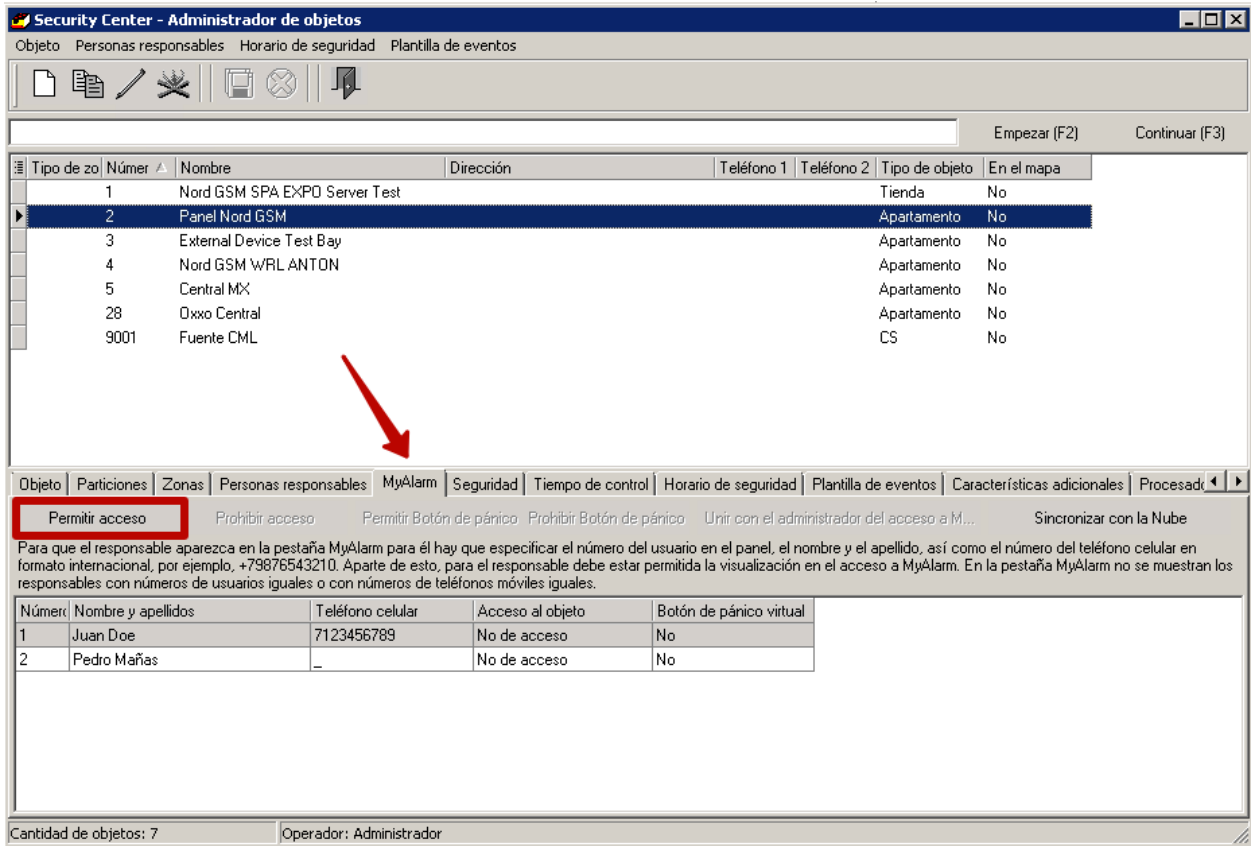
4. Haga clic en el botón **Agregar responsable** que ha aparecido en la parte inferior.



