

Comunicador Ethernet E16T_2

Manual de Instalación

Marzo, 2021



CONTENIDO

REQUERIMIENTOS DE SEGURIDAD	3
1 DESCRIPCIÓN	4
1.1 ESPECIFICACIONES.....	5
1.2 TABLERO DEL COMUNICADOR.....	5
1.3 PROPÓSITO DE LAS TERMINALES.....	5
1.4 LED INDICADOR DE OPERACIÓN	6
1.5 ESQUEMA ESTRUCTURAL DEL USO DEL DISPOSITIVO E16T_2	7
2 ¿CÓMO CONFIGURAR EL COMUNICADOR CON EL SOFTWARE DE TRIKDISCONFIG?.....	7
2.1 OPCIONES DE CONEXIÓN PARA LA APP DE PROTEGUS	8
2.2 CONFIGURACIÓN PARA CONECTARSE CON EL CRA	9
3 DIAGRAMAS DE CONEXIÓN, INSTALACIÓN Y PUESTA EN SERVICIO.....	10
3.1 CABLEADO DEL COMUNICADOR AL PANEL DE CONTROL DE SEGURIDAD	10
3.2 ESQUEMAS PARA CONECTAR A LA ZONA DEL INTERRUPTOR DE LLAVE DEL PANEL	10
3.3 DIAGRAMAS PARA LA CONEXIÓN DE ENTRADA.....	11
3.4 CONECTAR EL CABLE LAN	11
3.5 ESQUEMAS DE CABLEADO DE UN RELÉ	12
3.6 ESQUEMAS PARA LA CONEXIÓN DE MÓDULOS DE EXPANSIÓN DE LA SERIE DE IO	12
3.7 CAMBIANDO EN LA FUENTE DE ALIMENTACIÓN PARA EL PANEL DE CONTROL.....	12
4 PROGRAMACIÓN DEL PANEL DE CONTROL	12
4.1 PROGRAMACIÓN DE COMUNICADOR TELEFÓNICO DE HONEYWELL VISTA.....	13
4.2 AJUSTES ESPECIALES PARA PANEL DE HONEYWELL VISTA 48	13
5 CONECTADO EL COMUNICADOR A LA APP PROTEGUS	13
5.1 CONFIGURACIONES ADICIONALES PARA ARMAR/DESARMAR EL SISTEMA CON LA ZONA KEYSWITCH.....	14
5.2 CONTROL DEL SISTEMA CON PROTEGUS.....	15
6 DESCRIPCIÓN DE LA VENTANA DE TRIKDISCONFIG	16
6.1 BARRA DE ESTADO	16
6.2 VENTANA DE “AJUSTES DEL SISTEMA”	17
6.3 VENTANA DE “CRA INFORMES”	18
6.4 VENTANA DE “INFORMES PARA USUARIO”	20
6.5 VENTANA DE “AJUSTES DE ETHERNET”	20
6.6 VENTANA DE “IN/OUT”	21
6.7 VENTANA DE “RS485 MODULES”	21
6.8 VENTANA DE “RESUMEN DEL INCIDENTE”	23
6.9 RESTABLECER LA CONFIGURACIÓN DE FÁBRICA	24
7 CONFIGURACIÓN REMOTA	24
8 DESEMPEÑO DE LA PRUEBA DEL COMUNICADOR	24
9 ACTUALIZACIÓN DEL FIRMWARE	25
10 ANEXO 26	



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

E16T_2 es un comunicador y se conecta a cualquier panel de alarma que tenga un comunicador telefónico y soporta el envío de los eventos en protocolo Contacto ID en tonos DTMF.

El comunicador puede transmitir información de eventos completos al CRA.

El comunicador funciona con la aplicación **Proteagus**. Los usuarios pueden controlar su sistema de alarma de forma remota y recibir notificaciones acerca de eventos. **Proteagus** aplicación, funciona con todos los paneles de control de distintos fabricantes, a la que está conectado el comunicador. El comunicador puede transmitir notificaciones de eventos a la Central Receptora de Alarmas y trabajar con **Proteagus** simultáneamente.

Características

Conexión al comunicador telefónico del panel de control:

- Se conecta al comunicador telefónico del panel de control con 2 o 4 cables.
- La conexión con 4 cables monitoreará la línea telefónica entre el panel de control y el comunicador.

