CYGNUS electronics

GUIA DE INSTALACION DEL SOFTWARE DE MONITOREO

C.Nord

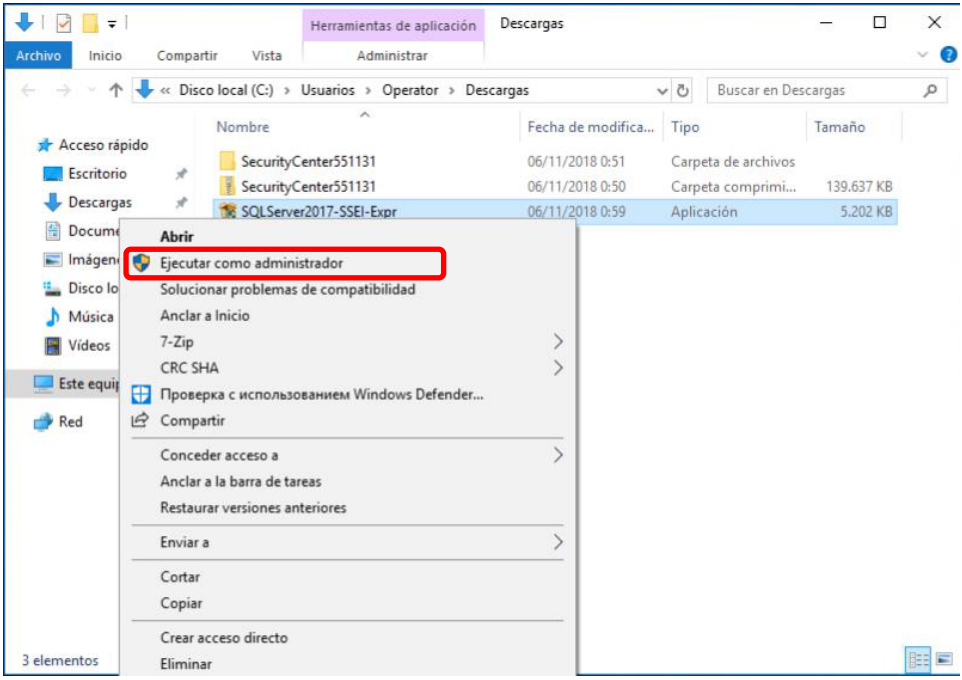
2. Instalación y configuracion del software Security Center

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.*

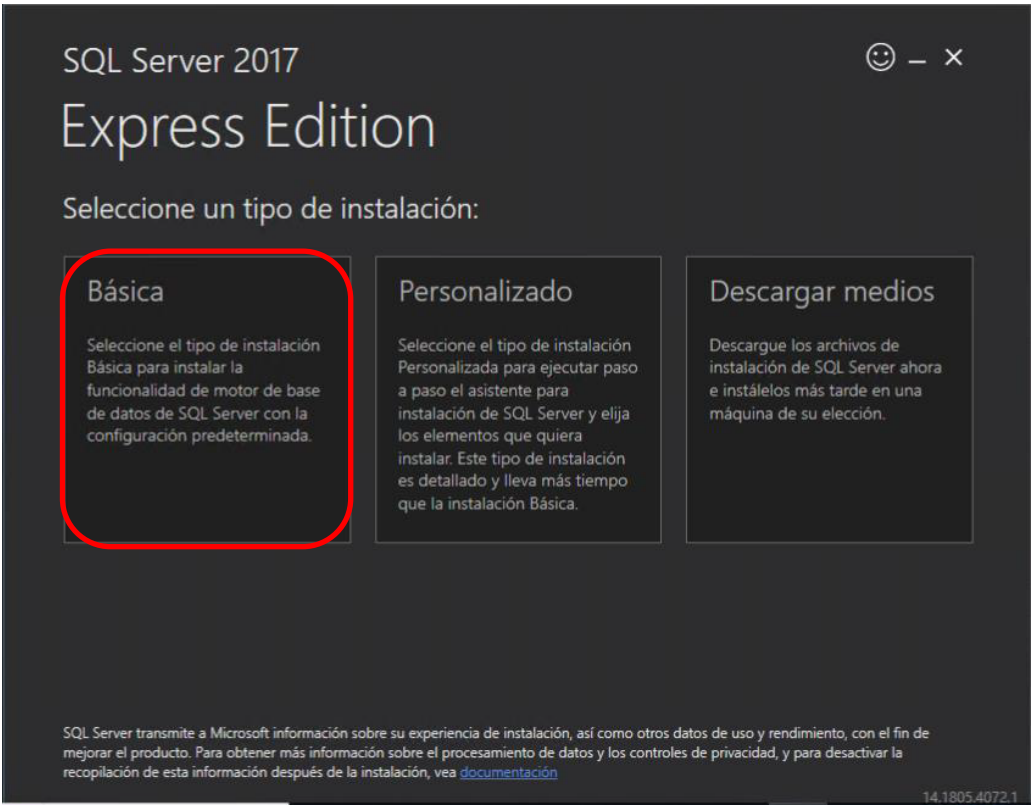
2.1 Instalación del Microsoft SQL Server 2017 Express

1. Descargar desde el sitio web oficial el programa Microsoft SQL Server 2017 Express

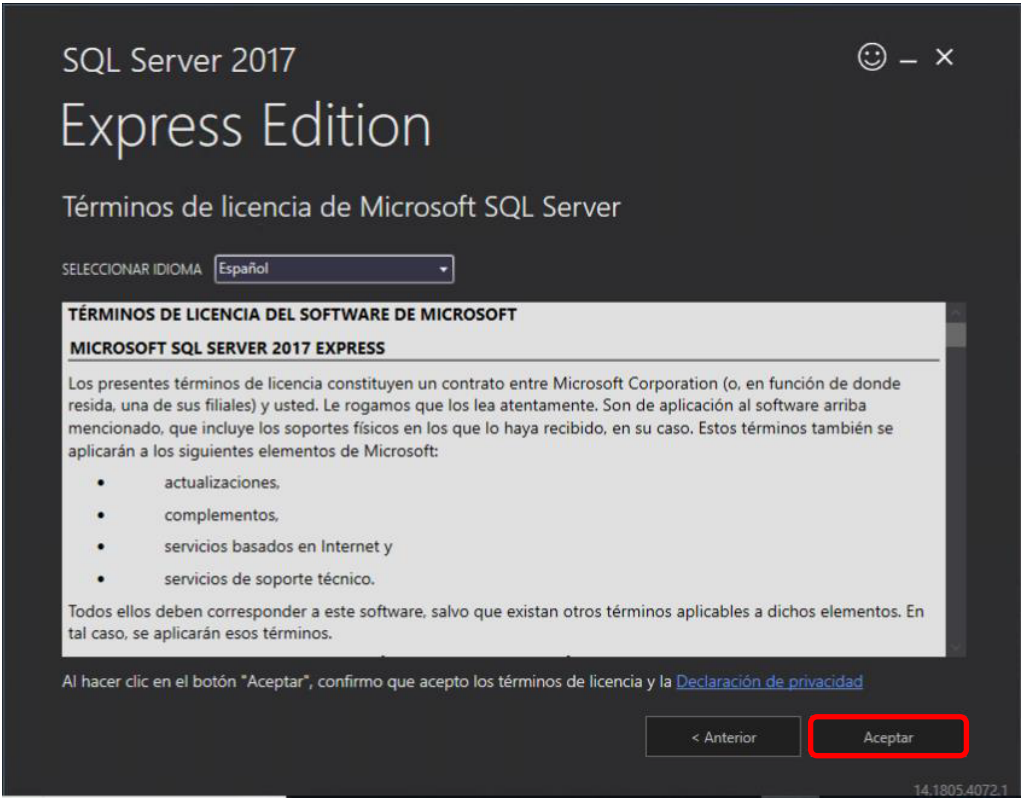
2. Ejecutar el archivo **SQLServer2017-SSEI-Expr** como Administrador



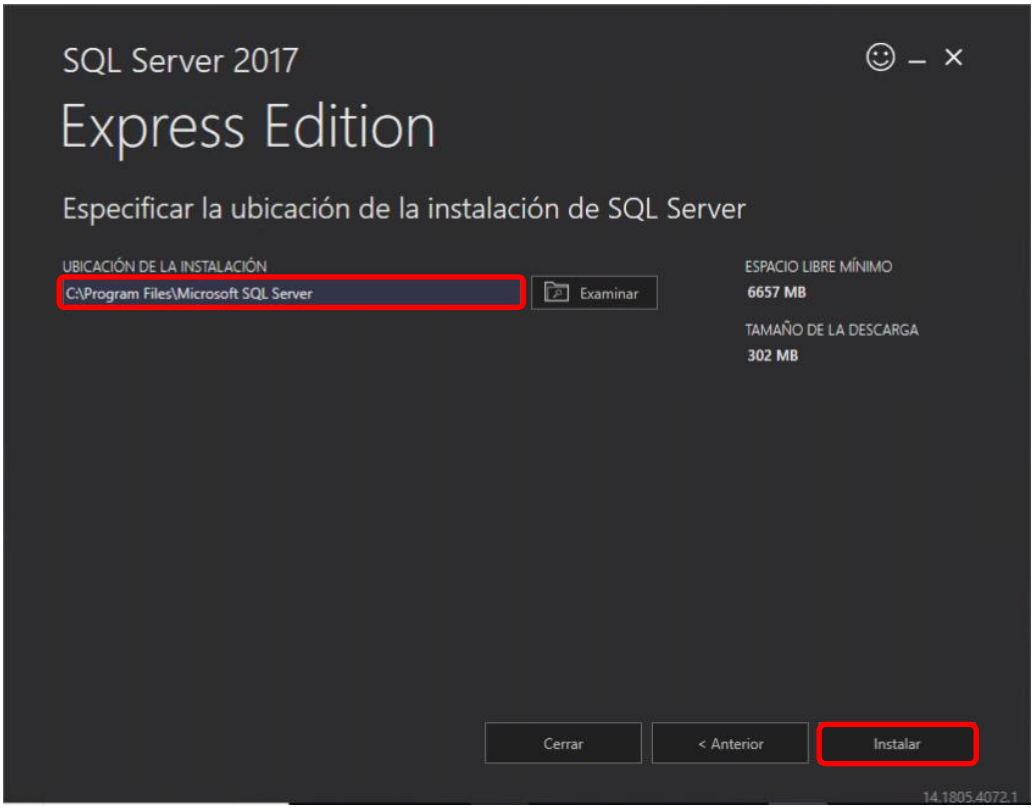
3. Seleccionar el tipo de la instalación **Básica**



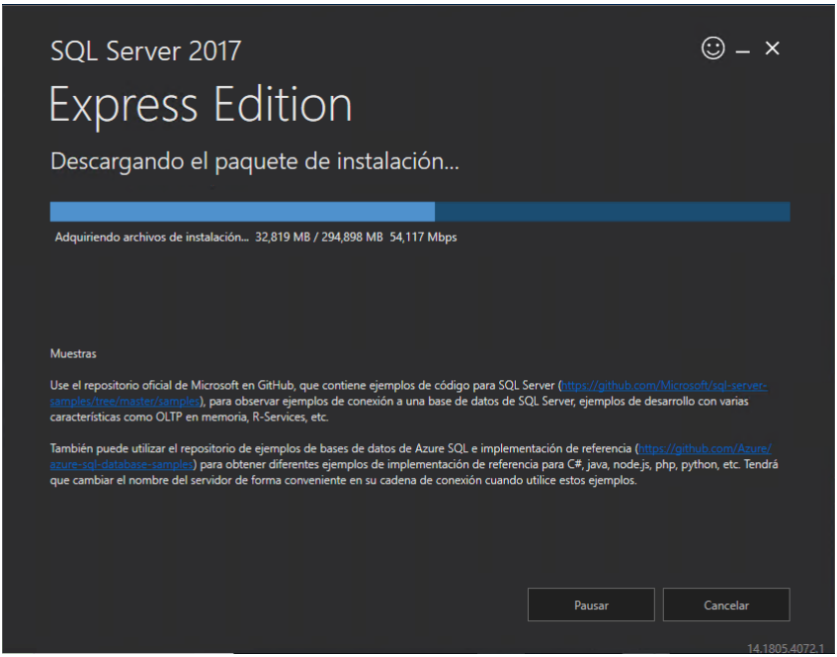
4. Seleccionar el idioma del **SQL Server 2017** y presionar **Aceptar**

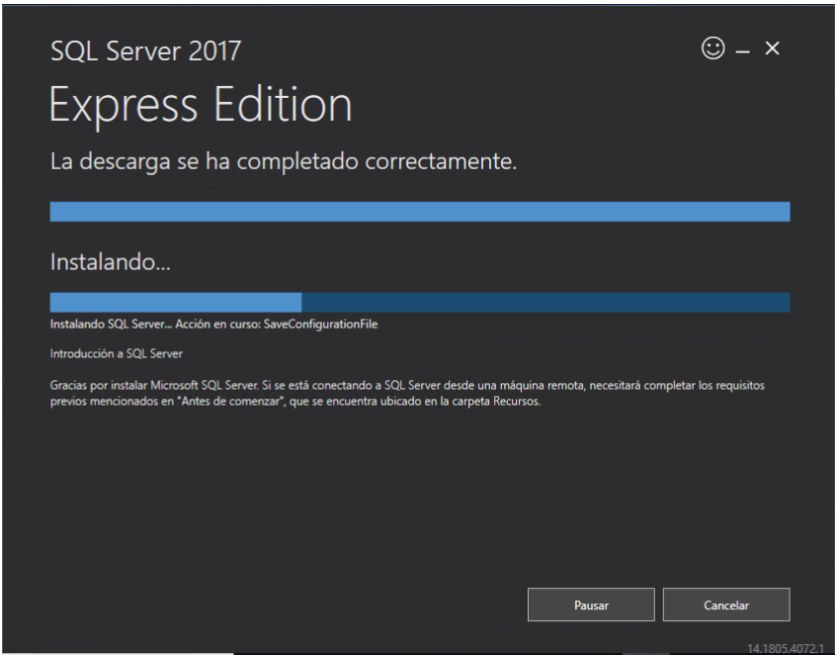


5. Seleccionar la carpeta para la instalación y presionar **Instalar**

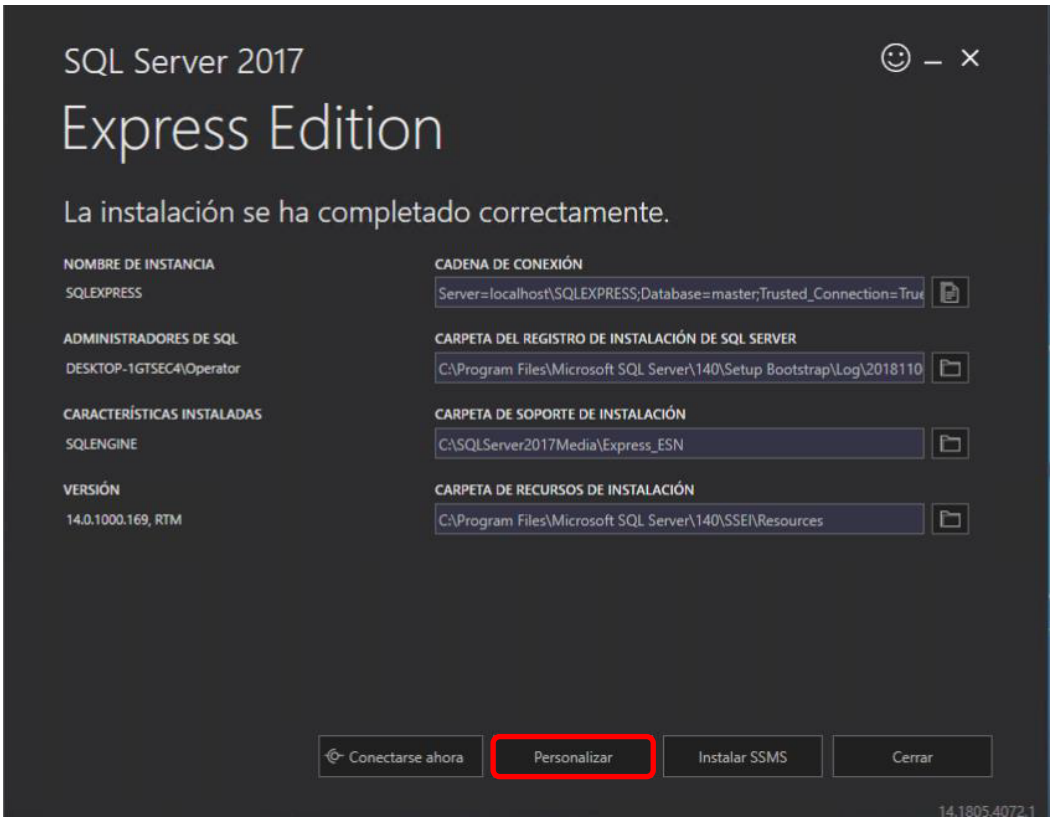


6. Esperar hasta el final de la descarga e instalación

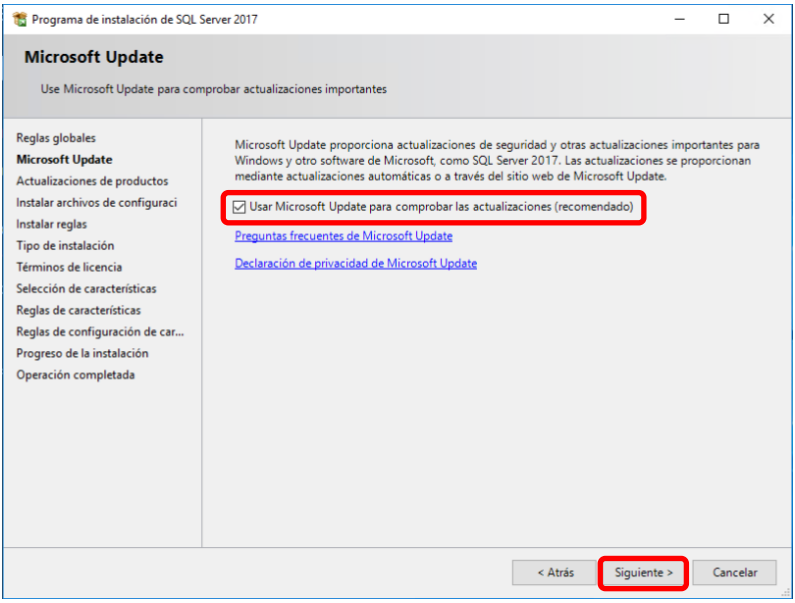

SQL Server 2017
Express Edition
Descargando el paquete de instalación...
Adquiriendo archivos de instalación... 32,819 MB / 294,898 MB 54,117 Mbps
Muestras
Use el repositorio oficial de Microsoft en GitHub, que contiene ejemplos de código para SQL Server (https://github.com/Microsoft/sql-server-samples/tree/master/samples), 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

