



GUIA DE INSTALACION DEL SOFTWARE DE MONITOREO

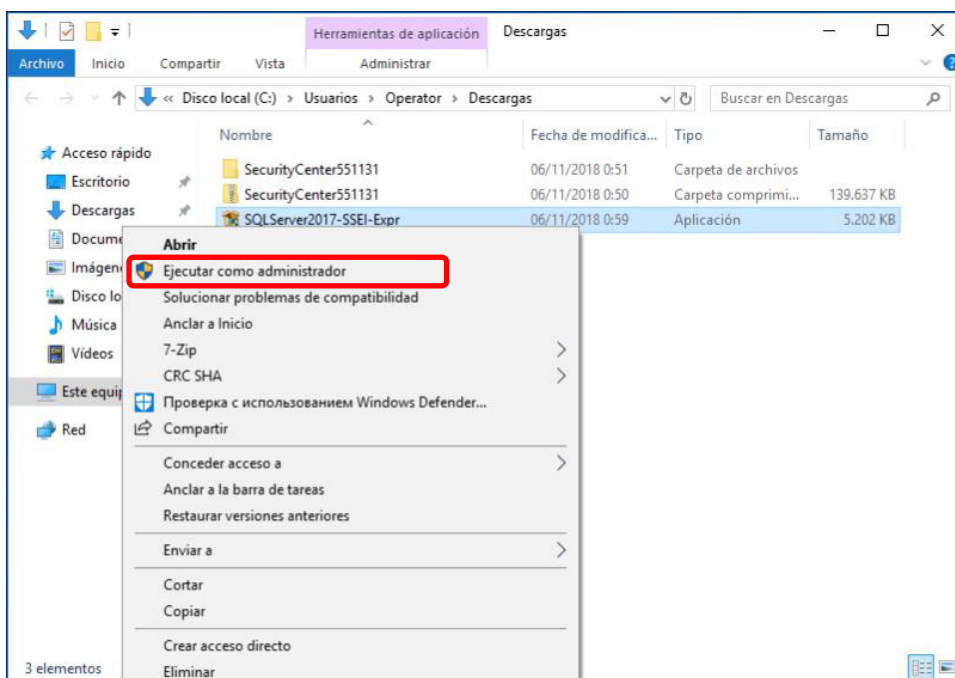
C.Nord

2. Instalación y configuración del software Security Center

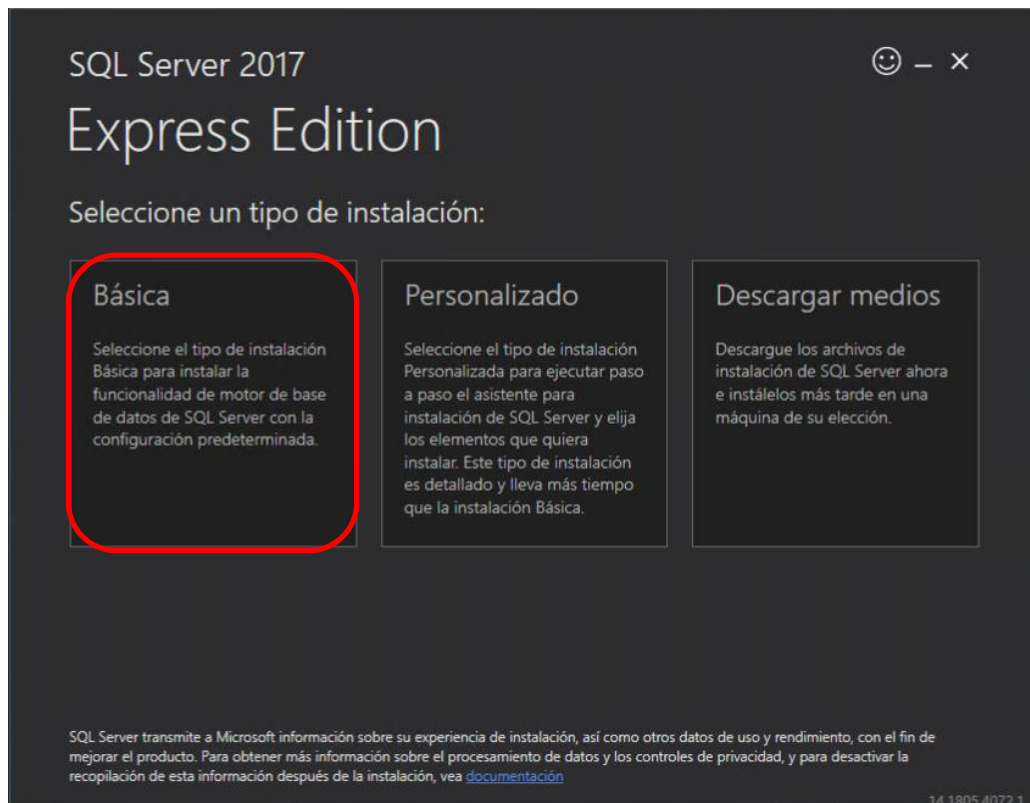
NB! Se recomienda hacer la instalación del programa Security Center en la PC con el SO licenciado Windows 7 or 10 con las últimas actualizaciones, 4GB de memoria RAM y disco duro SSD. Sería mejor que el sistema sea vacío, sin programas adicionales como bases de datos SQL, firewall, antivirus.

2.1 Instalación del Microsoft SQL Server 2017 Express

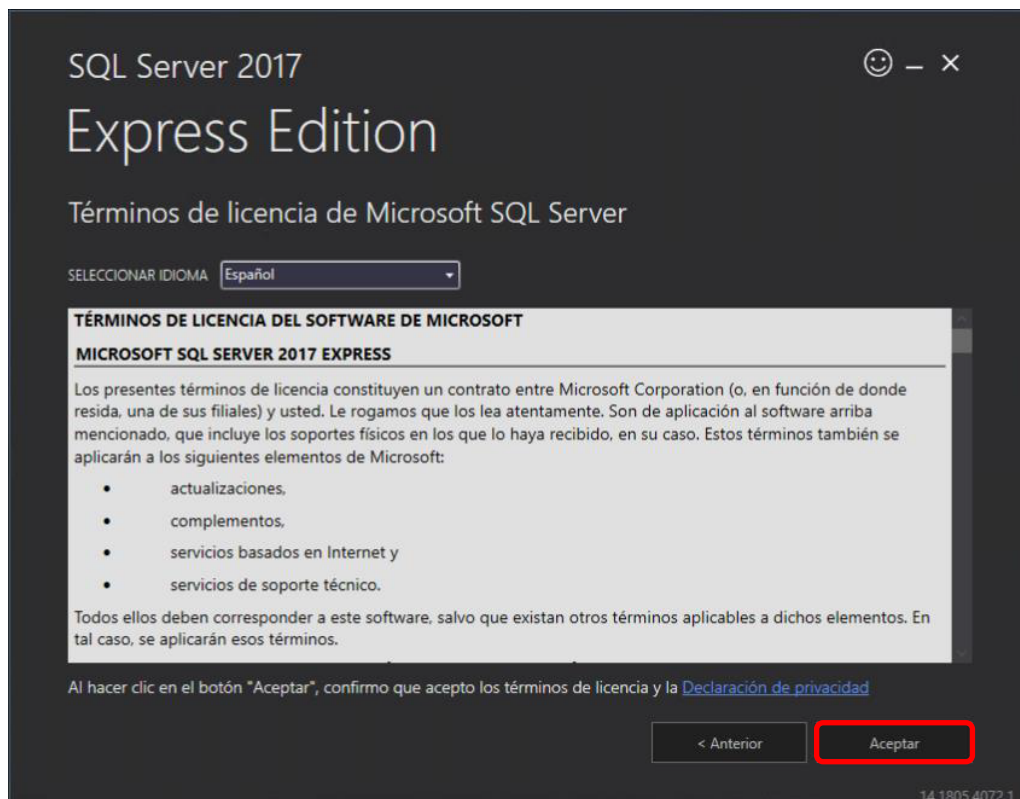
1. Descargar desde el sitio web oficial el programa [Microsoft SQL Server 2017 Express](#)
2. Ejecutar el archivo **SQLServer2017-SSEI-Expr** como Administrador



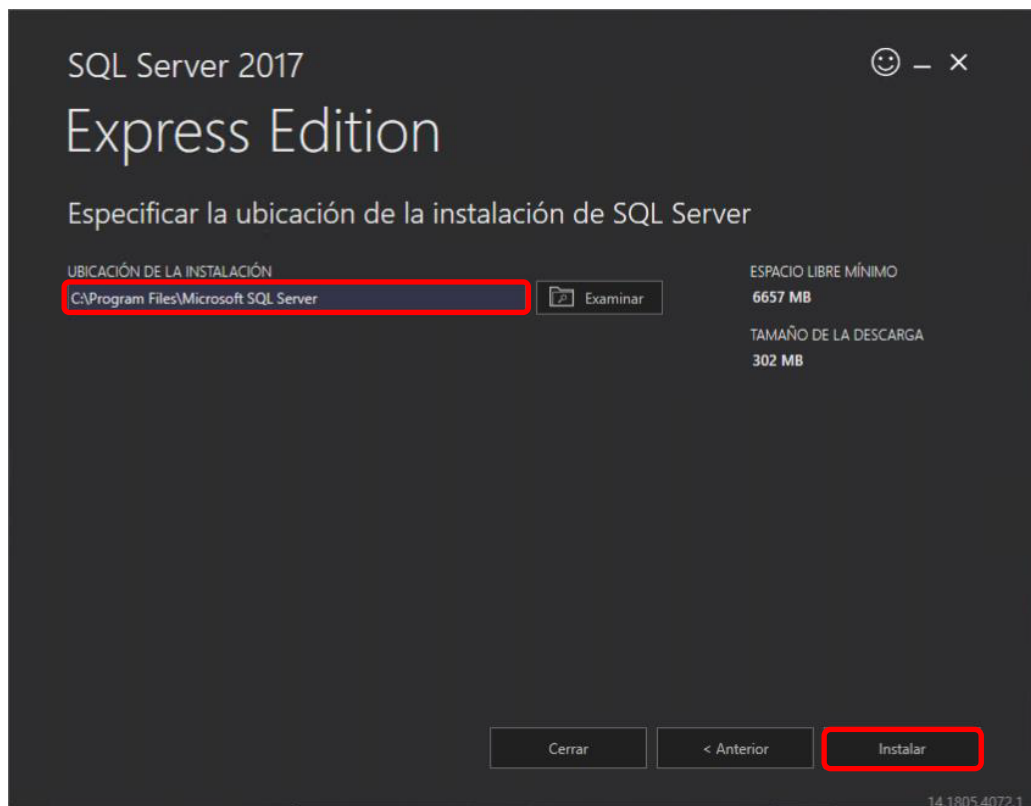
3. Seleccionar el tipo de la instalación **Básica**



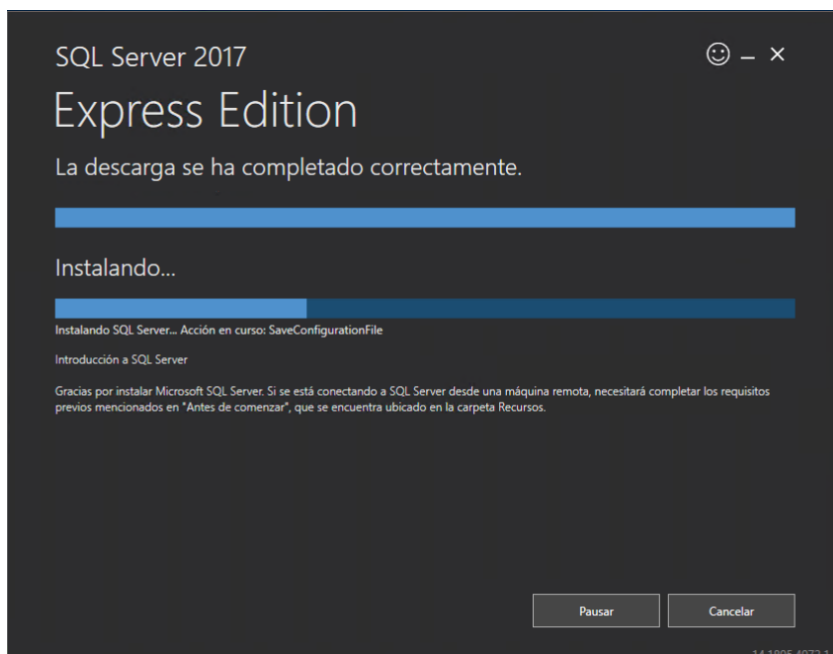
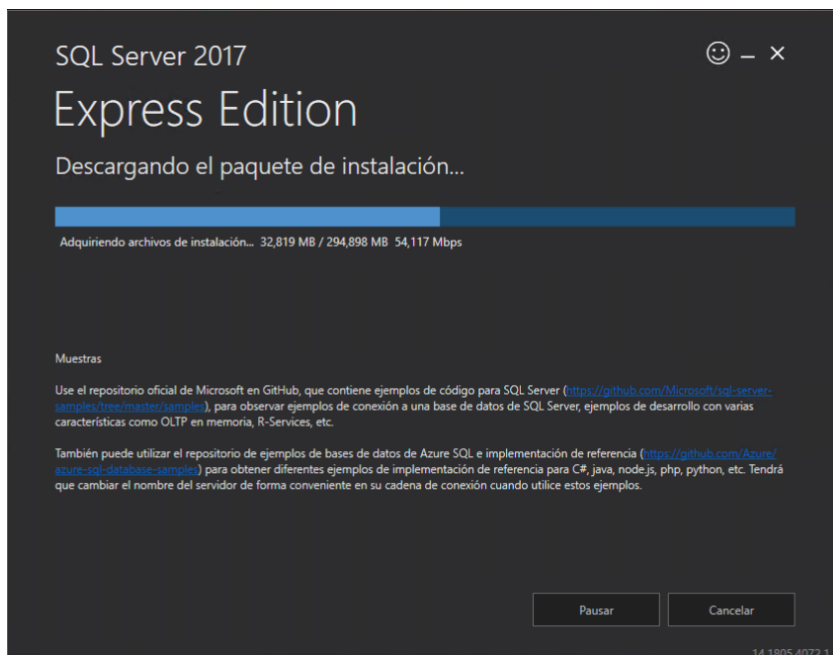
4. Seleccionar el idioma del **SQL Server 2017** y presionar **Aceptar**



