Comunicador GT

Manual de Instalación

Agosto, 2024

www.trikdis.lt • UAB Trikdis • Draugystės calle. 17, LT-51229 Kaunas, Lituania • +370 37 408 040 • info@trikdis.lt

CONTENIDO

Requerimientos de Seguridad

El sistema de alarma de seguridad deberá ser instalado y mantenido por personal calificado.

Antes de la instalación, por favor lea con cuidado este manual, para poder evitar cualquier error que lleve al mal funcionamiento o incluso daño del equipo.

Desconecte la fuente de alimentación antes de hacer cualquier conexión eléctrica.

Los cambios, modificaciones o reparaciones no están autorizadas por el fabricante, y esto eliminará sus derechos a una garantía.

Por favor actúe de acuerdo a sus reglas locales y no se deshaga de su sistema de alarma sin uso o sus componentes con otro desecho normal de su casa.

1 Descripción

El comunicador está diseñado para transmitir mensajes sobre eventos del panel de control la Centro de Monitoreo y a la aplicación ***Protegus2***.

El comunicador celular ***GT*** se puede conectar directamente a los paneles de control (DSC, Paradox, UTC Interlogix (CADDX), Texecom, Innerrange, Honeywell) o a un comunicador telefónico (que admite el protocolo de comunicación Contact ID transmitido por tonos DTMF) del panel de control.

El comunicador transmite información de eventos completos al Central de Monitoreo (CRA).

El comunicador también funciona con la aplicación ***Protegus2***. Con ***Protegus2***, los usuarios pueden controlar el sistema de alarma de forma remota y obtener notificaciones de cualquier evento de seguridad. La app de ***Protegus2*** es compatible con todos los paneles de control de varios fabricantes que son soportados por el comunicador ***GT***. El comunicador puede transmitir notificaciones de eventos al Central de Monitoreo y trabajar de forma simultánea con ***Protegus2***.

Características

El comunicador GT se puede conectar al bus serie (Serial bus) o al bus de teclado (Keypad bus) o al comunicador telefónico (TIP/RING) del panel de control.

Envía eventos al receptor en una CRA:

- Envía eventos a los receptores de hardware o software TRIKDIS que funcionan con cualquier software de monitoreo.
- Puede enviar información de eventos a SIA DC-09 receptores. El anexo contiene tabla de conversión de los códigos (Contacto ID a SIA).
- Puede enviar información de eventos a SUR-GARD receptores.
- Supervisión de la conexión mediante sondeo al receptor de IP cada 30 segundos (o por período definido por el usuario).
- Canal de respaldo, que se utilizará si se pierde la conexión con el canal primario.
- Con canales de comunicación paralelos se pueden enviar eventos a dos receptores al mismo tiempo.
- Cuando el servicio Protegus está habilitado, los eventos se envían primero a CRA, y solo luego se envían a los usuarios de la aplicación.

Funciona con la aplicación Protegus2:

- Notificaciones de sonidos especiales y "Push" que informan sobre eventos.
- Armado/Desarmado de forma remota.
- Control remoto de dispositivos conectados (luces, portones/barreras, sistemas de ventilación, calefacción, aspersores, etc.).
- Diferentes derechos de usuario para administrador, instalador y usuario.

Informes a los usuarios finales:

- Los usuarios pueden recibir notificaciones de eventos usando la aplicación ***Protegus2***.

Salidas y entradas controlables:

- 2 entradas/salidas universales. Modo de funcionamiento se establece como entrada o salida.
- Salidas controladas por ***Protegus2***.
- Agregue adicionales controladas entradas/salidas con expansor ***iO-8***.

Configuración rápida:

- Las configuraciones pueden guardarse en un archivo y escribirse rápidamente en otros comunicadores.
- Dos niveles de acceso para configurar el dispositivo para el administrador de CRA y para el instalador.
- Configuración remota y actualización de firmware.

1.1 Lista de paneles de Control compatibles

Fabricante	Modelo
DSC®	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020
PARADOX®	SPECTRA SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+
	MAGELLAN MG5000, MG5050, MG5050E, MG5075, MG5050+
	DIGIPLEX EVO48, EVO192, EVOHD, EVOHD+
	SPECTRA 1727, 1728, 1738
	ESPRIT E55
UTC Interlogix®	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom®	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Innerrange®	Inception, Integriti
Honeywell®	Ademco Vista-15, Ademco Vista-20, Ademco Vista-48

Subrayado - paneles de control controlados directamente por ***GT***. Paneles de control Paradox, que se controlan directamente, debe contener la versión de firmware V.4 o superior.

*Los paneles de control de otros fabricantes se conectan al comunicador ***GT*** a través de un comunicador telefónico (que admite el protocolo de comunicación Contact ID transmitido por tonos DTMF) del panel de control.

1.2 Tipos de Comunicador

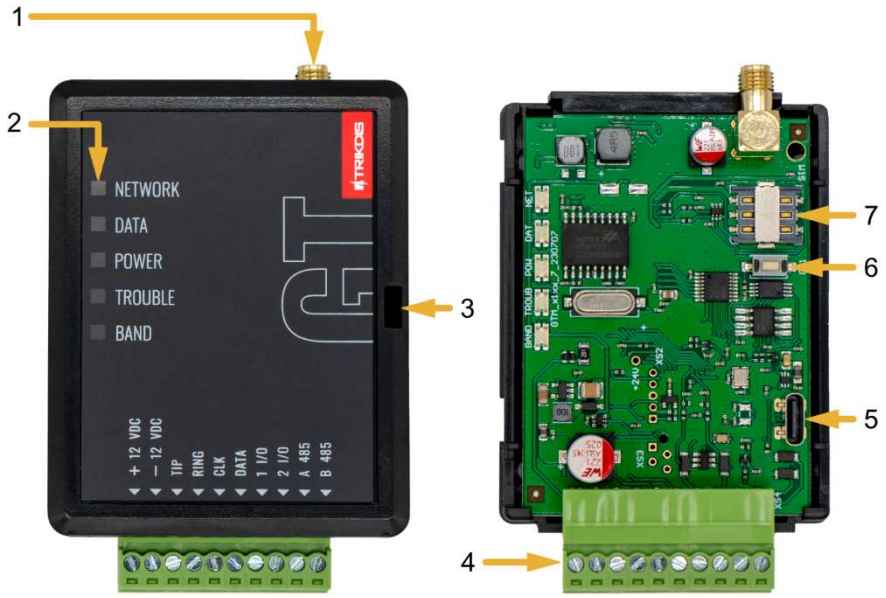
Este manual es para comunicadores 4G.

1.3 Especificaciones

Parámetro	Descripción
Conexión al panel de control	Bus serie, bus de teclado o TIP RING
Entradas /Salidas universales	2, se puede establecer ya sea como entrada IN con el tipo: NC, NO, NC con EOL, NO con EOL, NC con DEOL, NO con DEOL (EOL = 2,2 kΩ), o la salida OUT (colector abierto (OC) hasta 0,15 A, hasta 30 V CC). Con los expansores ***iO-8***, puede agregar entradas y salidas adicionales.
Modem EG915U-EU (Europa)	LTE FDD: B1/B3/B5/B7/B8/B20/B28
	GSM: B2/B3/B5/B8
Modem EG915U-LA (América Latina)	LTE FDD: B2/B3/B4/B5/B7/B8/B28/B66
	GSM: B2/B3/B5/B8
Modem BG95-M5 (Cat M1)	LTE-FDD: B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B27/B28/B66/B85
	EGPRS: 850/900/1800/1900 MHz
Voltaje de la fuente de alimentación	10-32 V DC
Consumo de corriente	125 mA
Protocolos de Transmisión	TRK8, DC-09_2007, DC-09_2012, TL150
Encriptación del mensaje	AES 128
Memoria de eventos no enviados	Hasta 60 eventos
Modificación de los ajustes	Con el software de configuración ***TrikdisConfig*** de forma remota o local a través del puerto USB-C

Parámetro	Descripción
Entorno de Operación	Temperatura de -10 °C a +50 °C, humedad relativa - desde 80% a +20 °C
Dimensiones del Comunicador	92 x 62 x 25 mm
Peso	80 g

1.4 Tablero del Comunicador



1. Antena GSM conector SMA.
2. Luces Indicadoras.
3. Ranura Frontal de Apertura de la Cubierta.
4. Terminal para conexiones externas.
5. Puerto USB-C para la programación del comunicador.
6. Botón “RESET”.
7. Ranura Tarjeta SIM.

1.5 Propósito de las terminales

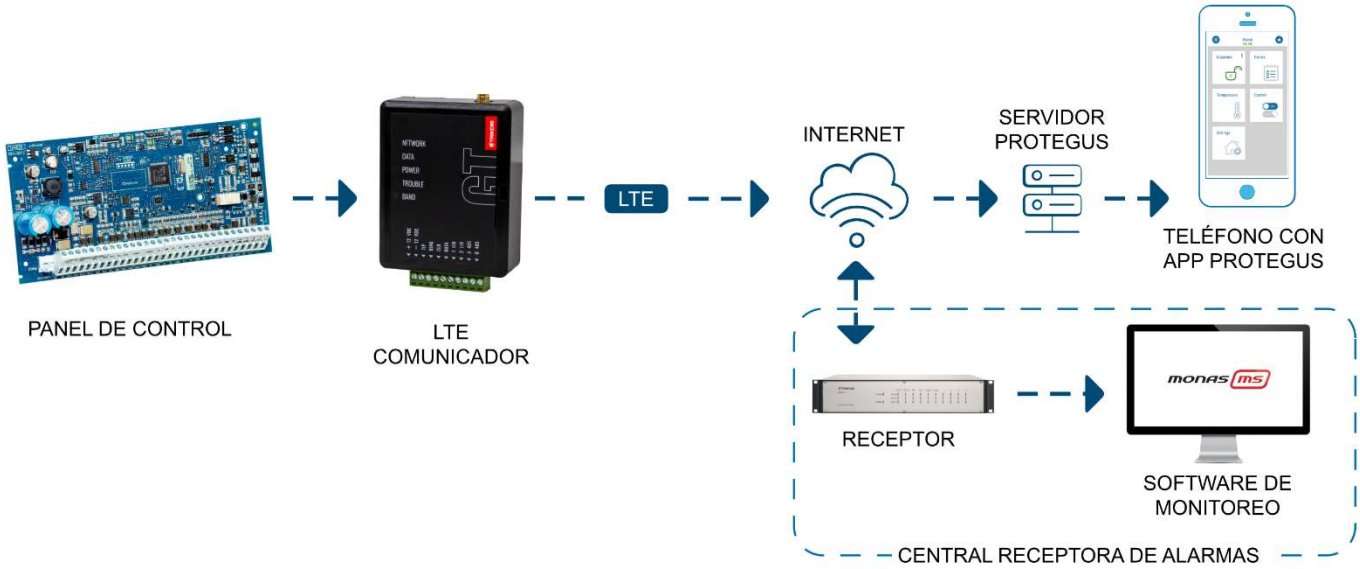
Terminal	Descripción
+12 VDC	Terminal de conexión de alimentación (terminal positivo de 10-32 V CC)
-12 VDC	Terminal de conexión de alimentación (terminal negativo 10-32V CC)
TIP	Terminal para conectar con panel de control TIP terminal
RING	Terminal para conectar con panel de control RING terminal
CLK	Terminal de bus serial para conexión directa al panel de control
DATA	
1 I/O	1r terminal de entrada/salida (configuración predeterminada - IN, NO circuito)
2 I/O	2do terminal de entrada/ salida (configuración predeterminada - IN, NO circuito)
A 485	Contacto RS485 para conectar expansores ***iO-8***
B 485	

1.6 LED indicador de operación

Indicador	Estado de la luz	Descripción
NETWORK	Off	Sin conexión a la red celular
	Amarillo parpadeando	Conectándose a la red celular
	Verde sólido con parpadeo amarillo	El comunicador está conectado a la red celular. La potencia de la señal celular suficiente para el nivel 3 de 3G/4G (tres parpadeos amarillos)

Indicador	Estado de la luz	Descripción
DATA	Off	No hay eventos no enviados
	Verde sólido	Los eventos no enviados se almacenan en el búfer
	Verde parpadeando	**(Modo de configuración)** Los datos se transfieren a/desde el comunicador
POWER	Off	La fuente de alimentación está apagada o desconectada
	Verde sólido	La fuente de alimentación está encendida con suficiente voltaje
	Amarillo sólido	La tensión de alimentación es insuficiente (≤11.5V)
	Verde sólido y parpadeo amarillo	**(Modo de configuración**) Comunicador está listo para la configuración
	Amarillo sólido	**(Modo de configuración)** No hay conexión con la computadora
TROUBLE	Off	No hay problemas de operación
	1 parpadeo rojo	Tarjeta SIM no encontrada
	2 parpadeos rojos	Problema con el código PIN de la tarjeta SIM (código PIN incorrecto)
	3 parpadeos rojos	Problema de programación (No APN)
	4 parpadeos rojos	Problema con el registro a la red GSM
	5 parpadeos rojos	Problemas con el registro a la red GPRS/UMTS
	6 parpadeos rojos	No hay conexión con el receptor
	7 parpadeos rojos	Conexión perdida con el panel de control
	8 parpadeos rojos	El número ICCID ingresado no coincide con el número ICCID de la tarjeta SIM
	Parpadeo rojo	**(Modo de configuración**) Fallo de memoria
	Rojo sólido	**(Modo de configuración)** El firmware está dañado
BAND	1 parpadeo verde	Ninguna
	2 parpadeos verdes	GSM
	3 parpadeos verdes	GPRS
	4 parpadeos verdes	EDGE
	5 parpadeos verdes	HSDPA, HSUPA, HSPA+, WCDMA
	6 parpadeos verdes	LTE TDD, LTE FDD

1.7 Esquema estructural del uso del dispositivo GT



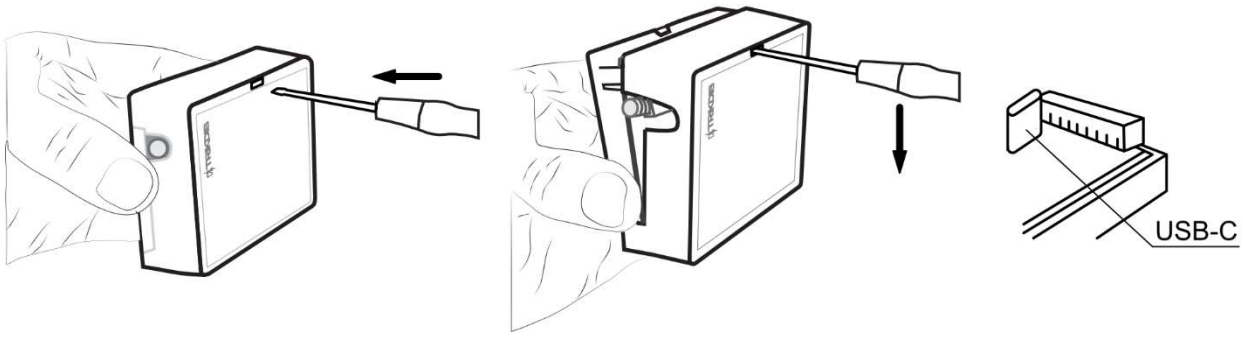
Nota: Antes de la instalación, asegúrese de tener:

1. Cable USB-C para configuración.
2. Cable de 4 hilos para conexión al panel de control.
3. Cable CRP2 para conexión al puerto serie del panel de control Paradox.
4. Destornillador de hoja plana de 2,5 mm.
5. Antena GSM externa si la conexión es débil.
6. Tarjeta SIM activada (la solicitud del código PIN se puede desactivar).
7. Instrucciones para el panel de control al que se conectará el comunicador.