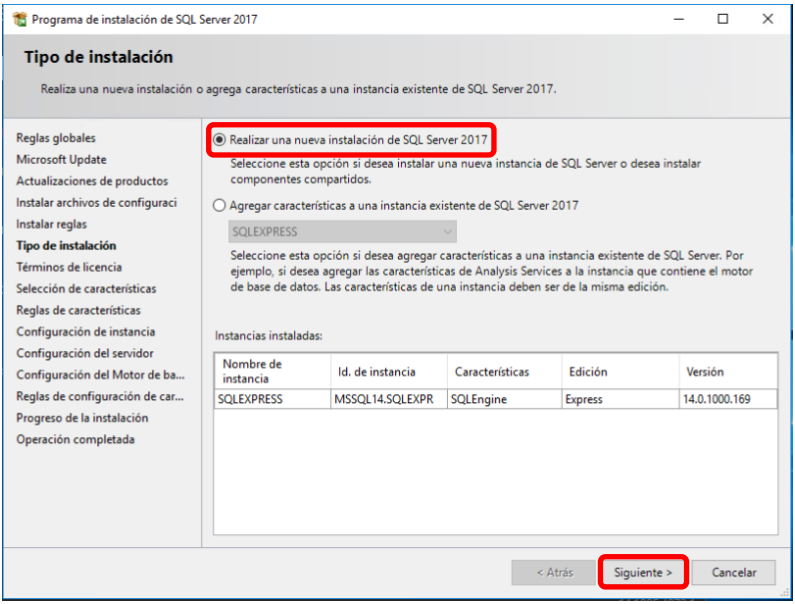
7. Al completar el proceso de la instalación presionar el botón **Personalizar**. Se abrirá la nueva ventana.



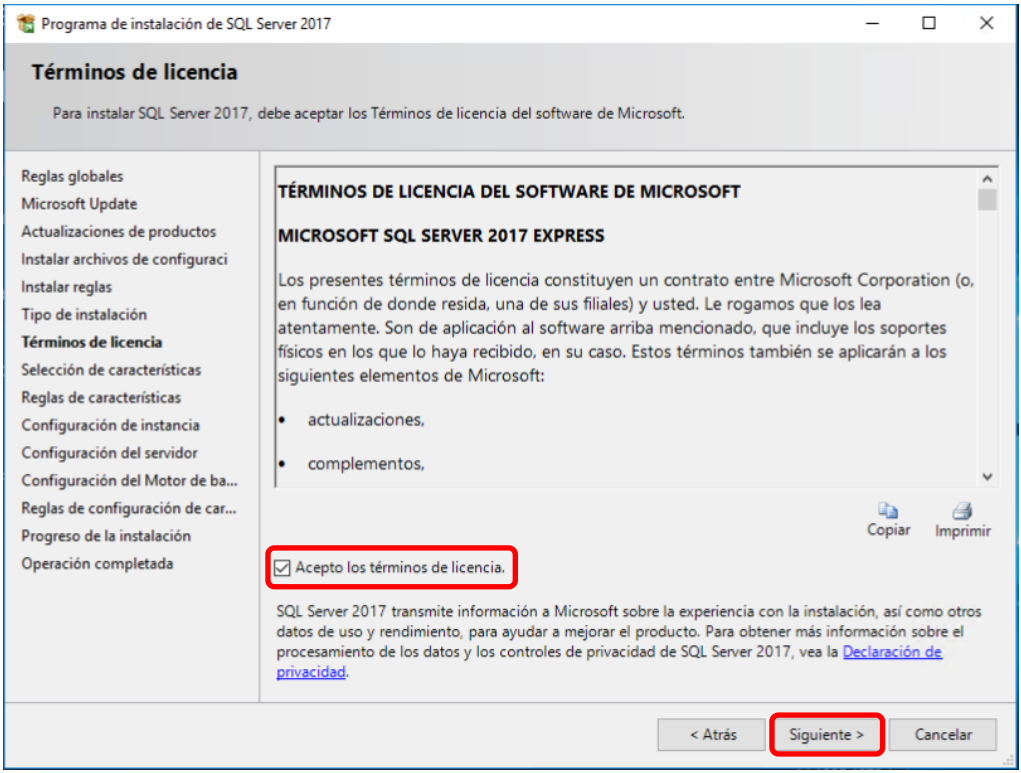
8. Seleccionar la opción **Usar Microsoft Update...** y presionar el botón **Siguiente**



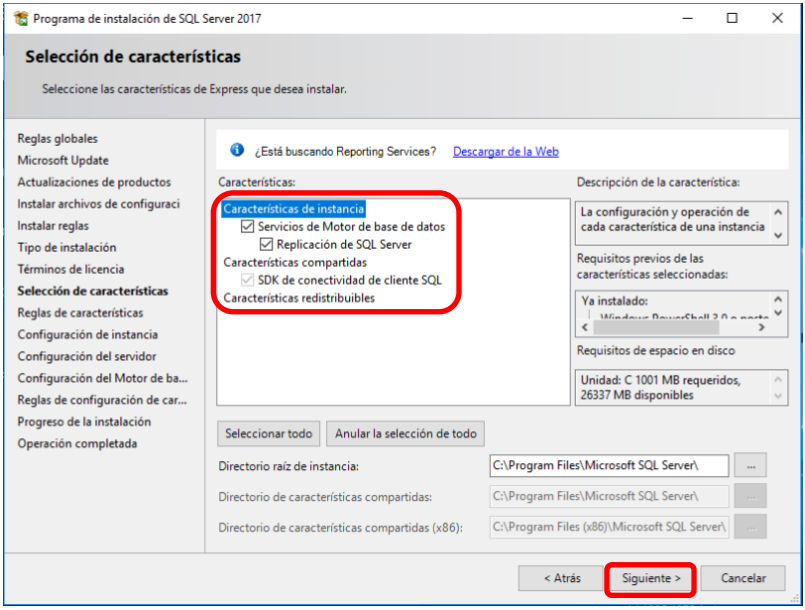
9. Seleccionar la opción **Realizar una nueva instalación del SQL Server 2017** y presionar **Siguiente**



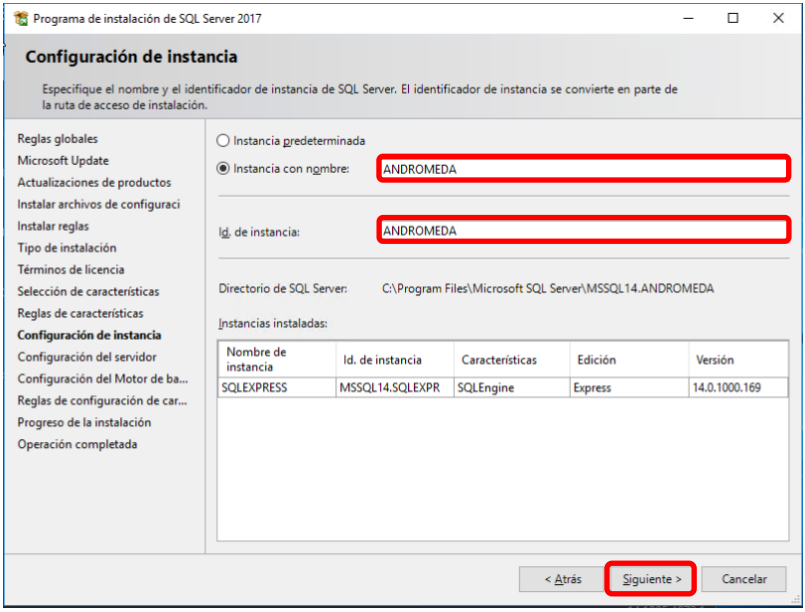
10. Aceptar los términos de la licencia y presionar **Siguiente**



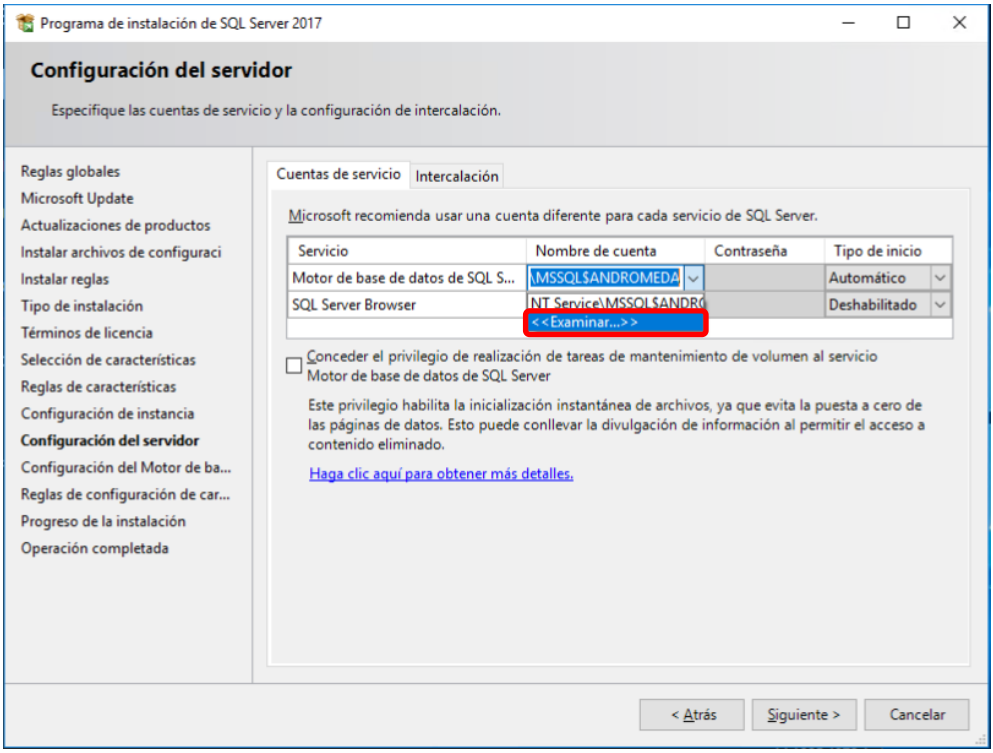
11. Verificar que todas las tres casillas esten marcadas y presionar **Siguiente**



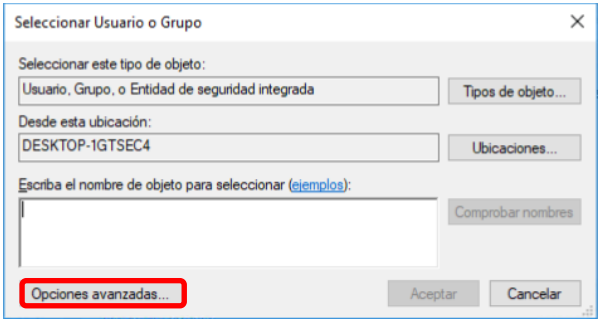
12. Especificar el nombre y el identificador de instancia de SQL Server: **ANDROMEDA**. Presionar el botón **Siguiente**



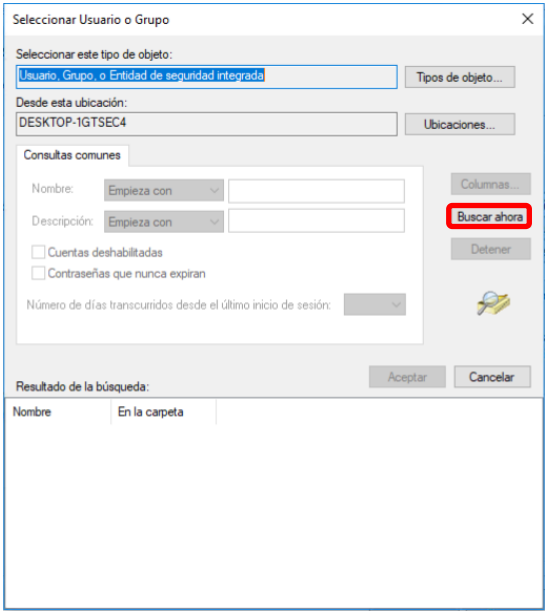
13. Para el servicio **Motor de base de datos de SQL Server** ingresar en los parametros de redacción del nombre de la cuenta. Para eso en el menú deslizante seleccionar **Examinar**



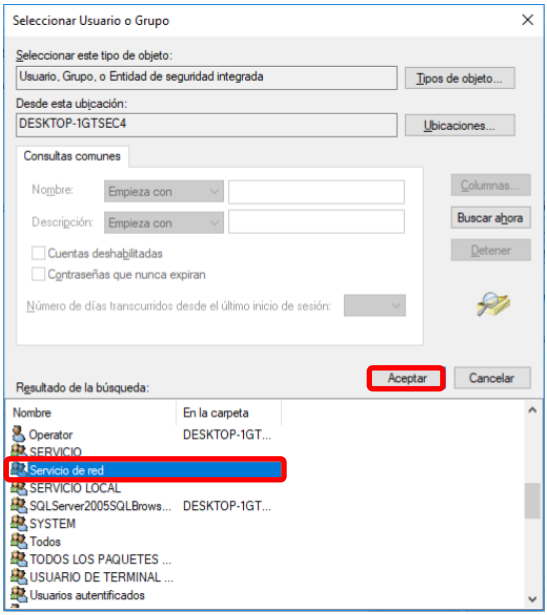
14. En la ventana emergente presionar el botón **Opciones avanzadas...**



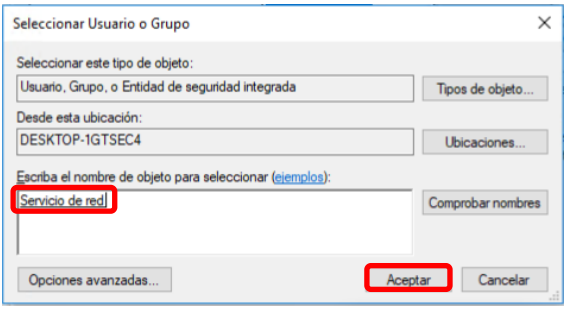
15. En la siguiente ventana presionar el botón **Buscar ahora**



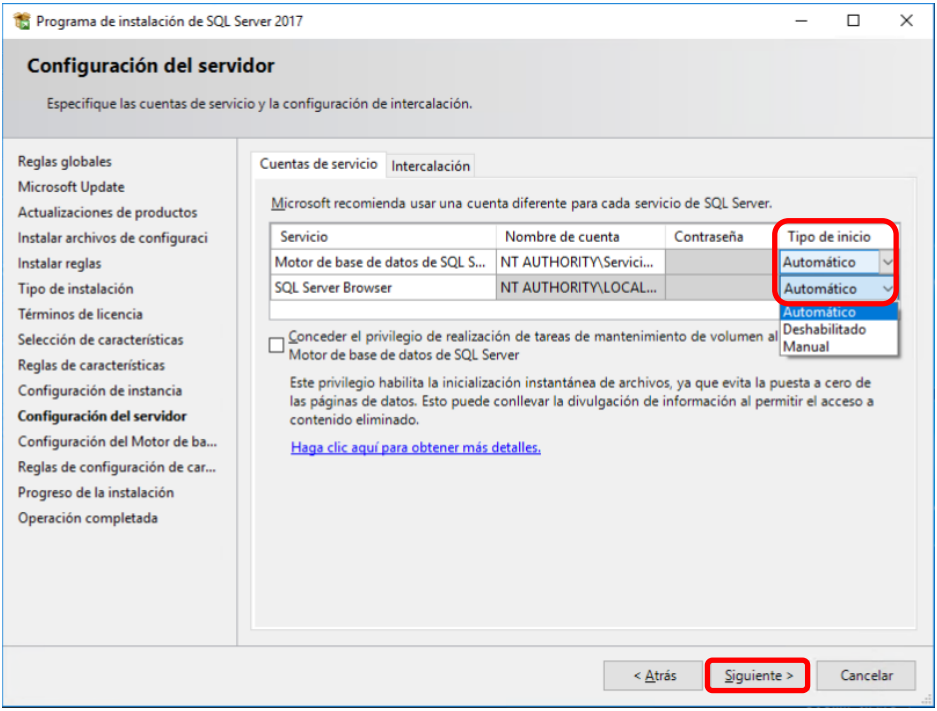
16. En la ventana emergente seleccionar la opción **Servicio de red** y presionar **Aceptar**