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.
- Puede enviar información de eventos a SUR-GARD receptores. El anexo contiene tabla de conversión de los códigos (Contacto ID a SIA).
- 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 **Proteagus** está habilitado, los eventos se envían primero a CRA, y solo luego se envían a los usuarios de la aplicación.

Funciona con la aplicación Proteagus:

- Notificaciones de "Push" que informan sobre eventos.
- Armado/Desarmado de forma remota.
- Control remoto de dispositivos conectados (luces, portones/barreras, sistemas de ventilación, calefacción, aspersores, etc.).
- Monitorización remota de la temperatura (con los expansores **iO** y **iO-WL**).
- Diferentes derechos de usuario para administrador, instalador y usuario.

Informes a los usuarios finales:

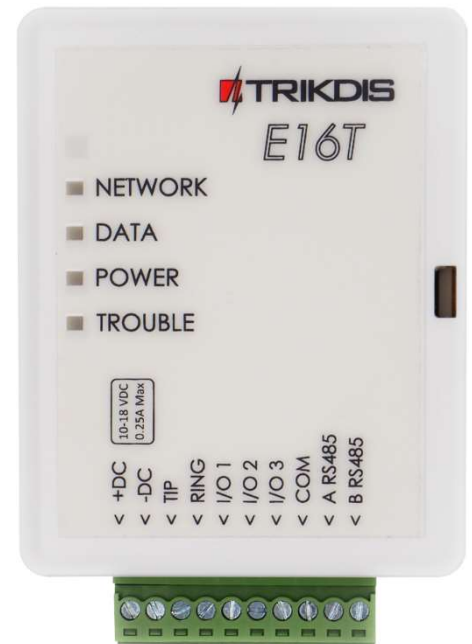
- Los usuarios pueden ser informados sobre eventos con aplicación **Proteagus**.

Salidas y entradas controlables:

- 3 entradas/salidas universales. Modo de funcionamiento se establece como entrada o salida.
- Salidas controladas por **Proteagus**.
- Añada controlable entradas y salidas adicionales con expansores **iO** cableados e inalámbricos.

Configuración rápida:

- Las configuraciones pueden guardarse en un archivo y escribirse rápidamente en otros comunicadores.



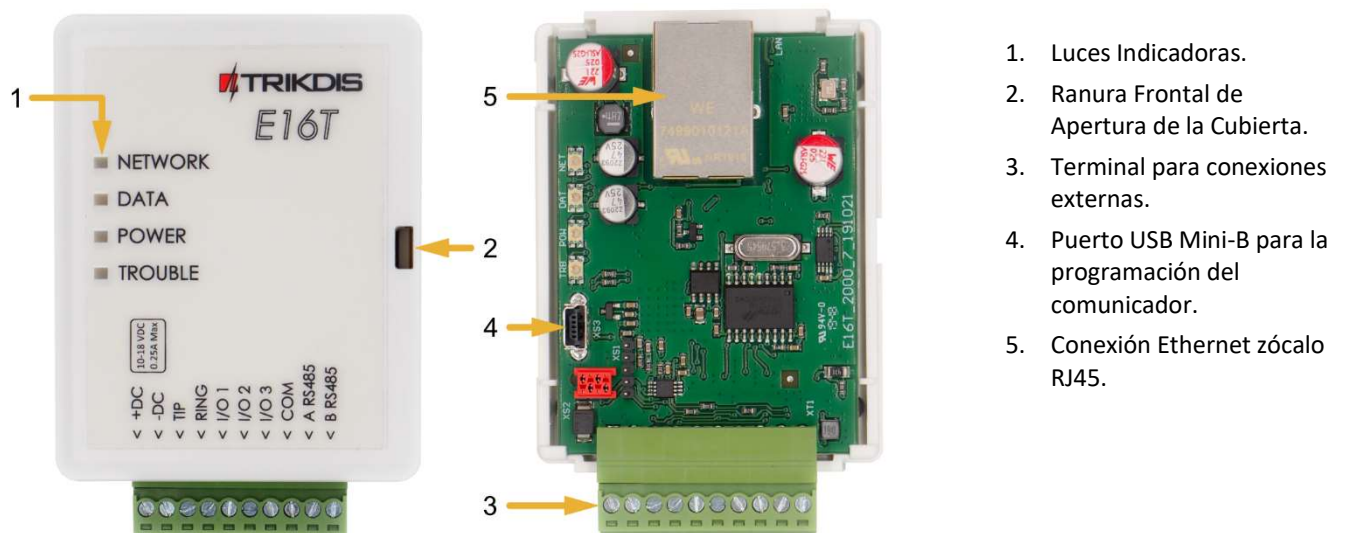


- Dos niveles de acceso para configurar el dispositivo para el administrador de CRA y para el instalador.
- Configuración remota y actualizaciones de firmware.