Puede solicitar los materiales necesarios a su proveedor local.

2 ¿Cómo configurar el comunicador con el software de TrikdisConfig?

1. Descargue el software de ***TrikdisConfig*** de www.trikdis.com (en la barra de búsqueda ponga TrikdisConfig) e instálelo.
2. Abra la cubierta del ***GT*** con el desatornillador de cabeza plana como se muestra a continuación:



3. Usando el cable USB-C conecte el ***GT*** a la computadora.
4. Abra el programa de configuración de ***TrikdisConfig***. El software reconocerá de forma automática el comunicador conectado y abrirá una ventana para su configuración.
5. De clic en Read (F4) para leer la información sobre los parámetros del comunicador e ingrese el código del Administrador o del Instalador en la ventana saliente.

A continuación, habrá una descripción de las opciones que necesitan ser configurados para el comunicador, para que este empiece a enviar notificaciones al CRA y para permitir que el control de seguridad sea controlado por la app de ***Protegus2***.

2.1 Configuración para conectarse a la aplicación Protegus2

En la ventana de "Configuración del panel":

1. Si el comunicador está conectado a los terminales TIP/RING del panel de control, entonces debe configurarse en "**Dual tone**".

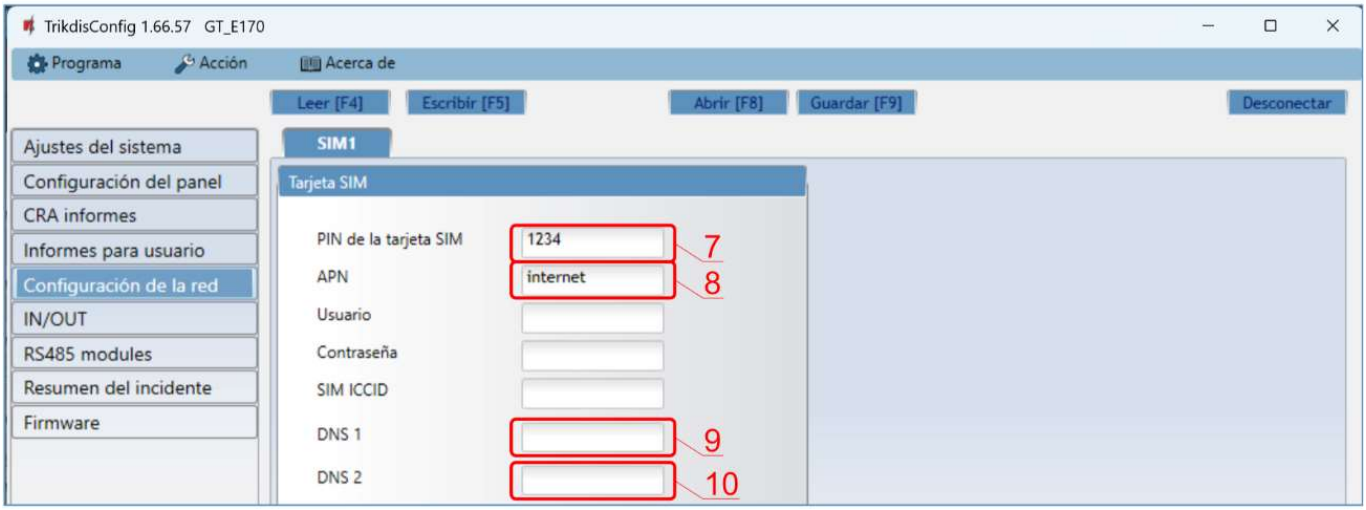
2. Si el comunicador está conectado al bus del teclado o al bus serie del panel de control, seleccione el modelo de panel de control que se conectará al comunicador.
3. Marque la casilla "**Control directo**" si desea que el usuario pueda controlar el panel de control con un código (código de usuario del panel de control) y la aplicación ***Protegus2***. Esta configuración se especifica para paneles de seguridad con control directo.
4. Para controlar directamente los paneles de control de Paradox y Texecom, ingrese la "**Contraseña de descarga de PC**". El código debe coincidir con el código ingresado en el panel de control.

Nota:	Para que funcione el control directo del panel, usted necesitará cambiar las opciones del panel. El cómo hacer esto está descrito en el capítulo 4 "Programando el panel de control para leer eventos y tener control directo". En esta sección usted encontrará información de como cambiar la contraseña de la descarga de PC/UDL.

Ventana de "Informes para usuario", pestaña de "Servicio Protegus":

5. Habilitar la conexión a la "**Servicio Protegus**".
6. Cambie el Código de acceso de la nube para iniciar sesión con ***Protegus*** si usted desea que los usuarios requieran ingresarlo cuando se agrega el sistema a la app de ***Protegus2*** (contraseña por defecto – 123456). Importante: si cambias el código vía ***TrikdisConfig***, también debes cambiarlo en la aplicación ***Protegus2***.

En la ventana de la "Configuración de la red"



7. Ingrese el código PIN para la tarjeta SIM.
8. Cambie el nombre **APN**, el **APN** puede ser encontrado en el sitio del operador de la tarjeta SIM (el "Internet" es universal y funciona en muchas redes de los operadores).
9. **DNS1** - dirección predeterminada del servidor DNS de Google. **Independientemente de su configuración de IP, asegúrese de que sus direcciones DNS coincidan con las admitidas por su ISP**.
10. **DNS2** - dirección predeterminada del servidor DNS de Google. **Independientemente de su configuración de IP, asegúrese de que sus direcciones DNS coincidan con las admitidas por su ISP**.

Cuando termine con la configuración, de clic en **Escribir [F5]** y desconecte el cable USB.

Nota:	Para más información sobre otras opciones de ***GT*** en ***TrikdisConfig*** vea el capítulo 6 de "Descripción de la ventana de TrikdisConfig".

2.2 Configuración para conectarse con el CRA

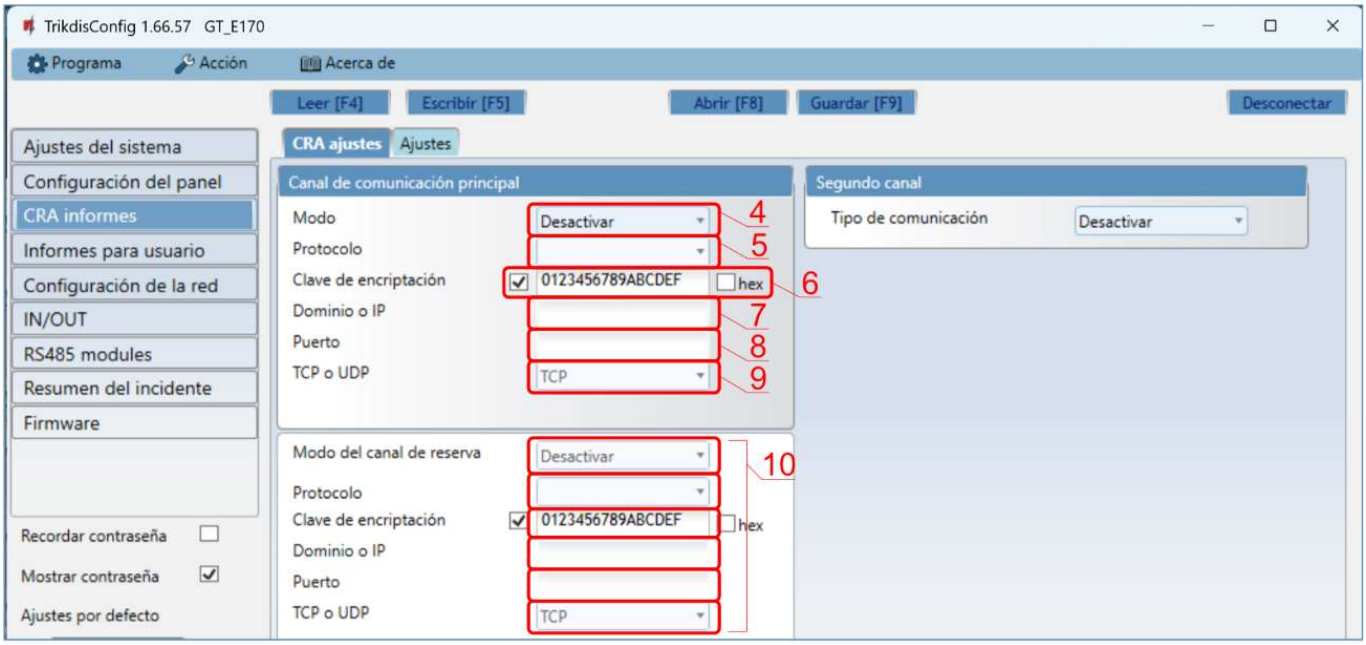
En la ventana de "Ajustes del sistema":

1. Ingrese el **Número de objeto** (**No utilice números de objeto FFFE, FFFF**.).

2. Si el comunicador está conectado a los terminales TIP/RING del panel de control, entonces debe configurarse en "**Dual tone**".

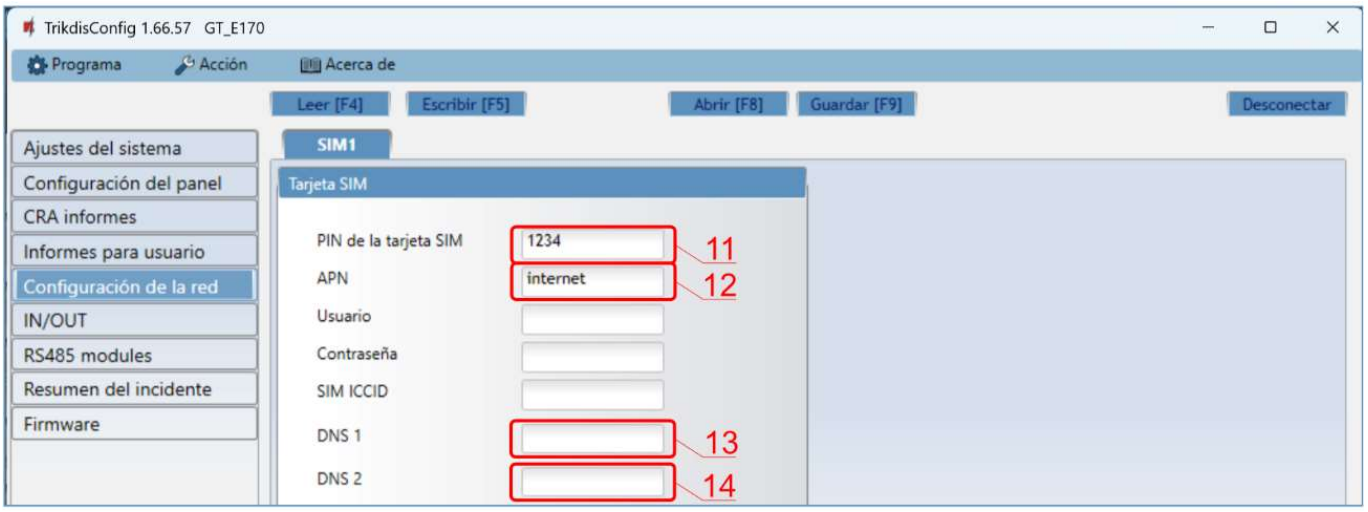
3. Si el comunicador está conectado al bus del teclado o al bus serie del panel de control, seleccione el modelo de panel de control que se conectará al comunicador.

En la ventana de opciones de "Ajustes CRA" para el "Canal de comunicación principal":



4. **Modo** – seleccione el método de conexión IP.
5. **Protocolo** – seleccione el tipo de protocolo para mensajes de evento: **TRK8** (para los receptores de TRIKDIS), **DC-09_2007** o **DC-09_2012** (a receptores universales), **TL150** (para los receptores de SUR-GARD).
6. **Clave de encriptación** – Ingrese la llave de encriptación que está establecida en el receptor.
7. **Dominio o IP** – ingrese la dirección del dominio o IP del receptor.
8. **Puerto** – ingrese el número de puerto de la red del receptor.
9. **TCP o UDP** – elija un protocolo de transmisión de evento (TCP o UDP, en donde se transmitirán los eventos.
10. (Recomendado) Realice ajustes para el "**Modo del canal de reserva**".

En la ventana de "Configuración de la red":



11. Ingrese el código PIN para la tarjeta SIM.
12. Cambie el nombre APN, el APN puede ser encontrado en el sitio del operador de la tarjeta SIM (el "Internet" es universal y funciona en muchas redes de los operadores).
13. **DNS1** - dirección predeterminada del servidor DNS de Google. **Independientemente de su configuración de IP, asegúrese de que sus direcciones DNS coincidan con las admitidas por su ISP**.
14. **DNS2** - dirección predeterminada del servidor DNS de Google. **Independientemente de su configuración de IP, asegúrese de que sus direcciones DNS coincidan con las admitidas por su ISP**.

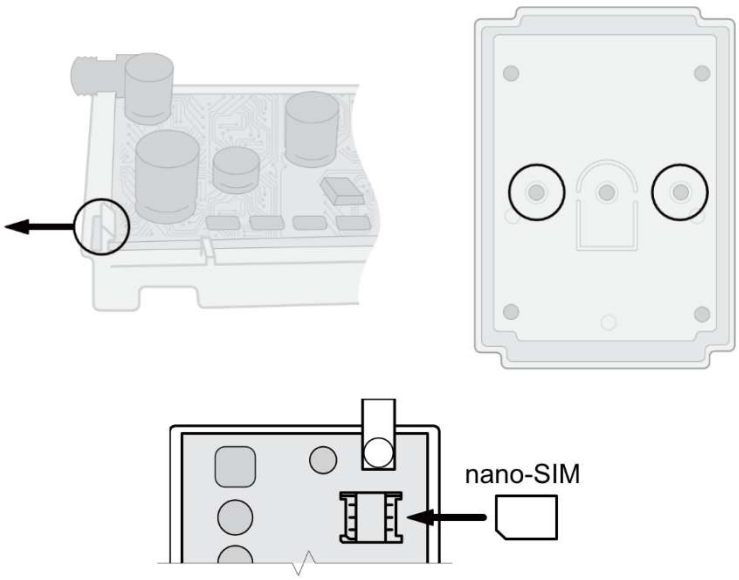
Cuando la configuración esté lista, de clic en **Escribir [F5]** y desconecte el cable USB.

Nota:	Para más información sobre otras opciones de ***GT*** en TrikdisConfig vea el capítulo 6 de "Descripción de la ventana de TrikdisConfig".

3 Instalación y cableado

3.1 Proceso de instalación

1. Retire la cubierta superior y extraiga la terminal de contacto.
2. Retire la placa PCB.
3. Fije la parte inferior para el lugar adecuado para poner los tornillos.
4. Coloque la placa PCB de nuevo en la caja, inserte terminal de contacto.
5. Atornille la antena celular
6. Inserte la tarjeta nano-SIM.
7. Cierre la cubierta superior.



Nota:	Cheque si la tarjeta SIM ha sido activada.

Asegúrese que el servicio de internet móvil se encuentra habilitado (datos móviles) si se conecta a través del canal de IP.