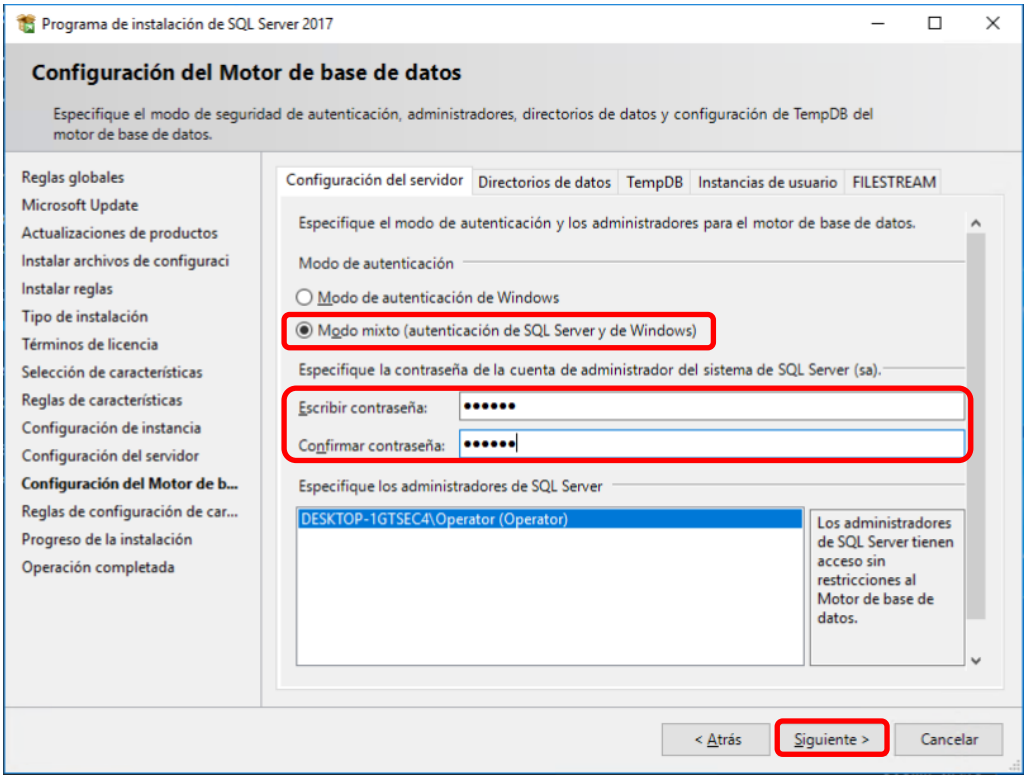
17. Comprobar que en el campo inferior apareció el objeto con el nombre **Servicio de red**. Presionar **Aceptar**.



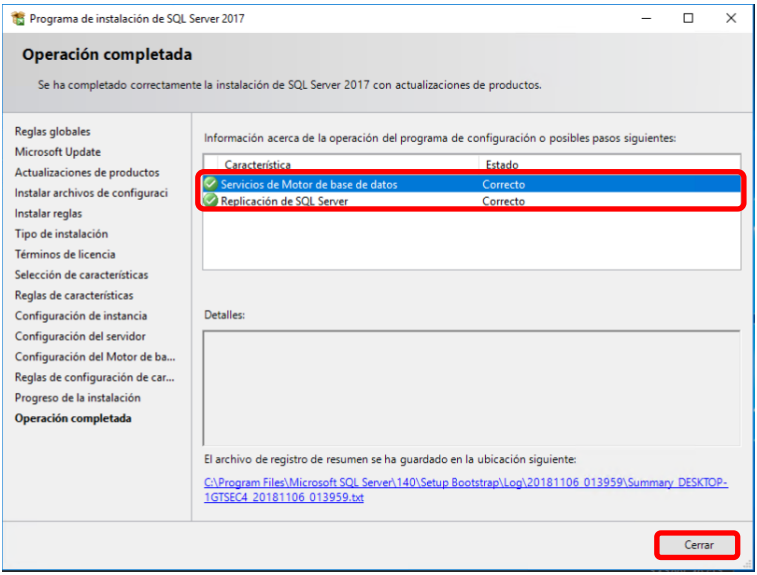
18. Para los servicios **Motor de base de datos SQL Server** y **SQL Server Browser** seleccionar el tipo de inicio **Automático**. Presionar el botón **Siguiente.**



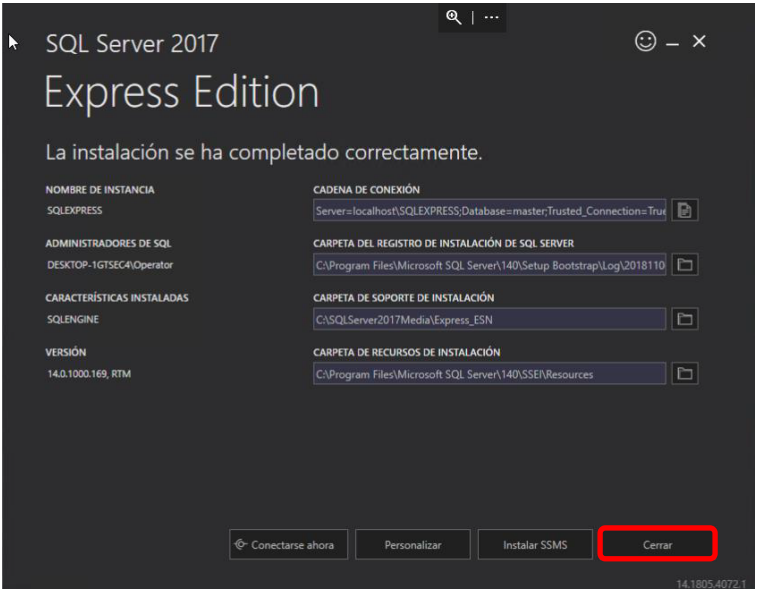
19. Especificar **Modo mixto** para la autenticación e ingresar dos veces la contraseña (puede ser cualquiera).



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



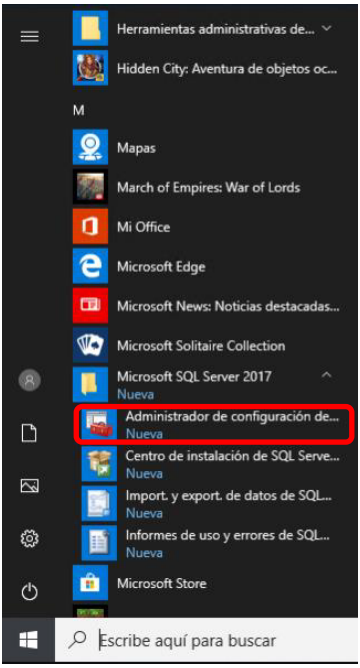
21. Presionar **Cerrar** segunda vez



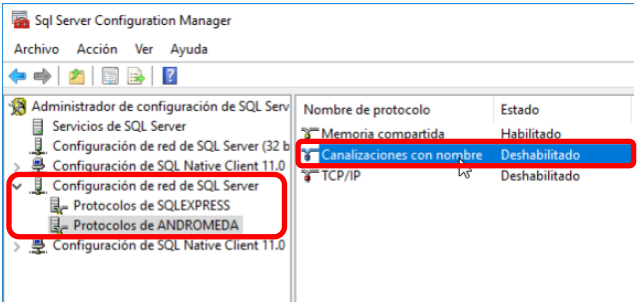
2.2 Configuración del Microsoft SQL Server 2017 Express

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

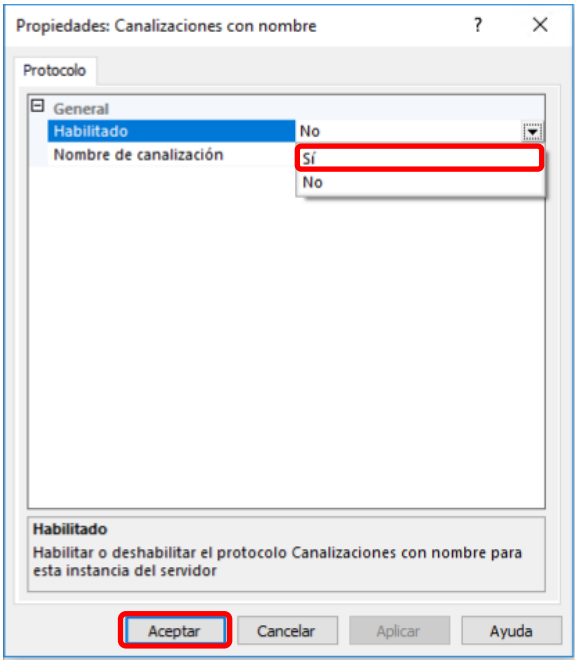
1. Ejecutar **Administrador de configuración de SQL Server 2017**



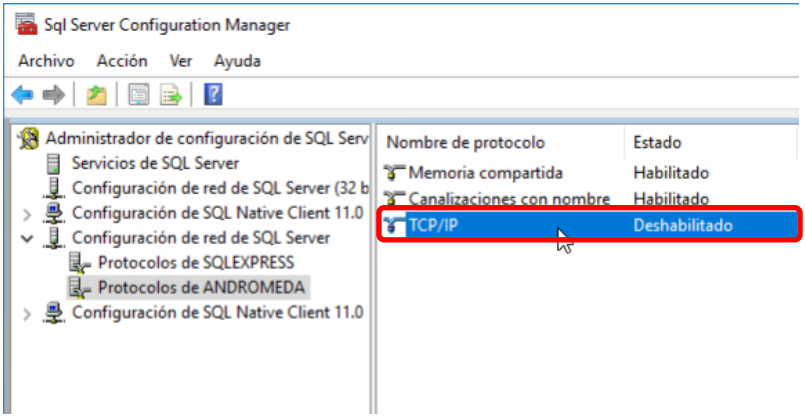
2. En la ventana emergente seleccionar **Configuración de red de SQL Server** -> **Protocolos de ANDROMEDA.** Hacer el doble click en el protocolo **Canalizaciones con nombre** en la parte derecha.



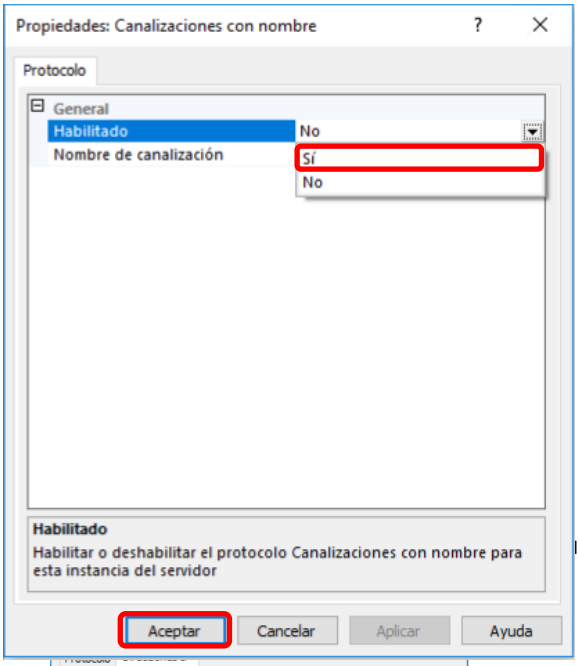
3. En la ventana siguiente seleccionar **Sí** frente a la opción **Habilitado**. Presionar **Aceptar**.



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

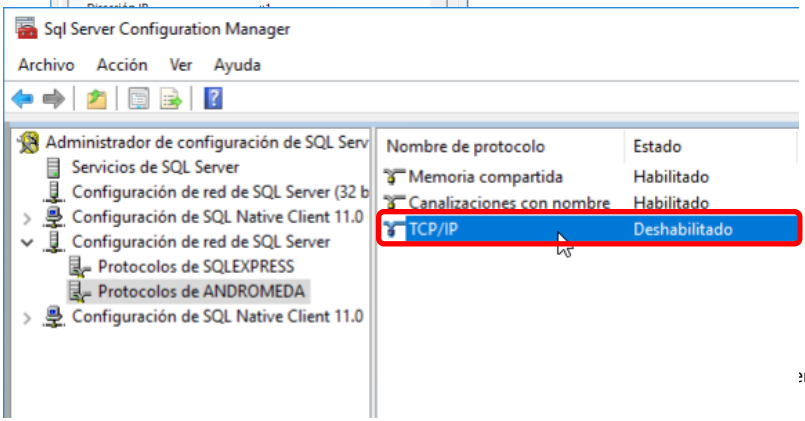


5. En la ventana siguiente seleccionar **Sí** frente a la opción **Habilitado**.



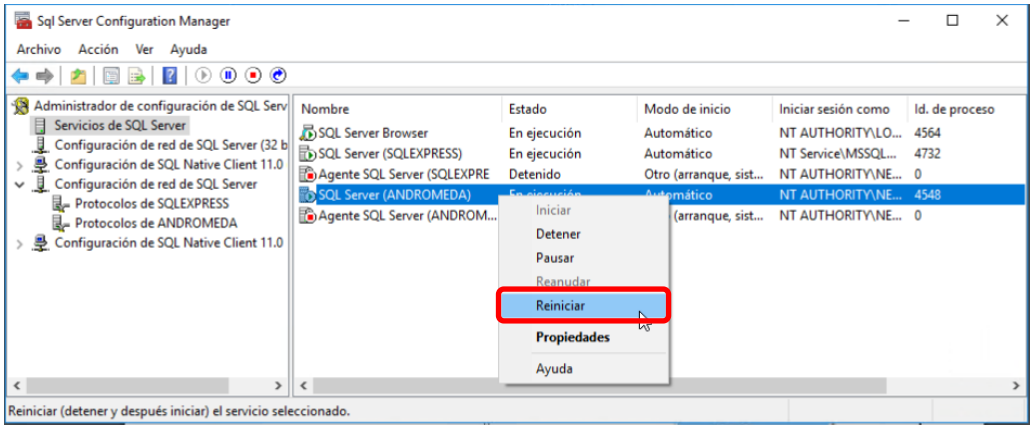
l valor frente a **Puertos dinámicos TCP**.

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



erecho del

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

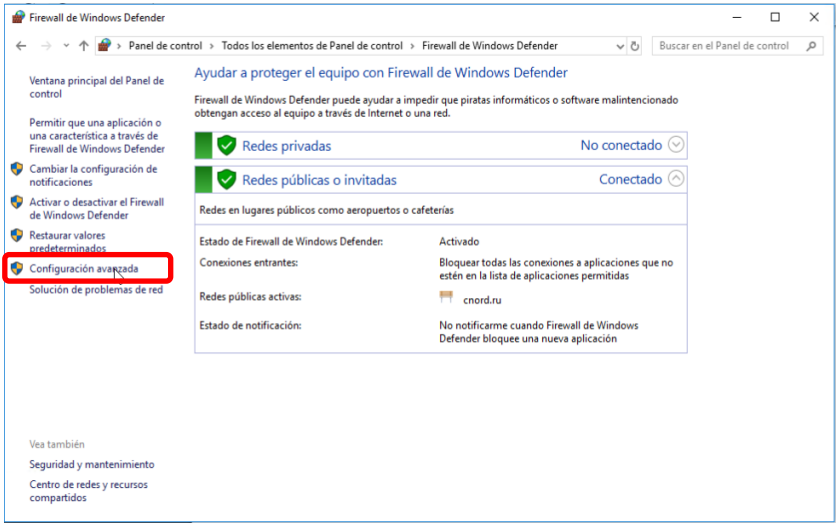


La configuración del **SQL Server** está completada.