1.1 Especificaciones

Parámetro	Descripción
Voltaje de la fuente de alimentación	10-18 V DC
Consumo de Energía	60-100 mA (en modo de espera) Up to 250 mA (mientras envía datos)
Conexión Ethernet	Toma de corriente IEEE 802.3, 10 Base-T, RJ45
Entradas /Salidas universales	3, 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 = 10 k Ω), o la salida OUT (colector abierto (OC) 150 mA). Expandible con expansores de la serie <i>iO</i> .
Protocolos de Transmisión	TRK, DC-09_2007, DC-09_2012, TL150
Cifrado de mensajes	AES 128
Modificación de los ajustes	Con el software de configuración <i>TrikdisConfig</i> de forma remota o local a través del puerto USB Mini-B
Memoria	Hasta 60 mensajes
Entorno de Operación	Temperatura de -10 °C a 50 °C, humedad relativa - desde 80% a +20 °C
Dimensiones del Comunicador	88 x 65 x 25 mm
Peso	80 g

1.2 Tablero del Comunicador



1. Luces Indicadoras.
2. Ranura Frontal de Apertura de la Cubierta.
3. Terminal para conexiones externas.
4. Puerto USB Mini-B para la programación del comunicador.
5. Conexión Ethernet zócalo RJ45.

1.3 Propósito de las terminales

Terminal	Descripción
+DC	Terminal de fuente de alimentación (terminal positivo de 10-18 V CC)
-DC	Terminal de alimentación (terminal negativo de 10-18 V CC)
TIP	Terminal para conectar con panel de control TIP terminal
RING	Terminal para conectar con panel de control RING terminal



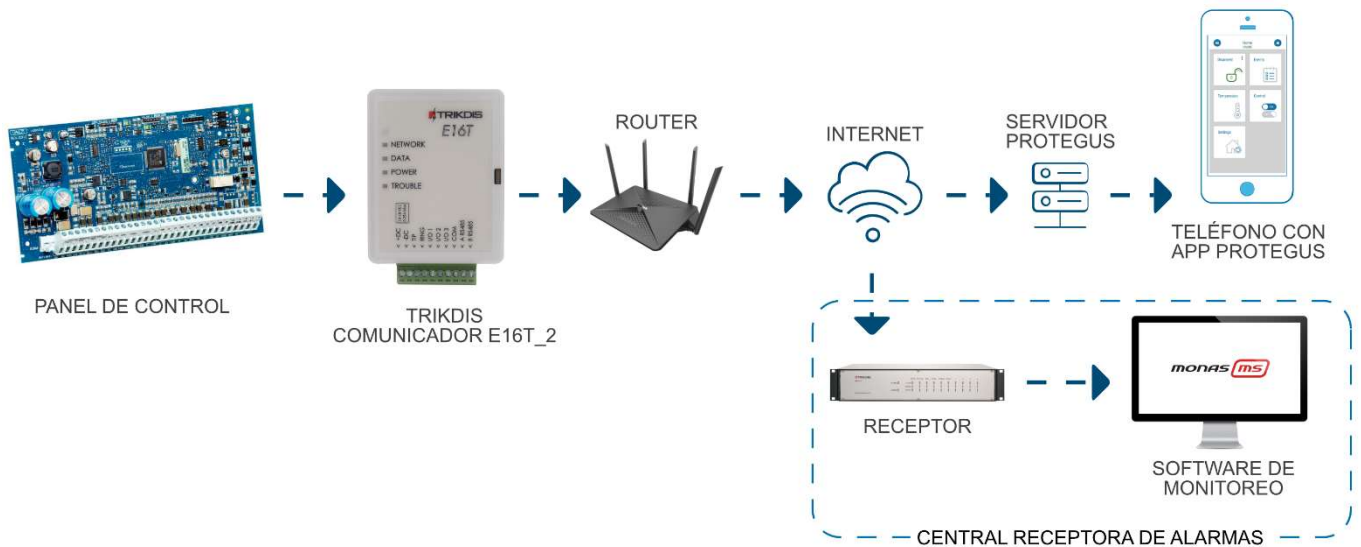
Terminal	Descripción
I/O 1 (T-1)	Terminal para el control de la línea telefónica o un terminal de entrada/salida, el tipo seleccionable: NC; NO; NC / EOL; NO / EOL; NC / DEOL; NO / DEOL. (predeterminado de fábrica - APAGADO)
I/O 2 (R-1)	Terminal para el control de la línea telefónica o un terminal de entrada/salida, el tipo seleccionable: NC; NO; NC / EOL; NO / EOL; NC / DEOL; NO / DEOL. (predeterminado de fábrica - ENTRADA, NO circuito)
I/O 3	Terminal de entrada/salida, el tipo seleccionable: NC; NO; NC / EOL; NO / EOL; NC / DEOL; NO / DEOL. (predeterminado de fábrica - SALIDA)
COM	Común (negativo)
A RS485	Contacto RS485 para conectar la entrada iO o expansor de salida u otros aditamentos
B RS485	