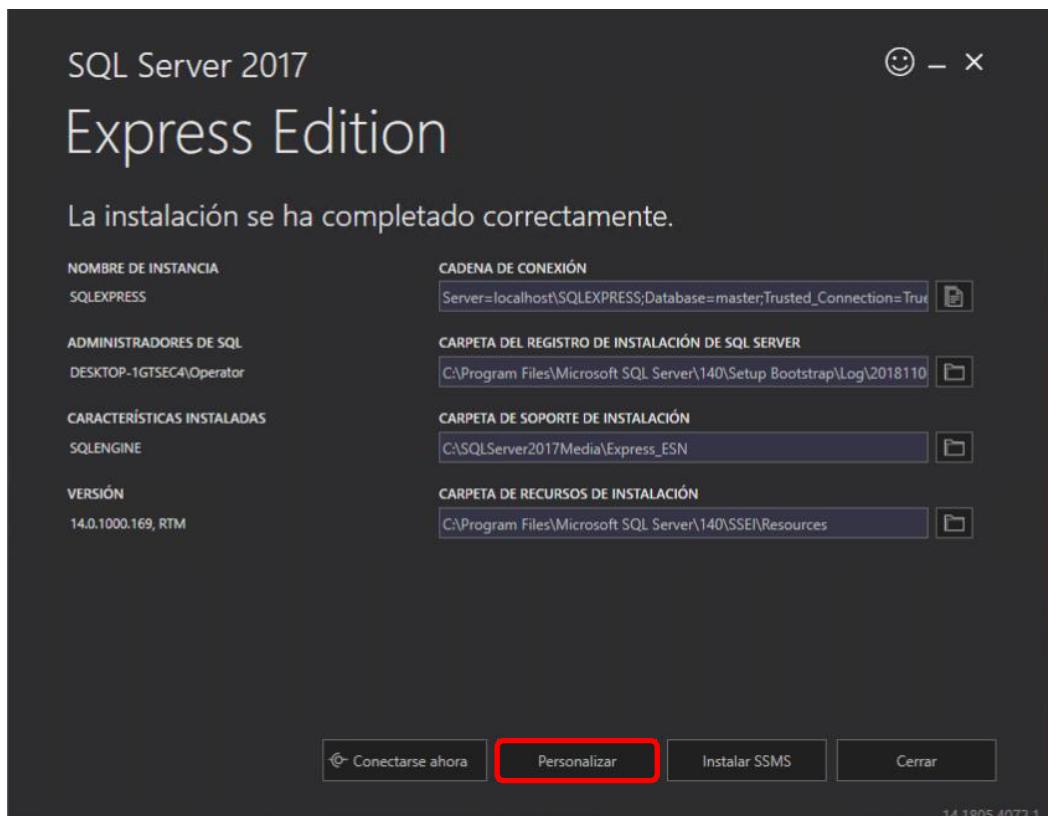
5. Seleccionar la carpeta para la instalación y presionar **Instalar**



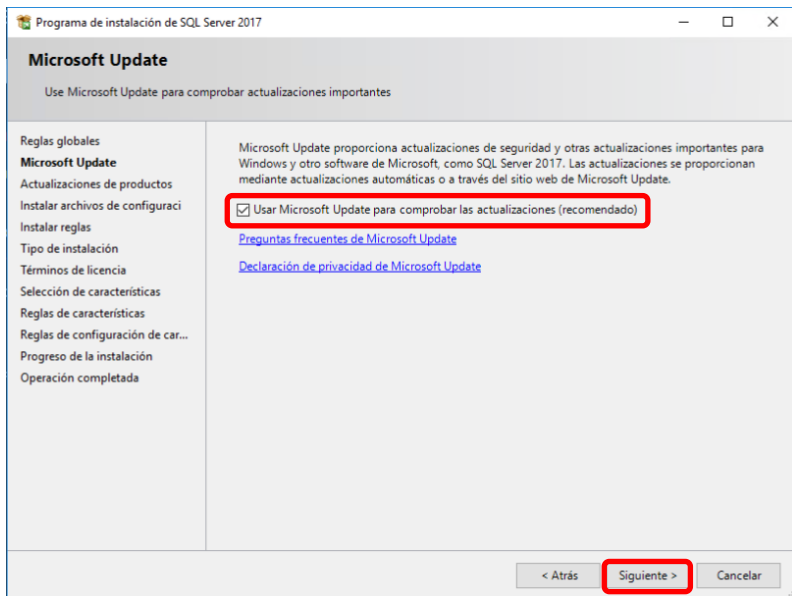
6. Esperar hasta el final de la descarga e instalación



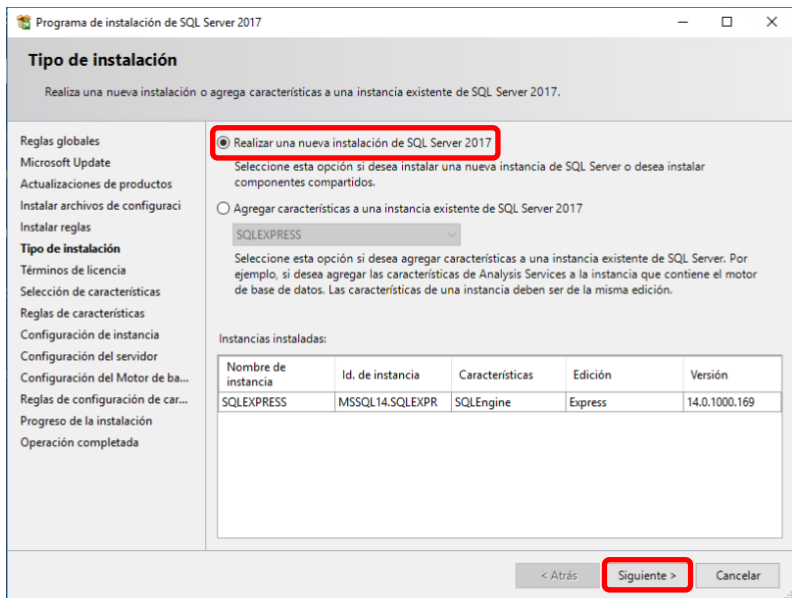
7. Al completar el proceso de la instalación presionar el botón **Personalizar**. Se abrirá la nueva ventana.



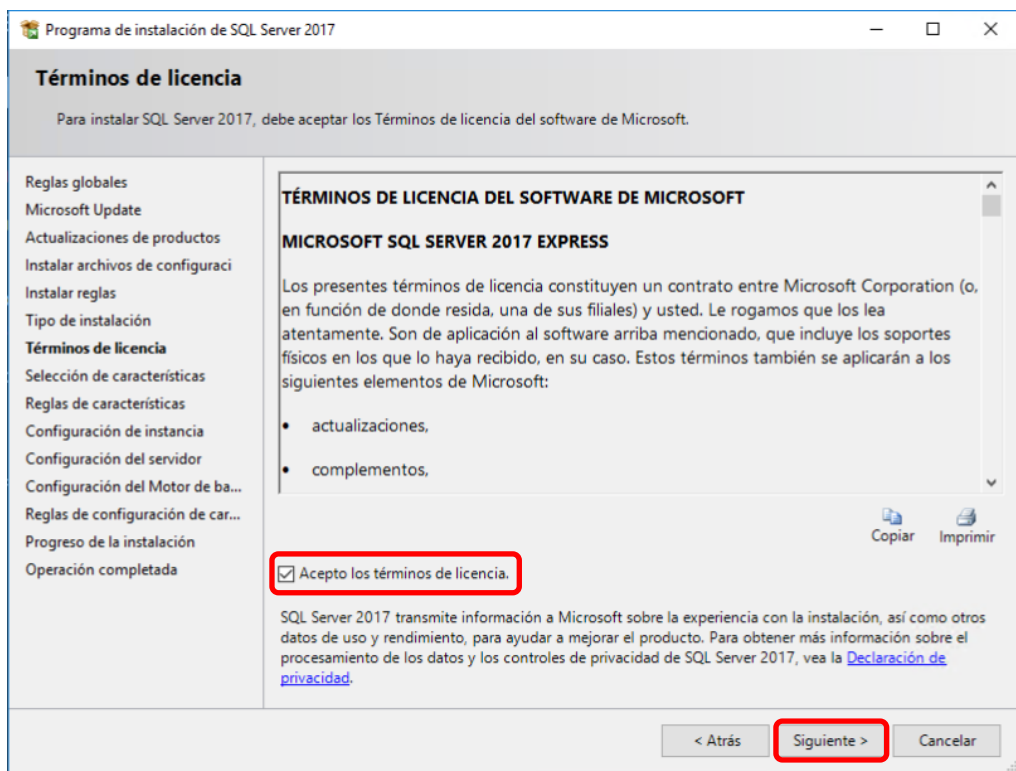
8. Seleccionar la opción **Usar Microsoft Update...** y presionar el botón **Siguiente**



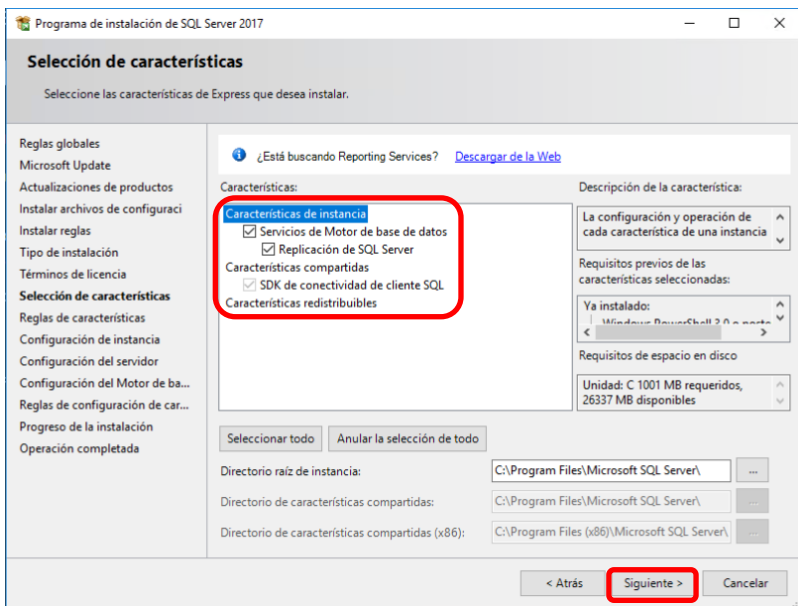
9. Seleccionar la opción **Realizar una nueva instalación del SQL Server 2017** y presionar **Siguiente**



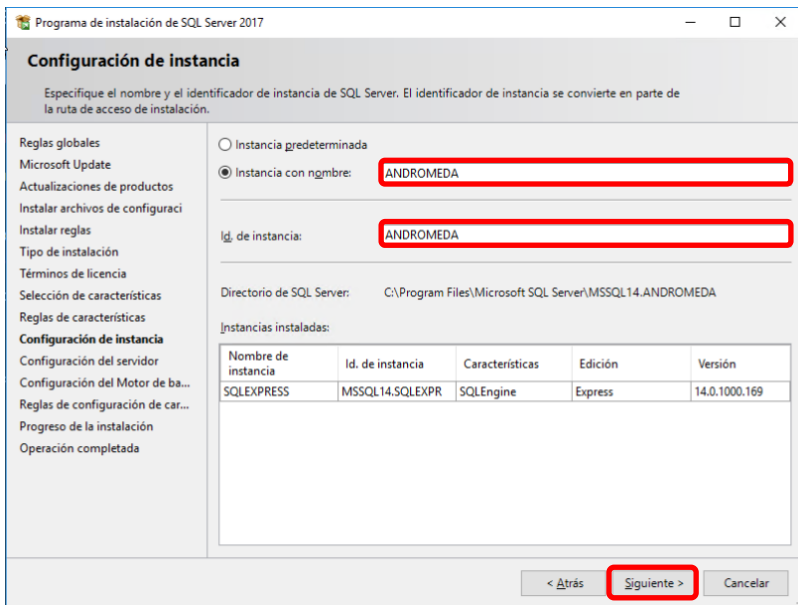
10. Aceptar los términos de la licencia y presionar **Siguiente**



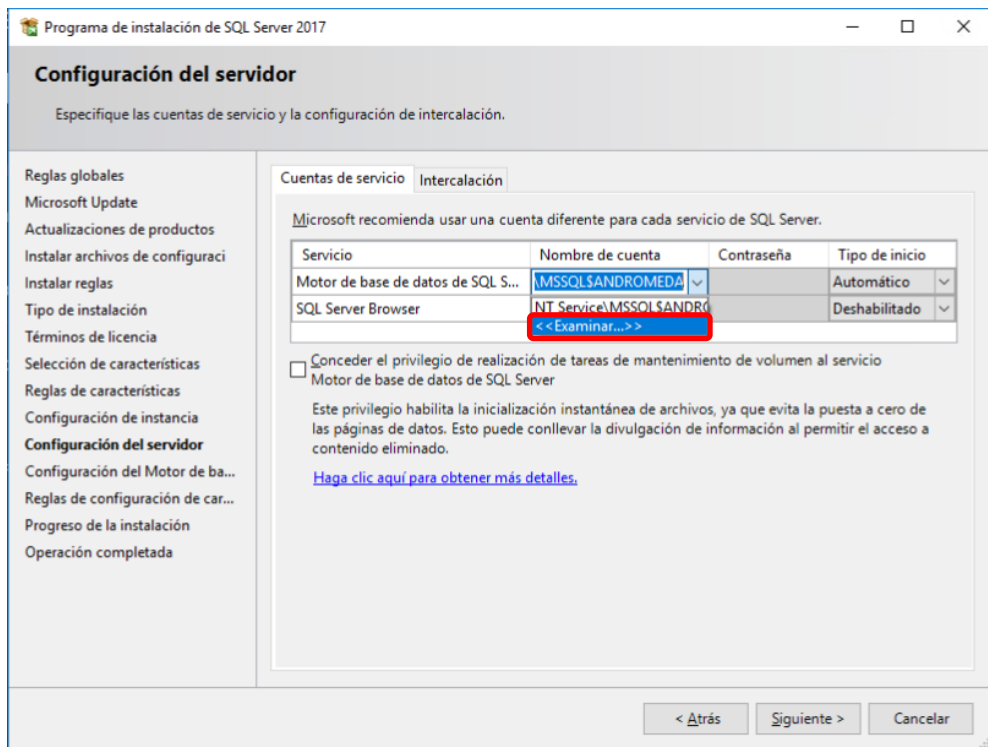
11. Verificar que todas las tres casillas estén marcadas y presionar **Siguiente**



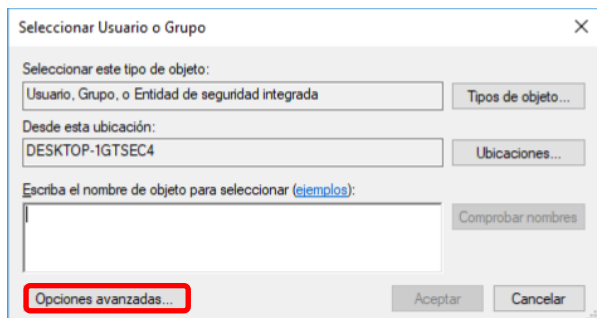
12. Especificar el nombre y el identificador de instancia de SQL Server: **ANDROMEDA**. Presionar el botón **Siguiente**



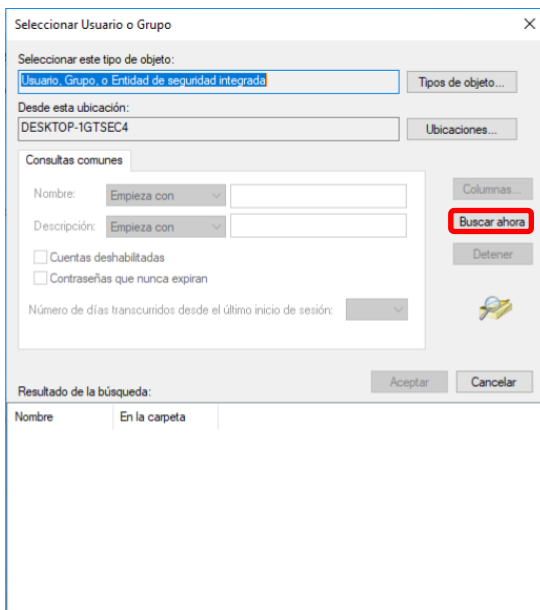
13. Para el servicio **Motor de base de datos de SQL Server** ingresar en los parametros de redacción del nombre de la cuenta. Para eso en el menú deslizante seleccionar **Examinar**



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



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



Seleccionar Usuario o Grupo

Seleccionar este tipo de objeto:
 Tipos de objeto...