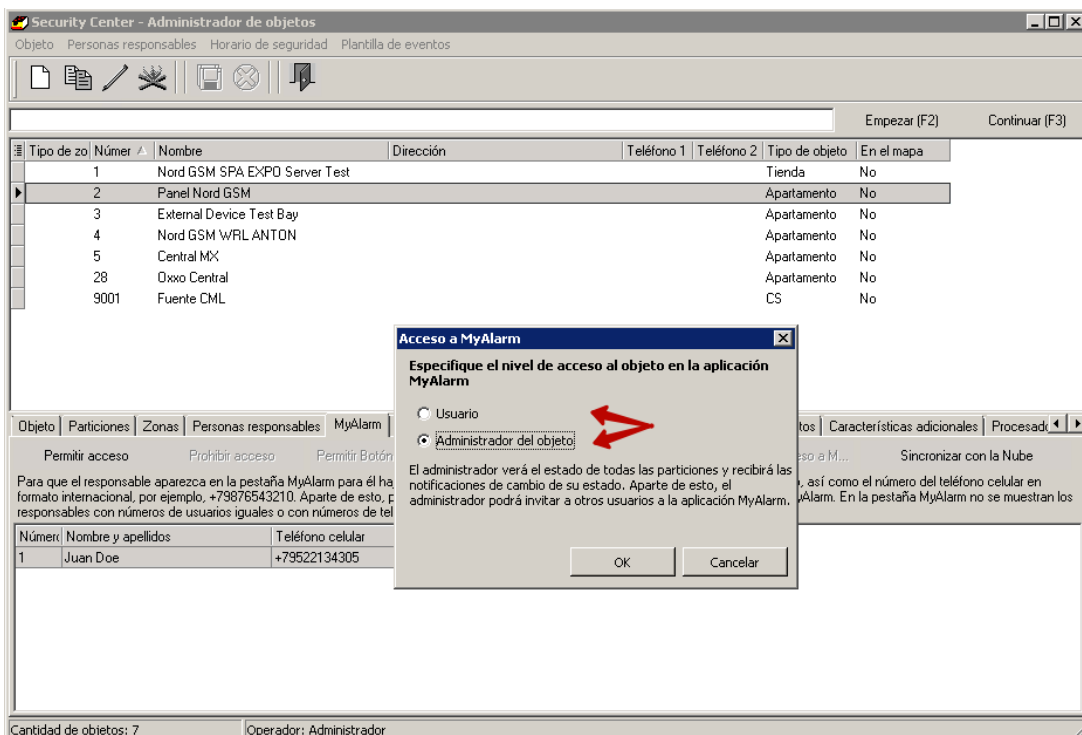
5. Ingrese el número de la *Persona responsable* (campo obligatorio), su nombre y su número de teléfono móvil en formato internacional (por ejemplo, +12345678900). Y haga clic en **Guardar**.



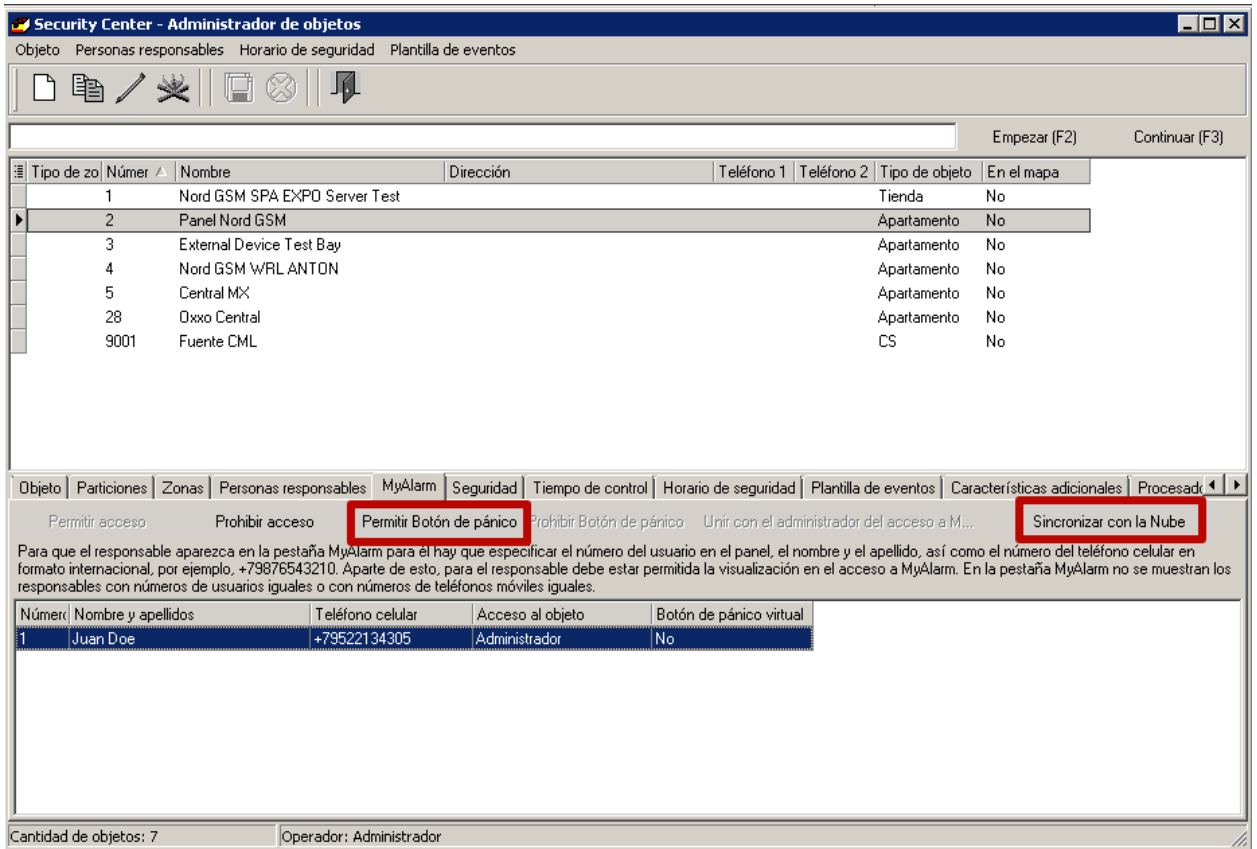
6. Vaya a la pestaña **MyAlarm** y haga clic en **Editar**. Todas las personas responsables que ha agregado en las pestañas anteriores aparecerán automáticamente aquí. Ahora puede **Permitir acceso** a la persona responsable seleccionada.