2.3 Configuración del Firewall de Windows Defender

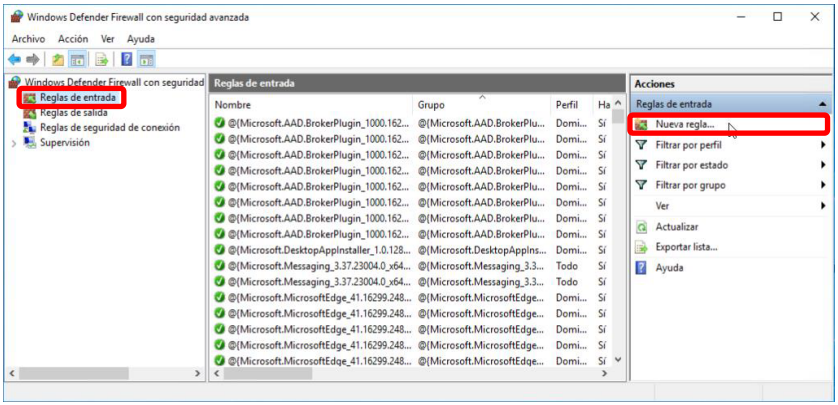
Para configurar **Firewall de Windows Defender** realice las siguientes acciones

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

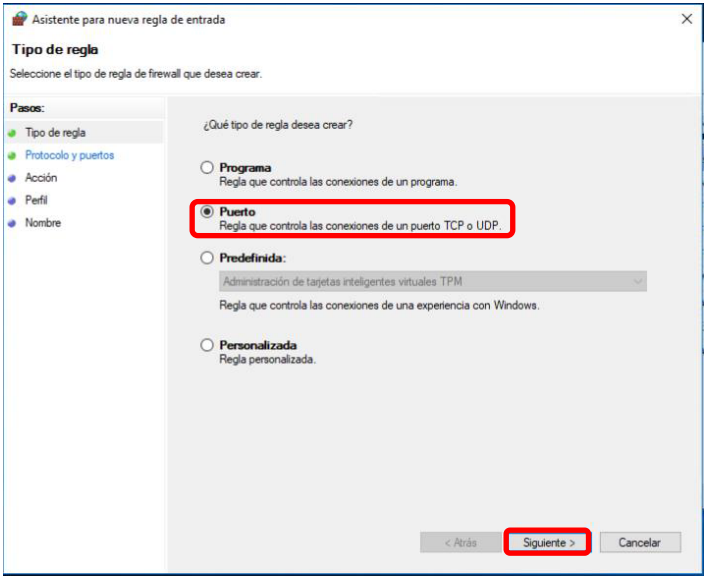


2. Agregar la regla para el puerto TCP/IP

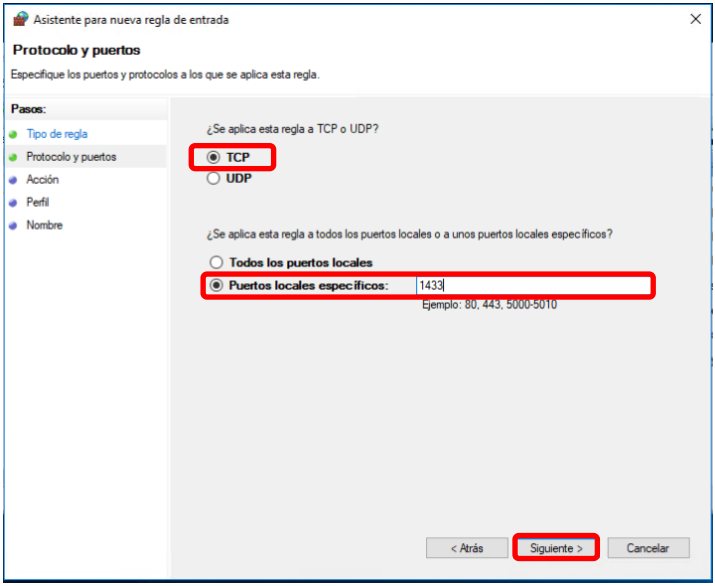
En la nueva ventana seguir a la sección **Reglas de entrada** y en la parte derecha hacer click en **Nueva regla**.



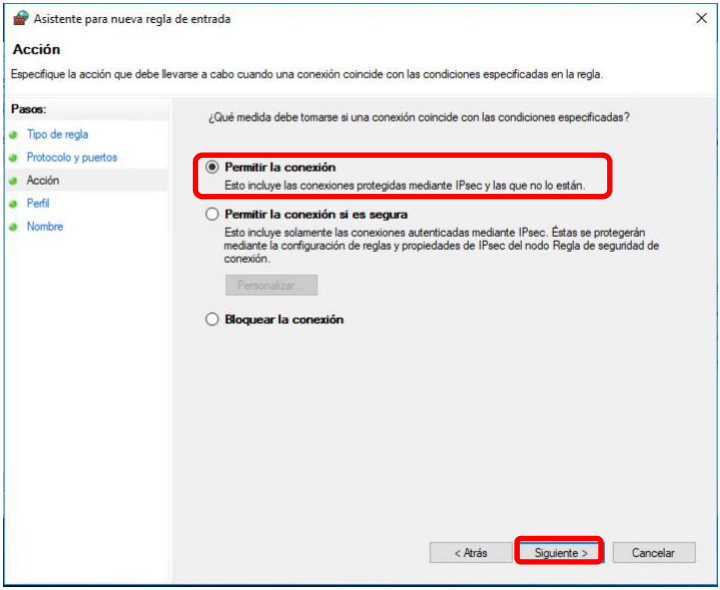
3. En la ventana emergente seleccionar **Puerto** y presionar **Siguiente**



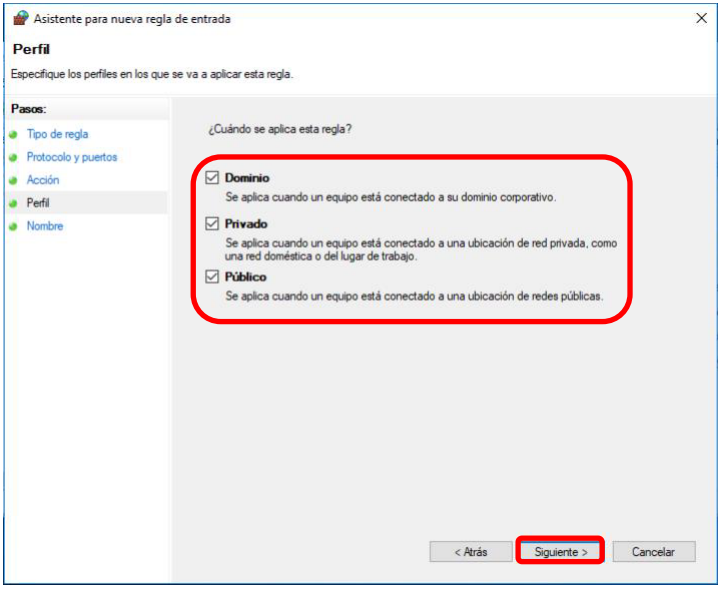
4. Marcar la casilla frente a **TCP** y en el campo **Puertos locales específicos** ingresar el valor **1433**. Presionar **Siguiente**.



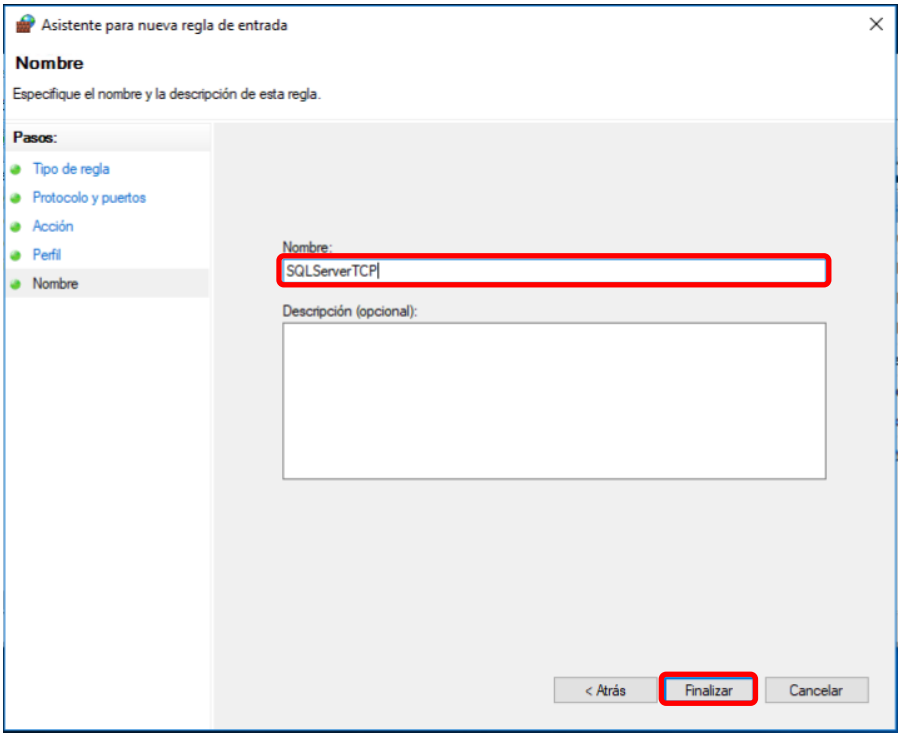
5. Asegurarse de que se haya seleccionado la opción **Permitir la conexión** y presionar **Siguiente**



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

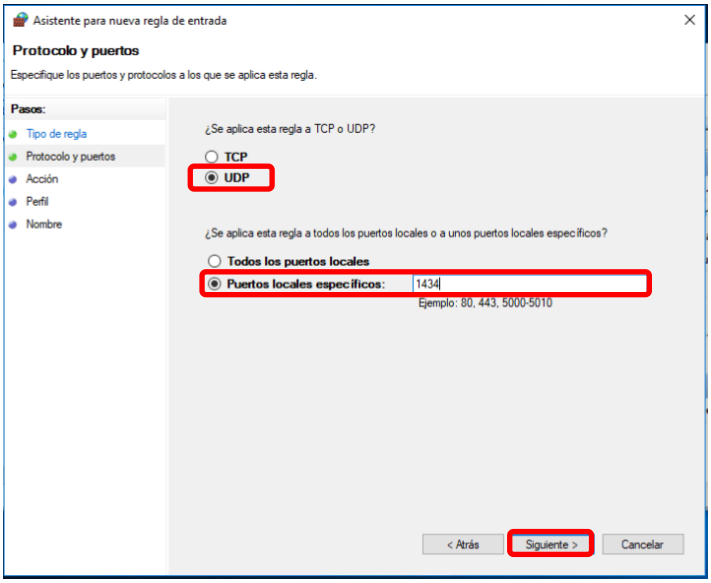


7. Ingresar el nombre para la regla, e.g. **SQLServerTCP** y presionar **Finalizar**

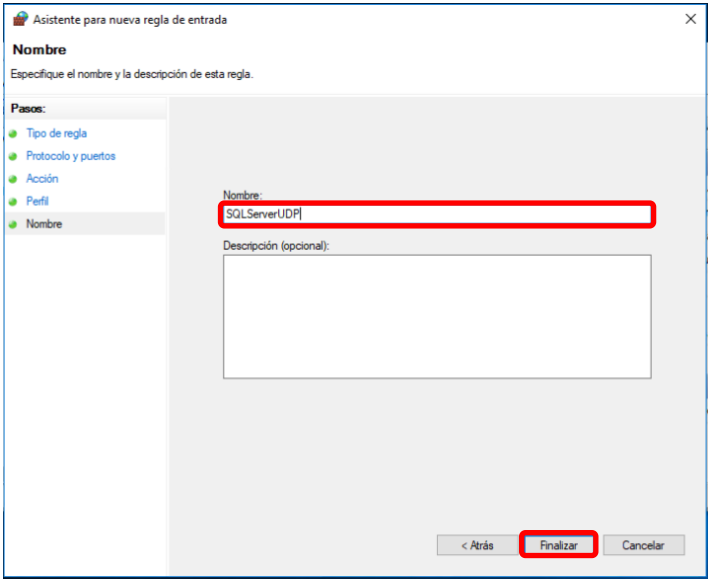


8. Agregar la regla para el puerto **UDP**

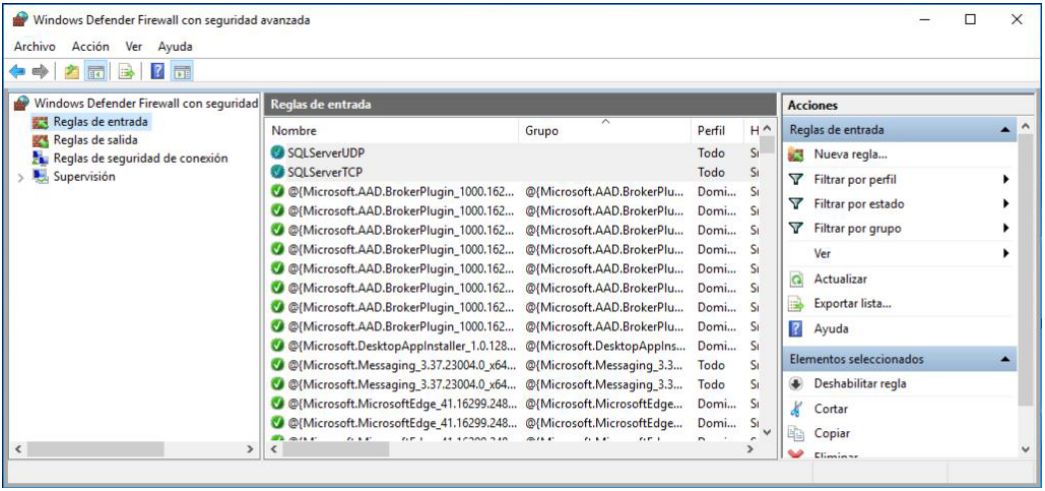
Repetir los pasos 2 y 3. Marcar la casilla frente a **UDP** y en el campo **Puertos locales específicos** ingresar el valor **1434**. Presionar **Siguiente**.



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



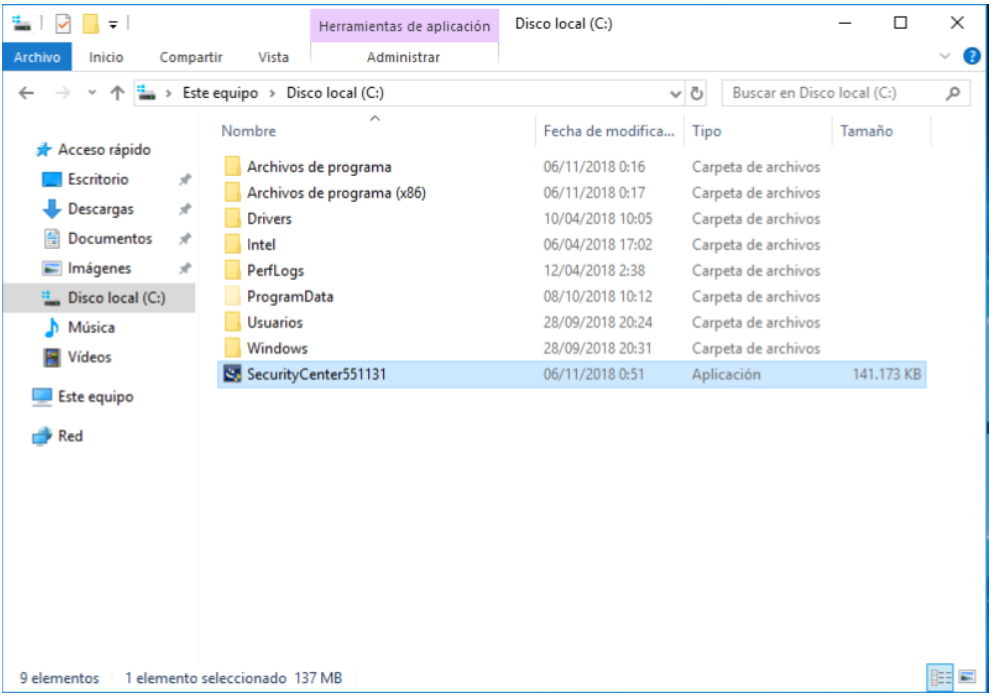
La configuración del **Firewall de Windows Defender** está finalizada.


Windows Defender Firewall con seguridad avanzada
Archivo Acción Ver Ayuda
Windows Defender Firewall con seguridad
Reglas de entrada
Reglas de salida
Reglas de seguridad de conexión
Supervisión
Reglas de entrada
Nombre
Grupo
Perfil
SQLServerUDP
SQLServerTCP
Todo
Acciones
Reglas de entrada
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda
Elementos seleccionados
Deshabilitar regla
Cortar
Copiar

2.4 Instalación del Security Center

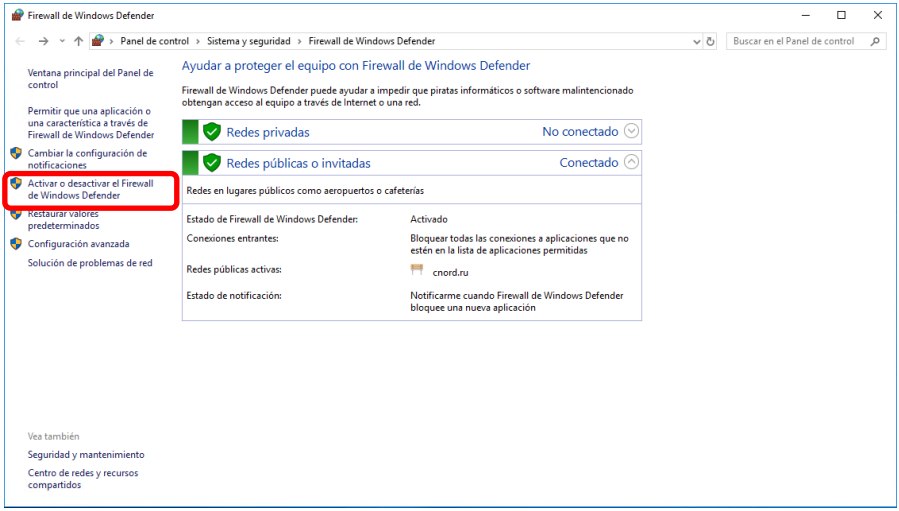
1. Descargar directamente la última versión del programa **Security Center** o desde nuestro sitio web