Desde esta ubicación:
 Ubicaciones...

Consultas comunes

Nombre:

Descripción:

☐ Cuentas deshabilitadas
☐ Contraseñas que nunca expiran

Número de días transcurridos desde el último inicio de sesión:

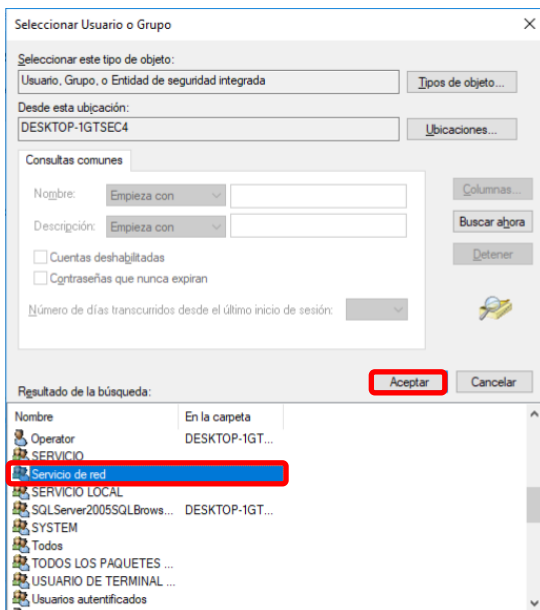
Columnas...
 Buscar ahora
 Detener

Resultado de la búsqueda:

Nombre	En la carpeta
--------	---------------

Aceptar Cancelar

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



Seleccionar Usuario o Grupo

Seleccionar este tipo de objeto:
 Tipos de objeto...

Desde esta ubicación:
 Ubicaciones...

Consultas comunes

Nombre:

Descripción:

☐ Cuentas deshabilitadas
☐ Contraseñas que nunca expiran

Número de días transcurridos desde el último inicio de sesión:

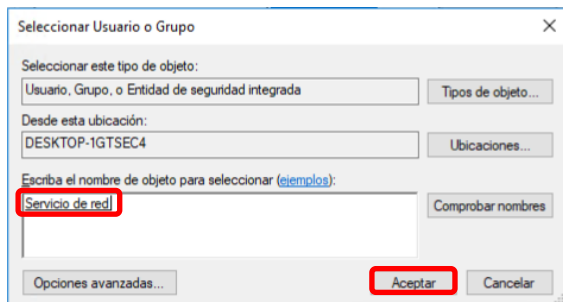
Columnas...
 Buscar ahora
 Detener

Resultado de la búsqueda:

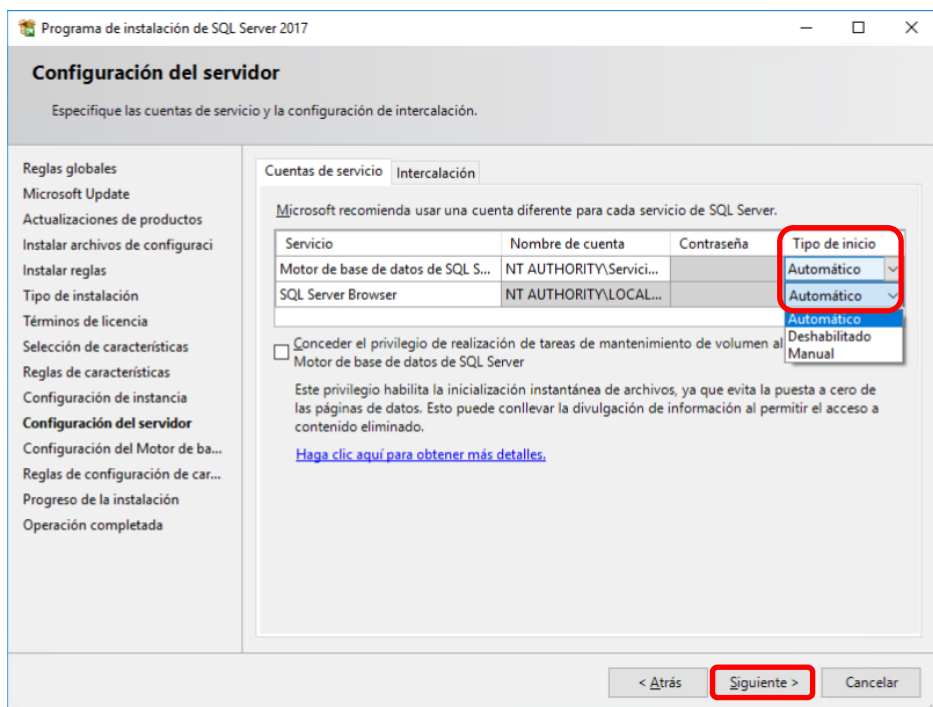
Nombre	En la carpeta
Operator	DESKTOP-1GT...
SERVICIO	
Servicio de red	
SERVICIO LOCAL	
SQLServer2005SQLBrows...	DESKTOP-1GT...
SYSTEM	
Todos	
TODOS LOS PAQUETES ...	
USUARIO DE TERMINAL ...	
Usuarios autenticados	

Aceptar Cancelar

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).

Programa de instalación de SQL Server 2017

Configuración del Motor de base de datos

Especifique el modo de seguridad de autenticación, administradores, directorios de datos y configuración de TempDB del motor de base de datos.

Reglas globales
Microsoft Update
Actualizaciones de productos
Instalar archivos de configuraci
Instalar reglas
Tipo de instalación
Términos de licencia
Selección de características
Reglas de características
Configuración de instancia
Configuración del servidor
Configuración del Motor de b...
Reglas de configuración de car...
Progreso de la instalación
Operación completada

Configuración del servidor | Directorios de datos | TempDB | Instancias de usuario | FILESTREAM

Especifique el modo de autenticación y los administradores para el motor de base de datos.

Modo de autenticación

☐ Modo de autenticación de Windows

☒ **Modo mixto (autenticación de SQL Server y de Windows)**

Especifique la contraseña de la cuenta de administrador del sistema de SQL Server (sa).

Escribir contraseña:

Confirmar contraseña:

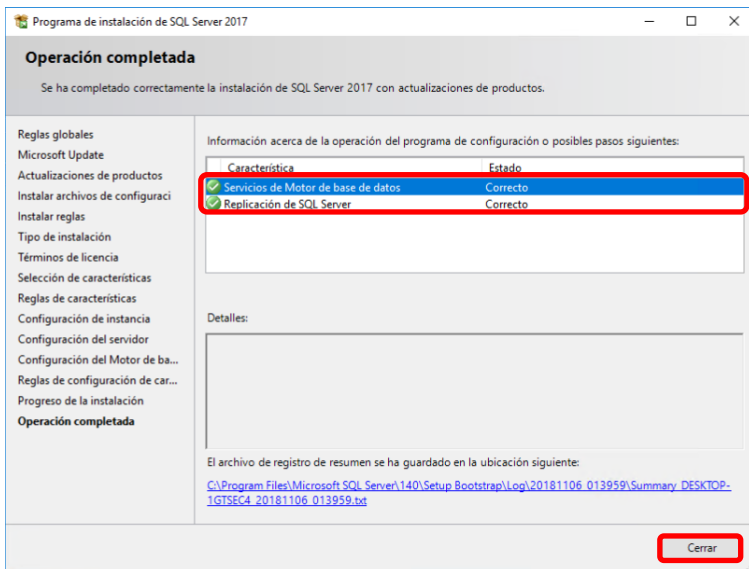
Especifique los administradores de SQL Server

DESKTOP-1GTSECA\Operator (Operator)

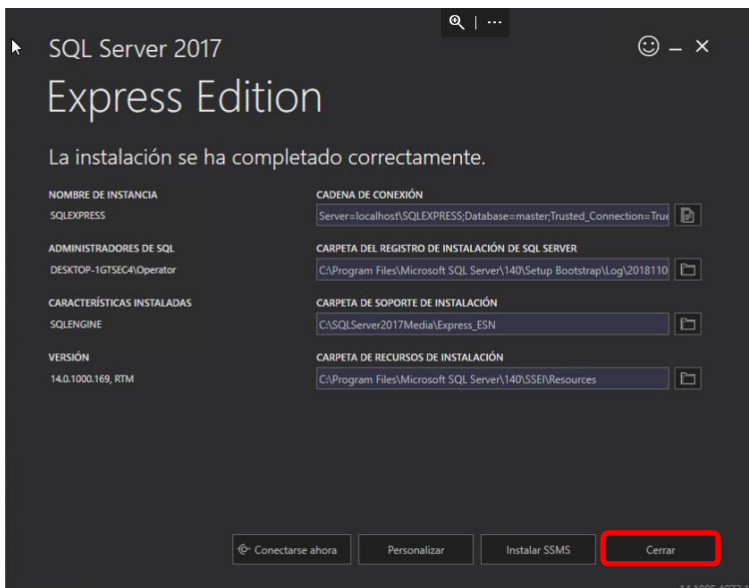
Los administradores de SQL Server tienen acceso sin restricciones al Motor de base de datos.

< Atrás **Siguiente >** Cancelar

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



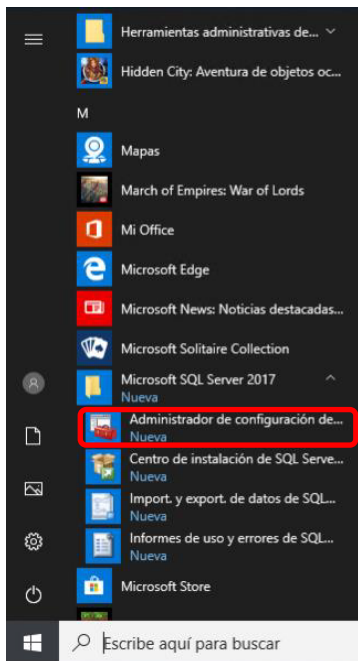
21. Presionar **Cerrar** segunda vez



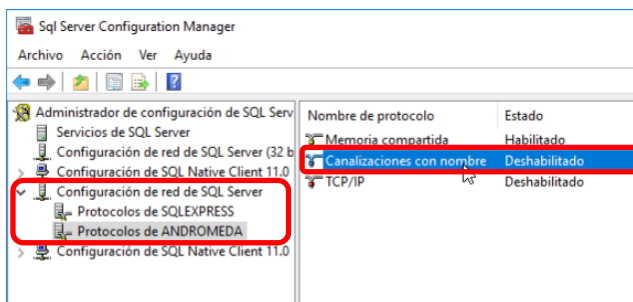
2.2 Configuración del Microsoft SQL Server 2017 Express

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

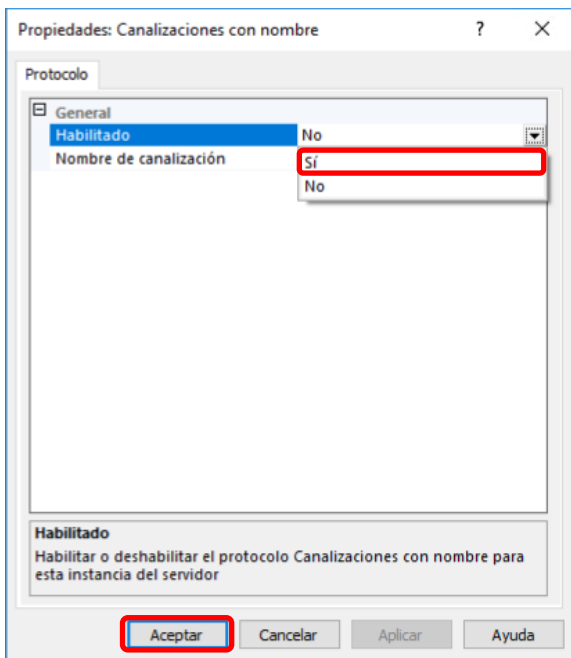
1. Ejecutar **Administrador de configuración de SQL Server 2017**



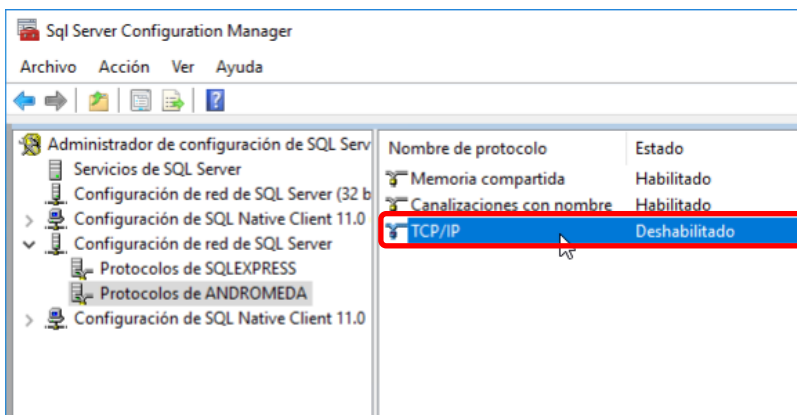
2. En la ventana emergente seleccionar **Configuración de red de SQL Server -> Protocolos de ANDROMEDA**. Hacer el doble click en el protocolo **Canalizaciones con nombre** en la parte derecha.



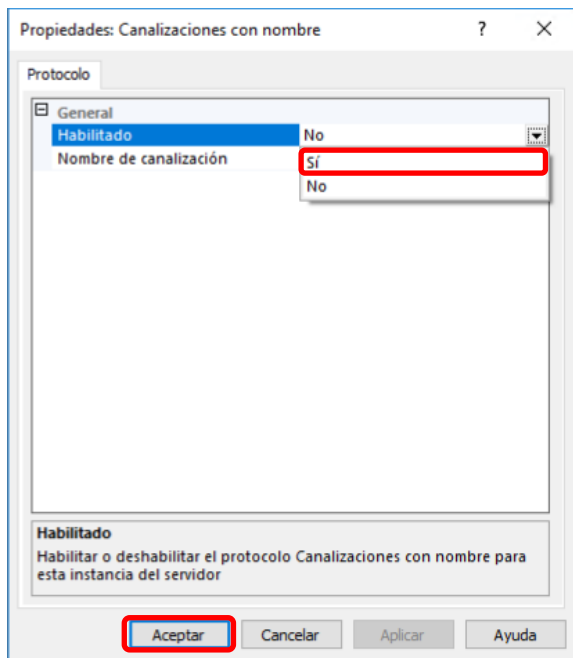
3. En la ventana siguiente seleccionar **Sí** frente a la opción **Habilitado**. Presionar **Aceptar**.