1.4 LED indicador de operación

Indicador	Estado de la luz	Descripción
NETWORK (Red)	Off	No conectado a una red de computador
	Verde sólido	El comunicador está conectado a una red de computador
DATA (Datos)	Off	No hay eventos no enviados
	Verde sólido	Los eventos no enviados se almacenan en el búfer
	Amarillo sólido	El panel de control llama al CRA
	Verde parpadeando	(Modo de configuración) Los datos se transfieren a/desde el comunicador
POWER (Poder)	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 ($\leq 11.5V$)
	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 (Problema)	Off	No hay problemas de operación
	1 parpadeo rojo	Error de conexión en el nivel "físico" (PHY Link status error)
	2 parpadeos rojos	Error de DHCP
	3 parpadeos rojos	Error de DNS
	6 parpadeos rojos	No hay conexión con el receptor
	7 parpadeos rojos	Conexión perdida con el panel de control
	Parpadeo rojo	(Modo de configuración) Fallo de memoria
	Rojo sólido	(Modo de configuración) El firmware está dañado



1.5 Esquema estructural del uso del dispositivo E16T_2



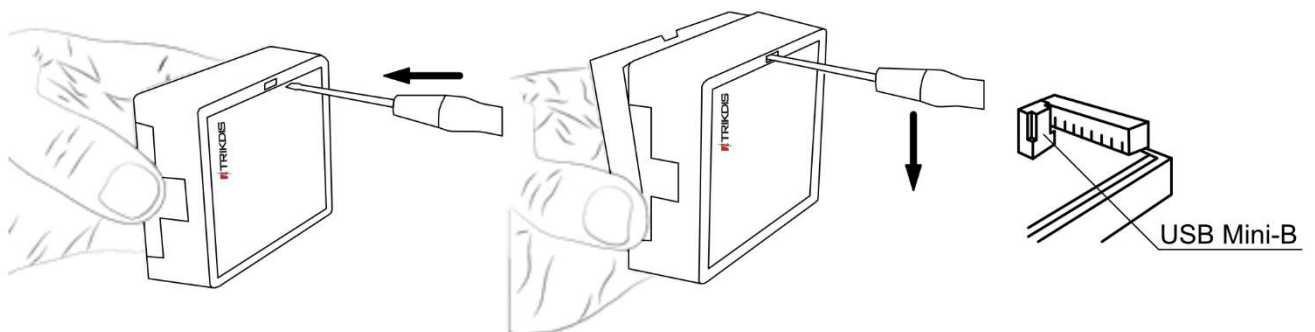
Nota: Antes de empezar, asegúrese de tener todo lo necesario:

1. Cable USB (tipo Mini-B) para la configuración.
2. Cable Ethernet CAT-5 (hasta 100 m de largo).
3. Por lo menos 4 alambres para conectar el comunicador con el panel de control.
4. Desatornillador de cabeza plana.
5. Manual de instalación del panel de control de seguridad.

Ordene los componentes necesarios de forma separada de su distribuidor 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 **E16T_2** con el desatornillador de cabeza plana como se muestra a continuación:



3. Usando el cable USB mini-B conecte el **E16T_2** 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 **Leer [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 *Proteagus*.