2. Mover el fichero "**SecurityCenterXXXXXX.exe**" en el directorio raíz del disco **C:**

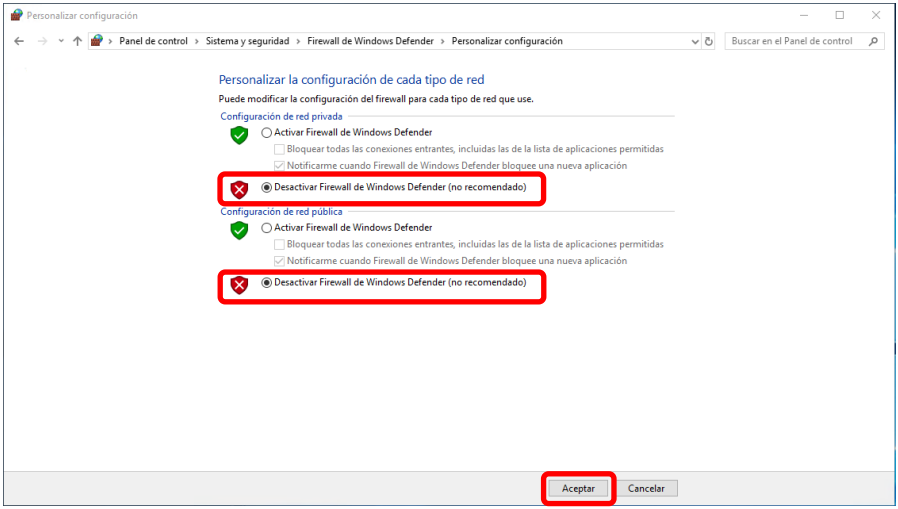


Antes de iniciar la instalación del SC modificar las siguientes configuraciones del SO (en el ejemplo de Win10)

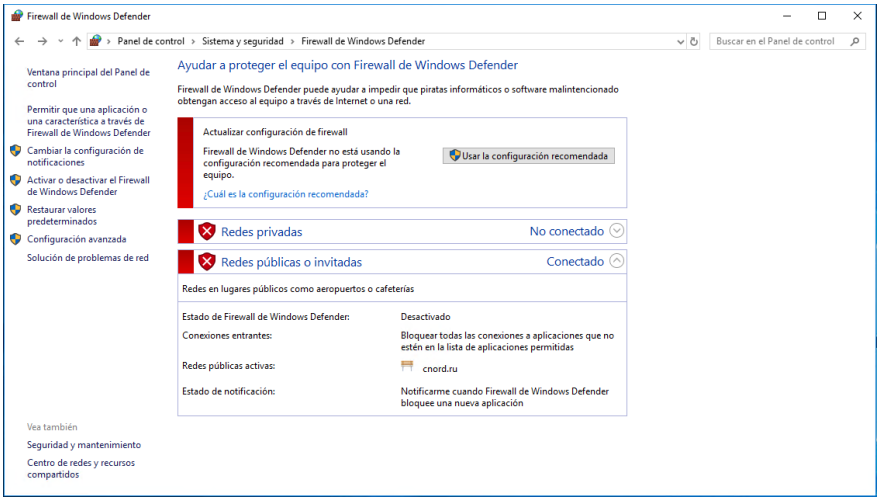
3. Seguir al **Panel de control** -> **Firewall de Window Defender** -> **Activar o desactivar el Firewall de Windows Defender**



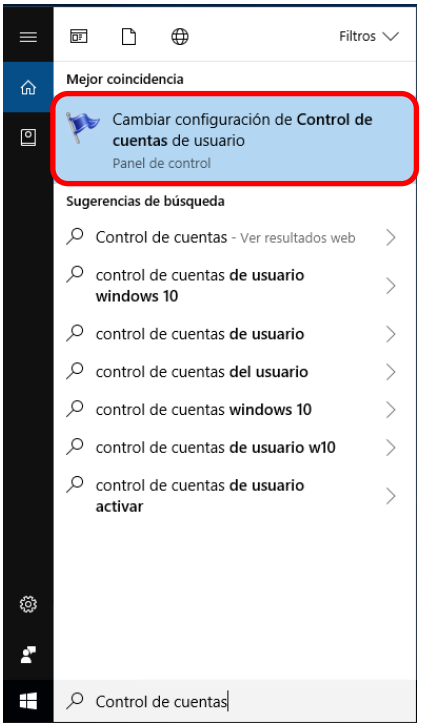
4. Marcar la opción **Desactivar Firewall de Windows Defender** en Configuraciones de red privada y red pública. Presionar **Aceptar**.



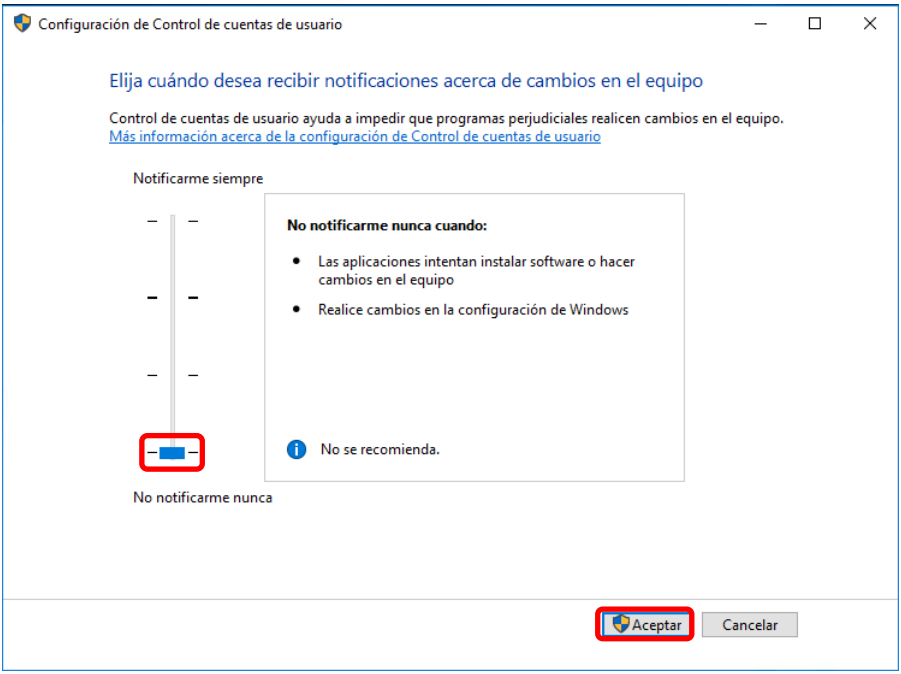
5. La configuración del **Firewall de Windows Defender** está finalizada



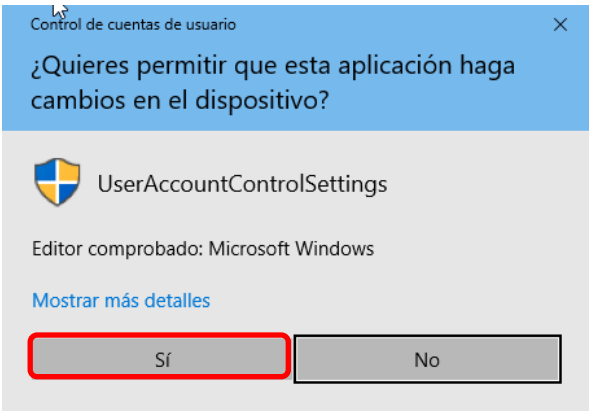
6. En la barra de búsqueda ingresar “Control de cuentas” y en los resultados selecionar la opción **Cambiar configuración de Control de cuentas de usuario**



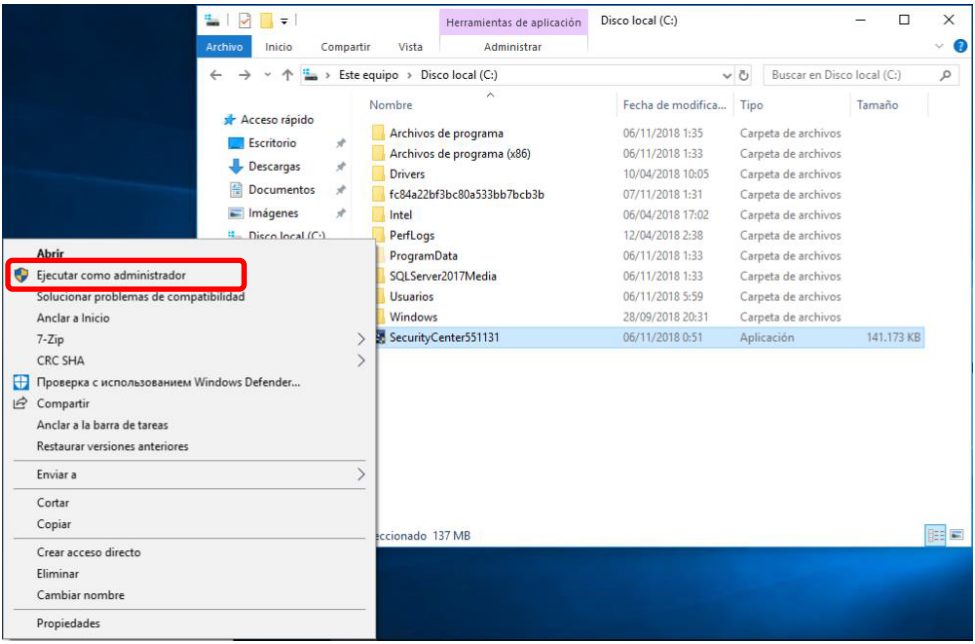
7. Con el control deslizante desactivar el recibo de notificaciones acerca de cambios en el equipo y presionar **Aceptar**



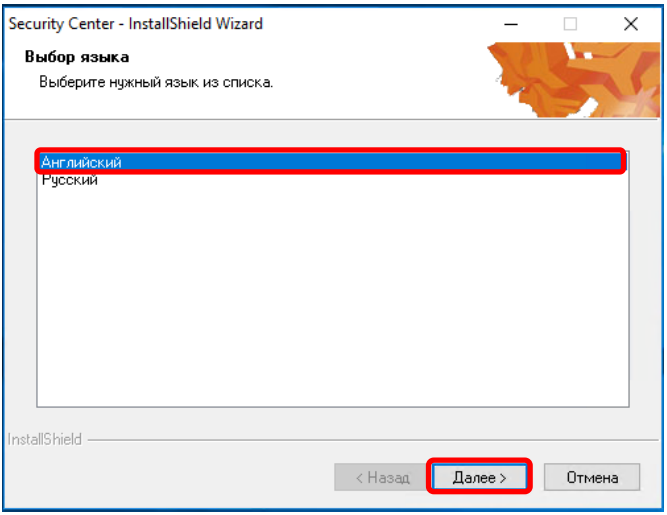
8. Aceptar los cambios en la ventana emergente



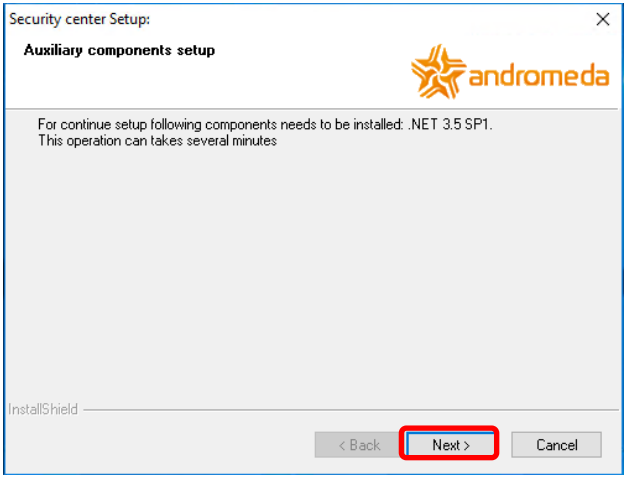
9. Ejecutar el archivo **C:\ SecurityCenterXXXXXX.exe** como administrador



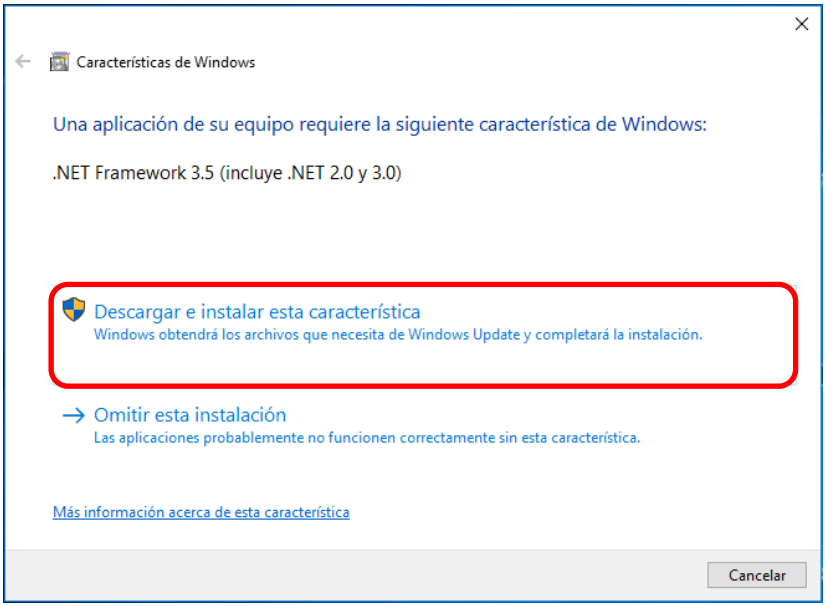
10. En la siguiente ventana seleccionar **inglés** como el idioma del instalador y presionar **Siguiente**



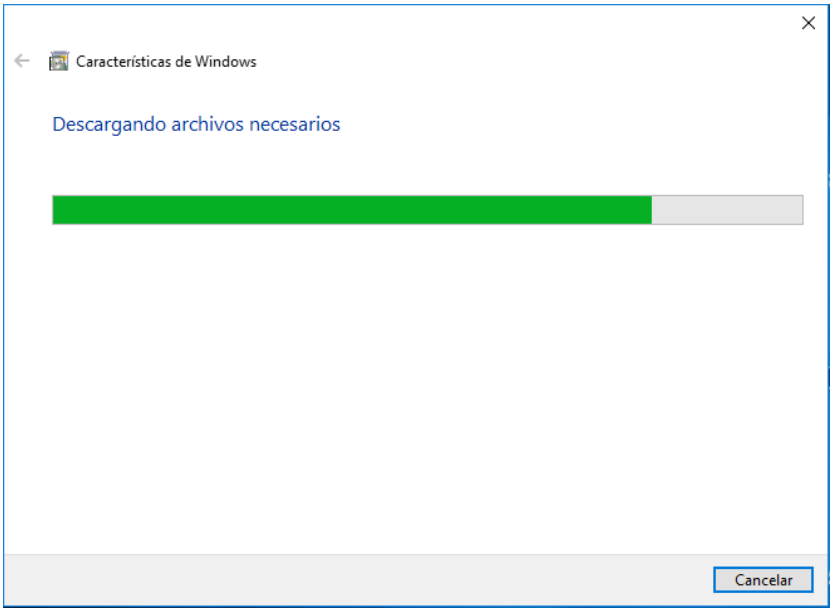
11. Presionar **Next** para instalar **.NET Framework 3.5**