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

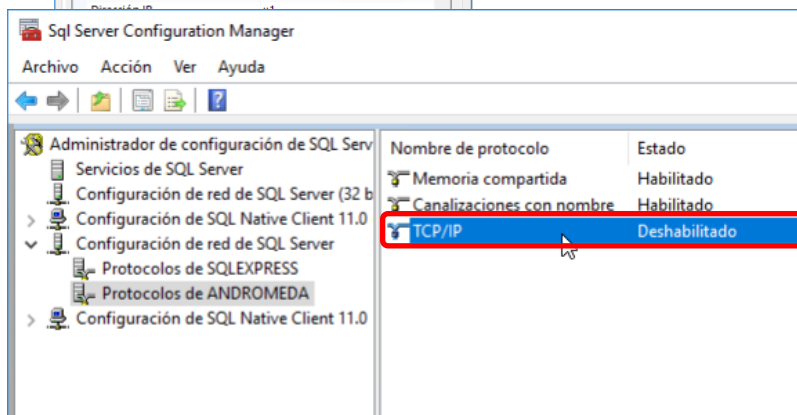


5. En la ventana siguiente seleccionar **Sí** frente a la opción **Habilitado**.



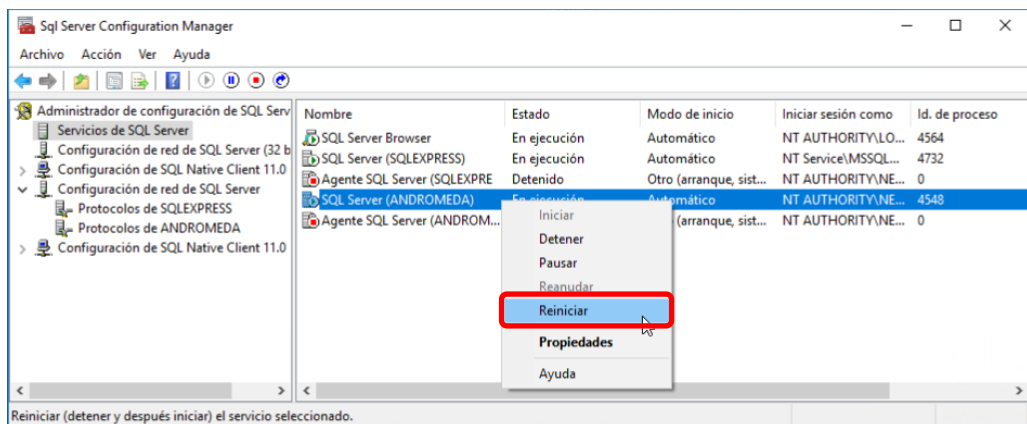
valor frente a **Puertos dinámicos TCP**.

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



recho del

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

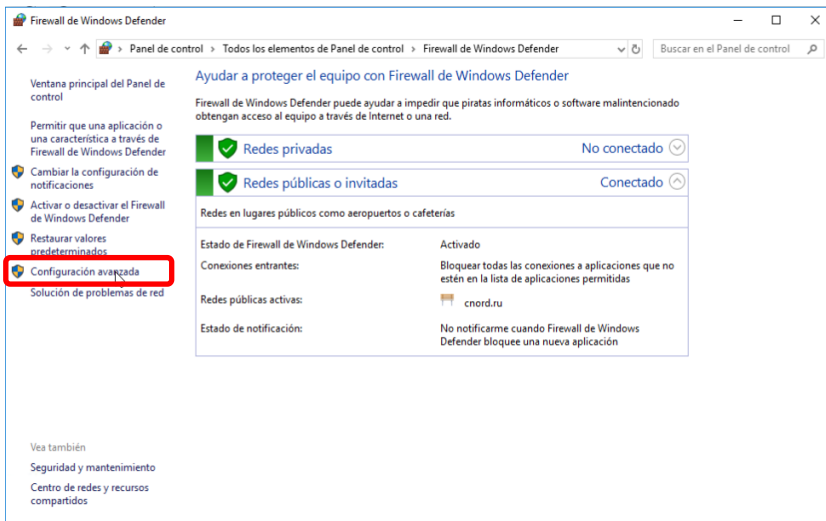


La configuración del **SQL Server** está completada.

2.3 Configuración del Firewall de Windows Defender

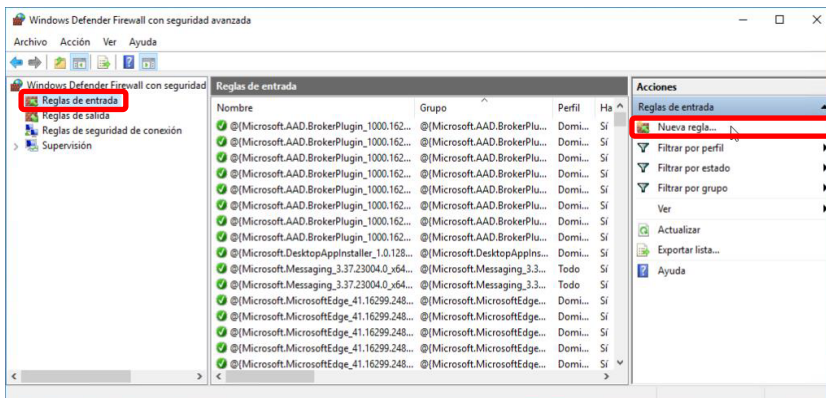
Para configurar **Firewall de Windows Defender** realice las siguientes acciones

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

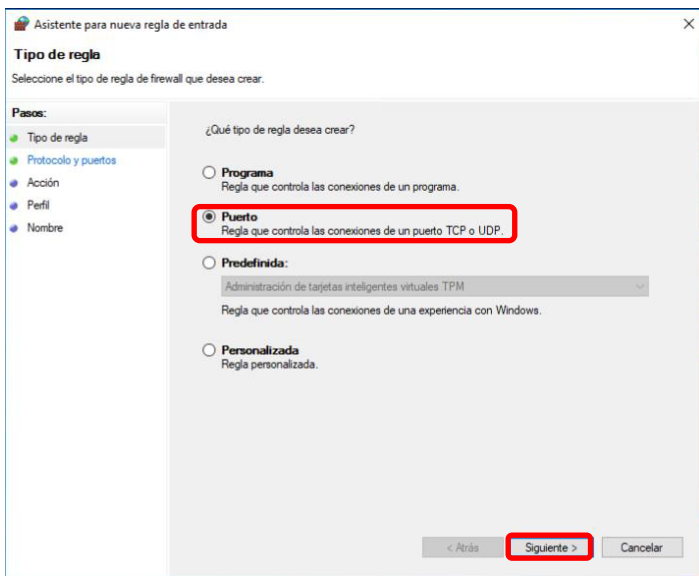


2. Agregar la regla para el puerto TCP/IP

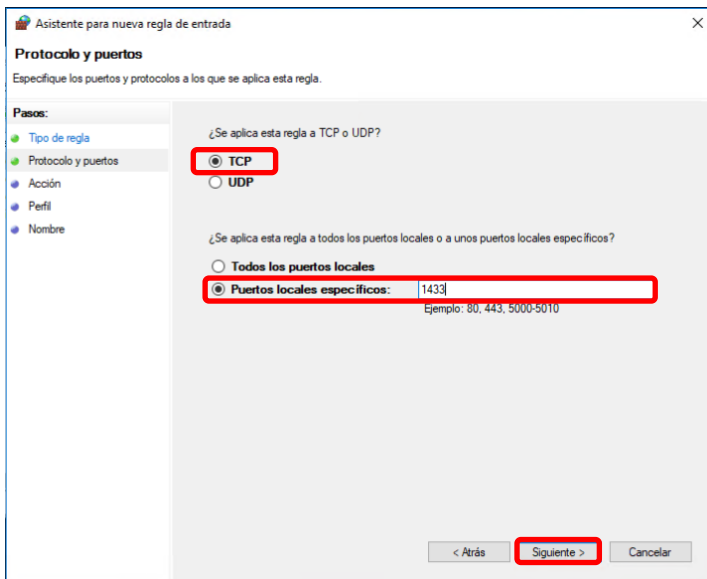
En la nueva ventana seguir a la sección **Reglas de entrada** y en la parte derecha hacer click en **Nueva regla**.



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**

Asistente para nueva regla de entrada

Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

Pasos:

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

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas en la regla?

☒ **Permitir la conexión**
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☐ **Bloquear la conexión**

Personalizar...

< Atrás **Siguiente >** Cancelar

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

Asistente para nueva regla de entrada

Perfil

Especifique los perfiles en los que se va a aplicar esta regla.

Pasos:

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

¿Cuándo se aplica esta regla?

☒ **Dominio**
Se aplica cuando un equipo está conectado a su dominio corporativo.

☒ **Privado**
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

☒ **Público**
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

< Atrás **Siguiente >** Cancelar

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**.

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:

Ejemplo: 80, 443, 5000-5010

< Atrás **Siguiente >** Cancelar

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

Asistente para nueva regla de entrada

Nombre
Especifique el nombre y la descripción de esta regla.

Pasos:

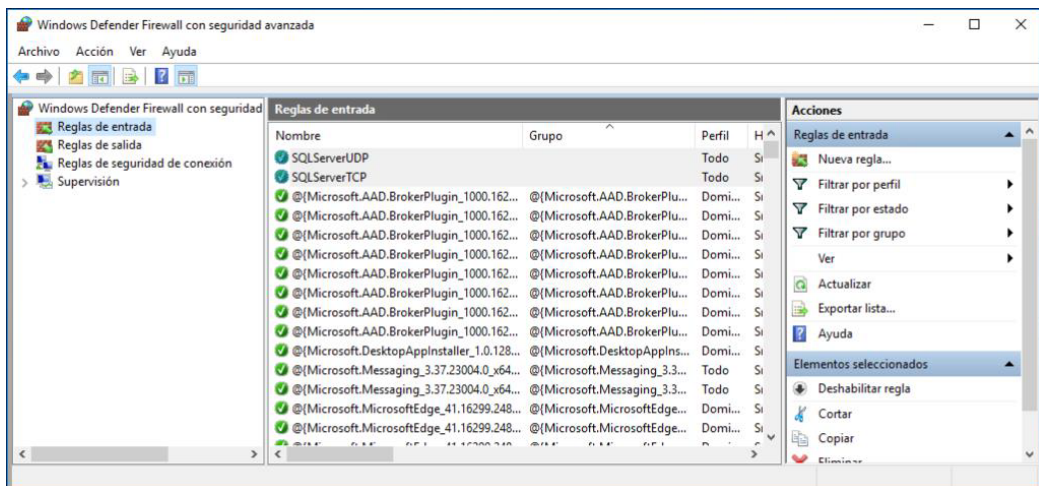
- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

Nombre:

Descripción (opcional):

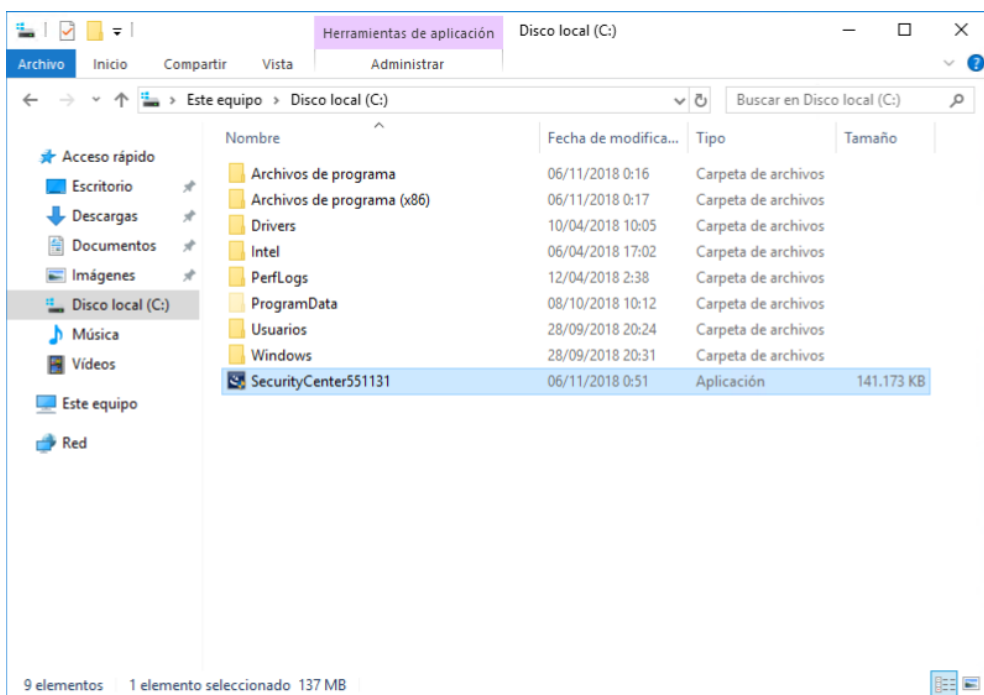
< Atrás **Finalizar** Cancelar

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



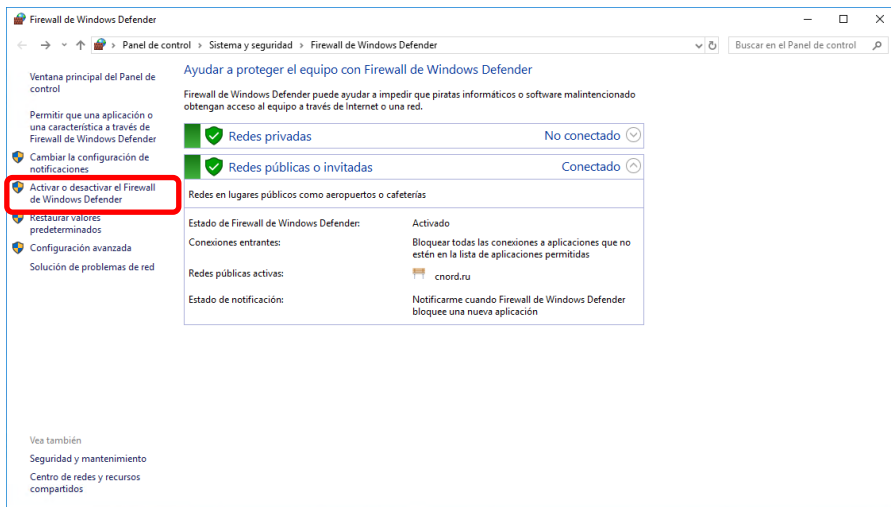
2.4 Instalación del Security Center

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:\

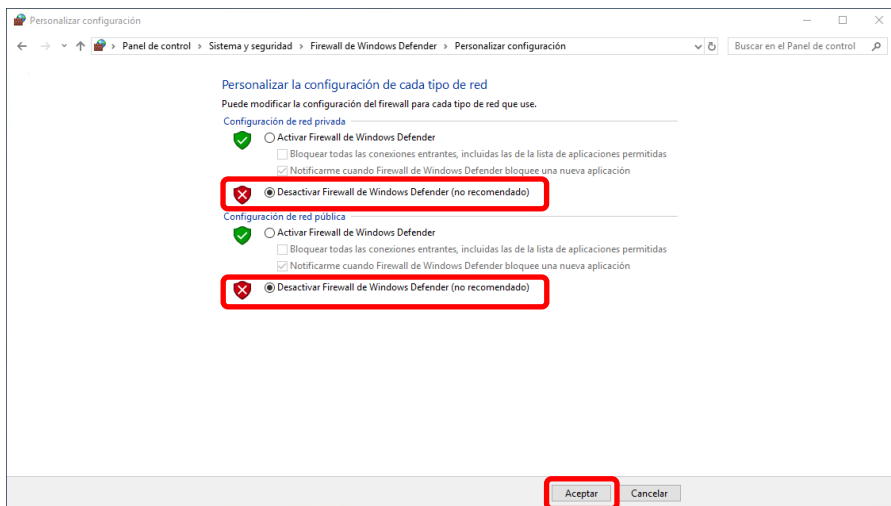


Antes de iniciar la instalación del SC modificar las siguientes configuraciones del SO (en el ejemplo de Win10)