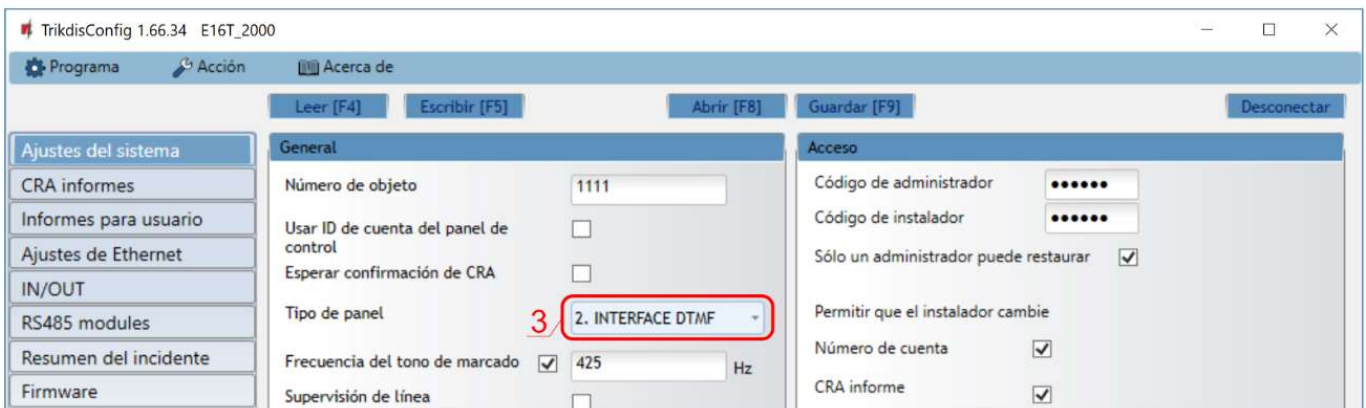
2.1 Opciones de conexión para la app de Protegus

En la ventana de “Informes para usuario”:



1. Seleccione la casilla “Activar conexión” a la nube de **PROTEGUS**.
2. Puede cambiar el **Contraseña Protegus** para iniciar sesión en **Protegus** si desea que se le pida a los usuarios que ingresen al agregar el sistema a la aplicación **Protegus** (contraseña predeterminada - 123456).

Ventana de “Ajustes del sistema”:



3. Seleccione el tipo de panel que será conectado al comunicador.

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

Nota: Para más información sobre otras opciones de **E16T_2** en **TrikidisConfig** vea el capítulo 6 de “Descripción de la ventana de TrikidisConfig”.

Importante: No se olvide de activar comunicador telefónico del panel de control y configurarlo correctamente, por lo que el panel enviaría a los eventos. Configuración del panel de control se describe en el capítulo 4 „Programación del panel de control”.



2.2 Configuración para conectarse con el CRA

En la ventana de “Ajustes del sistema”:

1. Ingrese el número de ID del objeto (No utilice números de objeto FFFE, FFFF.).
2. Seleccione el tipo de panel que será conectado al comunicador.

En la ventana de opciones de “CRA informes” para el “CRA ajustes”:

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

Nota: Si usted seleccione el protocolo DC-09, adicionalmente en la pestaña de Opciones ingrese los números del objeto, línea y receptor.

9. (Recomendado) Configure las opciones de respaldo del canal primario.
10. (Recomendado) Configure el canal segundo y su configuración de canal de respaldo paralelo.

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



Nota: Para más información sobre otras opciones de **E16T_2** en **TrikdisConfig**, vea el capítulo 6 “Descripción de la ventana de TrikdisConfig”.

Importante: No se olvide de activar comunicador telefónico del panel de control y configurarlo correctamente, por lo que el panel enviaría a los eventos. Configuración del panel de control se describe en el capítulo 4 „Programación del panel de control”.

3 Diagramas de conexión, instalación y puesta en servicio

3.1 Cableado del comunicador al panel de control de seguridad

Siguiendo uno de los esquemas proporcionados a continuación, conecte el comunicador hacia el panel de control.