Para evitar ingresar el código PIN en TrikdisConfig, inserte la tarjeta SIM en su celular y apague la función de petición de PIN.

3.2 Diagramas para conectar los paneles de control

Siguiendo uno de estos diagramas provistos a continuación, conecte el comunicador con el panel de control.

Diagrama de conexión de **DSC** con **GT**

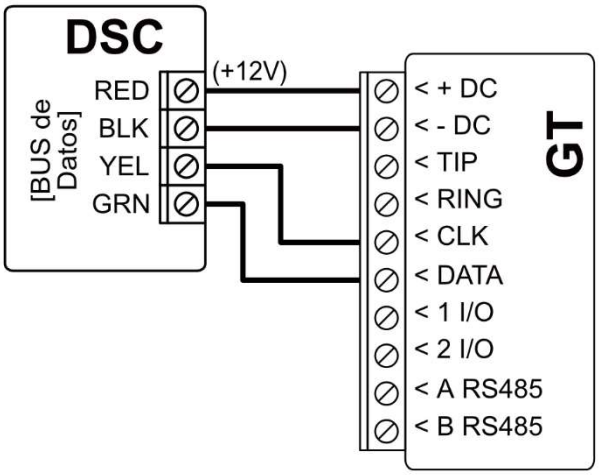


Diagrama de conexión de **Paradox** con **GT**

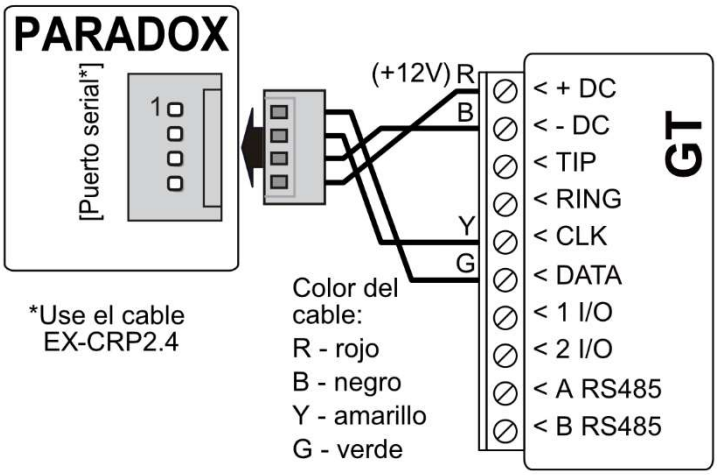


Diagrama de conexión de **CADDX** con **GT**

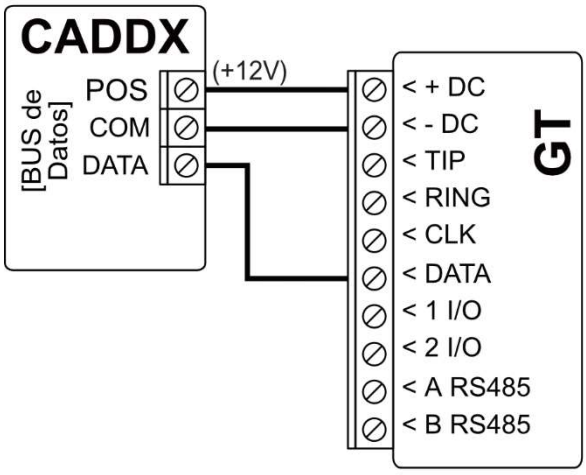


Diagrama de conexión de **TEXECOM** con **GT**

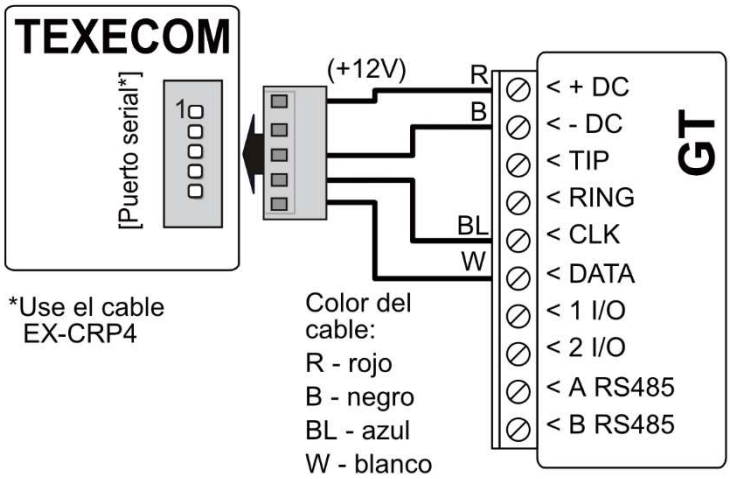


Diagrama de conexión de
INNERRANGE INCEPTION con **GT**

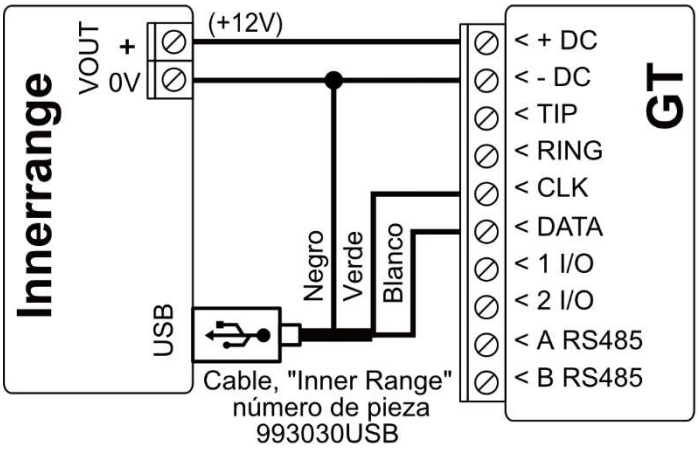


Diagrama de conexión de
INNERRANGE INTEGRITI con **GT**

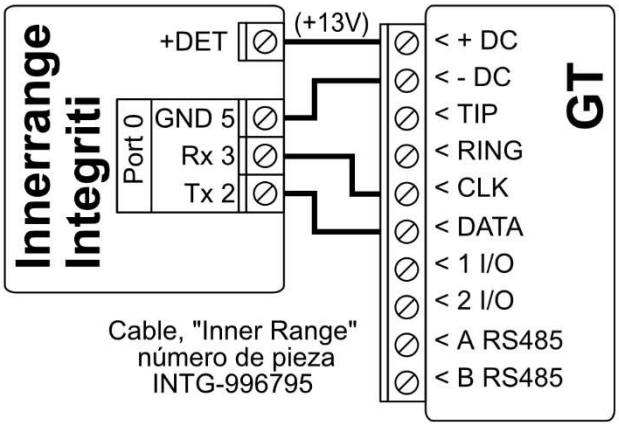


Diagrama de conexión de
Honeywell Vista-15, Vista-20, **Vista-48** con **GT**

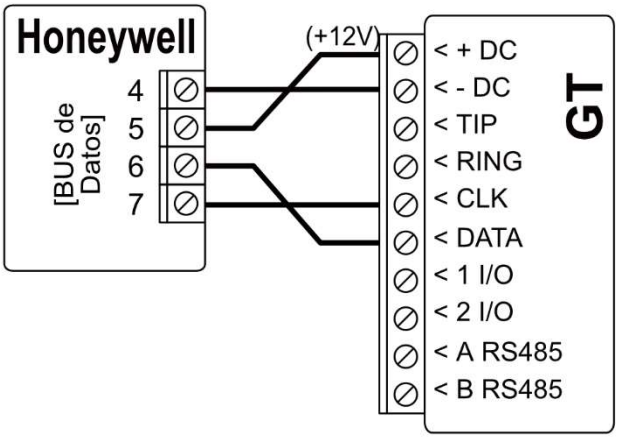
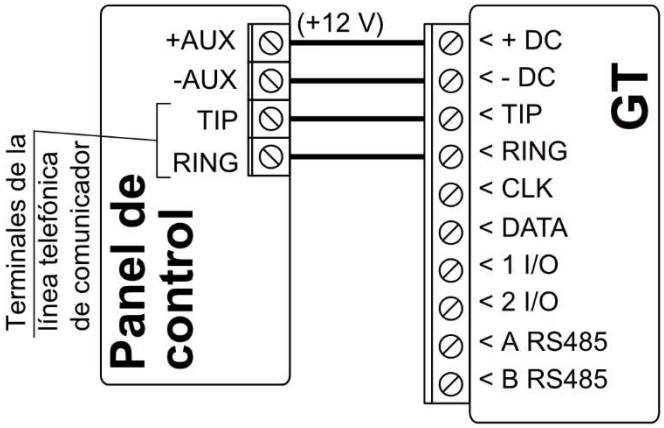
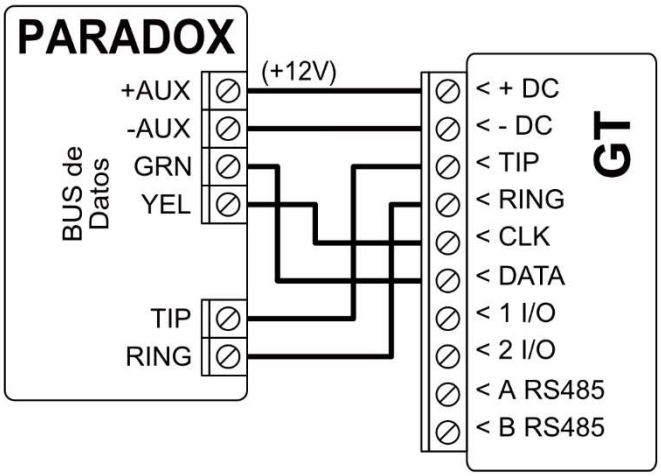


Diagrama de conexión del panel de control



3.3 Diagrama para conectar el comunicador al bus de teclado y comunicador telefónico (terminales TIP/RING) del panel PARADOX SP/SP+/MG/MG+

Diagrama de conexión de
PARADOX SP/SP+/MG/MG+ con **GT**



Al conectar el comunicador al bus del teclado y a los terminales TIP/RING del panel de control, debe realizar las siguientes configuraciones para el comunicador ***GT***:

1. Seleccione "**Dual tone**".

2. Seleccione el modelo de panel de control "**7. Paradox SP+/MG+ series KeyBus**".
3. Seleccione "**Control directo**" si desea que los usuarios puedan controlar el panel usando la aplicación ***Protegus2*** usando su propio código de teclado.
2. Para controlar directamente el panel de control, ingrese la "**Contraseña de descarga de PC**". Debe coincidir con la contraseña ingresada en el panel de control.

El panel de control Paradox debe programarse para transmitir eventos al CMS y para control remoto desde la aplicación ***Protegus2***.

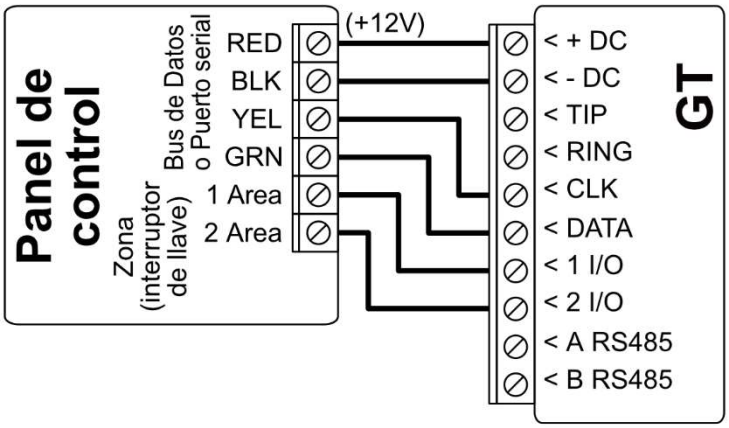
Celda	Datos
801	********
811	1111
812	2222

Celda	Datos
815	123456
911	1234

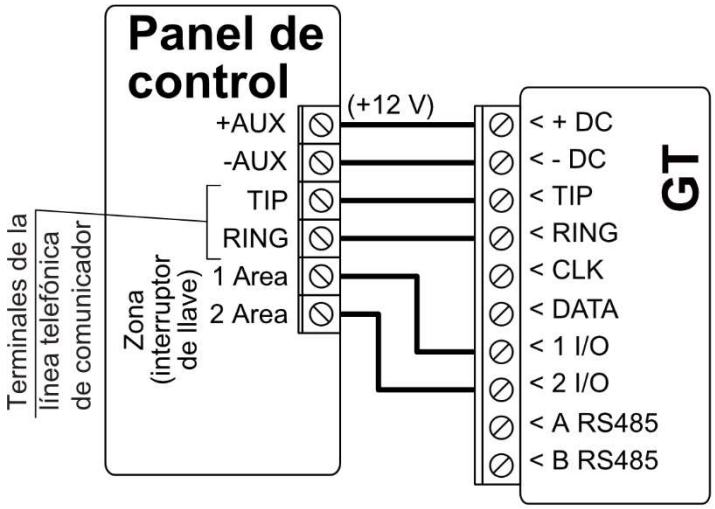
3.4 Diagramas de conexión para control el panel de control a través de la zona de keyswitch

El comunicador está conectado al bus del teclado o al bus serie del panel de control.

El Armado/Desarmado del panel de control se realiza a través de la zona del interruptor (keyswitch).



El comunicador está conectado a los terminales TIP/RING del panel de control.
El Armado/Desarmado del panel de control se realiza a través de la zona del interruptor (keyswitch).

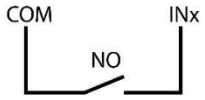


3.5 Diagramas para la conexión de entrada

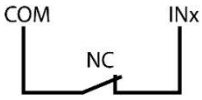
El comunicador tiene 2 terminales de entrada/salida universales que se pueden configurar en el modo de entrada IN. Los circuitos NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL pueden conectarse al terminal de entrada. Configuración de entrada de fábrica: 1 I/O – NO (normalmente abierto); 2 I/O – NO (normalmente abierto). El tipo de entrada se puede cambiar en la ventana ***TrikdisConfig*** **IN / OUT -> Tipo**.

Conecte la entrada de acuerdo al tipo de entrada seleccionada (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL), como se muestra en los esquemas de abajo:

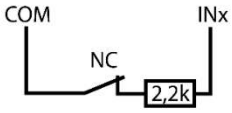
NA o normalmente abierto.
Short - Alarm;
Open - Restore.



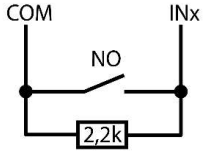
NC o normalmente cerrado.
Short - Restore;
Open - Alarm.



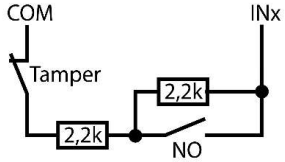
Circuito normalmente cerrado con resistencia 2,2k de fin de línea (EOL o fin de línea). Short - Alarm; Open - Alarm; 2,2k - Restore.



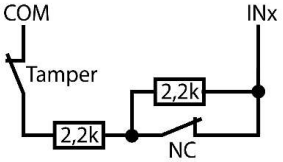
Circuito normalmente abierto con resistencia 2,2k de fin de línea (EOL o fin de línea).
Short - Alarm; Open - Alarm; 2,2k - Restore.



Circuito normalmente abierto con resistencia de fin de línea y reconocimiento de manipulación (NO con EOL y con sabotaje).
Short - Tamper; Open - Tamper; 2,2k - Alarm; 3,3k-5,5k - Restore.