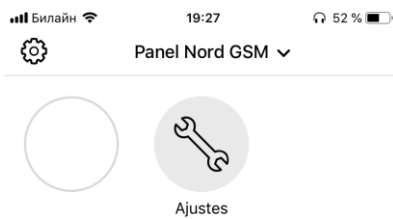
7. Elija el nivel de acceso al objeto en la aplicación MyAlarm para la persona responsable elegida. Haga clic en **OK**.



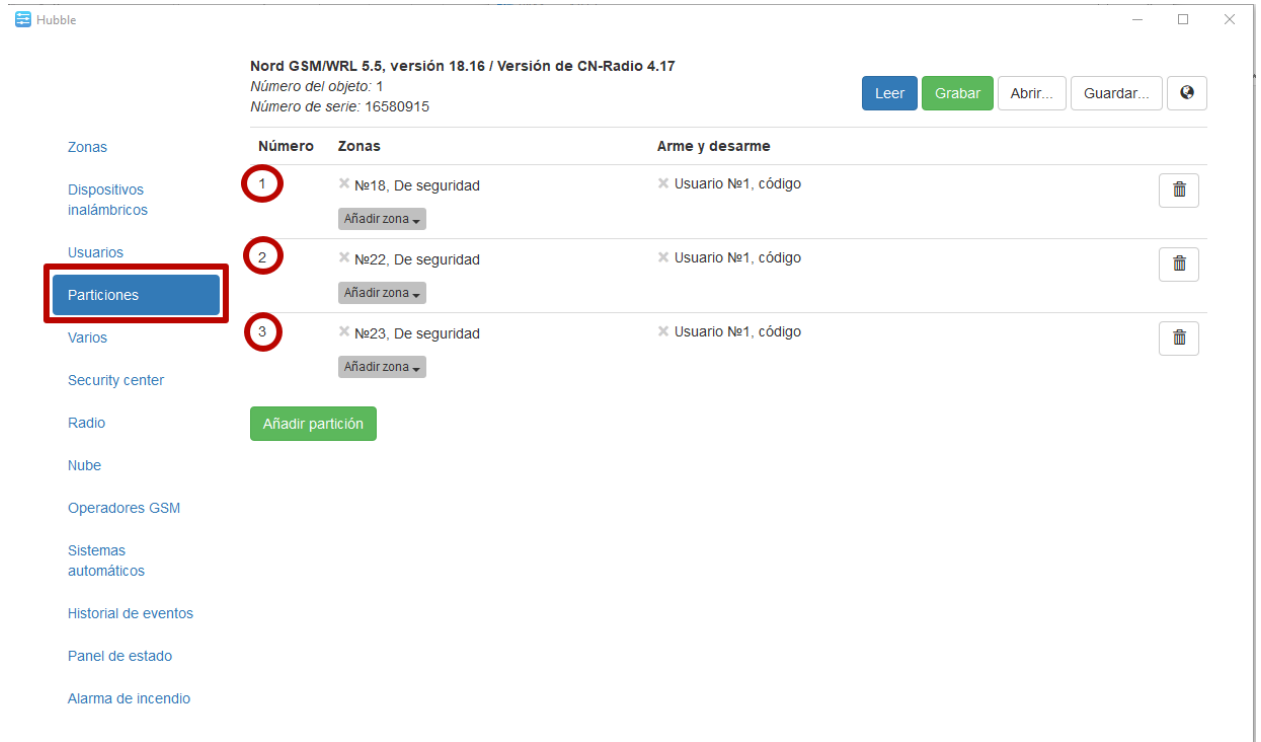
8. **Habilite el botón de pánico virtual** (opcional) y aparecerá en su escritorio MyAlarm . Se recomienda **Sincronizar** los cambios realizados con la Nube.



9. Abra la aplicación **MyAlarm** en su teléfono. El nombre del objeto se muestra sobre todos los iconos. Por defecto, no habrá particiones para activar (círculo blanco).