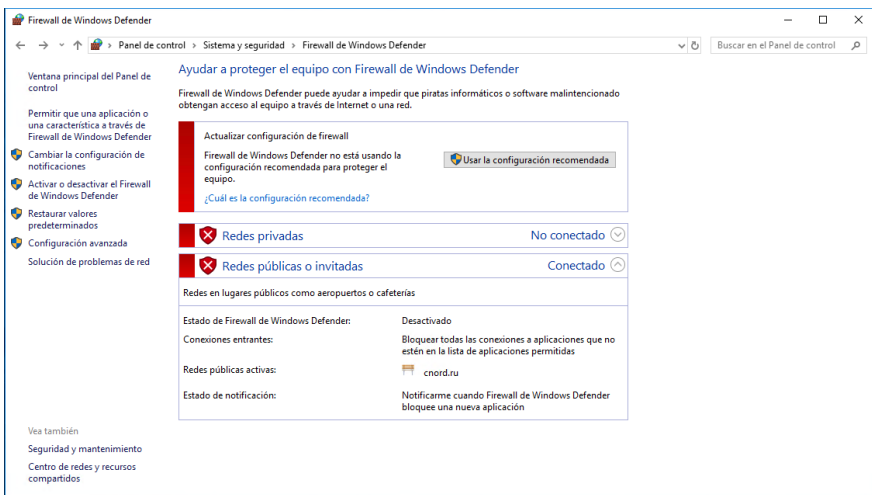
3. Seguir al Panel de control -> Firewall de Window Defender -> Activar o desactivar el Firewall de Windows Defender



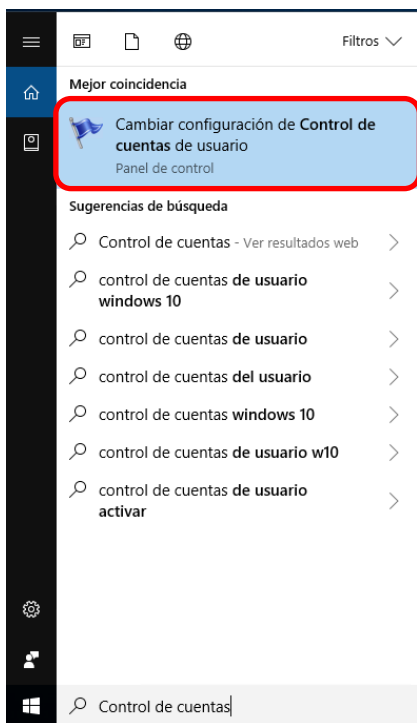
4. Marcar la opción **Desactivar Firewall de Windows Defender** en Configuraciones de red privada y red pública. Presionar **Aceptar**.



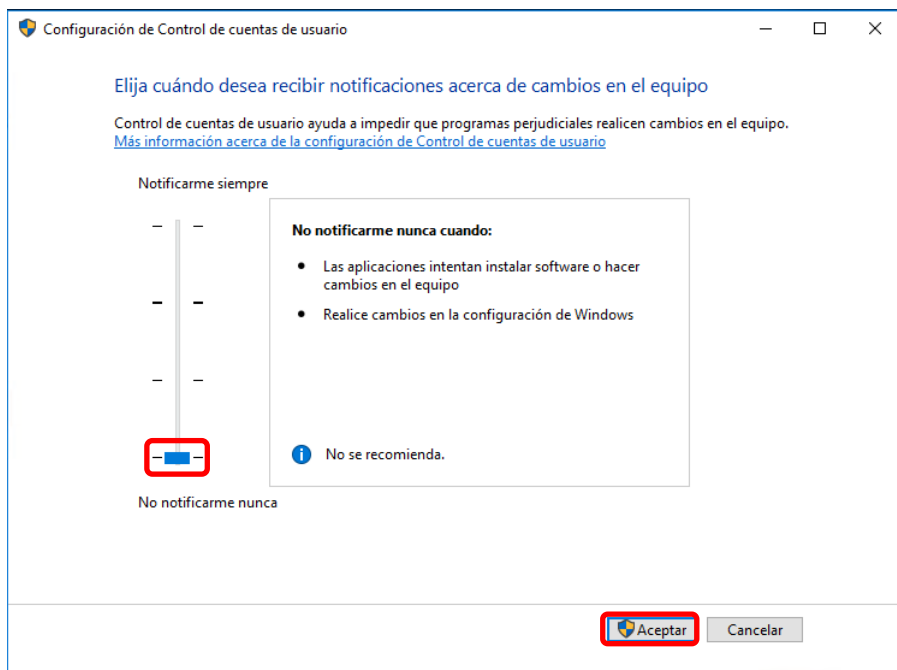
5. La configuración del **Firewall de Windows Defender** está finalizada



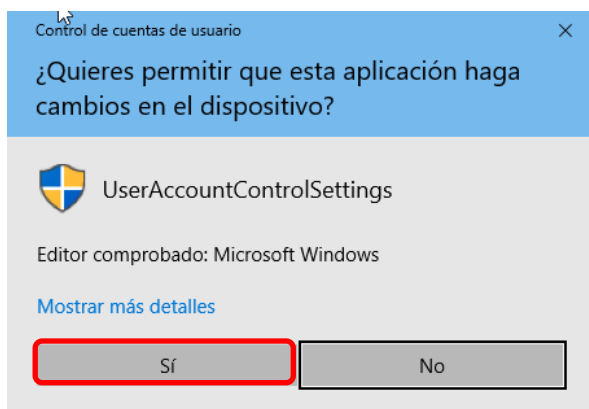
6. En la barra de búsqueda ingresar “Control de cuentas” y en los resultados seleccionar la opción **Cambiar configuración de Control de cuentas de usuario**



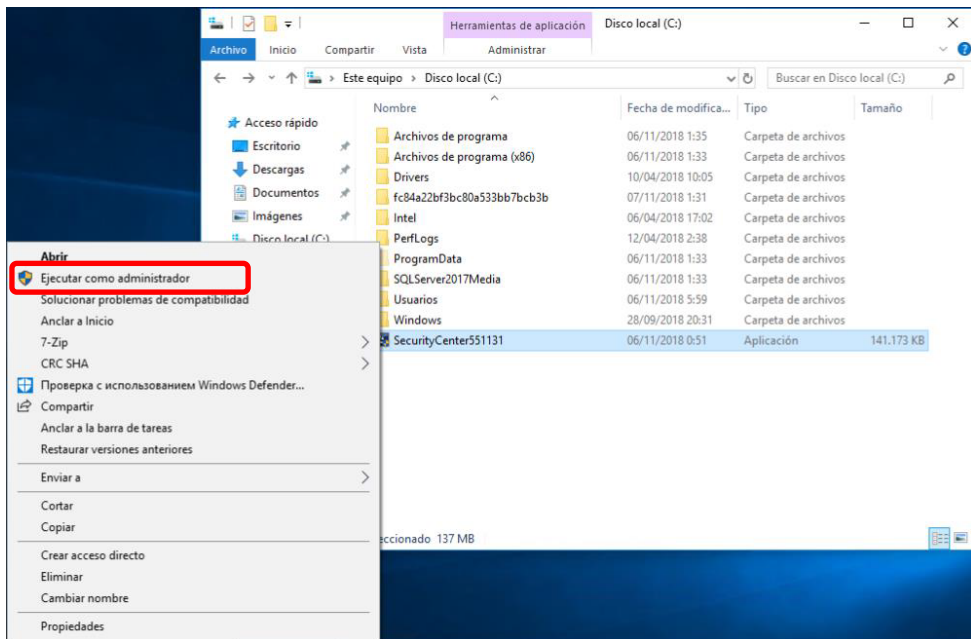
7. Con el control deslizante desactivar el recibo de notificaciones acerca de cambios en el equipo y presionar **Aceptar**



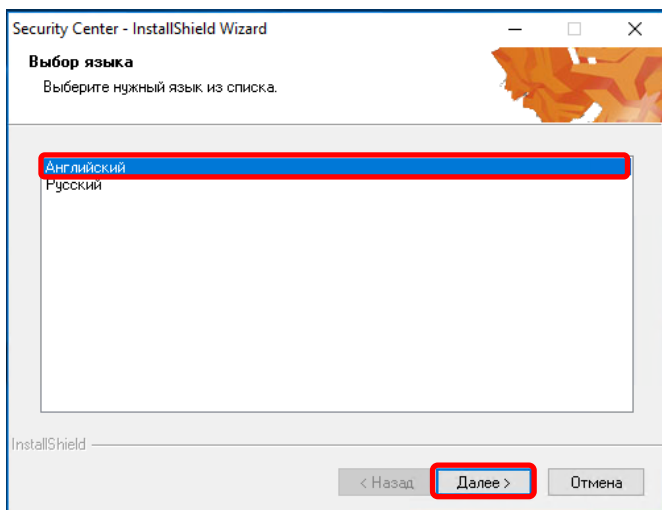
8. Aceptar los cambios en la ventana emergente



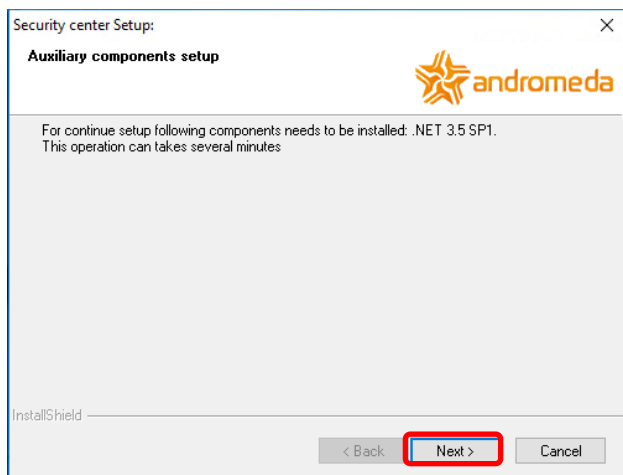
9. Ejecutar el archivo C:\SecurityCenterXXXXXX.exe como administrador



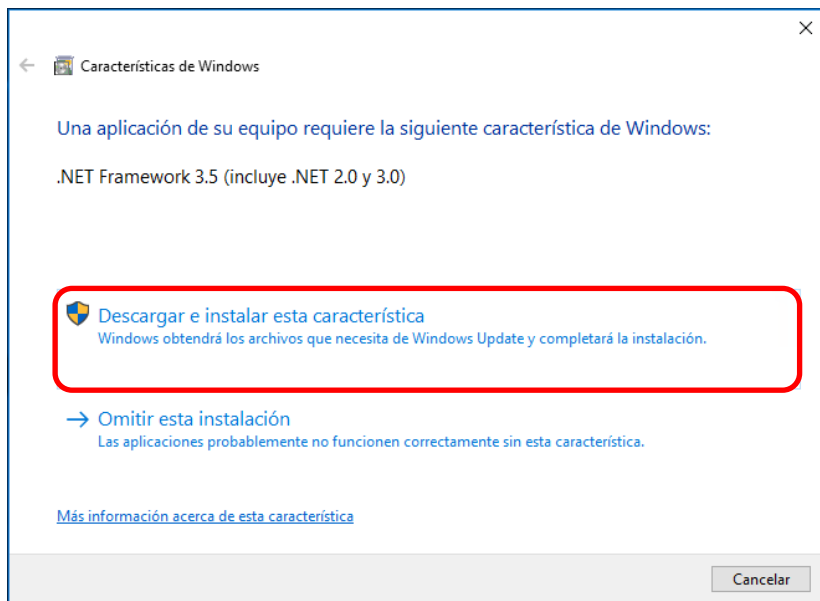
10. En la siguiente ventana seleccionar **inglés** como el idioma del instalador y presionar **Siguiente**



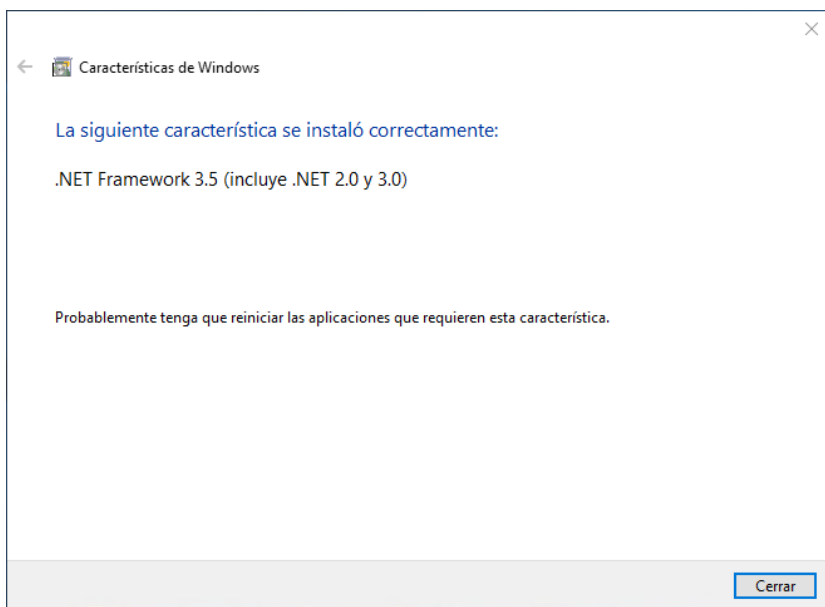
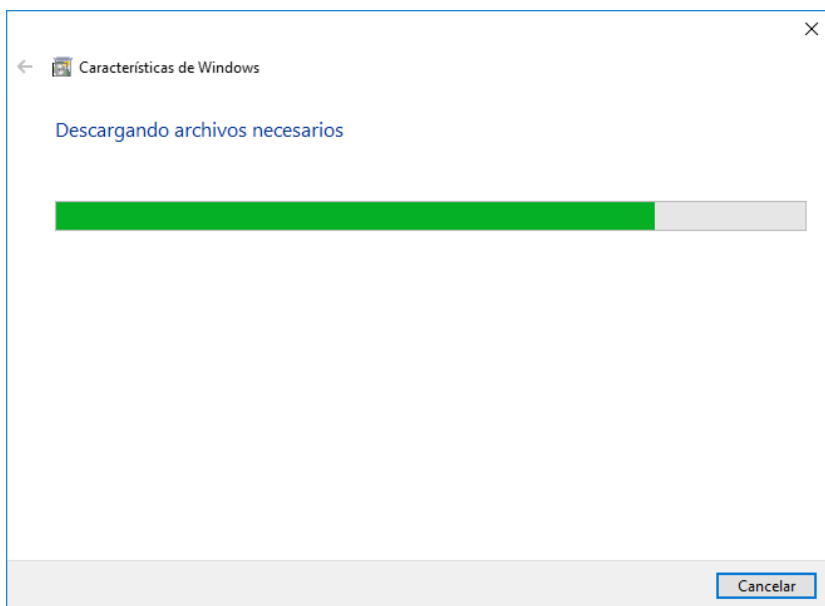
11. Presionar **Next** para instalar **.NET Framework 3.5**