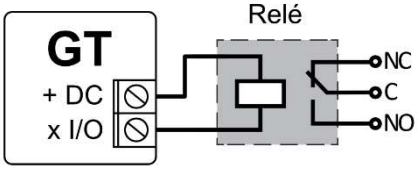
Circuito normalmente cerrado con resistencia de fin de línea y reconocimiento de manipulación (NC con EOL y reconocimiento de manipulación).
Short - Tamper; Open - Tamper; 2,2k - Restore; 3,3k-5,5k - Alarm.



Nota:	Si necesita que el comunicador tenga más entradas (IN) o salidas (OUT), conecte el expansor TRIKDIS ***iO-8***.

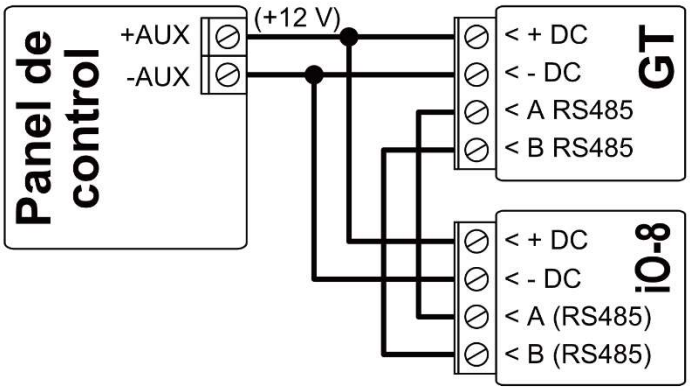
3.6 Diagrama de conexión de un relé

Con los contactos de relé se puede controlar (encender/ apagar) diversos aparatos electrónicos. El terminal de I/O del comunicador debe configurarse en un modo de salida (OUT).



3.7 Diagrama de conexión de un módulo expansor iO-8

Si necesita que el comunicador tenga más entradas IN o salidas OUT, conecte un expansor de entradas/salidas TRIKDIS iO-8 cableado. La configuración del ***GT*** con módulos de expansión se describe en la pág. 6.8 “Ventana “RS485 modules”.



3.8 Cambiando en la fuente de alimentación para el panel de control

Prenda la fuente de alimentación del panel de control. El indicador de luz LED en el comunicador ***GT*** debe mostrar:

- El LED de “POWER” se iluminará de color verde cuando se encuentre prendido;
- El LED de “NETWORK” se iluminará de color verde y parpadeará de color amarilla cuando se registre a una red.

Nota: Nivel de señal 4G suficiente: 3 (la luz indicadora de “NETWORK” deberá parpadear de color amarillo tres veces). Si usted ve una indicación LED distinta, esto quiere decir que hay algún error.

Si cuenta menos destellos amarillos del indicador "NETWORK", entonces el nivel de señal de la red GSM es insuficiente. Se recomienda buscar otra ubicación para instalar el comunicador o utilizar una antena externa.

Diagnostique y remuévalo siguiendo la información de la sección 1.6 “Indicación LED de Operación”.

Si el ***GT*** no se ilumina por ninguna circunstancia, revise la fuente de alimentación y las conexiones.

4 Programando el panel de control para leer eventos y tener control directo

4.1 Programación de paneles de control cuando el comunicador está conectado al bus de teclado o al puerto serie

A continuación, se describirá cómo programar los paneles de control para que el comunicador ***GT*** puede leer eventos del panel y pueda controlarlo de forma remota.

Para habilitar el control remoto del panel de control, debe marcar el campo "**Control directo**" en la ventana del programa "**Configuración del panel**".

DSC

Los paneles DSC no necesitan ser programados.

PARADOX

Los paneles de control de Paradox necesitan ser programados sólo para control directo con ***Protegus2***. No necesita programar los paneles de Paradox para que puedan leer eventos.

Para el control remoto de los paneles de Paradox, usted necesita establecer la contraseña de descarga de la computadora. Esta contraseña debe ser igual a la contraseña que fue establecida en la ventana de “Configuración del sistema” de ***TrikdisConfig***, cuando la casilla a un lado de Armado/Desarmado Remoto fue seleccionada.

Para establecer esta contraseña, con el teclado conectado al panel de control:

- Para las series MAGELLAN, SPECTRA: vaya a la celda 911 e ingrese la contraseña de cuatro dígitos de la descarga de computadora.
- Para las series DIGIPLEX EVO: vaya a la celda 3012 e ingrese la contraseña de cuatro dígitos de la descarga de computadora.

TEXECOM

Los paneles de control de Texecom necesitan ser programados para leer eventos y tener control remoto.

Usted necesita establecer el código UDL del panel de Texecom. Esta contraseña debe ser igual a ala contraseña que fue establecida en la ventana de "Configuración del panel", cuando la casilla a un lado de Armado/Desarmado remoto fue seleccionada.

El panel de control puede ser programado con el software de Texecom – Wintex. Ingrese el código UDL (4-digitos) en la ventana de Opción de Comunicación, en la pestaña de Opciones.

También, puede programar con el teclado conectado al panel de control:

1. Ingrese el código de 4-digitos del instalador y presione el botón de [Menu} para entrar al menú de programación.
2. Presione el [9] inmediatamente después de esto.
3. Presione [7][6], y luego [2]. Ingrese el código UDL de 4-digitos (el código UDL debe ser igual a la contraseña de inicio de sesión de la computadora para el comunicador ***GT***).
4. Presione [Yes] y salgase del modo de programación presionando [Menu].

UTC INTERLOGIX (CADDX)

Programar el panel de control desde el teclado del panel:

1. Presione [*][8] e ingrese el código del instalador (por defecto es – 9713).
2. Ingrese el número del dispositivo asignado al comunicador conectado (por defecto – 0)
3. Establezca la configuración de abajo para cada fila. En secuencia, presione la posición, número del segmento e ingrese la configuración requerida. Si da clic [*][asterisco] usted regresará al campo de entrada local.

Posición	**Segmento**	***Configuración***
23	3	12345678
37 (no es necesario)	3	12345678
	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

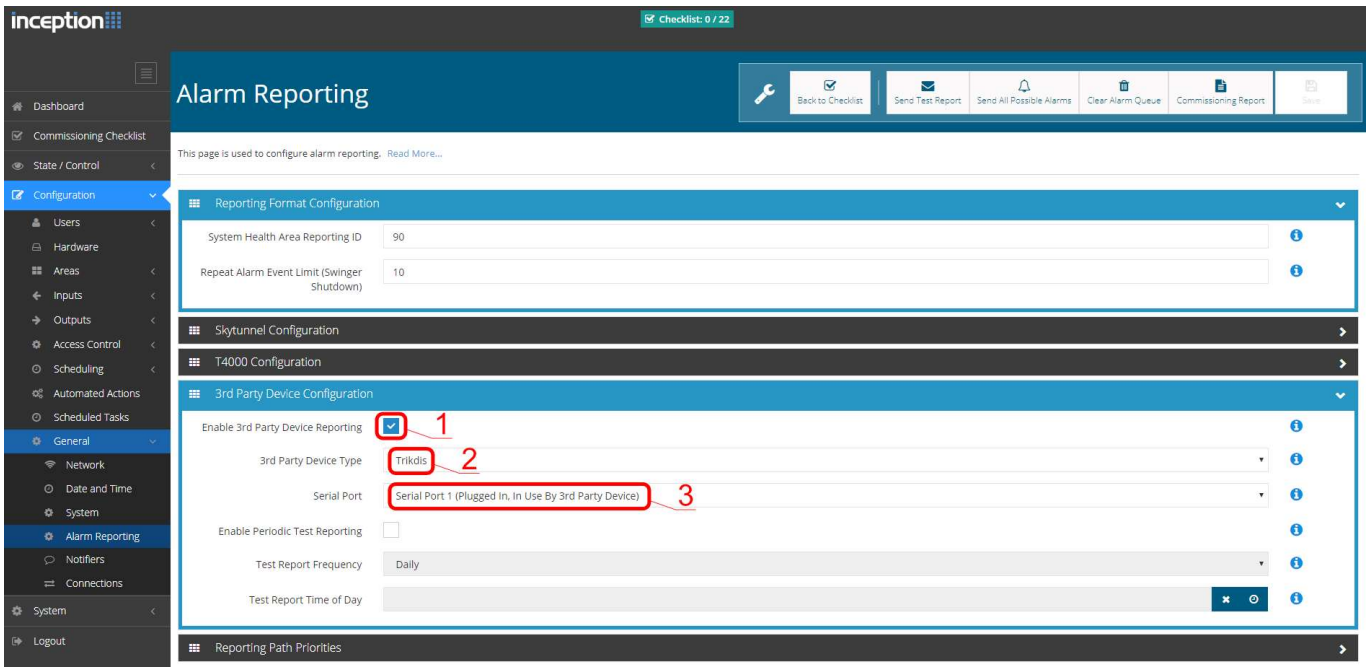
Después de haber programado todos los campos enlistados, presione [Exit] dos veces para salir del modo de programación.

INNERRANGE

La versión del panel de control de **Innerrange Inception** debe ser el **2.3.0.3507-r0** o mayor.

El panel de control debe estar conectado al internet. Conéctese con **Innerrange Inception** al ingresar en: https://skytunnel.com.au/inception/SERIALNUMBER, donde el **SERIALNUMBER** es el número del controlador que podrá encontrar en la cubierta del panel.

Abra la ventana de **Configuration>General>Alarm Reporting**. En el grupo "**3rd Party Device Reporting** ", debe instalar:



1. **Enable 3rd Party Device Reporting** – seleccione esta casilla.
2. **3rd Party Device Type** – establezca “Trikdis”.
3. **Serial port** – establezca “Serial Port 1 (Plugged In, In Use By 3rd Party Device)”.
4. Guarde la configuración y salgase de la aplicación.

HONEYWELL ADEMCO VISTA

Siga estos pasos para los paneles **Honeywell Ademco Vista-20 y Honeywell Ademco Vista-48**. **La versión del firmware del panel debe ser V5.3 o superior**. Con un teclado que está conectado al panel:

1. Ingrese al modo de programación. Ingrese el código de instalador [4][1][1][2] y luego ingrese [8][0][0]. O encienda el panel de control y dentro de los 50 segundos posteriores a encenderlo, presione los botones [*] y [#] simultáneamente (este método para ingresar al modo de programación se usa cuando salió del modo de programación presionando el botones del teclado [*][9][8]).
2. Active el envío de información de Contacto ID del evento a través de LRR. Presione [*] [2] [9] [1] [#] en el teclado.
3. Cuando use la función „Armar/Desarmar Remoto“, permita usar la segunda dirección AUI. En el teclado, presione [*] [1] [8] [9] [1] [1] [#].
4. Salga del modo de programación. En el teclado presione [*] [9] [9].

4.2 Programación de paneles de control al conectar un comunicador a los terminales TIP/RING del panel de control

Para que el panel de control envíe eventos a través del comunicador telefónico, debe estar encendido y configurado correctamente. Siguiendo el manual de programación del panel, configure el comunicador telefónico del panel de control:

1. Active el comunicador telefónico del panel PSTN.
2. Introduzca el número de teléfono receptor de la Centro de Monitoreo (se puede utilizar cualquier número de más de 4 dígitos. El ***GT*** recogerá y responderá cuando la central llama a cualquier número de teléfono).
3. Elegir el modo DTMF.
4. Seleccione el protocolo de comunicación Contact ID.
5. Introduzca el número de cuenta de 4 dígitos del panel.

Establezca la zona de panel de control, al que está conectada la salida OUT ***GT***, para utilizarse con el interruptor de llave de zona para activar/ desactivar el panel de control de forma remota.

Nota: La llave de zona puede ser momentánea (pulso) o nivel. Por defecto, la salida controlable del ***GT*** se establece en modo de pulso por 3 segundos. Se puede cambiar la duración del impulso o cambiar al modo de configuración de nivel en ***Protegus2***. véase el capítulo **Error! Reference source not found.** "**Error! Reference source not found.**.

PROGRAMACIÓN DE COMUNICADOR TELEFÓNICO DE HONEYWELL VISTA

Usando el teclado del panel de control ingrese a estas secciones y configúrelas como se describe:

- *41 - introduzca el número de teléfono de receptor de la CRA;
- *43 - introduzca el número de cuenta del panel de control;
- *47 - establezca el tono de marcación a [1] e introduzca el número de intentos de llamada;
- *48 – utilice la configuración predeterminada, *48 debe ajustarse a 7;
- *49 - Spit/ doble mensaje. *49 debe ajustarse a 5;
- *50 – el retardo para el envío de eventos de alarma de robo (opcional). El valor por defecto es [2,0]. Con ella la transmisión de mensajes de evento se retrasa durante 30 segundos. Si desea que el mensaje se envíe de inmediato, ajuste [0,0].

Después de configurar los parámetros necesarios, salga del modo de programación. Marque [*][9][9] en el teclado.

AJUSTES ESPECIALES PARA PANEL DE HONEYWELL VISTA 48

Si desea utilizar el comunicador ***GT*** con el panel Honeywell Vista 48, configure las siguientes secciones como se describe:

Sección	Datos
* 41	111 (# telefónico receptor)
* 42	1111
* 43	1234 (número de cuenta panel)
* 44	1234
* 45	1111
* 47	1
* 48	7
* 50	1
* 59	0

Sección	Datos
* 60	1
* 61	1
* 62	1
* 63	1
* 64	1
*65	1
* 66	1
* 67	1
* 68	1

S

Sección	Datos
* 69	1
* 70	1
* 71	1
* 72	1
* 73	1
* 74	1
* 75	1
* 76	1

Cuando todos los ajustes necesarios están configurados, es necesario salir del modo de programación. Ingrese [*][9][9] en el teclado.

UTC INTERLOGIX(CADDX)

Programación del panel de control **Interlogix NX-4V2** (**NX-6V2, NX-8V2**) cuando el comunicador está conectado a los terminales TIP/RING del panel de control.

	Keypad Entry	Description
	*89713	Ingrese al modo de programación
	0#	
Location 0	0#	
	1*2*3*4*#	
Location 1	1#	
	1*2*3*4*#	
Location 2	2#	
	1*#	

	Keypad Entry	Description
Location 4	4#	
	12345678*	Todos los LED de zonas están encendidos (segment 1)
	12345678*#	Todos los LED de zonas están encendidos (segment 2)
Location 23	23#	
	**	
	12345678*#	Todos los LED de zonas están encendidos (segment 3)
Location 37	37#	
	**	
	12345678*	Todos los LED de zonas están encendidos (segment 3)
	12345678*#	Todos los LED de zonas están encendidos (segment 4)
	EXIT EXIT	Salir del modo de programación

5 Control remoto

5.1 Agregar el sistema de seguridad a la aplicación Protegus2

Con ***Protegus2***, los usuarios podrán controlar su sistema de alamas de forma remota. Podrán ver el estado del sistema y recibir notificaciones sobre eventos del sistema.

1. Descargue y abra la aplicación ***Protegus2*** o utilice la versión de navegador de internet: web.protegus.app:

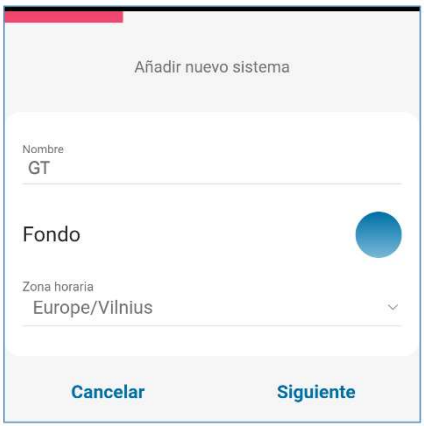
2. Inicie sesión con su nombre de usuario y contraseña o regístrese para crear una nueva cuenta.