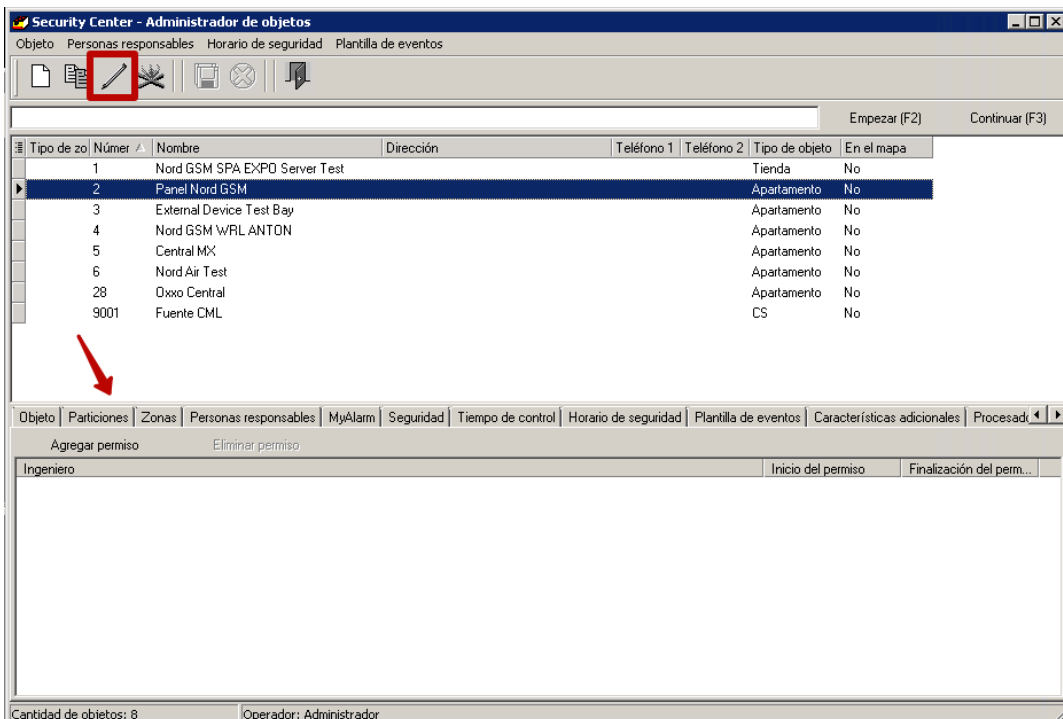


10. Abra el configurador de **Hubble** y verifique el número de particiones creadas.

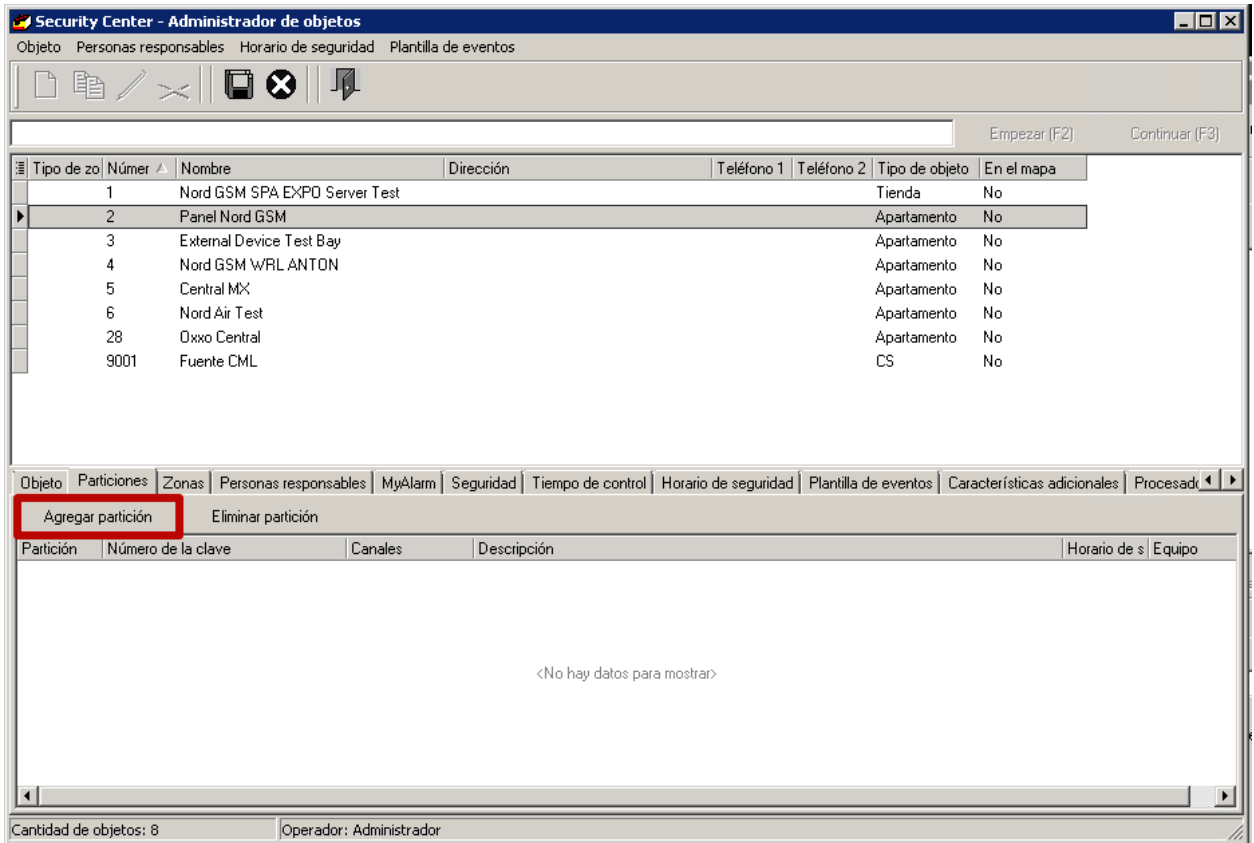


NB! El número de Particiones agregadas al Administrador del sitio debe ser el mismo que el número correspondiente configurado en el configurador de Hubble.