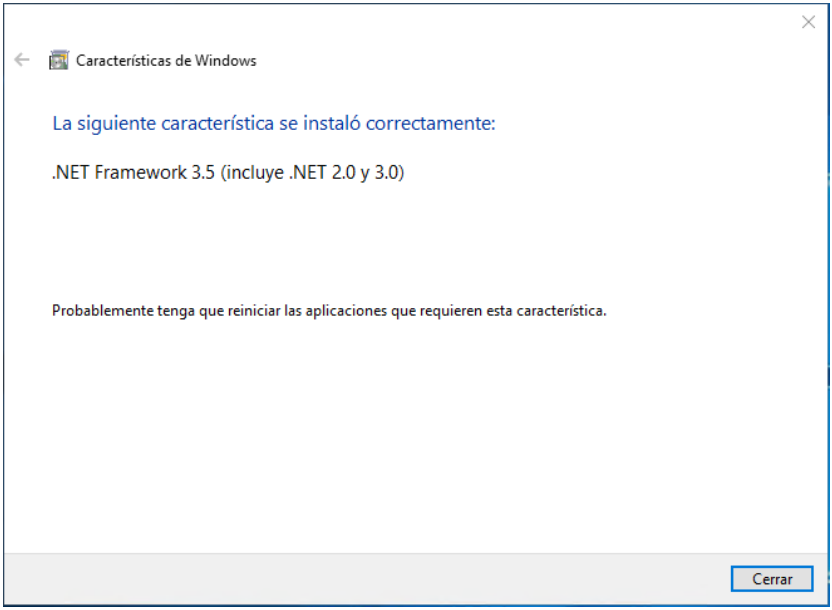


12. Presionar **Descargar e instalar esta característica**

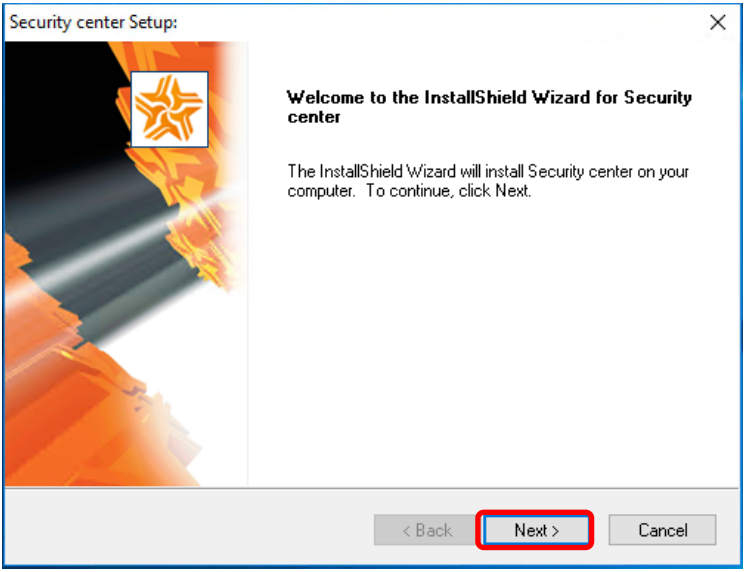


13. Espere mientras se descarguen e instalen los archivos necesarios

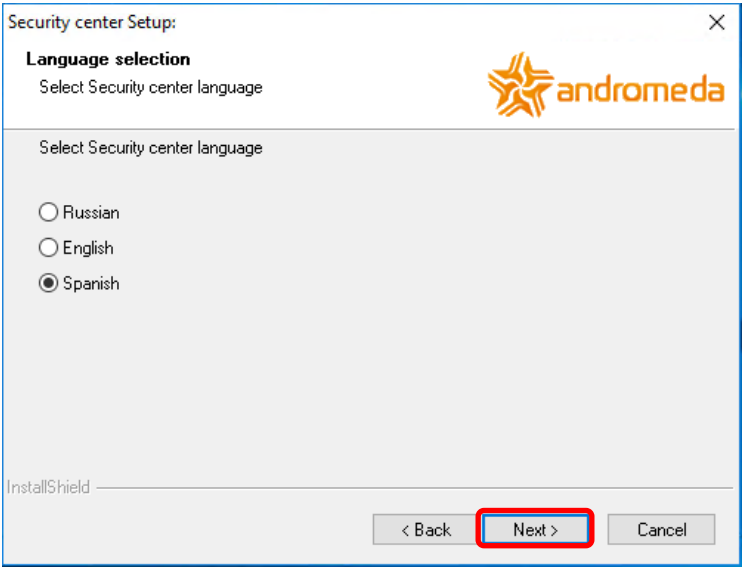




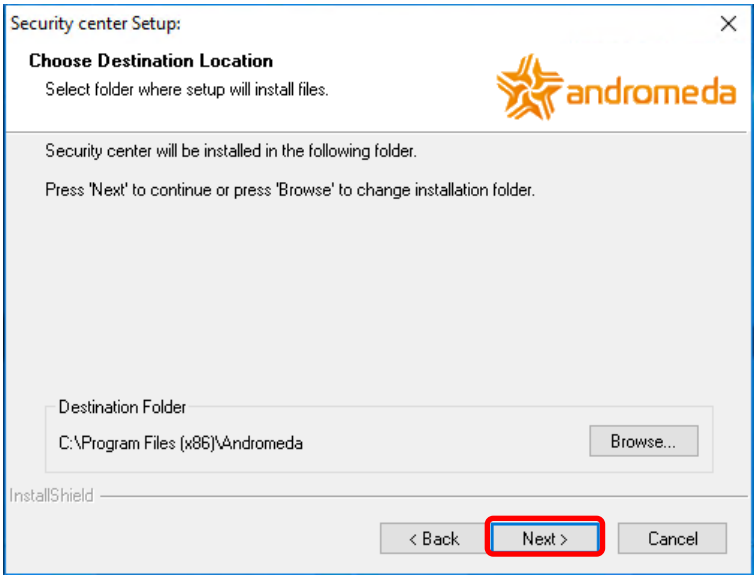
14. En la siguiente ventana presionar **Next**



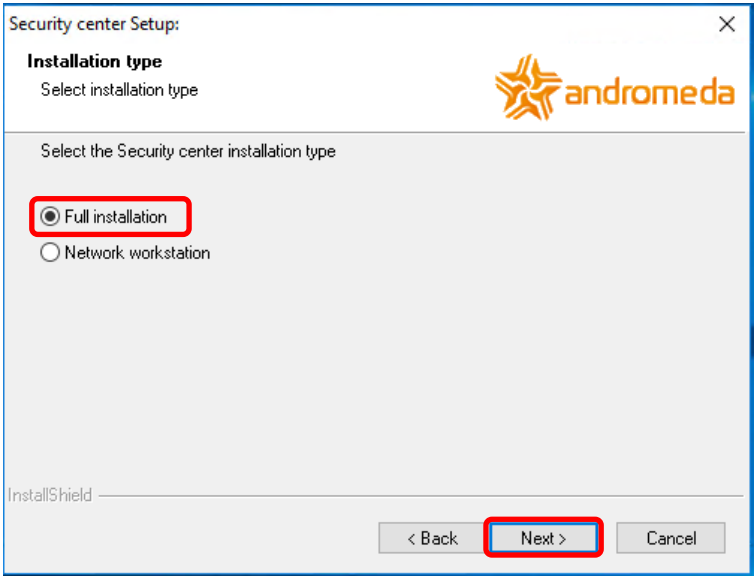
15. Eligir el idioma del Security Center y presionar **Next**



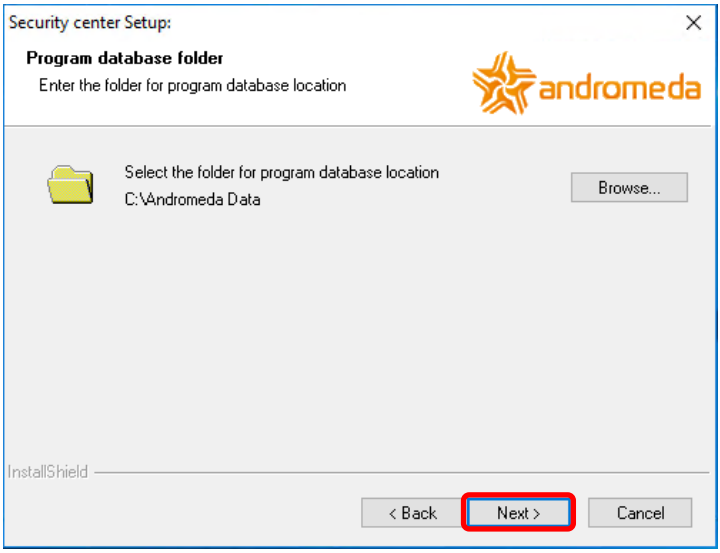
16. Confirmar la carpeta de destino presionando **Next**



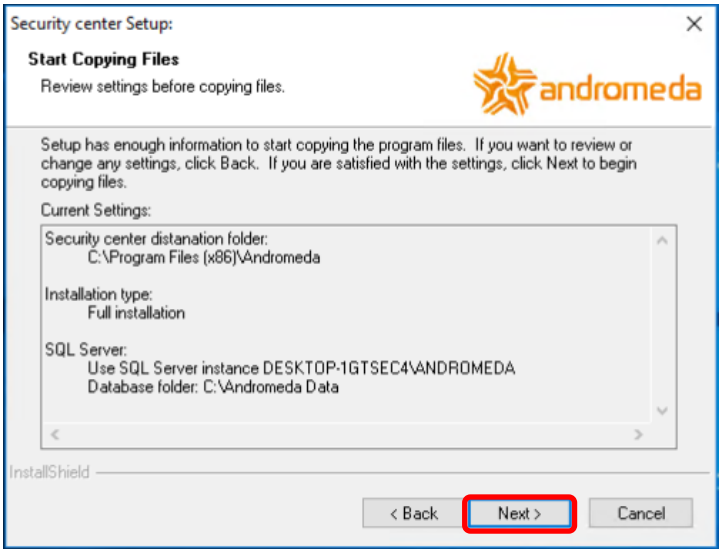
17. Selecionar **Instalación completa** y oprimir **Next**



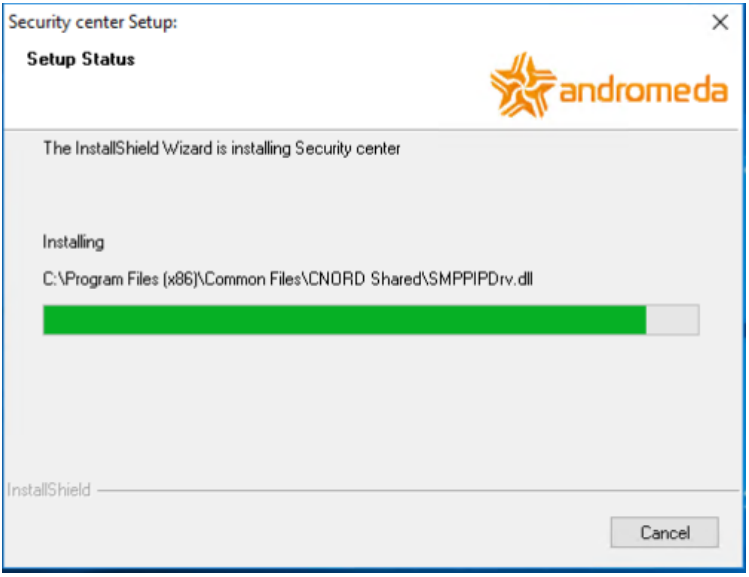
18. Confirmar la carpeta para instalación de la base de datos SQL oprimiendo **Next**



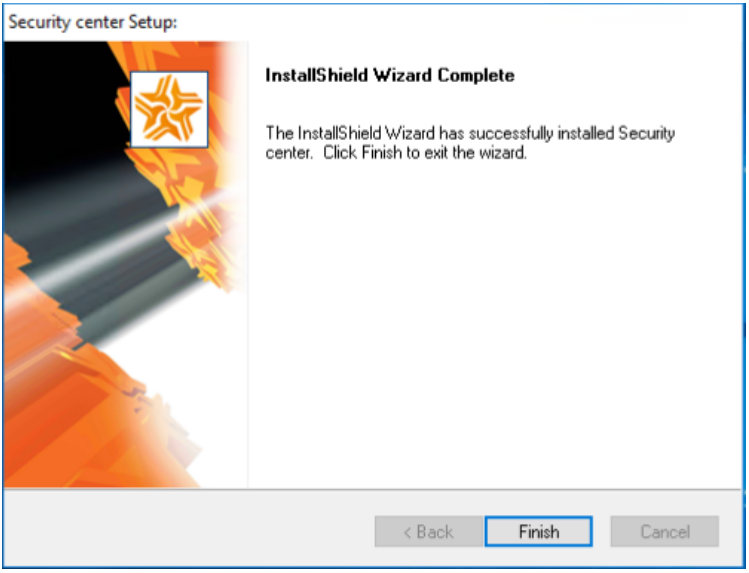
19. Verificar la informacion en la siguiente ventana y presionar **Next**



20. Esperar hasta el final de la instalación.



La instalación del **Security Cent**er está finalizada.

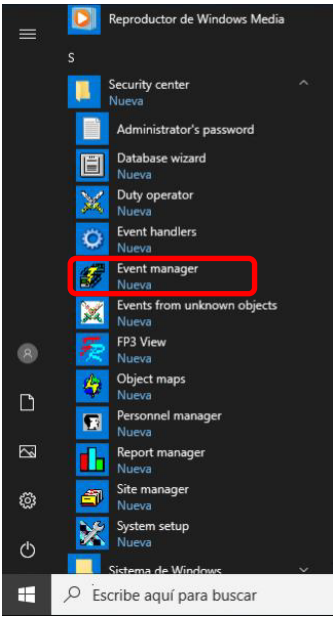


Ahora se puede volver a activar el **Firewall de Windows Defender**.

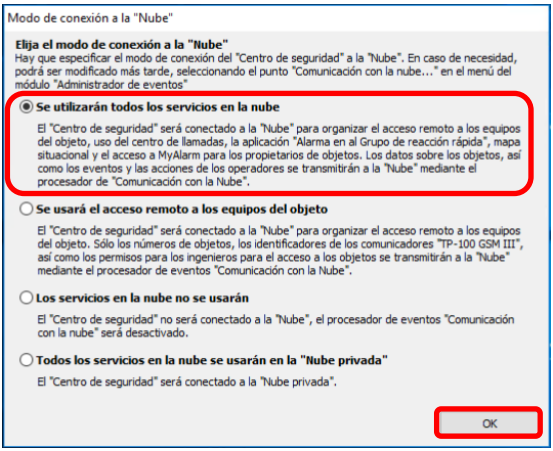
2.5 Configuración y puesta en macrha del Security Center

2.5.1 Configuración del Administrador de eventos

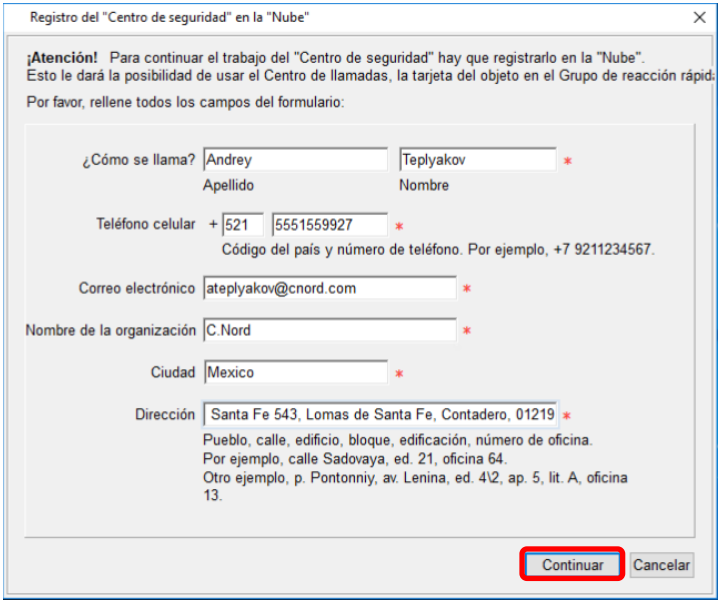
1. Ejecutar el **Event manager** (Administrador de eventos)



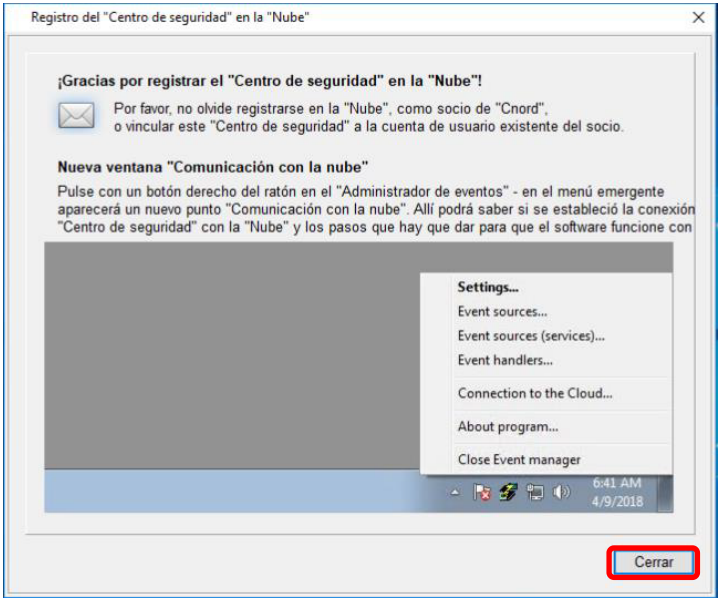
2. En la ventana emergente seleccionar el modo de la conexión a la **Nube C.Nord** – **Se utilizarán todos los servicios en la nube**. Presionar **OK**.



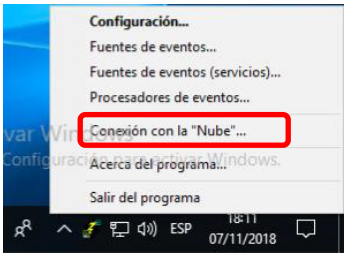
3. Ingresar los datos de su empresa y de la persona de contacto. Presionar **Continuar**.



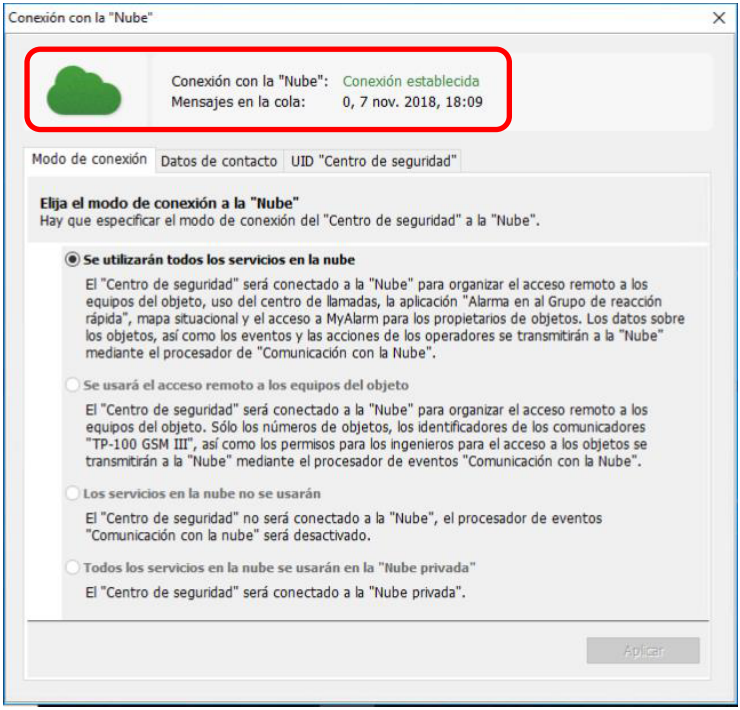
4. El proceso de registro está finalizado. Presionar **Cerrar**.