IMPORTANTE: Al agregar ***GT*** a ***Protegus2***, revise si:

1. La tarjeta SIM insertada ha sido activada y el código PIN ha sido ingresado o deshabilitado;
2. La servicio ***Protegus2*** está activada. Podrá encontrar información sobre como activar la nube en la sección 6.4 Ventana de “Informes para Usuario”.
3. La fuente de alimentación está conectada (el LED de “POWER” debe iluminarse de color verde);
4. El comunicador ***GT*** está conectado a la red móvil (el LED de “NETWORK” de iluminarse de color verde y parpadear de color amarillo).

3. De clic en "**Añadir nuevo sistema**" e ingrese el número de ***GT*** "**IMEI/Unique ID**". Este número puede ser encontrado en el dispositivo y en la etiqueta del empaque. Haga clic en "**Siguiente**".

4. Ingrese el nombre del sistema. Haga clic en el botón "**Siguiente**".



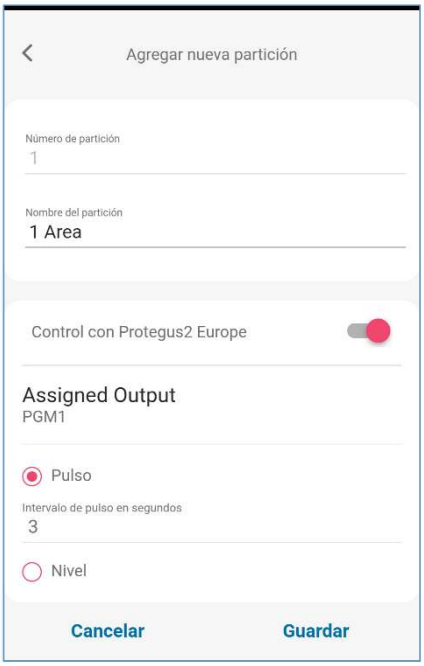
5.2 Configuraciones adicionales para armar/desarmar el sistema con la zona keyswitch

IMPORTANTE: La zona de panel de control, donde la salida del ***GT*** se encuentra conectada, tiene que ser establecida a modo de keyswitch.

Siga las instrucciones de abajo si el panel de control no será controlado de forma directa, pero con la salida del ***GT*** PGM, prendiendo/apagando el panel de control de la zona de keyswitch.

1. Haga clic en el botón "**Continuar**".

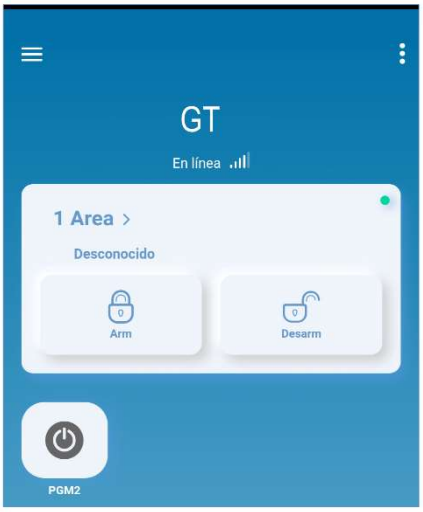
2. Ingrese "**Nombre de partición**". Habilite el control de salida PGM mediante la aplicación ***Protegus2***.
3. Seleccione "**Pulso**" o "**Nivel**", dependiendo de cómo esté configurado el tipo de zona del interruptor de llave. Si es necesario, puede cambiar el intervalo de pulso.
4. Haga clic en el botón "**Guardar**".



5. Si hay otra sección área, debes hacer clic en “**Haga clic para agregar una partición**”. La configuración de la salida PGM es similar a la descrita anteriormente.
6. Después de completar la configuración, haga clic en el botón "**Saltar**".

5.3 Control del sistema con Protegus2

1. Haga clic en el icono de estado del sistema "**Desarm**".
2. ***Protegus2*** recibirá un mensaje sobre el cambio en el estado del sistema de seguridad y el ícono de estado cambiará de estado.



6 Descripción de la ventana de TrikdisConfig

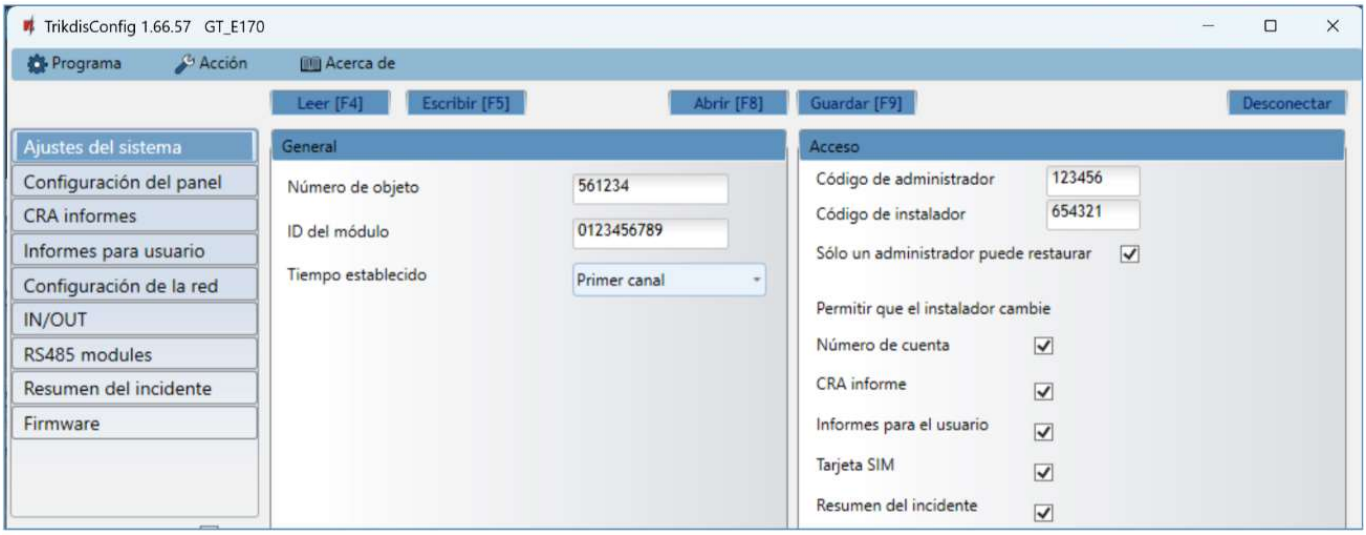
6.1 Barra de Estado

Barra de Estado

Nombre	Descripción
IMEI/Identificador única	Número IMEI del dispositivo
Estado	Estado de acción
Dispositivo	Tipo de dispositivo (***GT***)
SN	Número de serie
BL	Versión del cargador de arranque
FW	Versión de firmware
HW	Versión del hardware
Estado	Estado de conexión
Administrador	Nivel de acceso (aparece después de que sea confirmado el código de acceso)

Al presionar el botón **Leer [F4]**, el programa ***TrikdisConfig*** lee y muestra la configuración del comunicador ***GT***. Con ***TrikdisConfig*** realice los ajustes necesarios como se describe a continuación.

6.2 Ventana de "Ajustes del sistema"



Grupo de opciones "General"

- **Número de objeto** – - si los mensajes se enviarán al CRA, debe especificar el número de objeto (número hexadecimal de 6 dígitos, 0-9, A-F. **No use números de objeto FFFE, FFFF**). que es proporcionado por el Centro de Monitoreo.
- **ID del módulo** - ingrese "ID" el número del módulo.
- **Tiempo de sincronización** – elija qué servidor usar para la sincronización de hora.

Grupo de opciones de "Acceso"

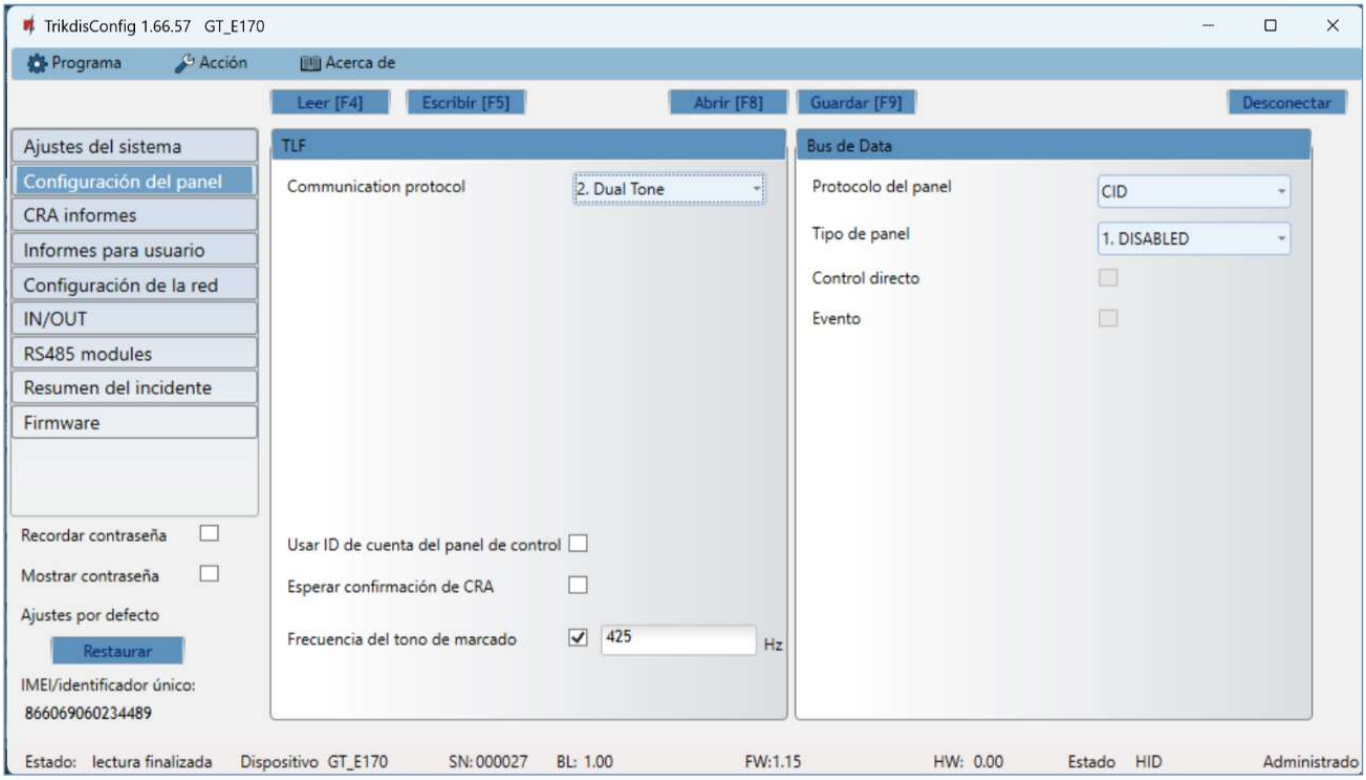
Al configurar el comunicador ***GT*** hay dos niveles de acceso para el administrador e instalador:

- **Código de administrador** – da acceso total a la configuración del comunicador (código de fábrica - 123456).
- **Código de instalador** – brinda acceso limitado a la configuración del comunicador (el código de fábrica es 654321).
- **Sólo un administrador puede restaurar -** al marcar la casilla, será posible restaurar la configuración de fábrica del comunicador solo después de ingresar el código de administrador.

  Nota: Si el campo " **Sólo un administrador puede restaurar** " está marcado y no conoce el código del administrador, entonces el fabricante UAB "Trikdis" puede restaurar la configuración de fábrica (este es un servicio pago).
- **Permitir que el instalador cambie** – el administrador establece qué parámetros podrá cambiar el instalador.

6.3 Ventana de “Configuración del panel”

Grupo de opciones de “TLF”



El comunicador se conecta a los terminales TIP/RING del panel de control.

- **Protocolo de comunicación** – configurado en "**Dual tone**".
- **Usar ID de cuenta del panel de control** – si el campo está marcado, el comunicador enviará mensajes con el número de objeto ingresado en el panel de control.
- **Esperar confirmación de CRA** – si este campo está marcado, luego de cada mensaje enviado, el comunicador esperará la confirmación del receptor IP de que el mensaje ha sido recibido. Si el comunicador no recibe un reconocimiento, no generará una señal de “kiss-off”. El comunicador telefónico de la central de alarma reenviará el mensaje si no recibe la señal de fin de comunicación.
- **Frecuencia del tono de marcado** - la frecuencia con la que el comunicador ***GT*** se comunica con el comunicador telefónico del panel de control.

Grupo de opciones de “Bus de Data”

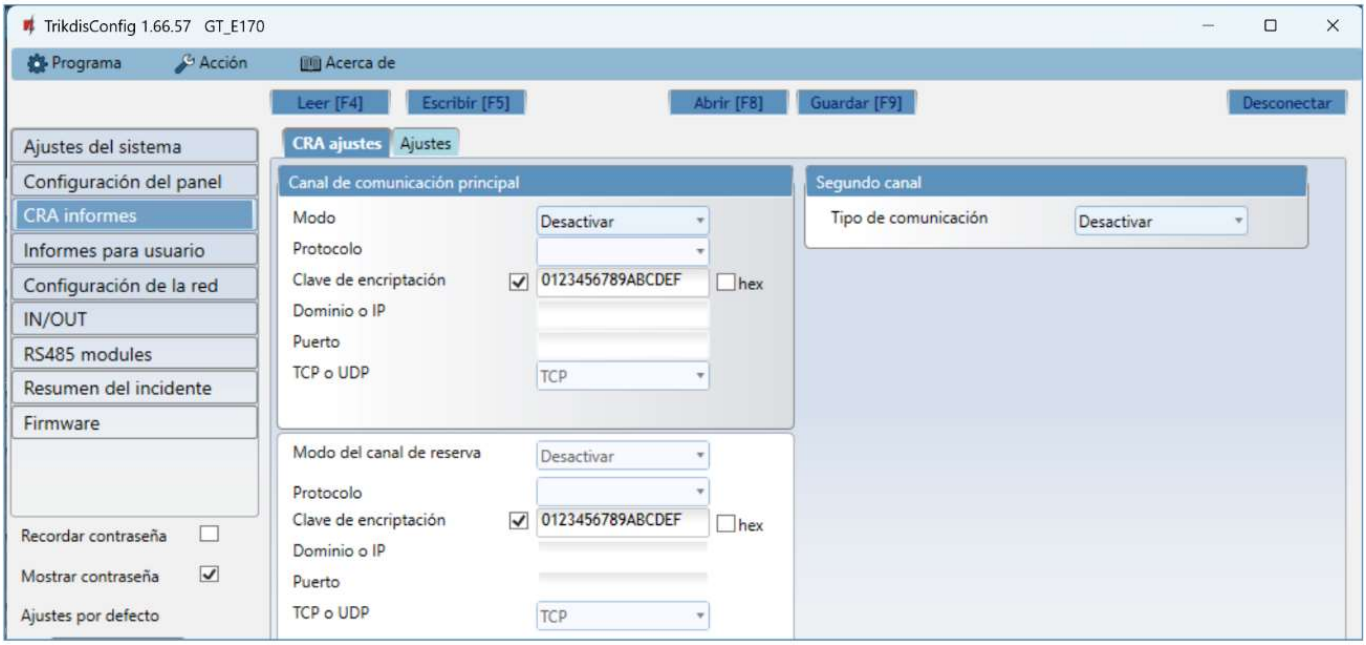
El comunicador está conectado al bus del teclado o al bus serie del panel de control.