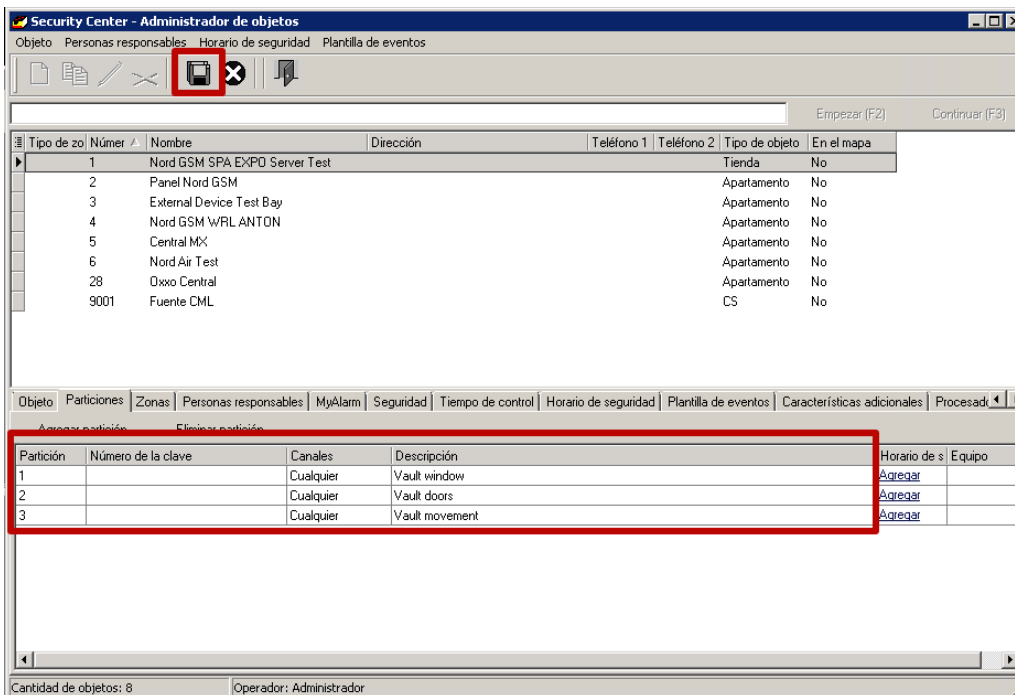
11. Vuelva al **Administrador de recintos** para registrar las particiones correspondientes. Abra la pestaña **MyAlarm** y haga clic en **Editar**.



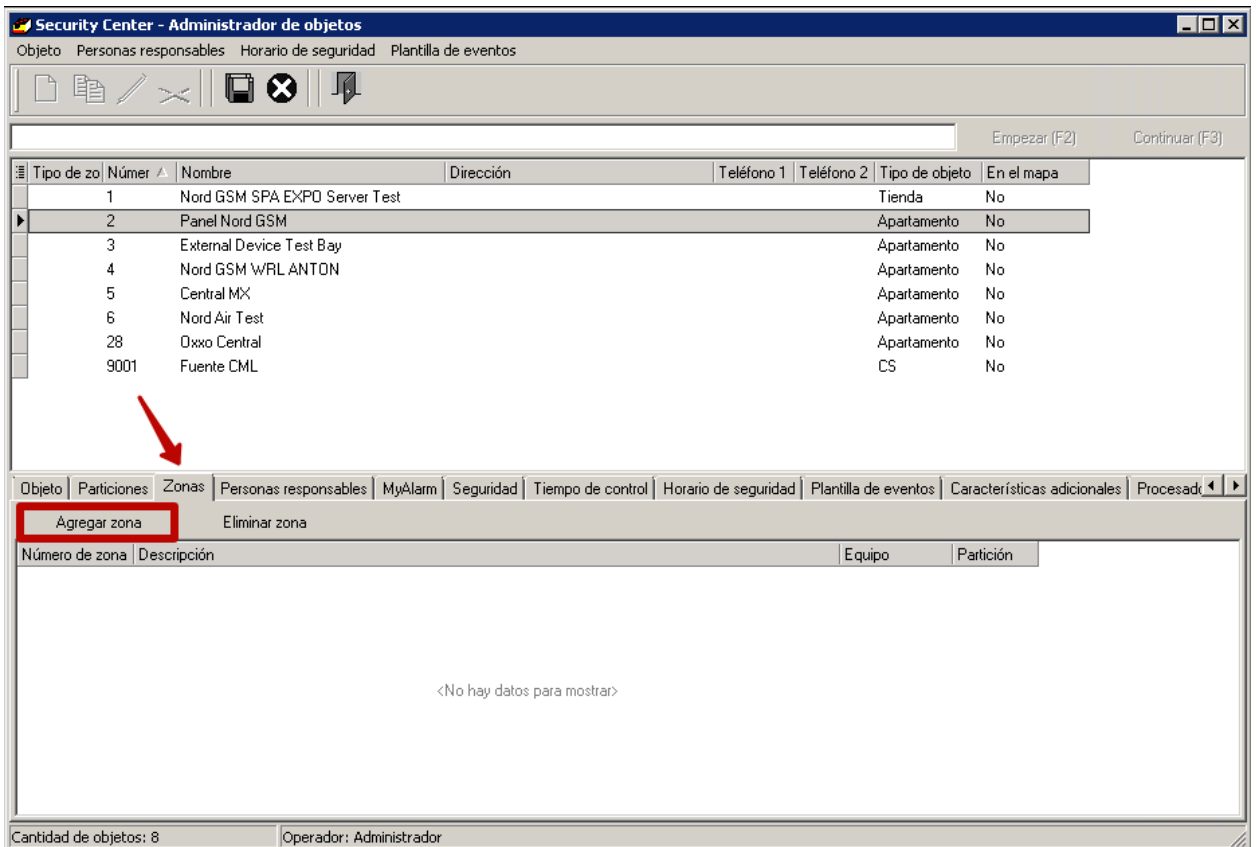
12. Haga clic en el botón **Agregar partición**.