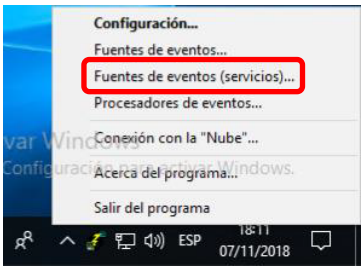
5. Para verificar que el Security Center se conectó a la Nube C.Nord hacer click derecho en el icono del **Administrador de eventos** que se encuentra en la parte derecha de la barra de tareas y eligir **Conexión con la "Nube"** desde el menú deslizante.



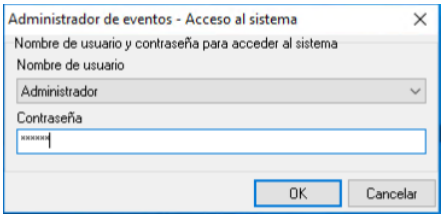
En la ventana emergente aparecerá el estado de la conexión con la **Nube C.Nord**. Se puede cerrar la ventana.



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

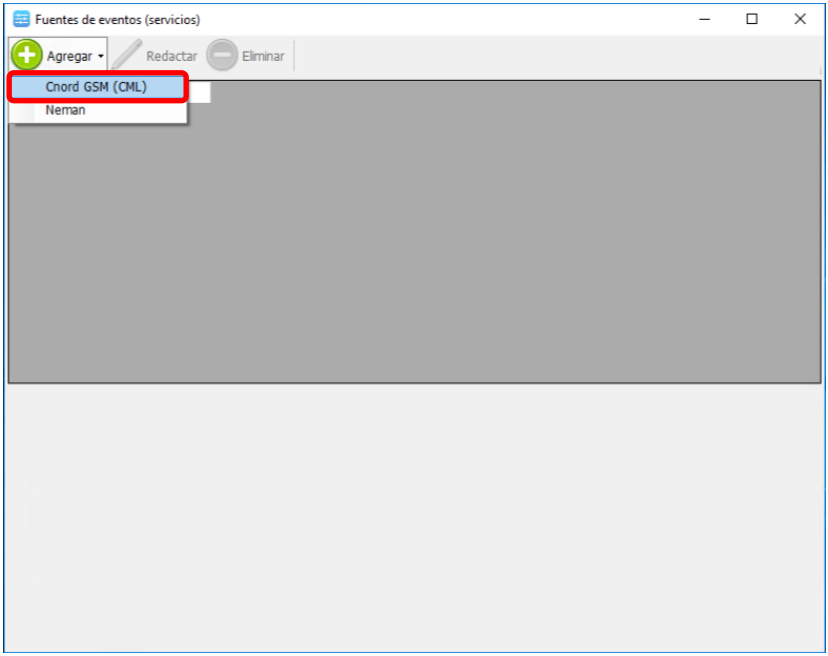


7. En la siguiente ventana ingresar el código del Administrador que por defecto es “222222”.

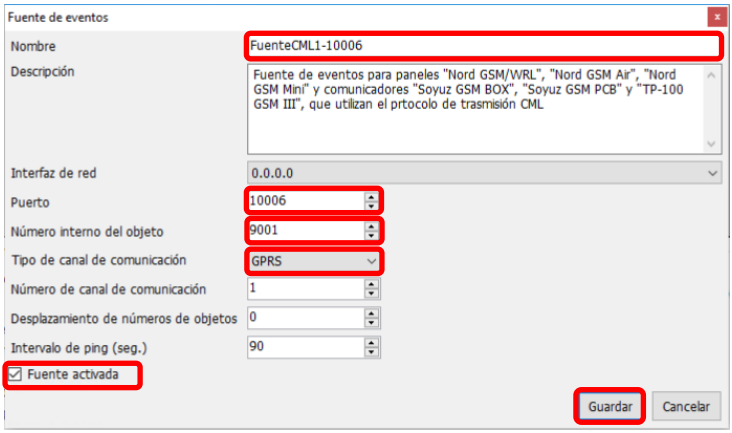


NB! *Para poder configurar el SC para la recepción de los eventos directamente desde los paneles mediante el canal GSM-GPRS o Ethernet el servidor (PC) donde se instaló el SC debe tener la conexión al Internet con la IP pública (en vez de IP se recomienda usar el nombre DNS). Además de la IP habrá que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

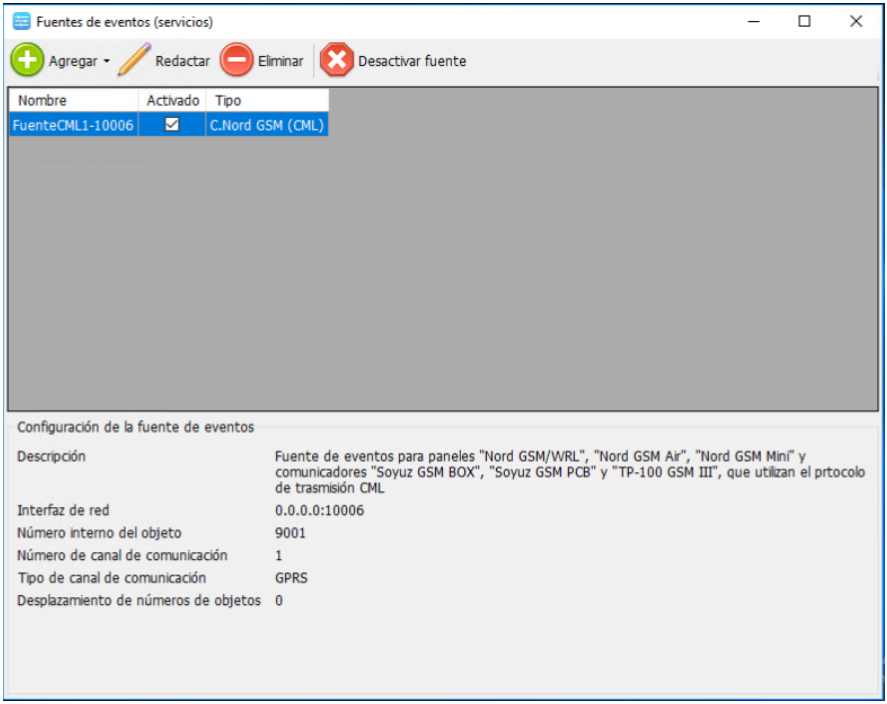
8. En la ventana emergente presionar el botón **Agregar** y seleccionar la fuente **Cnord GSM (CML)**



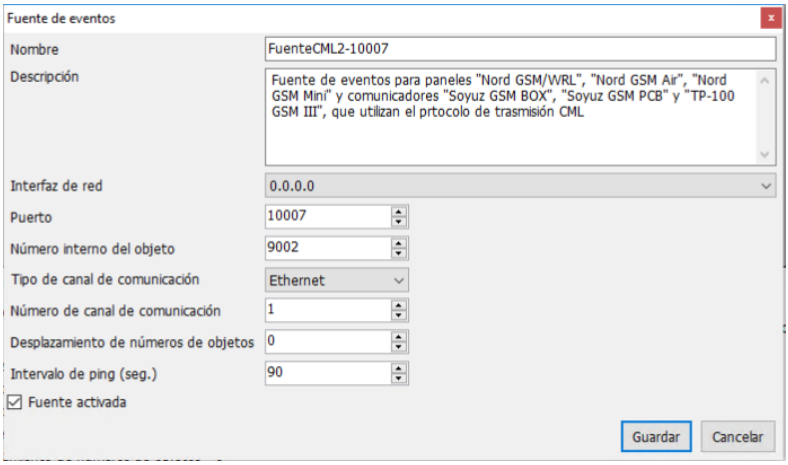
9. En la ventana que aparcerá ingresar el **Nombre** de la fuente, el **Puerto** (para evitar conflictos con los puertos usados en el SO Windows se recomienda usar el valor del puerto que sea superior a 10000), **Número interno del objeto** (que es el numero del objeto en la base de datos del SC) y seleccionar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

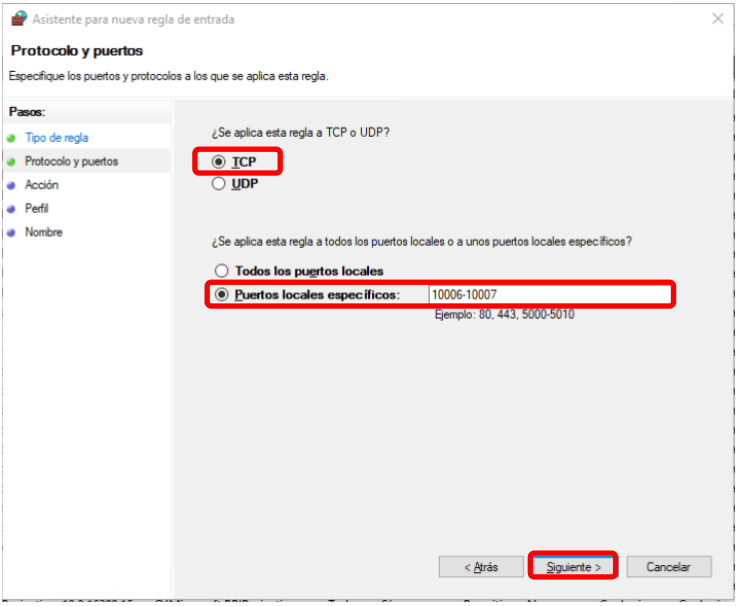


En la ventana **Fuentes de eventos (sericios)** aparecerá la fuente nueva

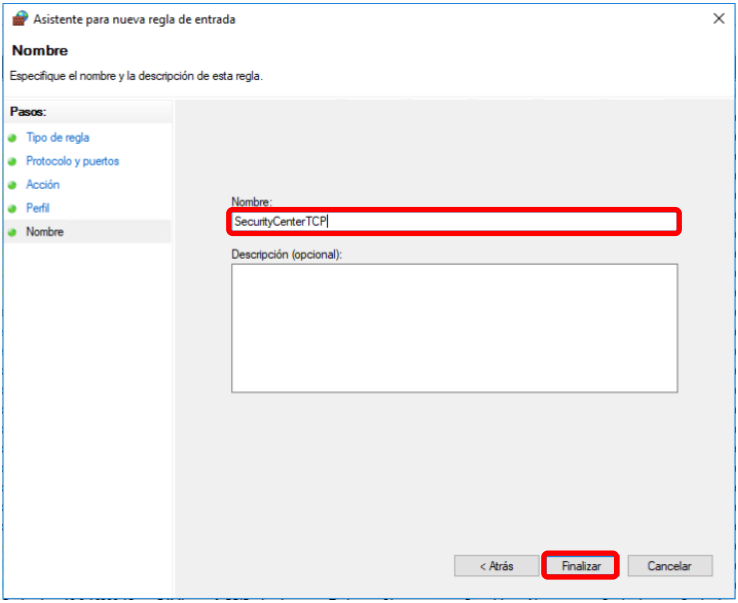


10. Vamos a agregar la segunda fuente para el canal Ethernet. Para eso repetimos los pasos 8 y 9.

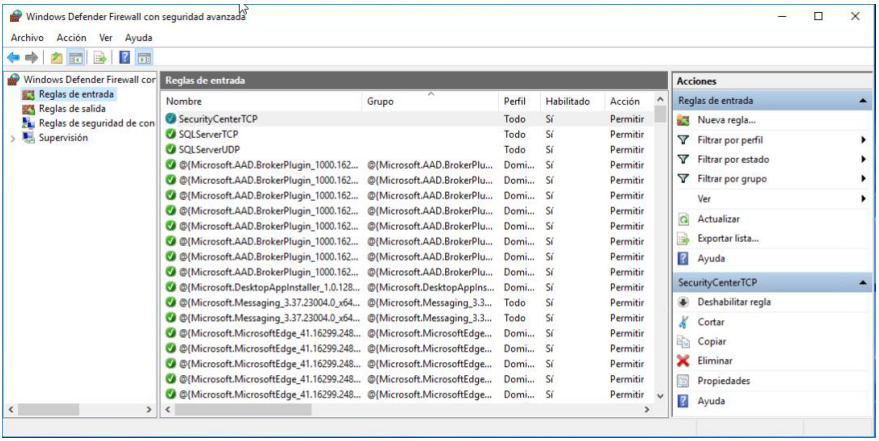




12. Repetir los pasos 5-6 descritos en la sección **2.3**. Luego ingresar el nombre para la regla, e.g. **SecurityCenterTCP** y presionar **Finalizar**

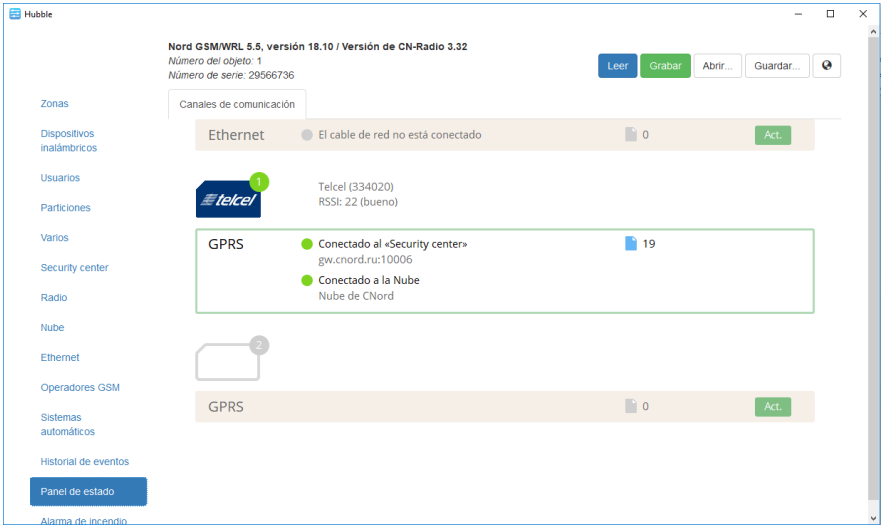


La configuración del **Firewall de Window Defender** está finalizada



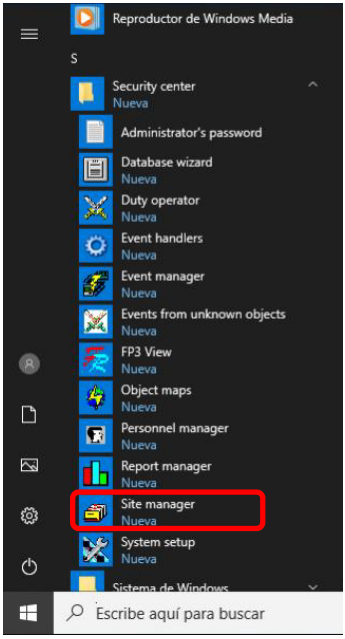
13. Para verificar que su servidor tiene la IP pública y los puertosTCP están abiertos para las conexiones entrantes se puede utilizar la [pagina especial] en nuestro sitio web

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

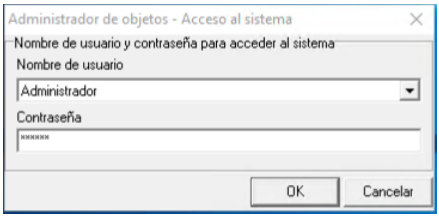


2.5.2 Adición de nuevos objetos en Administrador de objetos

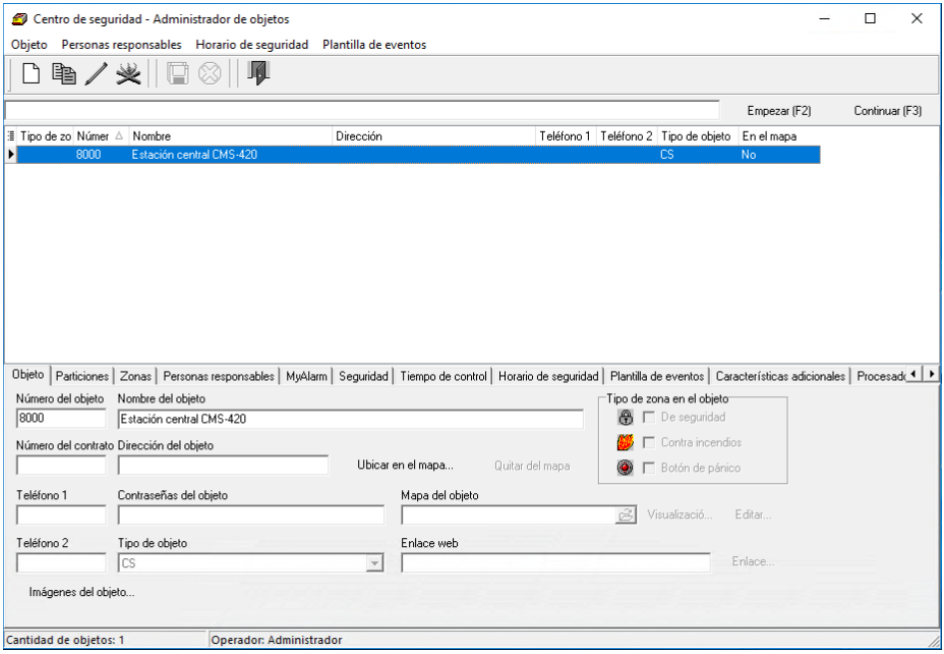
1. Ejecutar el **Site manager** (Administrador de objetos)



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



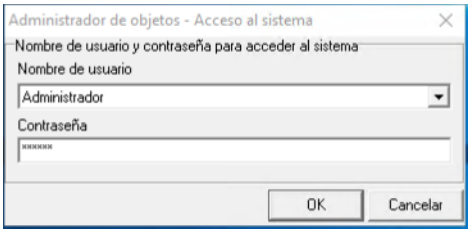
3. Se abrirá la ventana principal del módulo **Administrador de objetos**