- **Protocolo del panel** - seleccione el protocolo de notificación de eventos (CID o SIA).
- Seleccione el „**Tipo de Panel”** al que está conectado el comunicador.

- **Control directo** – marque la casilla y el comunicador ***GT*** controlará directamente el panel de control. Este parámetro se muestra para paneles de intrusión con control directo. La sección 4.1 "Programación de paneles de control cuando el comunicador está conectado al bus de teclado o al puerto serie" describe cómo configurar paneles de control con control directo.
- **Evento** - marque la casilla para que el comunicador envíe mensajes de eventos a la CRA ya ***Protegus2***.
- **Contraseña de descarga de PC** – para el control directo de los paneles de control de Paradox y Texecom, se debe ingresar un código de PC/UDL. El código debe coincidir con el código ingresado en el panel de control. La programación de paneles de control se describe en la sección 4.1 "Programación de paneles de control cuando el comunicador está conectado al bus de teclado o al puerto serie".

6.4 Ventana de “CRA informes”

Pestaña de “CRA ajustes”



Los eventos pueden ser enviados a través de varios canales de comunicación. Los primeros y segundos canales de comunicación pueden ser operados de forma simultánea y el comunicador puede enviar eventos a dos receptores al mismo tiempo. El canal de respaldo puede ser asignado para los primeros y segundos canales, los cuales serán usados cuando la conexión al canal primario es interrumpida.

La comunicación está codificada y está protegida por una contraseña. El receptor ***TRIKDIS*** es requerido para recibir y enviar información de evento al software de monitoreo:

- **Para conectarse a través de IP** – software receptor IPcom Windows/Linux, hardware IP/SMS receptor RL14.

Grupo de opciones del “Canal de comunicación principal”

- **Modo** – seleccione el método de comunicación (IP) con el receptor CRA.
- **Protocolo** – seleccione en que tipo de código serán enviados los eventos: **TRK8** (a receptor TRIKDIS), **DC-09_2007** o **DC-09_2012** (a receptores universales), **TL150** (para los receptores de SUR-GARD).
- **Clave de encriptación** – clave de cifrado de mensajes. La clave de cifrado ingresada en el comunicador debe coincidir con la clave de cifrado almacenada en el receptor CRA.
- **Dominio o IP** – ingrese la dirección del dominio o IP del receptor.
- **Puerto** – ingrese el número del puerto de la red.
- **TCP o UDP** – seleccione en que protocolo (TCP o UDP) deberían ser enviados los eventos.

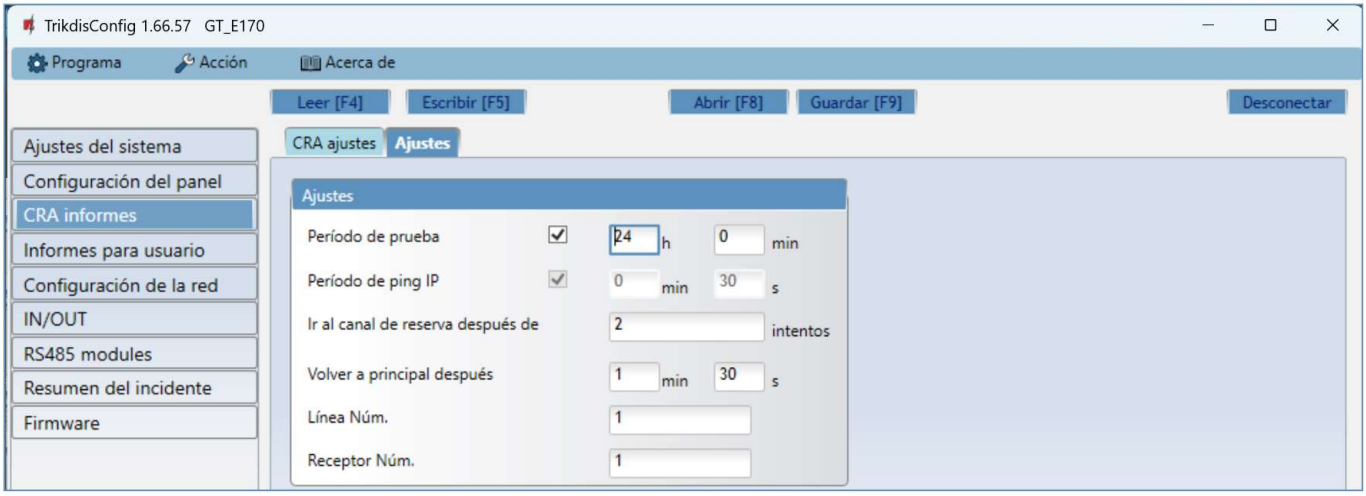
Grupo de opciones de “Modo del canal de reserva”

Habilite el modo de respaldo de canal para enviar eventos a través de canales de respaldo si la conexión se ha perdido. Las opciones de los canales de respaldo son las mismas que las descritas arriba.

Grupo de opciones de "Segundo canal"

Los eventos de este canal son transmitidos en paralelo con el primer canal. Cuando el segundo canal es habilitado, los eventos pueden ser enviados de forma simultanea por dos receptores (por ejemplo, CRA local y centralizado) Las opciones del canal paralelo son las mismas que las descritas anteriormente.

Pestaña de "Ajustes"



Grupo de opciones de "Ajustes"

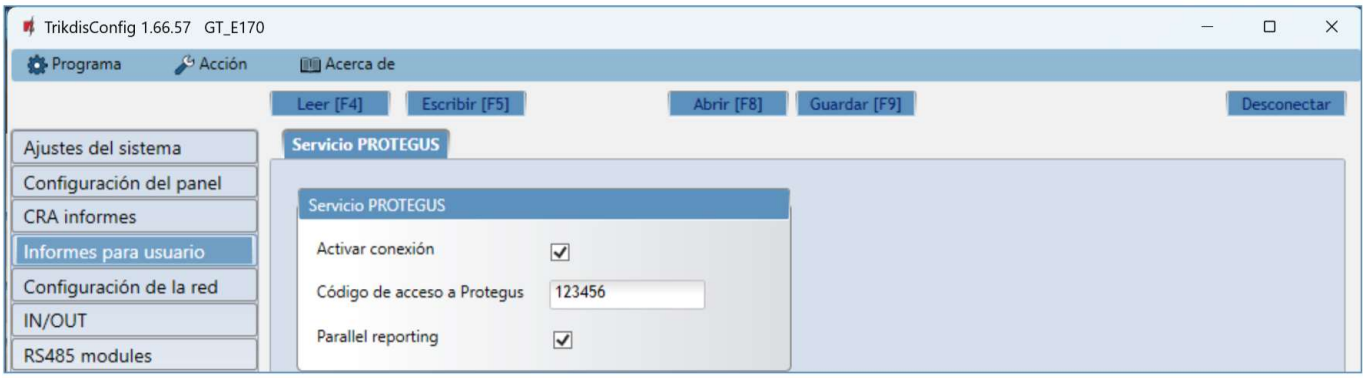
- **Periodo de prueba** – el período de envío de mensajes de prueba para verificar el canal de comunicación. Los mensajes de prueba se envían mediante códigos Contact ID y se transfieren al software de monitoreo.
- **Periodo de ping IP** – período para enviar señales de ping PING internas. Estos mensajes se envían únicamente por el canal IP. El receptor no envía mensajes PING al software de monitoreo sin sobrecargarlo. El software de monitoreo recibe información solo cuando el receptor no recibe mensajes PING del comunicador dentro de un período de tiempo establecido.

  De manera predeterminada, el receptor enviará un mensaje de "Conexión perdida" al software de monitoreo después de que haya transcurrido tres veces el período de tiempo establecido para el mensaje PING del comunicador. Por ejemplo: si el período PING se establece en 3 minutos. El receptor transmitirá un mensaje de pérdida de comunicación después de 9 minutos.

  Juntos, los mensajes PING mantienen una sesión de comunicación activa entre el dispositivo y el receptor. Se requiere una sesión de comunicación activa para la configuración y el control remotos del comunicador. Se recomienda establecer la duración del período PING en no más de 5 minutos.
- **Ir al canal de reserva después de... intentos** – indica el número de intentos fallidos al tratar de enviar el mensaje a través del canal primario. Si es dispositivo falla en la transmisión un número específico de veces, el dispositivo se conectará para transmitir el mensaje a través del canal de Respaldo.
- **Volver a principal después** – ingrese el período de tiempo después del cual el comunicador ***GT*** intentará restablecer la comunicación y enviar mensajes a través del canal "Principal".
- **Linea Núm.** – ingrese el número de línea en el receptor.
- **Receptor Núm.** - ingrese el número del receptor.

6.5 Ventana de “Informes para usuario”

Pestaña de “Servicio Protegus”

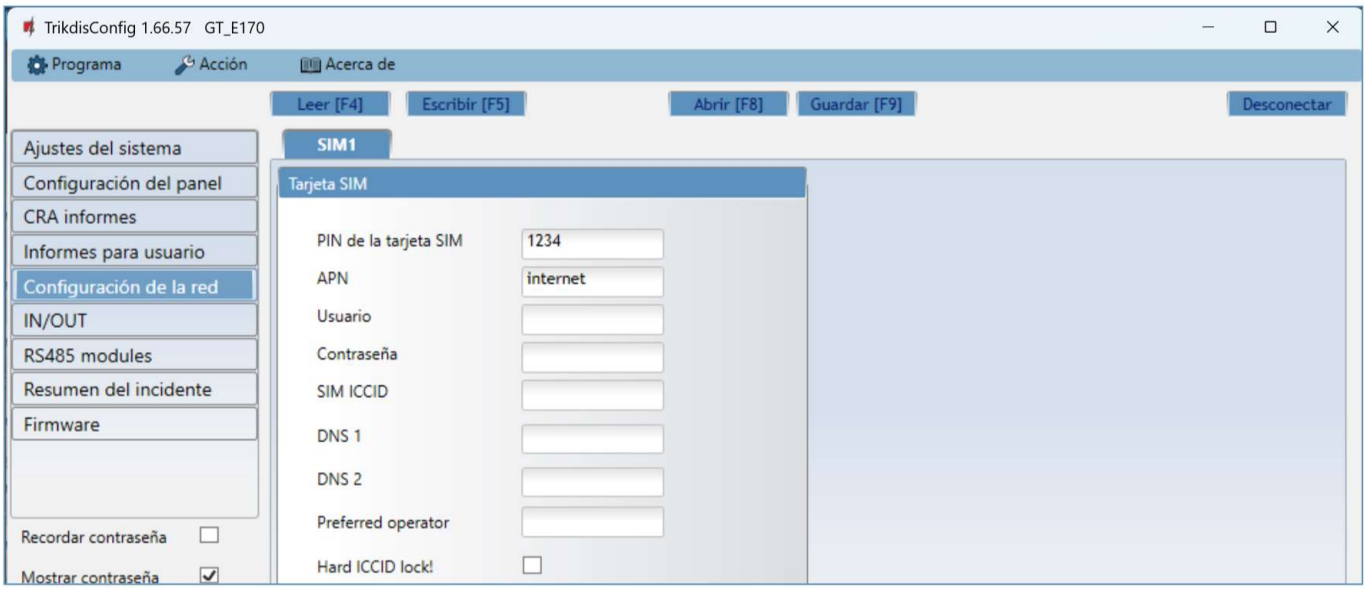


El servicio ***Protegus*** permite a los usuarios monitorear y controlar remotamente el comunicador. Puede encontrar más información sobre el servicio de ***Protegus*** en www.protegus.app.

- **Activar conexión** – marque la casilla para habilitar el servicio ***Protegus2***. El comunicador ***GT*** podrá intercambiar datos con la aplicación ***Protegus2***. Con el programa ***TrikdisConfig*** podrás configurar tu comunicador de forma remota.
- **Código de accesso a Protegus** – aquí puede cambiar la contraseña para conectarse al servidor de ***Protegus2*** (por defecto esta es – 123456). Si la contraseña ha sido cambiada usted tendrá que reingresarla cuando agregue el sistema en la app de ***Protegus2***. Esta es una medida de seguridad adicional. Importante: si cambias el código vía ***TrikdisConfig***, también debes cambiarlo en la aplicación ***Protegus2***.
- **Informes paralelos** – permite el envío de informes paralelos utilizando el *canal primario* y a ***Protegus2.*** Los mensajes a ***Protegus2*** sólo se enviarán después de que los mensajes hayan sido enviados a CRA.

6.6 Ventana de “Configuración de la red”

IMPORTANTE:
1. Asegúrese de que la tarjeta SIM ha sido activada y funciona, antes de usarla.
2. Si se usará internet móvil para enviar notificaciones a través del canal IP o a ***Protegus2***, asegúrese de que el servicio de datos móviles esté habilitado.

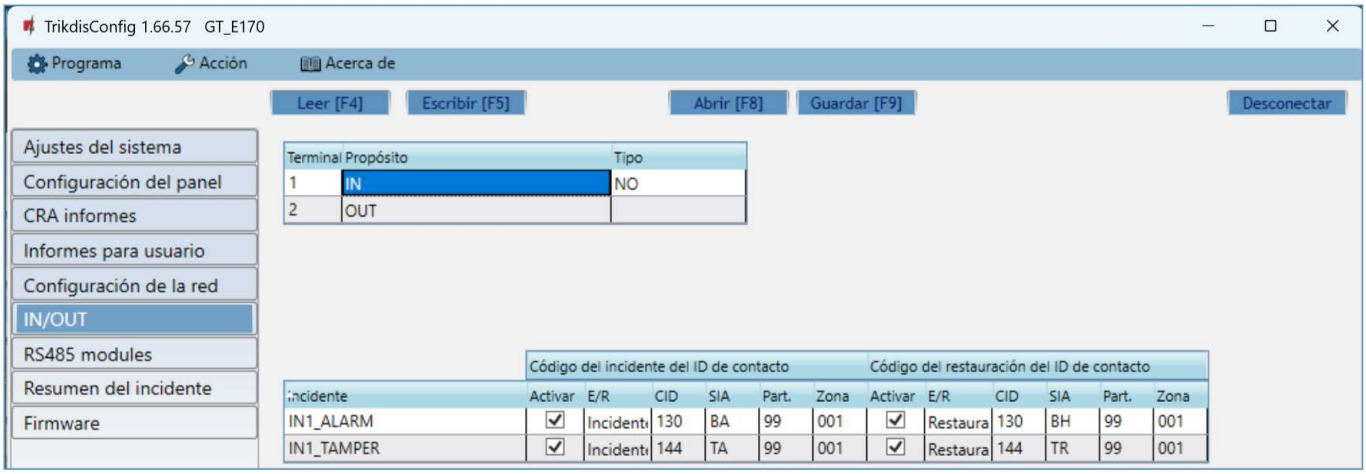


Grupo de opciones de la “Tarjeta SIM”

- **Pin de la tarjeta SIM** – Ingrese el código PIN de la tarjeta SIM. Este código puede ser deshabilitado al insertar la tarjeta SIM en el celular.