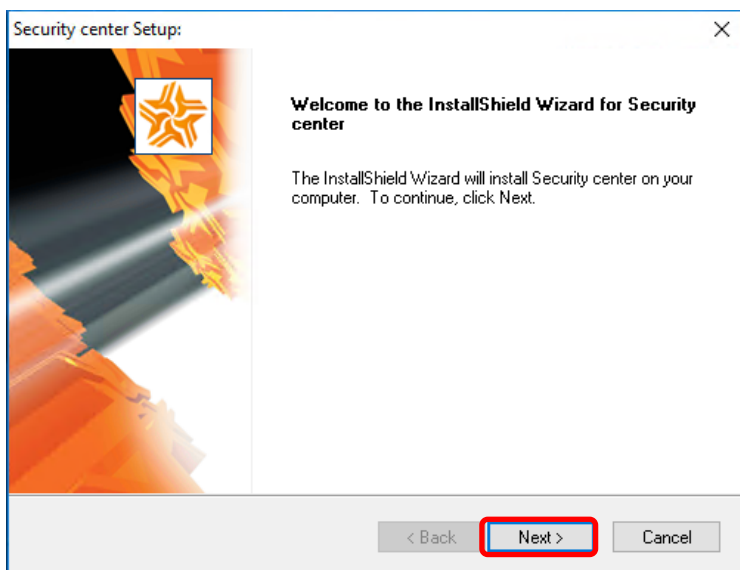
12. Presionar **Descargar e instalar esta característica**



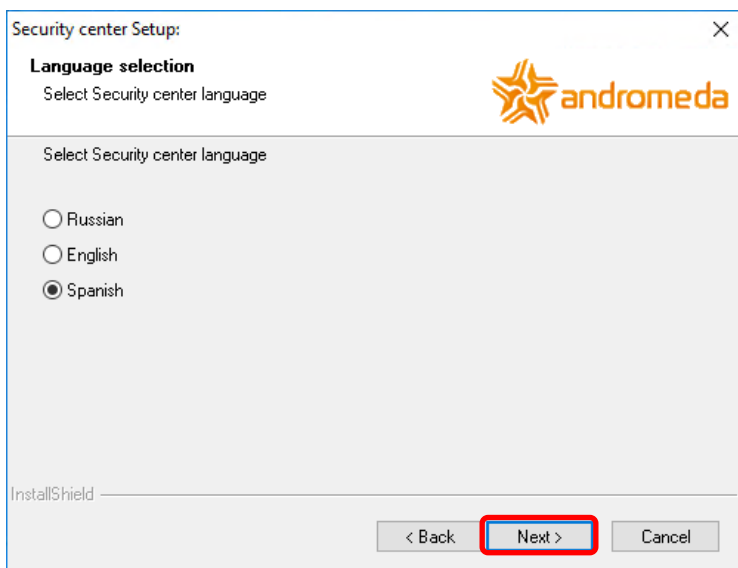
13. Espere mientras se descarguen e instalen los archivos necesarios



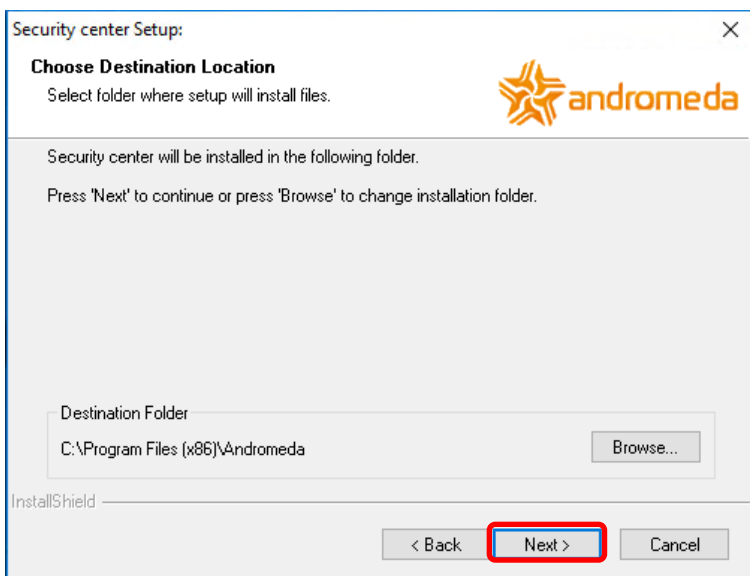
14. En la siguiente ventana presionar **Next**



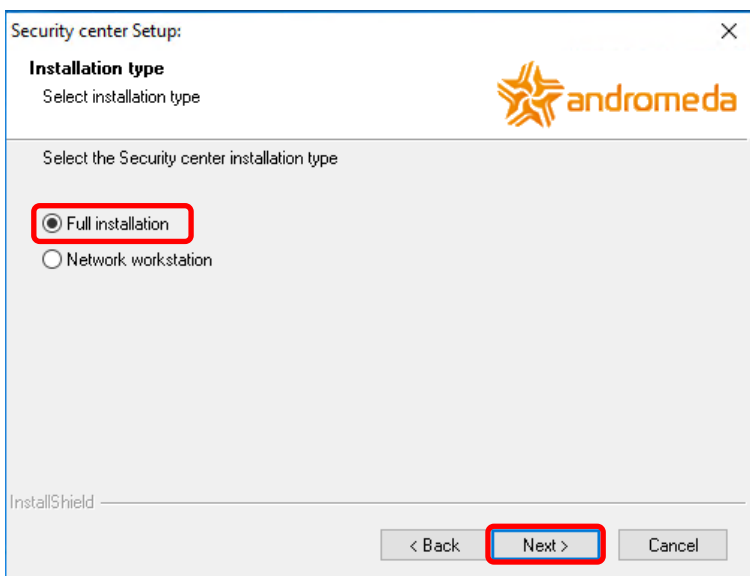
15. Elidir el idioma del Security Center y presionar **Next**



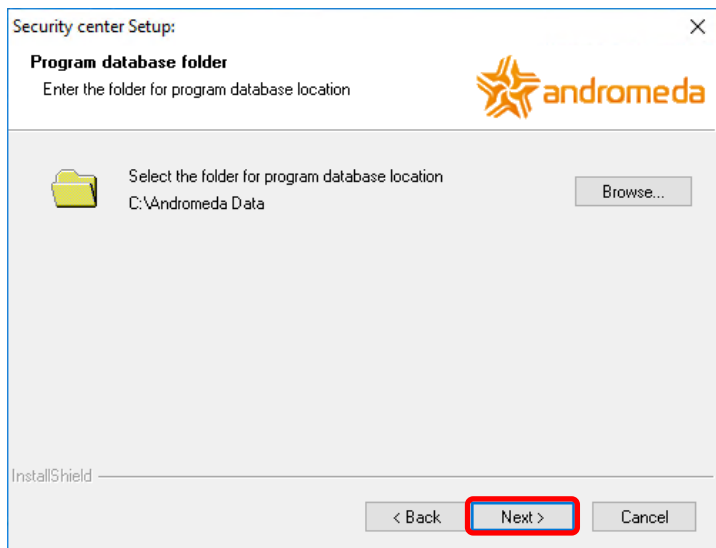
16. Confirmar la carpeta de destino presionando **Next**



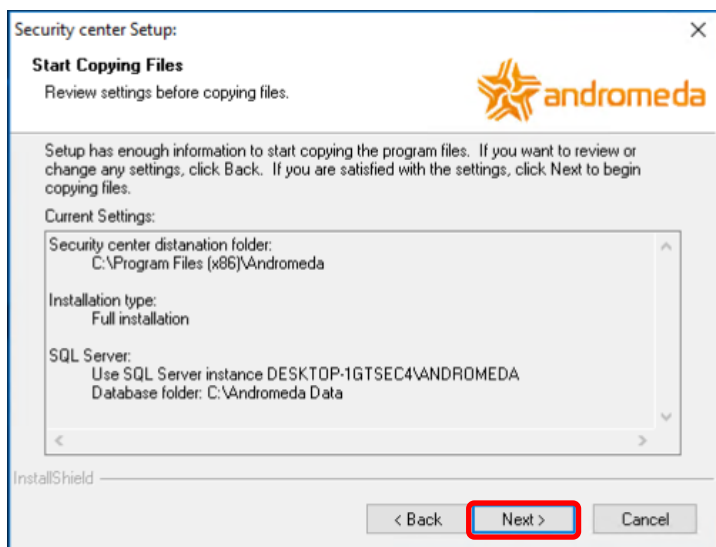
17. Seleccionar **Instalación completa** y oprimir **Next**



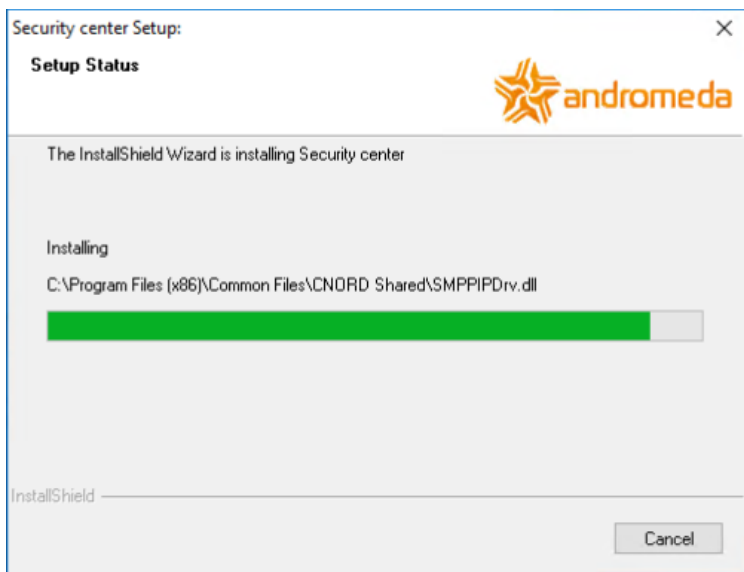
18. Confirmar la carpeta para instalación de la base de datos SQL oprimiendo **Next**



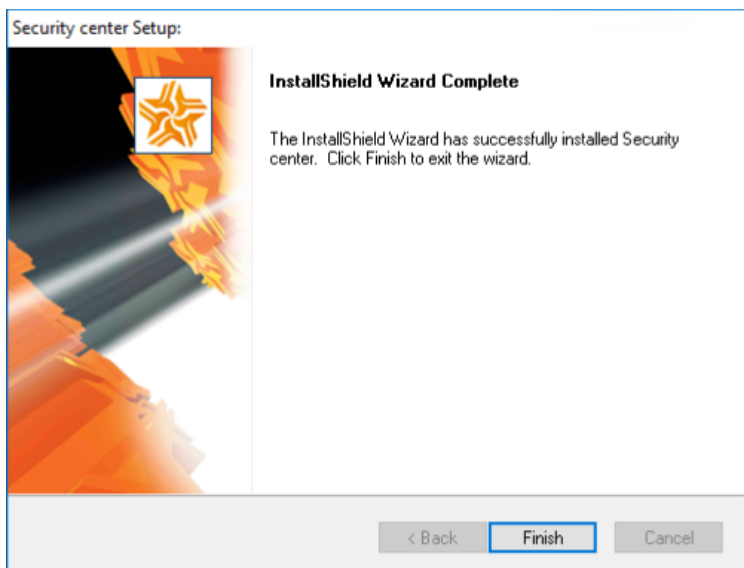
19. Verificar la informacion en la siguiente ventana y presionar **Next**



20. Esperar hasta el final de la instalación.



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

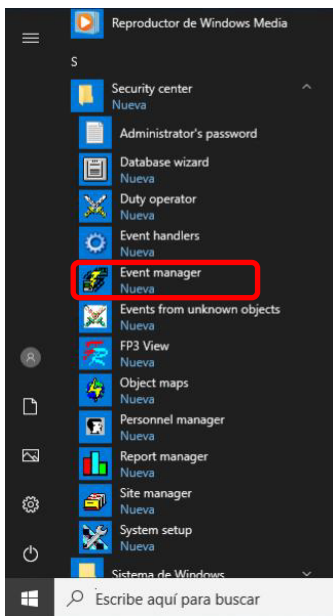


Ahora se puede volver a activar el **Firewall de Windows Defender**.

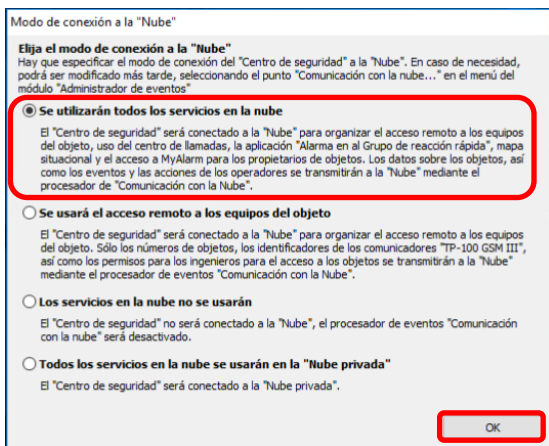
2.5 Configuración y puesta en marcha del Security Center

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"

¡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. 412, ap. 5, lit. A, oficina 13.

Continuar Cancelar

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

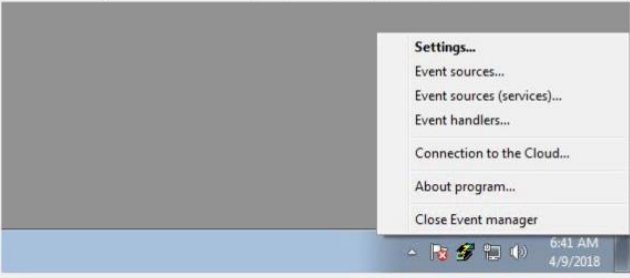
Registro del "Centro de seguridad" en la "Nube"

¡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.