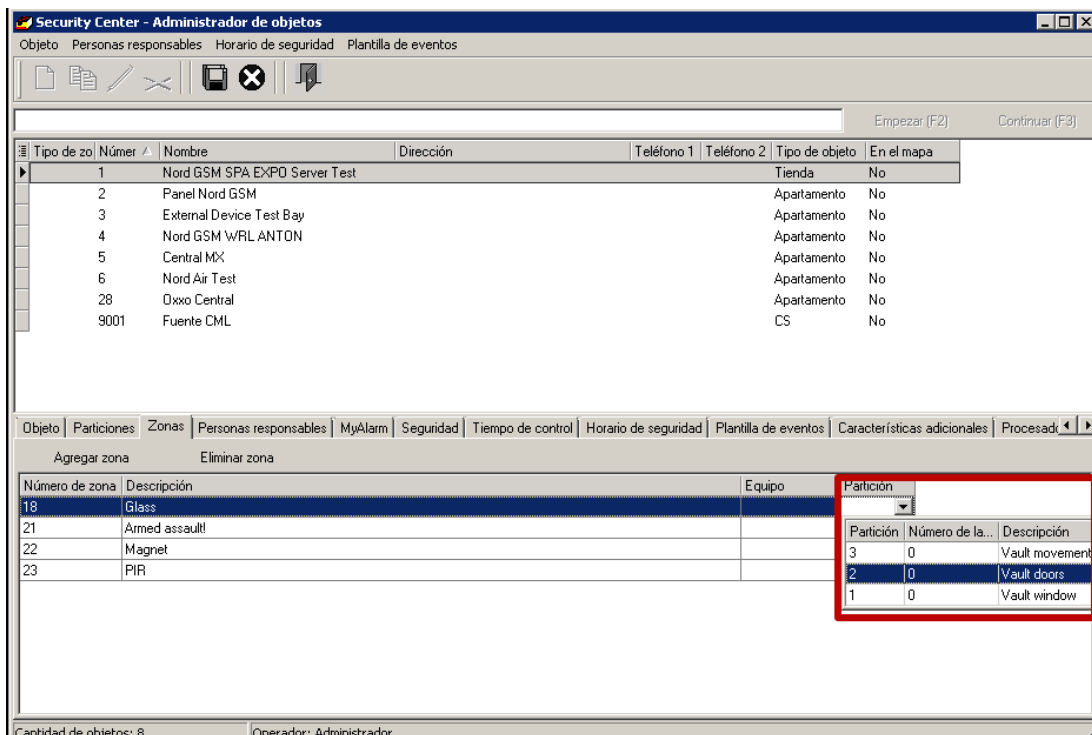
13. Asegúrese de agregar la misma cantidad de *Particiones* que haya configurado en Hubble con el número correspondiente y agregue la descripción de cada una en el campo *Descripción*. Esta información se transferirá a la aplicación MyAlarm inmediatamente después de hacer clic en **Guardar**. Verá los iconos de las particiones con sus nombres en el escritorio de la aplicación MyAlarm.