- **APN** – ingrese el APN (Nombre de Punto de Acceso). Es requerido para conectar el comunicador al internet. El APN puede ser encontrado en el sitio web del operador de la tarjeta SIM (el “Internet” es universal y funciona en muchas redes de los operadores.
- **Usuario, Contraseña** - contraseña: ingrese el nombre de usuario y la contraseña para APN si es necesario.
- **SIM ICCID** – ingrese el número ICCID de la tarjeta SIM si desea que el comunicador funcione solo con esta tarjeta SIM.
- **DNS1/DNS2** - (Domain Name System en inglés) ingrese la dirección IP del servidor de dominio. Se usa cuando el campo Dominio o IP especifica un dominio. De forma predeterminada, las direcciones del servidor DNS de Google están configuradas. **Independientemente de su configuración de IP, asegúrese de que sus direcciones DNS coincidan con las admitidas por su ISP.**
  - **Preferred operator (Operador preferido)** – después de ingresar el código del operador de la red móvil, el comunicador se conectará solo a la red del operador seleccionado. El código del operador de telefonía móvil consta de códigos MCC y MNS.
  - **Hard ICCID lock! (Bloqueo del ICCID)** - al marcar el campo y reiniciar el comunicador, estará estrictamente vinculado al código ICCID especificado de la tarjeta SIM.

6.7 Ventana de “IN/OUT“



El comunicador tiene 2 terminales universales (entrada/salida). La tabla puede configurar el modo de funcionamiento del terminal (Apagado, IN, OUT). La entrada debe especificar el tipo de circuito a conectar NC, NO, NO / EOL, NC / EOL, NO / DEOL, NC / DEOL.

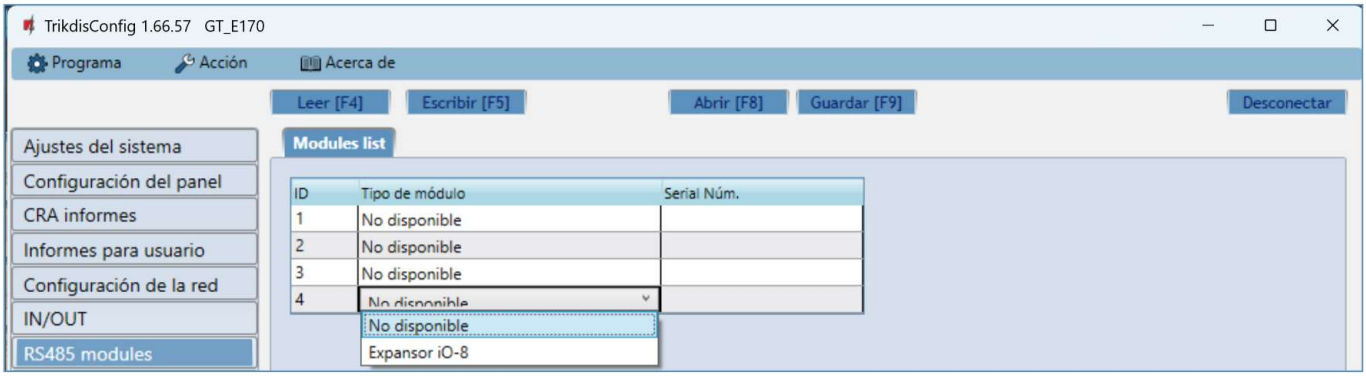
Se pueden conectar sensores adicionales a las entradas del comunicador. Cuando se activa el sensor, el comunicador enviará un mensaje de evento. A la entrada se le asigna un código de Contact ID (SIA), que se enviará a CRA y ***Protegus2***.

- **Activar** – verifique los campos de eventos qué mensajes se enviarán a CRA y ***Protegus2..***
- **E/R** – especifique la condición de envío del evento interno del comunicador (**Evento** o **Restaurar**).
- **CID** – código de evento.
- **SIA** - código de evento.
- **Part**. – especifique el número de área que se enviará cuando se active/restaurar un evento del comunicador interno.
- **Zona** - especifique el número de la zona que se enviará cuando se active/restaurar un evento del comunicador interno.

6.8 Ventana de “RS485 modules”

El comunicador se puede conectar a expansores ***iO-8*** (agregando contraladas entradas/salidas adicionales). Los módulos conectados deben ser agregados en la tabla "Modules list" (Lista de módulos).

Grupo de opciones de “Modules list”



- **ID** – número del módulo en la lista.
- **Tipo de Módulo** – seleccione el módulo que usted utiliza de la lista de módulos.
- **Serial Núm.** – número compulsorio de 6 dígitos, el cual está indicado en la etiqueta en la cuja del módulo y en el paquete.

Vaya a los **RS485 modules** → **Module 1**.

Pestañas “Module 1”

Después de añadir el expansor al comunicador como se ha descrito en el párrafo anterior, en la ventana de los “**RS485 modules**” aparecerá una nueva pestaña con los ajustes de este módulo. A la pestaña se le asignará un número. A continuación se describen los ajustes para los expansores de las series ***iO-8.***

Ventana de ajustes del expansor iO-8

El expansor ***iO-8*** tiene 8 contactos de terminal universales (entrada/salida). Se pueden conectar hasta cuatro expansores ***iO-8***.

- **Recuento de entrada -** seleccione el número de contactos de la terminal que deben configurarse en modo de entrada (IN). El resto de los contactos de la terminal se convertirán en salidas (OUT).

Los ajustes para las salidas controlables se establecen directamente en la aplicación ***Protegus2***. Allí se puede asignar una salida para armar/desarmar el sistema de alarma o para el control remoto de los dispositivos.

En la tabla se pueden asignar entradas de eventos de Contacto ID (SIA) y códigos de restauración. Después de que se activa la entrada, el comunicador enviará un evento con el código de evento establecido al receptor en el CRA, a la aplicación ***Protegus2***.

Código de incidente del ID de contacto:

- **Activar -** permite la transmisión de mensajes cuando se activa la entrada.
- **E/R -** elija qué tipo de evento se enviará cuando se active la entrada, “**Evento**” o “**Restaurar**”.
- **CID** – código de evento.
- **SIA** - código de evento.

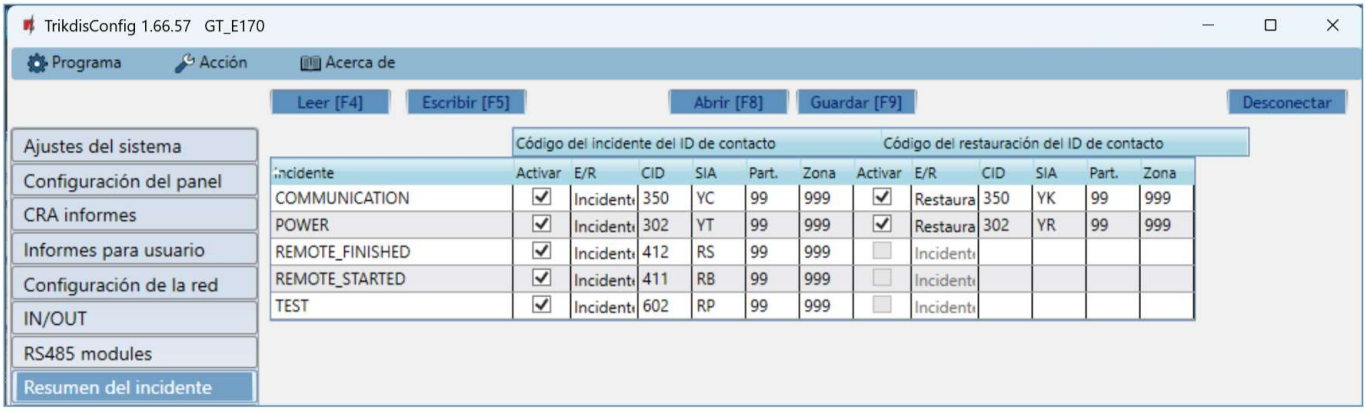
- **Part. -** asigne la partición (área) a la entrada. Esta se ajusta automáticamente: si el número de módulo es 1, la superficie es 91; si el número de módulo es 4, la superficie es 94.
- **Zona -** establezca el número de zona para la entrada.

Código de restauración del ID de contacto:

- **Activar -** permite la transmisión de mensajes cuando se restaura la entrada.
- **E/R -** elija qué tipo de evento se enviará cuando se restaure la entrada, "**Restaurar**" o "**Evento**".
- **CID** – código de evento.
- **SIA** - código de evento.
- **Part. -** asigne la partición (área) a la entrada. Esta se ajusta automáticamente: si el número de módulo es 1, la superficie es 91; si el número de módulo es 4, la superficie es 94.
- **Zona -** establezca el número de zona para la entrada.
- **Tipo de entrada -** seleccione el tipo de entrada (NO, NC o EOL).

6.9 Ventana de "Resumen del incidente"

Esta ventana le permitirá prender, apagar y modificar los mensajes internos enviados por su dispositivo. Deshabilitar el mensaje interno en esta ventana prevendrá que sea enviado a pesar de otras opciones.



- **COMMUNICATION** – mensaje de falla de comunicación entre el panel de control y ***GT***.
- **POWER** – aviso de baja tensión de red.
- **REMOTE_FINISHED** – mensaje sobre desconexión de configuración remota con ***TrikdisConfig***.
- **REMOTE_STARTED** – mensaje de inicio de sesión remoto para configurar ***GT*** con ***TrikdisConfig***.
- **TEST** – mensaje de prueba periódica.

Nota:	Para habilitar los mensajes de PRUEBA periódicos y establecer el período, vaya a la ventana "**CRA informes**" **→ Ajustes → Período de prueba.**

- **Activar** – marque la casilla para habilitar el envío de mensajes.

Puede cambiar el código de identificación de contacto para cada evento, así como el número de zona y área que se informará.

6.10 Restablecer la configuración de fábrica

Para restablecer el comunicador a la configuración de fábrica, presione el botón „**Restaurar**" en ***TrikdisConfig*.**

Otra forma de restaurar la configuración de fábrica.

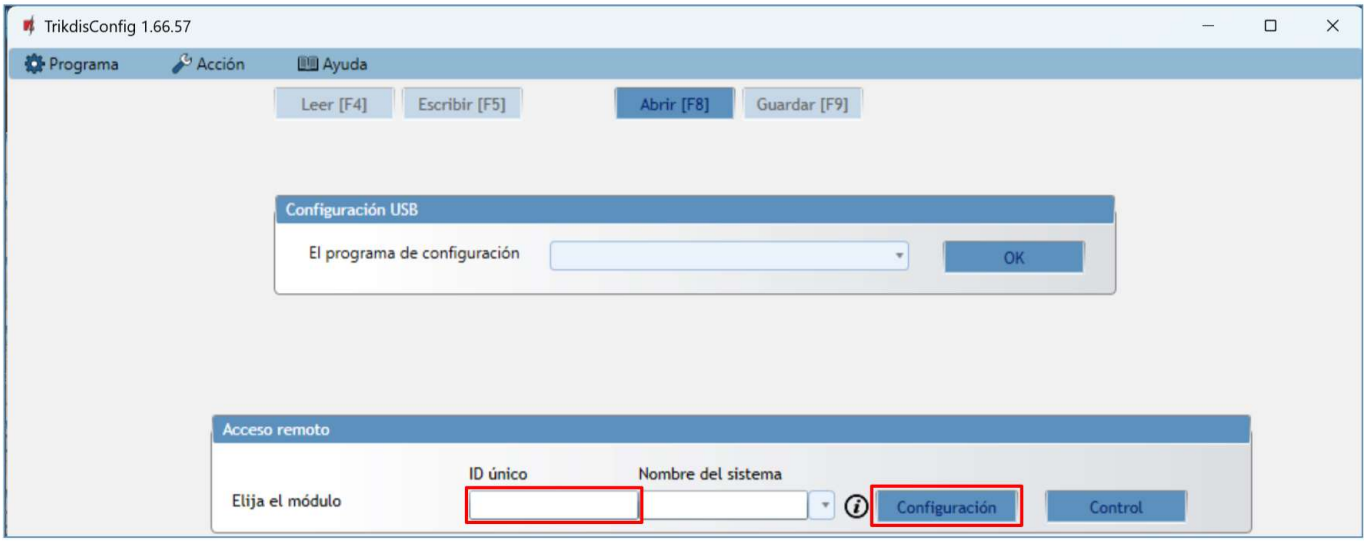
La fuente de alimentación está conectada al comunicador. Mantenga presionado el botón "REINICIO" en el tablero del comunicador durante 10 segundos hasta que los indicadores LED ("NETWORK", "POWER", "TROUBLE") se apaguen y el indicador LED "POWER" se encienda. Suelte el botón "REINICIO". Se han restablecido los ajustes de fábrica del comunicador.

7 Configuración Remota

IMPORTANTE: La configuración remota sólo funcionará sí:

1. La tarjeta SIM insertada ha sido activada y el código PIN ha sido ingresado o deshabilitado;
2. El servicio ***Protegus2*** está activada. Podrá encontrar información sobre como activar la nube en la sección 6.4 Ventana de “Informes para Usuario”;
3. La fuente de alimentación está conectada (el LED de “POWER” debe iluminarse de color verde);
4. Estar registrado en la red (el LED de “NETWORK de iluminarse de color verde y parpadear de color amarillo).

1. En su PC abra el software de configuración de ***TrikdisConfig***.
2. En la sección de acceso remoto ingrese el **IMEI/ID único**. Este número puede ser encontrado en el dispositivo y en la etiqueta del empaque.



3. (Opcional) en el espacio del „**Nombre de sistema**” ingrese el nombre deseado para el comunicador.
4. Presione “**Configuración**”.
5. En la nueva ventana de clic en **Leer [F4].** A petición, ingrese el código del administrador o instalador. Para guardar la contraseña, seleccione “Recordar contraseña” en la ventana principal.
6. Establezca las opciones deseadas y presione **Escribir [F5].**

8 Desempeño de la Prueba del Comunicador

Después de que la configuración y la instalación hayan sido completadas, lleve a cabo una prueba de sistema:

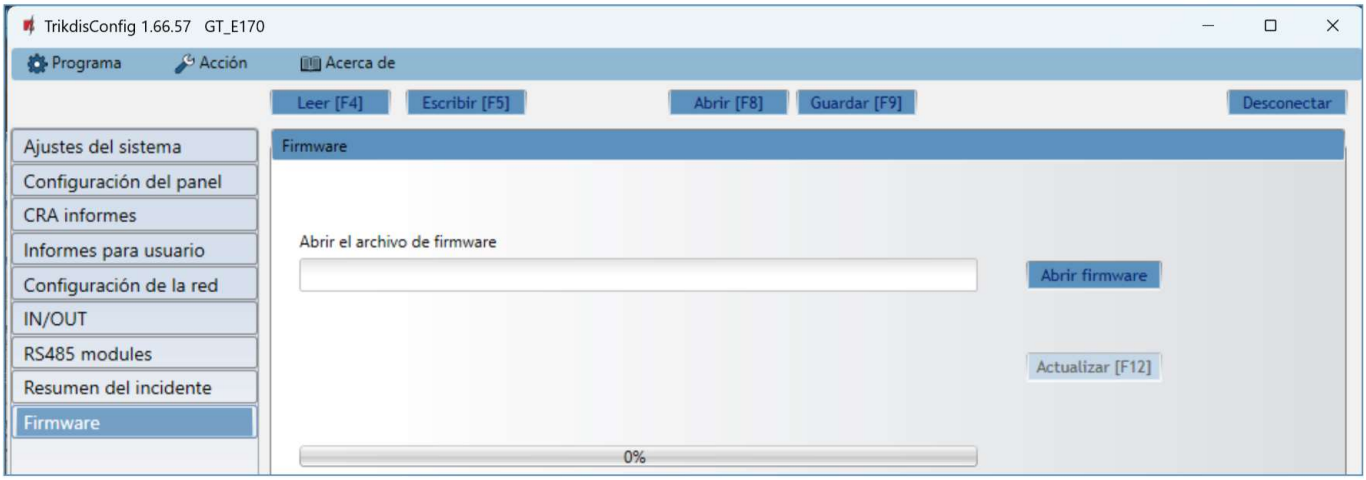
1. Generar un evento:
   - Armando y desarmando el modo de seguridad usando el teclado del panel de control.
   - Activando una alarma de zona cuando el sistema de seguridad esté armado.
2. Asegúrese de que el evento llegue al CRA y/o sea recibido en la aplicación de ***Protegus2***.
3. Active la entrada del comunicador y verifique que los usuarios reciban mensajes de eventos.
4. Active las salidas del comunicador de forma remota y asegúrese de que las salidas se activen y que los usuarios reciban mensajes de eventos.
5. Si el panel de control será controlado de forma remota, arme/desarme el sistema de seguridad de forma remota al usar la app ***Protegus2***.