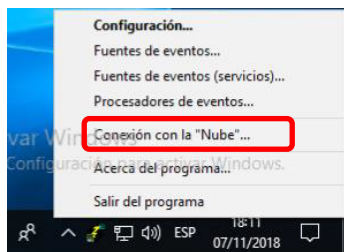
Nueva ventana "Comunicación con la nube"

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

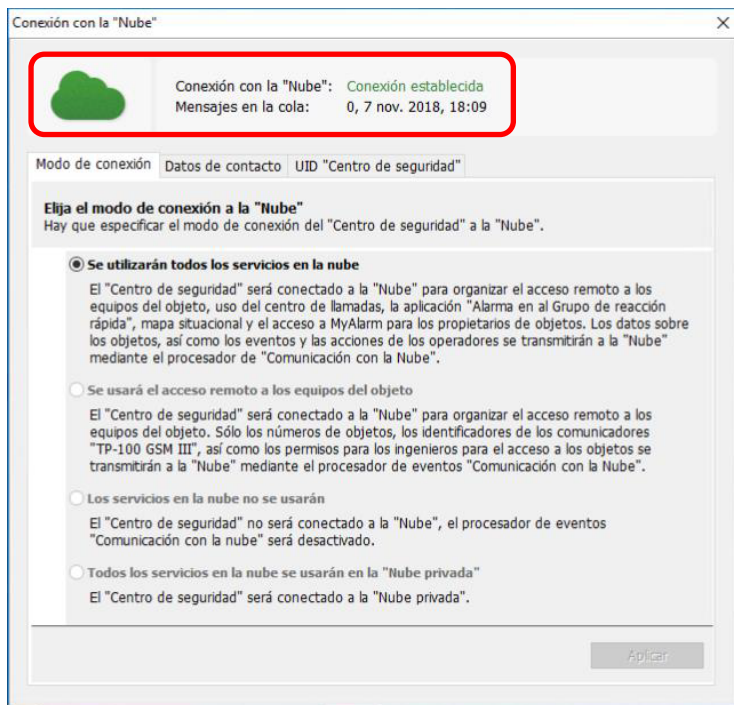


Cerrar

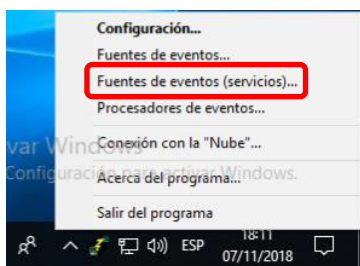
5. Para verificar que el Security Center se conectó a la Nube C.Nord hacer click derecho en el icono del **Administrador de eventos** que se encuentra en la parte derecha de la barra de tareas y elegir **Conexión con la "Nube"** desde el menú deslizante.



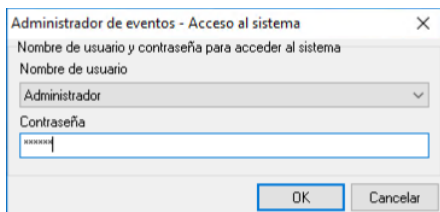
En la ventana emergente aparecerá el estado de la conexión con la **Nube C.Nord**. Se puede cerrar la ventana.



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

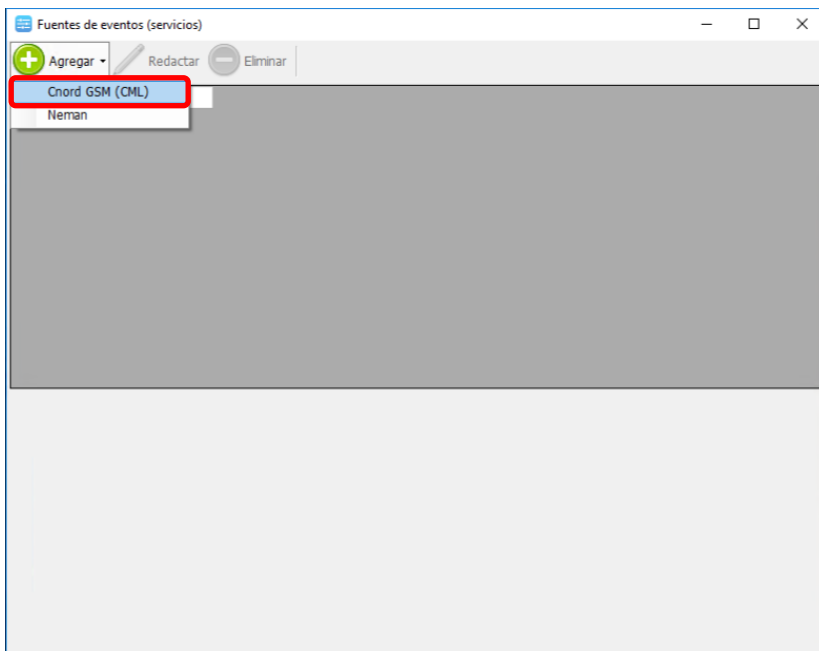


7. En la siguiente ventana ingresar el código del Administrador que por defecto es “222222”.



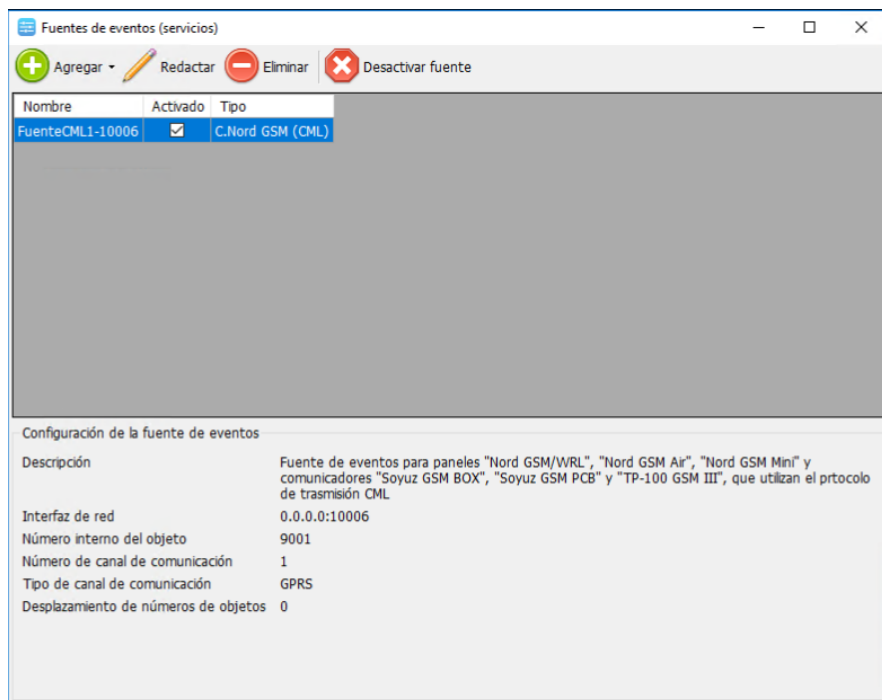
NB! Para poder configurar el SC para la recepción de los eventos directamente desde los paneles mediante el canal GSM-GPRS o Ethernet el servidor (PC) donde se instaló el SC debe tener la conexión al Internet con la IP pública (en vez de IP se recomienda usar el nombre DNS). Además de la IP habrá que 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)**

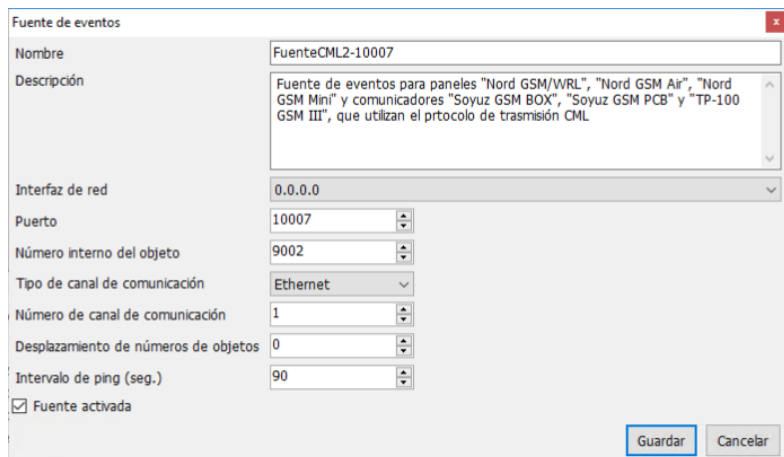


9. En la ventana que aparecerá ingresar el **Nombre** de la fuente, el **Puerto** (para evitar conflictos con los puertos usados en el SO Windows se recomienda usar el valor del puerto que sea superior a 10000), **Número interno del objeto** (que es el numero del objeto en la base de datos del SC) y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

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

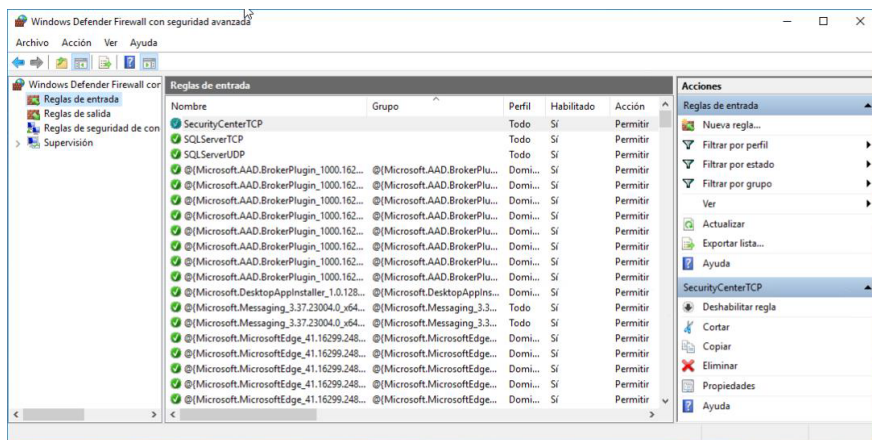


10. Vamos a agregar la segunda fuente para el canal Ethernet. Para eso repetimos los pasos 8 y 9.



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

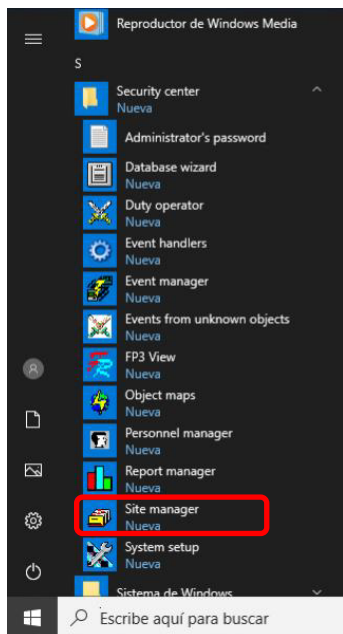


14. Si todo está configurado correctamente los paneles se conectarán automáticamente al **Security Center** y en el Panel de estado en **Hubble** se visualizará el estado de la conexión

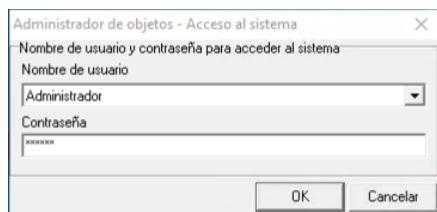


2.5.2 Adición de nuevos objetos en Administrador de objetos

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



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



Administrador de objetos - Acceso al sistema

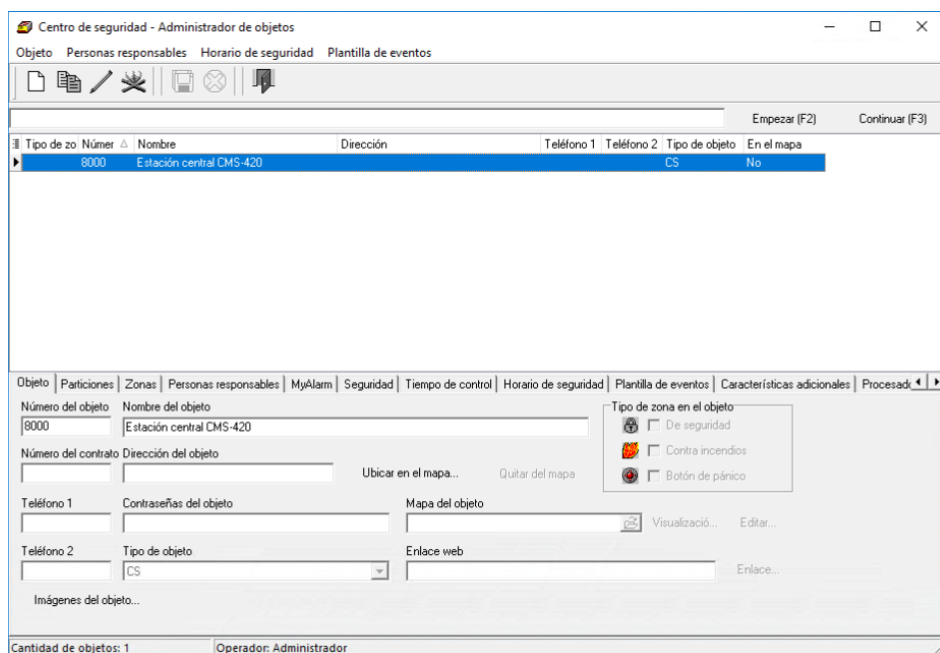
Nombre de usuario y contraseña para acceder al sistema

Nombre de usuario
Administrador

Contraseña
XXXXXX

OK Cancelar

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



Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Empezar (F2) Continuar (F3)

Tipo de zo	Númer	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
	8000	Estación central CMS-420				CS	No

Objeto Particiones Zonas Personas responsables MyAlarm Seguridad Tiempo de control Horario de seguridad Plantilla de eventos Características adicionales Procesad

Número del objeto Nombre del objeto

8000 Estación central CMS-420

Número del contrato Dirección del objeto

Ubicar en el mapa... Quitar del mapa

Teléfono 1 Contraseñas del objeto Mapa del objeto

Teléfono 2 Tipo de objeto Enlace web

Imágenes del objeto...

Tipo de zona en el objeto

- ☐ De seguridad
- ☐ Contra incendios
- ☐ Botón de pánico

Visualizació... Editar...

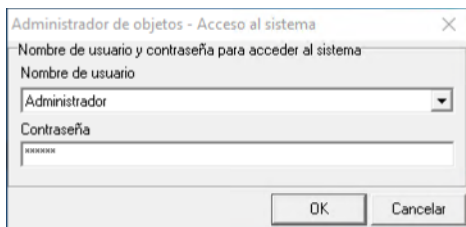
Enlace...

Cantidad de objetos: 1 Operador: Administrador

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.