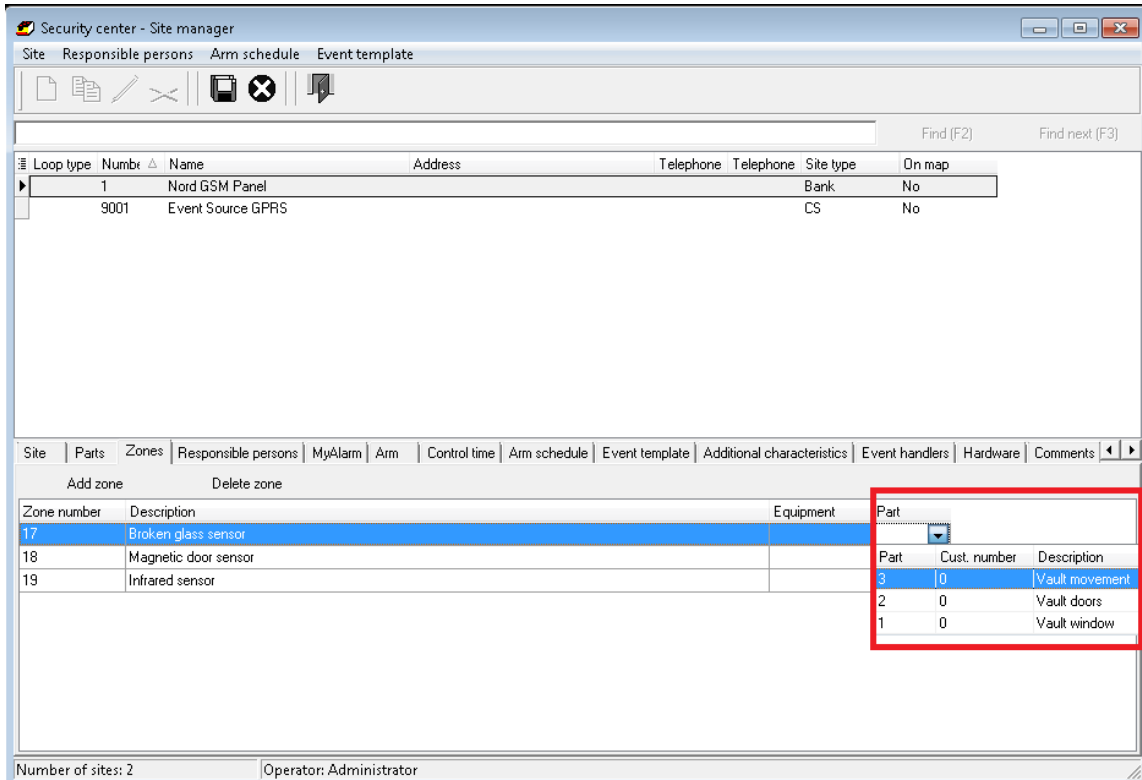
14. Para especificar la relación entre los sensores y las particiones, vaya a la pestaña **Zonas**. Haga clic en **Editar** primero y luego presione el botón **Agregar Zona**.



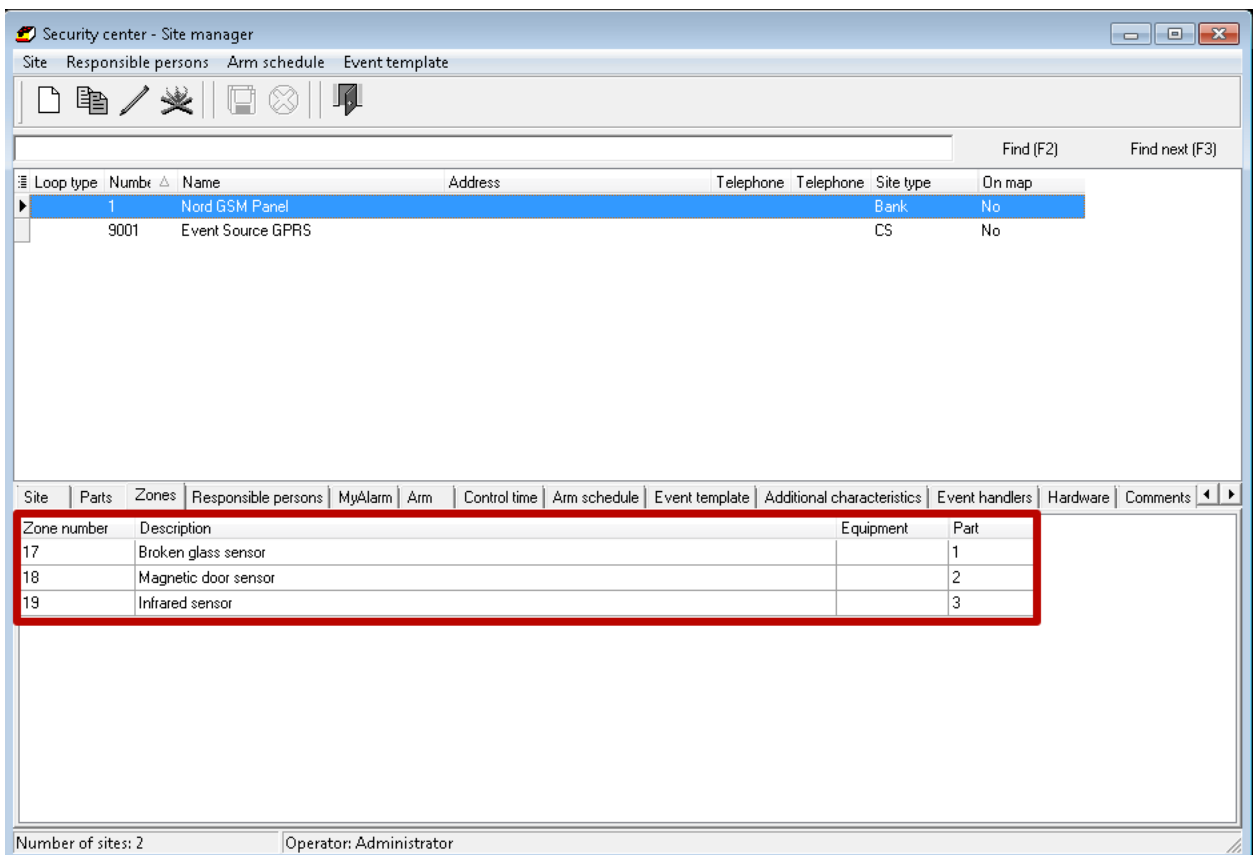
15. Especifique las **zonas** de los sensores que ha conectado al panel. Una vez más puede comprobar las zonas de los sensores en el Hubble. Por defecto, el rango de numeración de zona para todos los sensores *cableados* es **1-16**. El rango de numeración de la zona para todos los sensores *inalámbricos* es **17-48**. Agregue la descripción a cada sensor para hacer notificaciones de MyAlarm más informativos.