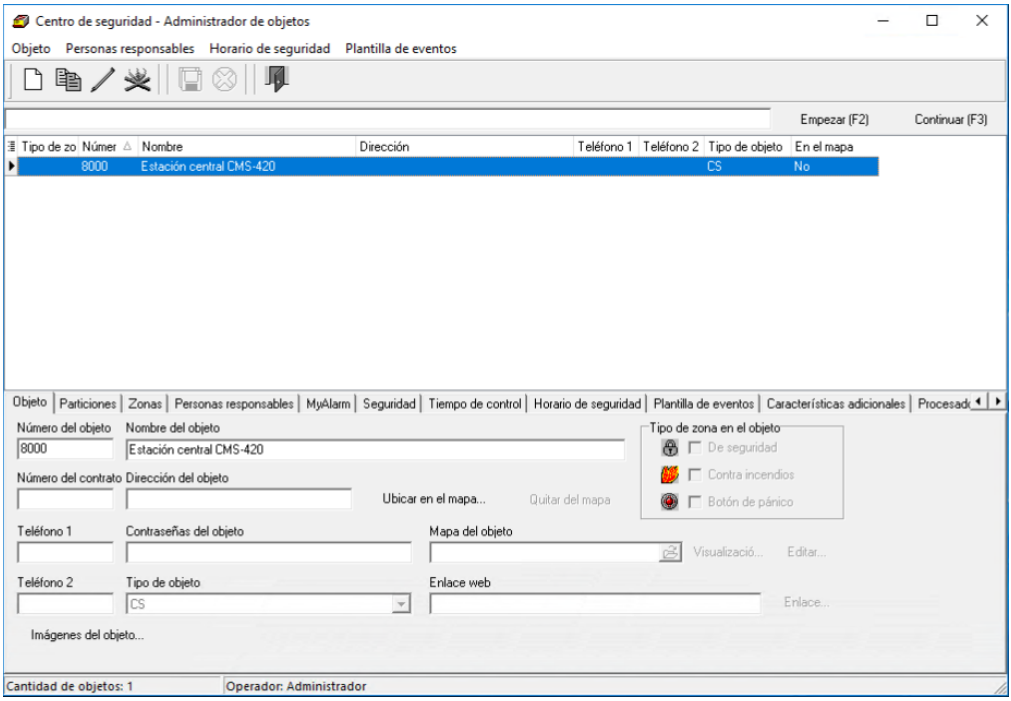
4. Para poder identificar los paneles que no están registrados en la base de datos primero tendremos que crear dos objetos virtuales para los fuentes de eventos – GPRS y Ethernet

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

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

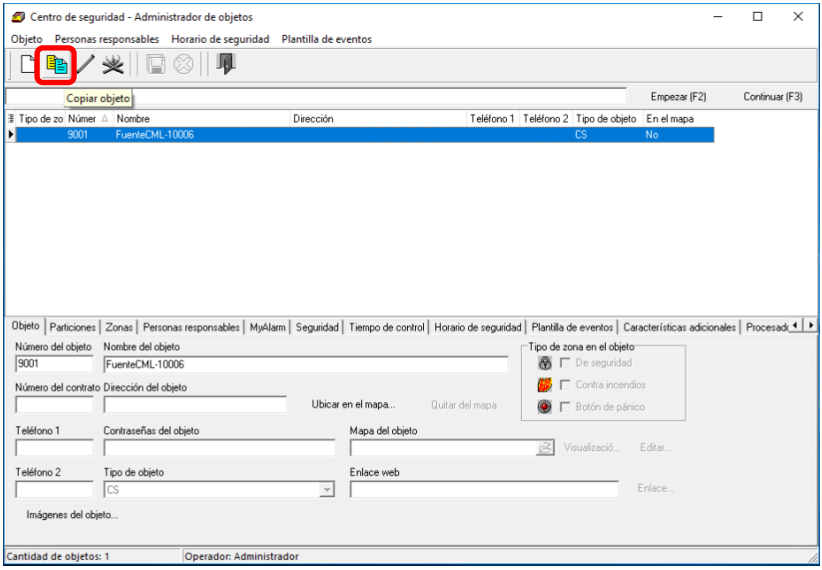


3. Se abrirá la ventana principal del módulo **Administrador de objetos**

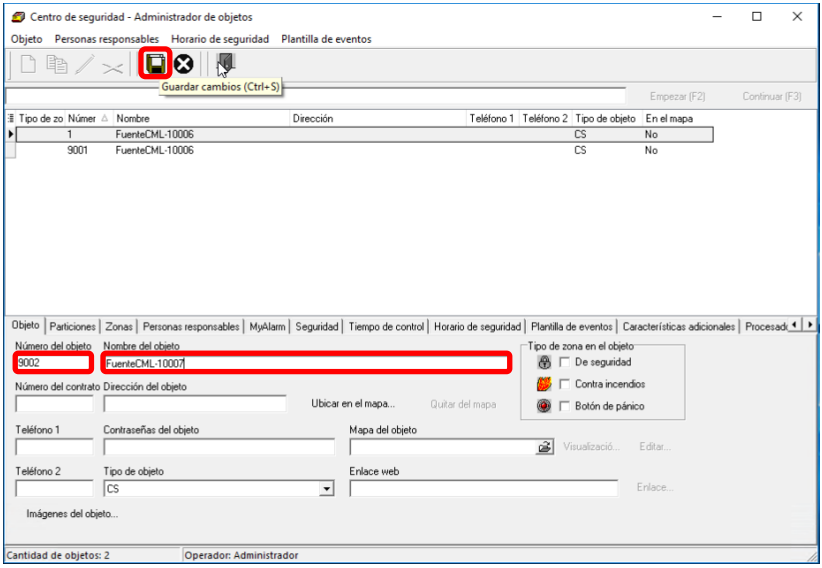


4. Para poder identificar los paneles que no están registrados en la base de datos primero tendremos que crear dos objetos virtuales para los fuentes de eventos – GPRS y Ethernet

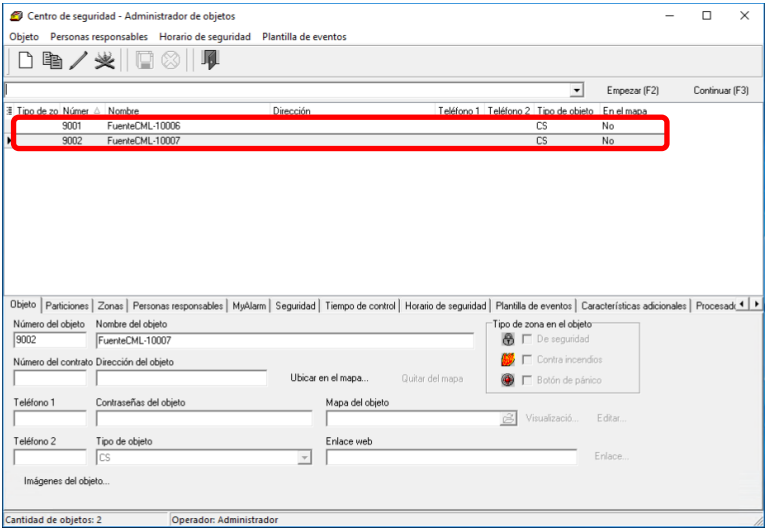
Para ello seleccionar el objeto existente en la base de datos con el nombre **Estación central CMS-420** y presionar el botón **Redacatar** en la barra de instrumentos de arriba.



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

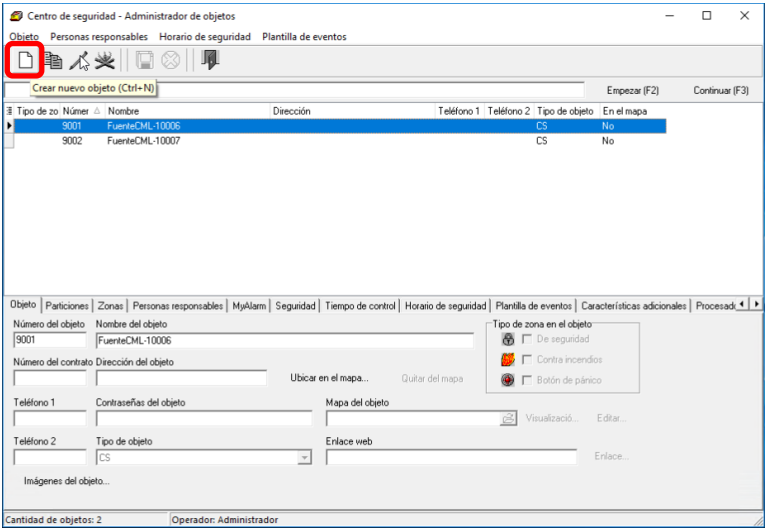


8. Como resultado en la base de datos deben aparecer dos objetos

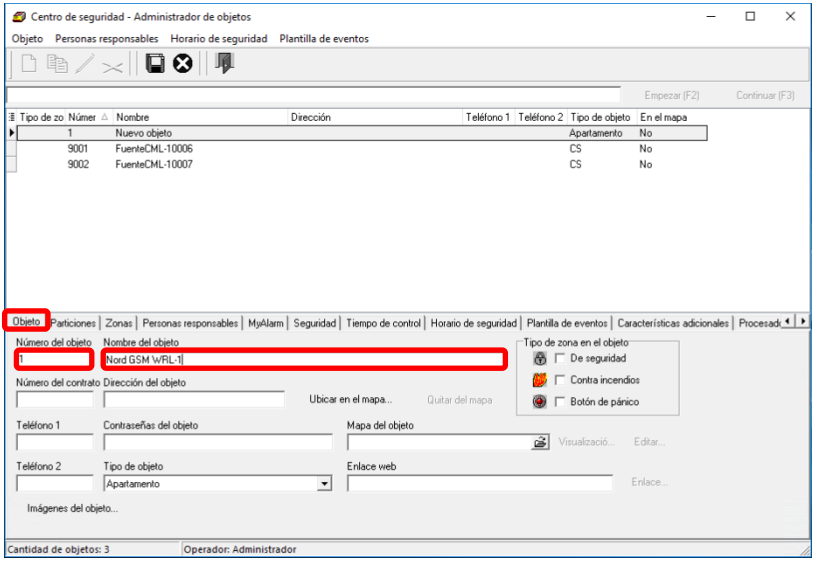


9. Vamos a crear un objeto físico para el panel que ya configuramos anteriormente (vease subsección 1.1)

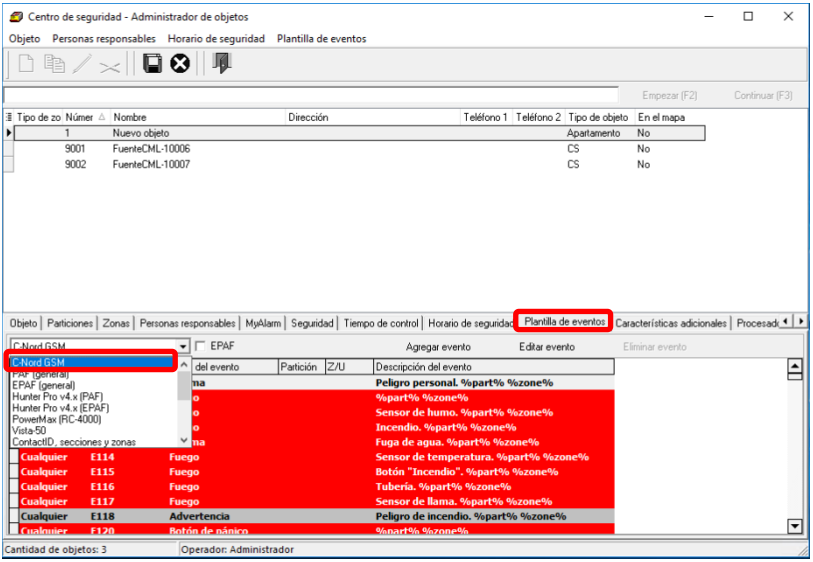
Presionar el botón **Crear nuevo** objeto o **Ctrl+N**



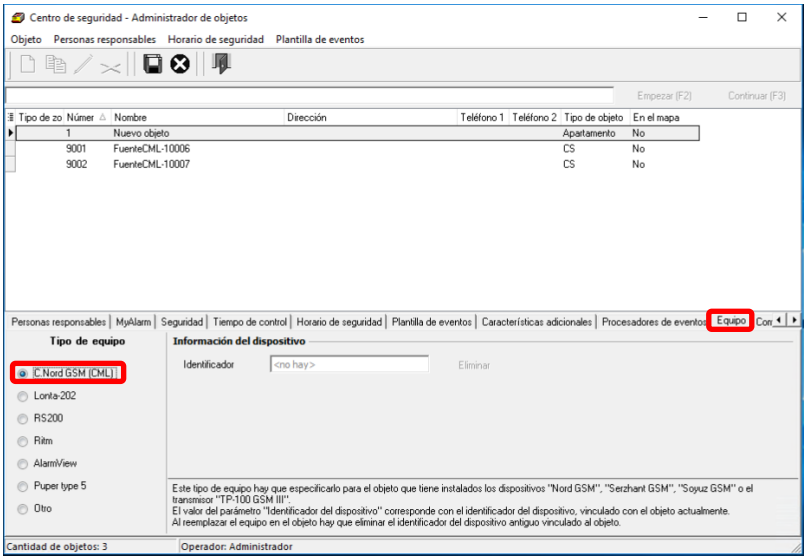
10. En la pestaña **Objeto** ingresar el Número del objeto **"1"** y el Nombre del objeto **"Nord GSM WRL-1"**



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

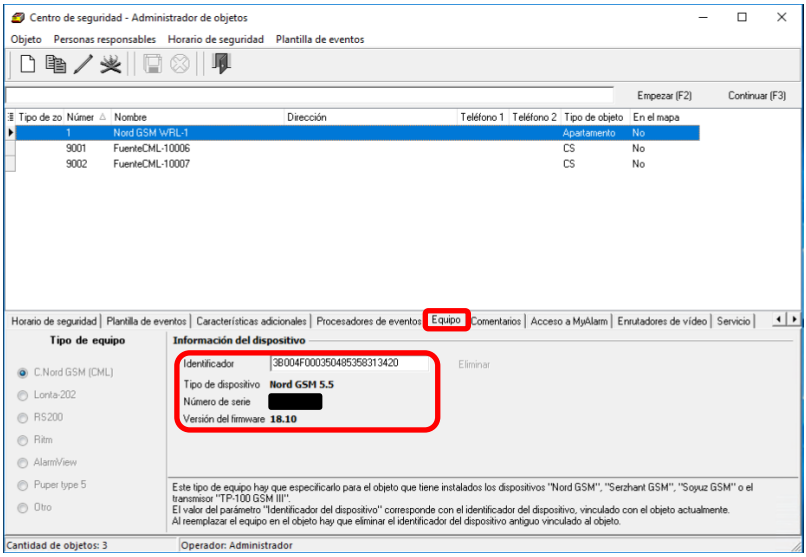


12. En la pestaña **Equipo** seleccionar **C.Nord GSM (CML)** entre las opciones del **Tipo de equipo** disponibles

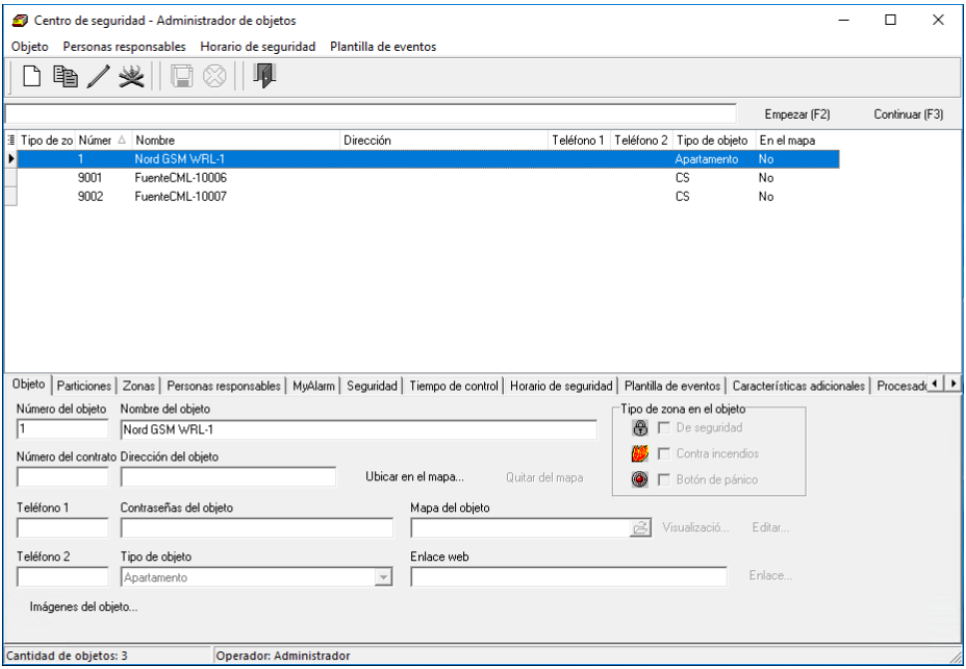


13. Presionar **Guardar cambios**

Para comprobar que el panel se itercambió 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 aparcer 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

2.5.4 Software Operador de guardia y funciones básicas

2.5.5 Acceso remoto al objeto mediante Virtual Expert

CYGNUS electronics

C.Nord