9 Actualización del firmware

Nota:	Cuando el comunicador esté conectado a ***TrikdisConfig***, el programa ofrecerá actualizar el firmware del dispositivo si es que hay alguna actualización disponible. Las actualizaciones requieren una conexión al internet. Si hay un antivirus instalado en su computadora, puede que este bloquee la opción de actualización de firmware. En este caso usted debe reconfigurar su software de antivirus.

El firmware del comunicador puede ser actualizado o cambiado de forma manual. Después de una actualización, el comunicador mantendrá cualquier opción establecida. Cuando escriba el firmware de forma manual, este puede ser cambiado a una versión más reciente o antigua. Para actualizar:

1. Abra ***TrikdisConfig***.
2. Conecte el comunicador a través de cable USB a la computadora o conéctese al comunicador de forma remota. Si hay nuevo firmware, ***TrikdisConfig*** ofrecerá actualizar el software ***GT***.
3. Seleccione la parte de "**Firmware**" del menú.



4. Presione "**Abrir firmware**" y seleccione el archivo de firmware requerido.
5. Presione **Actualizar [F12]**.
6. Espere a que se complete la actualización.

10 Anexo

El comunicador recibidos desde panel de control los códigos de Contacto ID convierte a códigos SIA.

Tabla de conversión de los códigos Contacto ID a código SIA

Evento del sistema	Código de informe CID	Código de informe de SIA
Alarma médica	E100	"MA"
Emergencia personal	E101	"QA"
Incendio en la zona: <z>	E110	"FA"
Flujo de aguas detectado en la zona: <z>	E113	"SA"
Alarma de la estación manual en la zona: <z>	E115	"FA"
Pánico en la zona: <z>	E120	"PA"
Alarma de pánico por el usuario: <v>	E121	"HA"
Alarma de pánico en la zona: <z>	E122	"HA"
Alarma de pánico en la zona: <z>	E123	"PA"
Alarma de pánico en la zona: <z>	E124	"HA"
Alarma de pánico en la zona: <z>	E125	"HA"
Alarma activa en la zona: <z>	E130	"BA"
Alarma activa en la zona: <z>	E131	"BA"
Alarma activa en la zona: <z>	E132	"BA"
Alarma activa en la zona: <z>	E133	"BA"
Alarma activa en la zona: <z>	E134	"BA"
Alarma activa en la zona: <z>	E135	"BA"
Tamper activo en la zona: <z>	E137	"TA"
Intrusión verificada en la zona: <z>	E139	"BV"
Alarma activa en la zona: <z>	E140	"UA"
Fallo del sistema (143)	E143	"UA"
Tamper activo en la zona: <z>	E144	"TA"
Tamper activo en la zona: <z>	E145	"TA"
Alarma activa en la zona: <z>	E146	"BA"
Alarma activa en la zona: <z>	E150	"UA"
Gas detectado en la zona: <z>	E151	"GA"
Pérdida de agua detectada en la zona: <z>	E154	"WA"
Foil Rotura detectado en la zona: <z>	E155	"BA"
Alta temperatura en el sensor: <n>	E158	"KA"
Baja temperatura en el sensor: <n>	E159	"ZA"
CO detectado en la zona: <z>	E162	"GA"
Falla en zona de fuego: <z>	E200	"FS"
Monitoreo de alarma	E220	"BA"
Fallo del sistema (300)	E300	"YP"
Pérdida de fuente de alimentación AC	E301	"AT"
Batería baja	E302	"YT"

Evento del sistema	Código de informe CID	Código de informe de SIA
Fallo del sistema (304)	E304	"YF"
Reiniciar sistema en zona: <z>	E305	"RR"
Programación del panel modificada	E306	"YG"
Apagado del sistema	E308	"RR"
Fallo en la batería (309)	E309	"YT"
Fallo de toma a tierra	E310	"US"
Fallo en batería (311)	E311	"YM"
Sobrecarga en fuente de alimentación (312)	E312	"YP"
Restablecimiento del ingeniero por usuario: <v> (313)	E313	"RR"
Fallo en Sirena/Relé	E320	"RC"
Fallo del sistema (321)	E321	"YA"
Fallo del sistema (330)	E330	"ET"
Fallo del sistema (332)	E332	"ET"
Fallo del sistema (333)	E333	"ET"
Fallo del sistema (336)	E336	"VT"
Fallo del sistema (338)	E338	"ET"
Fallo del sistema (341)	E341	"ET"
Fallo del sistema (342)	E342	"ET"
Fallo del sistema (343)	E343	"ET"
Fallo del sistema (344)	E344	"XQ"
Fallo de comunicación del sistema (350)	E350	"YC"
Fallo de comunicación del sistema (351)	E351	"LT"
Fallo de comunicación del sistema (352)	E352	"LT"
Fallo del sistema (353)	E353	"YC"
Fallo de comunicación del sistema (354)	E354	"YC"
Fallo del sistema (355)	E355	"UT"
Problema de fuego en zona: <z>	E373	"FT"
Problema en la zona: <z>	E374	"EE"
Problema en la zona: <z>	E378	"BG"
Problema en la zona: <z>	E380	"UT"
Avería en zona inalámbrica: <z>	E381	"US"
Fallo del módulo inalámbrico (382)	E382	"UY"
Tamper activo en la zona: <z>	E383	"TA"
Batería baja en zona inalámbrica: <z>	E384	"XT"
Problema en la zona: <z> (389)	E389	"ET"
Problema en la zona: <z> (391)	E391	"NA"
Problema en la zona: <z> (393)	E393	"NC"
Usuario <v> desarmó el sistema	E400	"OP"
Usuario <v> desarmó el sistema	E401	"OP"
Desarme automático	E403	"OA"

Evento del sistema	Código de informe CID	Código de informe de SIA
Desarmado diferido <v> usuario	E405	"OR"
Alarma cancelada por el usuario: <v>	E406	"BC"
Usuario <v> desarmó de forma remota	E407	"OP"
Usuario <v> armó rápido	E408	"OP"
Desarmado remoto	E409	"OS"
Solicitud de devolución de llamada realizada por CRA	E411	"RB"
Descarga de datos realizada con éxito	E412	"RS"
Acceso denegado para el usuario: <v>	E421	"JA"
Entrada por usuario <v>	E422	"DG"
Acceso Forzado <z> zona	E423	"DF"
Acceso de salida denegado para el usuario <v>	E424	"DD"
Salida usuario <v>	E425	"DR"
Usuario <v> desarmó demasiado pronto	E451	"OK"
Usuario <v> armó el sistema demasiado tarde	E452	"OJ"
Usuario <v> Falló al abrir	E453	"CT"
Usuario <v> Falló al cerrar	E454	"CI"
Auto armado fallido	E455	"CI"
Armado parcial por el usuario: <v>	E456	"CG"
Violación de salida por usuario: <v>	E457	"EE"
Armado parcial por el usuario: <v>	E458	"OR"
Recent arm <v> user	E459	"CR"
Introducido código incorrecto	E461	"JA"
Tiempo de auto-armado ampliado por usuario: <v>	E464	"CE"
Dispositivo deshabilitado (501)	E501	"RL"
Dispositivo deshabilitado (520)	E520	"RO"
Sensor inalámbrico deshabilitado en la zona: <z> (552)	E552	"YS"
Zona <z> anulada	E570	"UB"
Zona <z> anulada	E571	"FB"
Zona <z> anulada	E572	"MB"
Zona <z> anulada	E573	"BB"
Anulación de grupo por usuario: <v>	E574	"CG"
Zona <z> anulada	E576	"UB"
Bypass en zona <z> cancelado	E577	"UB"
Ventilación de zona anulada	E579	"UB"
Prueba de recorrido activada por usuario <v>	E607	"TS"
Informe de prueba manual	E601	"RX"
Informe de test periódico	E602	"RP"
Evento del sistema (605)	E605	"JL"
Evento del sistema (606)	E606	"LF"
Problema en el informe de test periódico	E608	"RY"

Evento del sistema	Código de informe CID	Código de informe de SIA
Evento del sistema (622)	E622	"JL"
Evento del sistema (623)	E623	"JL"
Hora y fecha restablecida por usuario <v>	E625	"JT"
Fecha/hora inexacta	E626	"JT"
Programación de sistema iniciada	E627	"LB"
Programación del sistema terminada	E628	"LS"
Evento del sistema (631)	E631	"JS"
Evento del sistema (632)	E632	"JS"
Sistema no activo (654)	E654	"CD"
Alarma médica restaurada	R100	"MH"
Emergencia personal restaurada	R101	"QH"
No más alarma de incendio en la zona: <z>	R110	"FH"
No más alarma de flujo de aguas en la zona: <z>	R113	"SH"
Alarma de pánico restablecida en la zona: <z>	R120	"PH"
Alarma de pánico cancelada por el usuario: <v>	R121	"HH"
Alarma de pánico restablecida en la zona: <z>	R122	"PH"
Alarma de pánico restablecida en la zona: <z>	R123	"PH"
Alarma de pánico restablecida en la zona: <z>	R124	"HH"
Alarma de pánico restablecida en la zona: <z>	R125	"HH"
No más alarma en la zona: <z>	R130	"BH"
No más alarma activa en la zona: <z>	R131	"BH"
No más alarma activa en la zona: <z>	R132	"BH"
No más alarma en la zona: <z>	R133	"BH"
No más alarma en la zona: <z>	R134	"BH"
No más alarma en la zona: <z>	R135	"BH"
No más tamper en la zona: <z>	R137	"TA"
No más alarma en la zona: <z>	R140	"UH"
No más fallo del sistema (143)	R143	"ER"
No más tamper en la zona: <z>	R144	"TR"
No más tamper en la zona: <z>	R145	"TR"
No más alarma en la zona: <z>	R146	"BH"
No más alarma en la zona: <z>	R150	"UH"
No más alarma de gas en la zona: <z>	R151	"GH"
No más alarma de pérdida de agua en la zona: <z>	R154	"WH"
Foil Rotura restaurado en la zona: <z>	R155	"BH"
La temperatura se ha normalizado en el sensor: <n>	R158	"KH"
La temperatura se ha normalizado en el sensor: <n>	R159	"ZH"
No más alarma de CO en la zona: <z>	R162	"GH"
No más falla en la zona de fuego: <z>	R200	"FV"
Monitoreo de restauración de alarma	R220	"BH"

Evento del sistema	Código de informe CID	Código de informe de SIA
No más fallo del sistema (300)	R300	"YA"
Fuente de alimentación AC OK	R301	"AR"
Batería OK	R302	"YR"
No más fallo del sistema (304)	R304	"YG"
Restablecimiento del sistema restaurado en la zona: <z>	R305	"RR"
No más fallo en batería (309)	R309	"YR"
Falla de tierra restablecido	R310	"UR"
No más fallo en batería (311)	R311	"YR"
Restaurar la sobrecarga de corriente de la fuente de alimentación (312)	R312	"YQ"
No más fallo en Sirena/Relé	R320	"RO"
No más fallo del sistema (321)	R321	"YH"
No más fallo del sistema (330)	R330	"ER"
No más fallo del sistema (332)	R332	"ER"
No más fallo del sistema (333)	R333	"ER"
No más fallo del sistema (336)	R336	"VR"
No más fallo del sistema (338)	R338	"ER"
No más fallo del sistema (341)	R341	"ER"
No más fallo del sistema (342)	R342	"ER"
No más fallo del sistema (344)	R344	"XH"
No más fallo de comunicación del sistema (350)	R350	"YK"
No más fallo de comunicación del sistema (351)	R351	"LR"
No más fallo de comunicación del sistema (352)	R352	"LR"
No más fallo del sistema (353)	R353	"YK"
No más fallo de comunicación del sistema (354)	R354	"YK"
No más fallo del sistema (355)	R355	"UJ"
Restablecido problema de fuego en zona: <z>	R373	"FJ"
No más problema en la zona: <z>	R374	"EA"
No más problema en la zona: <z>	R380	"UJ"
No más avería en zona inalámbrica: <z>	R381	"UR"
No más fallo del módulo inalámbrico (382)	R382	"BR"
No más tamper en la zona: <z>	R383	"TR"
Batería OK en zona inalámbrica: <z>	R384	"XR"
No más problema en la zona: <z> (391)	R391	"NS"
No más problema en la zona: <z> (393)	R393	"NS"
Usuario <v> armó el sistema	R400	"CL"
Usuario <v> armó el sistema	R401	"CL"
Armado automático	R403	"CA"
Usuario <v> armó de forma remota	R407	"CL"
Desarmado rápido	R408	"CL"
Armado remoto	R409	“CS”

Evento del sistema	Código de informe CID	Código de informe de SIA
Usuario <v> armó el modo Stay	R441	"CG"
Usuario <v> armó demasiado pronto	R451	“CK”
Usuario <v> desarmó el sistema demasiado tarde	R452	“CJ”
Usuario <v> Falló al cerrar	R454	“CI”
Armado parcial por el usuario: <v>	R456	"CG"
Recent disarm <v> user	R459	“CR”
Dispositivo habilitado (501)	R501	"RG"
Dispositivo habilitado (520)	R520	"RC"
Sensor inalámbrico habilitado en la zona: <z> (552)	R552	"YK"
Bypass en zona <z> cancelado	R570	"UU"
Bypass en zona <z> cancelado	R571	"FU"
Bypass en zona <z> cancelado	R572	"MU"
Bypass en zona <z> cancelado	R573	"BU"
Anulación de grupo por usuario: <v> cancelada	R574	"CF"
Bypass en zona <z> cancelado	R576	"UU"
Bypass en zona <z> cancelado	R577	"UU"
Bypass de la zona de ventilación cancelada	R579	"UU"
Prueba de recorrido desactivada por usuario <v>	R607	"TE"
Hora y fecha restablecida por usuario <v>	R625	"JT"
Sistema activo (654)	R654	"CD"