16. **Asigne** las particiones correspondientes de la lista a las zonas que ha creado.



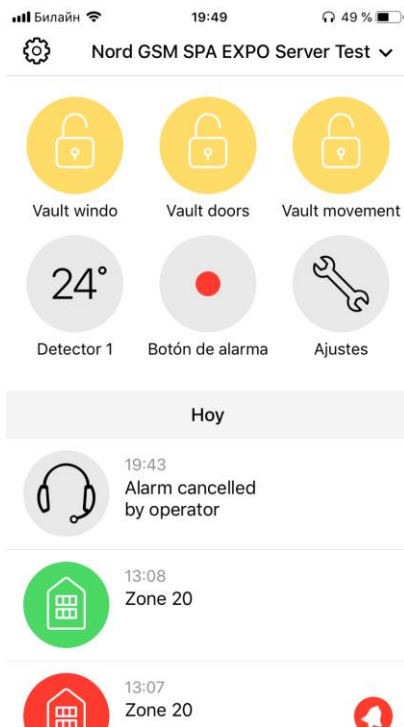
17. La configuración de la particiones para MyAlarm en el Centro de seguridad ahora está terminada.



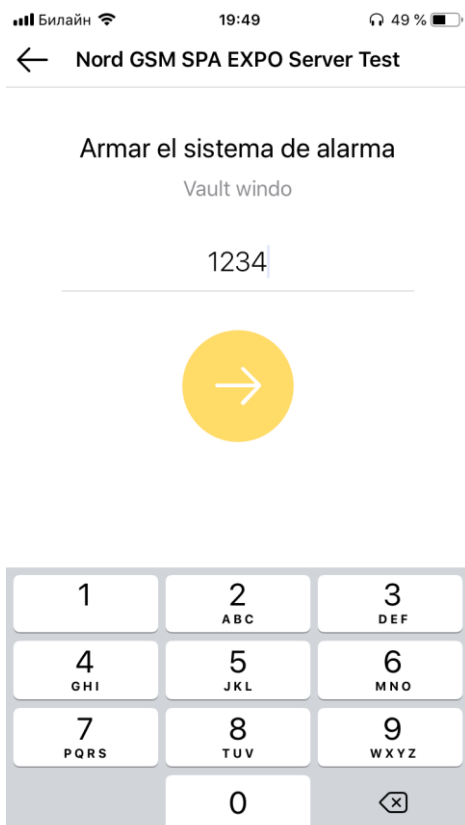
18. Abra la aplicación **MyAlarm** en su teléfono. Una vez que las particiones están configuradas en el módulo del Security Center, puede ver su estado y puede armarlas y desarmarlas desde su teléfono.

Todas las particiones desarmadas tienen iconos amarillos con un candado abierto. Todas las particiones armadas están marcadas en verde.

Si una partición tiene un icono blanco, tócala e ingresa la contraseña para activarla primero.



19. **Arme** la primera partición tocando su icono. La aplicación solicitará una contraseña para proceder. Compruebe el *Hubble* para ver qué usuario agregado a la partición e **ingrese** la contraseña correspondiente.



20. El icono verde confirma que la partición ahora está *armada*. La notificación correspondiente se incluye en el registro de eventos. Utilice el mismo procedimiento para **desarmar** la partición.



La configuración básica de MyAlarm ahora está finalizada.