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



Administrador de objetos - Acceso al sistema

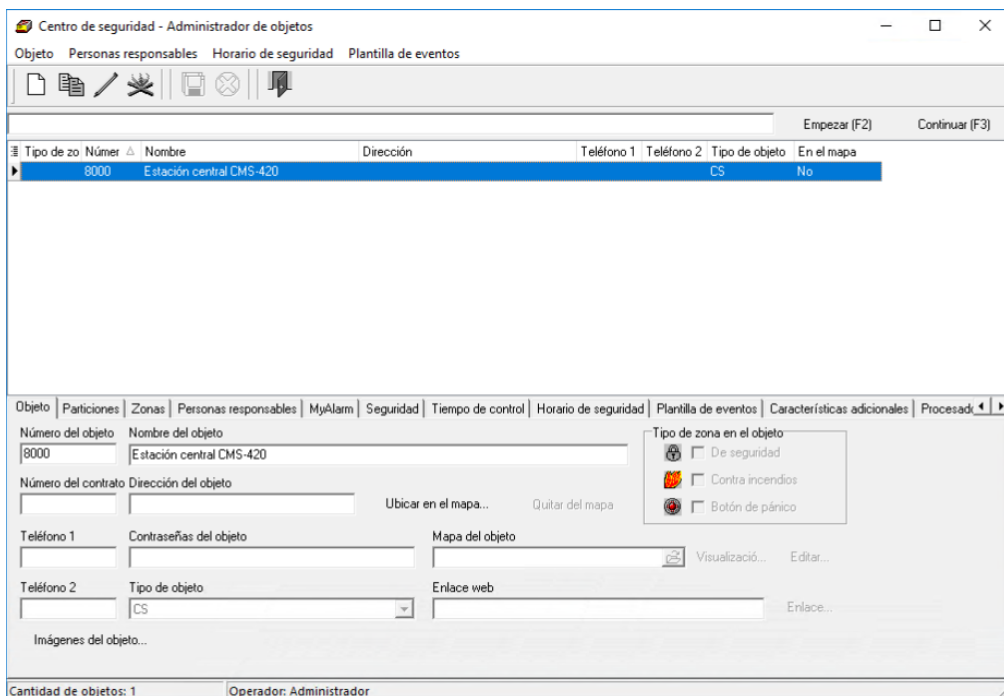
Nombre de usuario y contraseña para acceder al sistema

Nombre de usuario
Administrador

Contraseña
222222

OK Cancelar

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



Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Empezar (F2) Continuar (F3)

Objeto	Número	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
8000	Estación central CMS-420					CS	No

Objeto | Particiones | Zonas | Personas responsables | MyAlarm | Seguridad | Tiempo de control | Horario de seguridad | Plantilla de eventos | Características adicionales | Procesado

Número del objeto: 8000 Nombre del objeto: Estación central CMS-420

Número del contrato: Dirección del objeto: Ubicar en el mapa... Quitar del mapa

Teléfono 1: Contraseñas del objeto: Mapa del objeto: Visualización... Editar...

Teléfono 2: Tipo de objeto: CS Enlace web: Enlace...

Imágenes del objeto...

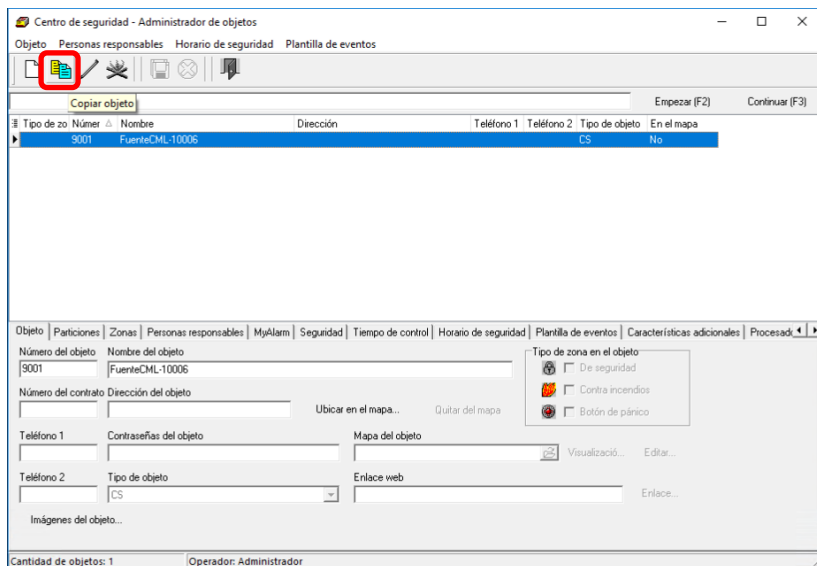
Tipo de zona en el objeto

- ☐ De seguridad
- ☐ Contra incendios
- ☐ Botón de pánico

Cantidad de objetos: 1 Operador: Administrador

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.



Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Copiar objeto Empezar (F2) Continuar (F3)

Tipo de zo	Númer	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
	9001	FuenteCML-10006				CS	No

Objeto | Particiones | Zonas | Personas responsables | MyAlarm | Seguridad | Tiempo de control | Horario de seguridad | Plantilla de eventos | Características adicionales | Procesado

Número del objeto: 9001 Nombre del objeto: FuenteCML-10006

Número del contrato: Dirección del objeto: Ubicar en el mapa... Quitar del mapa

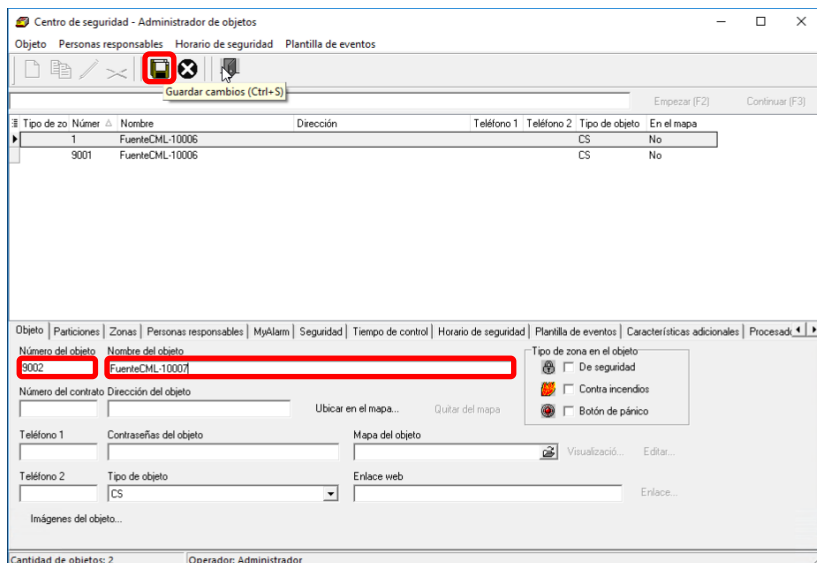
Teléfono 1: Contraseñas del objeto: Mapa del objeto: Visualizació... Editar...

Teléfono 2: Tipo de objeto: CS Enlace web: Enlace...

Imágenes del objeto...

Cantidad de objetos: 1 Operador: Administrador

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



Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Guardar cambios (Ctrl+S) Empezar (F2) Continuar (F3)

Tipo de zo	Númer	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
	1	FuenteCML-10006				CS	No
	9001	FuenteCML-10006				CS	No

Objeto | Particiones | Zonas | Personas responsables | MyAlarm | Seguridad | Tiempo de control | Horario de seguridad | Plantilla de eventos | Características adicionales | Procesado

Número del objeto: 9002 Nombre del objeto: FuenteCML-10007

Número del contrato: Dirección del objeto: Ubicar en el mapa... Quitar del mapa

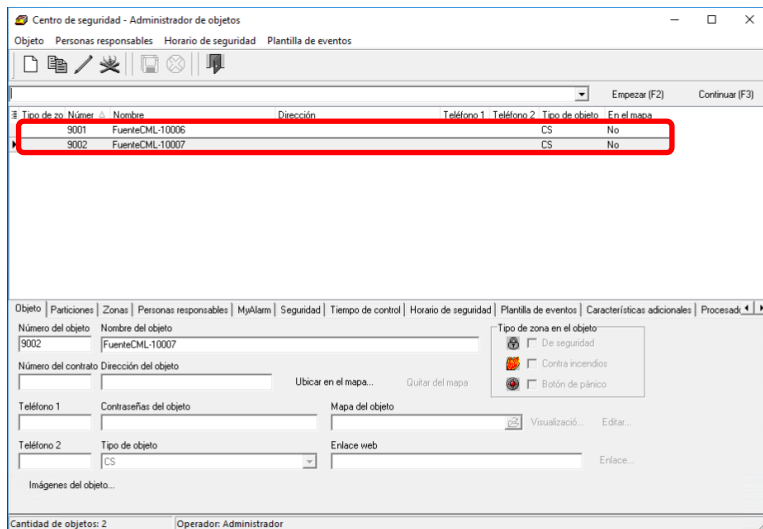
Teléfono 1: Contraseñas del objeto: Mapa del objeto: Visualizació... Editar...

Teléfono 2: Tipo de objeto: CS Enlace web: Enlace...

Imágenes del objeto...

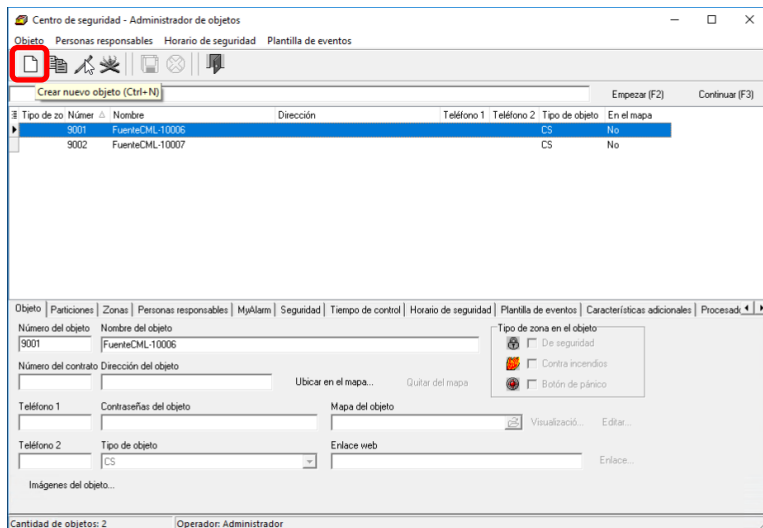
Cantidad de objetos: 2 Operador: Administrador

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"**

Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Empezar (F2) Continuar (F3)

Tipo de zo	Número	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
	1	Nuevo objeto				Apartamento	No
	9001	FuenteCML-10006				CS	No
	9002	FuenteCML-10007				CS	No

Objeto Particiones Zonas Personas responsables MyAlarm Seguridad Tiempo de control Horario de seguridad Plantilla de eventos Características adicionales Procesado

Número del objeto: 1 Nombre del objeto: Nord GSM WRL-1

Número del contrato: Dirección del objeto: Ubicar en el mapa... Quitar del mapa

Teléfono 1: Contraseñas del objeto: Mapa del objeto: Visualizació... Editar...

Teléfono 2: Tipo de objeto: Apartamento Enlace web: Enlace...

Imágenes del objeto...

Cantidad de objetos: 3 Operador: Administrador

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

Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Empezar (F2) Continuar (F3)

Tipo de zo	Número	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
	1	Nuevo objeto				Apartamento	No
	9001	FuenteCML-10006				CS	No
	9002	FuenteCML-10007				CS	No

Objeto Particiones Zonas Personas responsables MyAlarm Seguridad Tiempo de control Horario de seguridad **Plantilla de eventos** Características adicionales Procesado

C-Nord GSM EPAF Agregar evento Editar evento Eliminar evento

Tipo de evento	Partición	Z/U	Descripción del evento
ma			Peligro personal. %part% %zone%
o			%part% %zone%
o			Sensor de humo. %part% %zone%
o			Incendio. %part% %zone%
o			Fuga de agua. %part% %zone%
o			Sensor de temperatura. %part% %zone%
o			Botón "Incendio". %part% %zone%
o			Tubería. %part% %zone%
o			Sensor de llama. %part% %zone%
o			Peligro de incendio. %part% %zone%
o			%part% %zone%

Cualquier E114 Fuego

Cualquier E115 Fuego

Cualquier E116 Fuego

Cualquier E117 Fuego

Cualquier E118 Advertencia

Cualquier E120 Botón de pánico

Cantidad de objetos: 3 Operador: Administrador

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

Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Empezar (F2) Continuar (F3)

Tipo de zo	Número	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
1	Nuevo objeto					Apartamento	No
	9001	FuenteCML-10006				CS	No
	9002	FuenteCML-10007				CS	No

Personas responsables | MyAlarm | Seguridad | Tiempo de control | Horario de seguridad | Plantilla de eventos | Características adicionales | Procesadores de eventos | **Equipo** | Com |

Tipo de equipo

☒ C Nord GSM (CML)

☐ Lonts-202

☐ RS200

☐ Rltm

☐ AlarmView

☐ Puper type 5

☐ Otro

Información del dispositivo

Identificador: <no hay> Eliminar

Este tipo de equipo hay que especificarlo para el objeto que tiene instalados los dispositivos "Nord GSM", "Serzhan GSM", "Soyuz GSM" o el transmisor "TP-100 GSM III".
El valor del parámetro "Identificador del dispositivo" corresponde con el identificador del dispositivo, vinculado con el objeto actualmente.
Al reemplazar el equipo en el objeto hay que eliminar el identificador del dispositivo antiguo vinculado al objeto.

Cantidad de objetos: 3 Operador: Administrador

13. Presionar **Guardar cambios**

Para comprobar que el panel se intercambi6 los datos con el SC con 6xito verificar los valores de los par6metros **Identificador**, **Tipo de dispositivo**, **N6mero de serie**, **Versi6n de firmware** que deber6n aparecer en la pesta6a **Equipo**

Centro de seguridad - Administrador de objetos

Objeto Personas responsables Horario de seguridad Plantilla de eventos

Empezar (F2) Continuar (F3)

Tipo de zo	Número	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
1	Nord GSM wRL-1					Apartamento	No
	9001	FuenteCML-10006				CS	No
	9002	FuenteCML-10007				CS	No

Horario de seguridad | Plantilla de eventos | Características adicionales | Procesadores de eventos | **Equipo** | Comentarios | Acceso a MyAlarm | Enrutadores de v6deo | Servicio |

Tipo de equipo

☒ C Nord GSM (CML)

☐ Lonts-202

☐ RS200

☐ Rltm

☐ AlarmView

☐ Puper type 5

☐ Otro

Informaci6n del dispositivo

Identificador: 38004F000350495358313420 Eliminar

Tipo de dispositivo: **Nord GSM 5.5**

N6mero de serie: [REDACTED]

Versi6n del firmware: **18.10**

Este tipo de equipo hay que especificarlo para el objeto que tiene instalados los dispositivos "Nord GSM", "Serzhan GSM", "Soyuz GSM" o el transmisor "TP-100 GSM III".
El valor del par6metro "Identificador del dispositivo" corresponde con el identificador del dispositivo, vinculado con el objeto actualmente.
Al reemplazar el equipo en el objeto hay que eliminar el identificador del dispositivo antiguo vinculado al objeto.

Cantidad de objetos: 3 Operador: Administrador

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

Tipo de zona	Número	Nombre	Dirección	Teléfono 1	Teléfono 2	Tipo de objeto	En el mapa
1		Nord GSM WRL-1				Apartamento	No
	9001	FuenteCML-10006				CS	No
	9002	FuenteCML-10007				CS	No

Centro de seguridad - Administrador de objetos

Objeto | Personas responsables | Horario de seguridad | Plantilla de eventos

Empezar (F2) Continuar (F3)

Objeto | Particiones | Zonas | Personas responsables | MyAlarm | Seguridad | Tiempo de control | Horario de seguridad | Plantilla de eventos | Características adicionales | Procesado

Número del objeto: 1 Nombre del objeto: Nord GSM WRL-1

Número del contrato: Dirección del objeto: Ubicar en el mapa... Quitar del mapa

Teléfono 1: Contraseñas del objeto: Mapa del objeto: Visualización... Editar...

Teléfono 2: Tipo de objeto: Apartamento Enlace web: Enlace...

Imágenes del objeto...

Cantidad de objetos: 3 Operador: Administrador

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