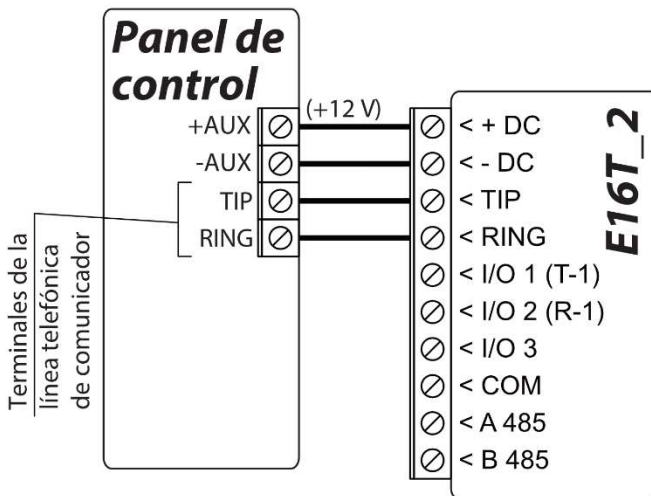


Diagrama de cableado del comunicador, cuando la supervisión de la línea telefónica no está configurada.

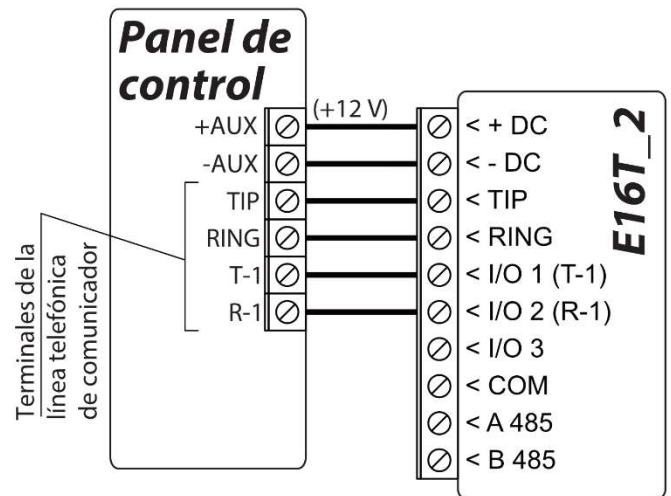
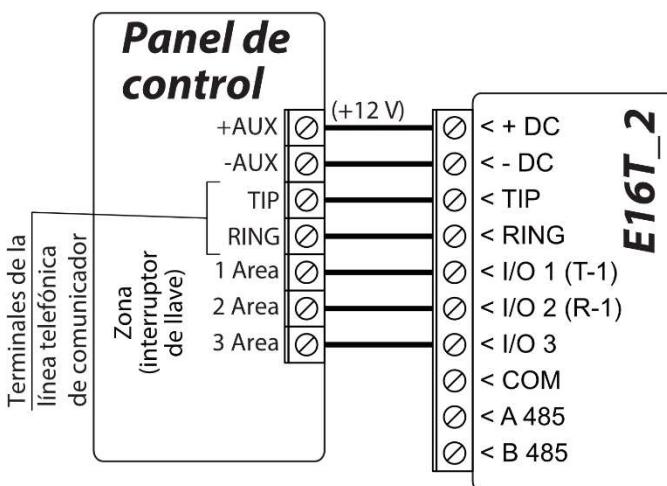
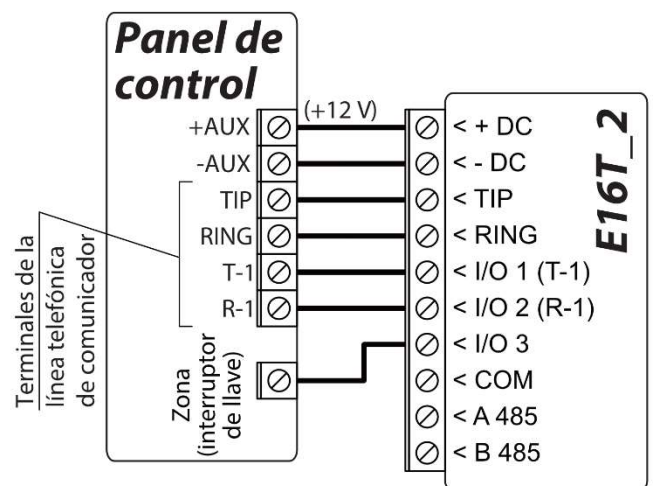


Diagrama de cableado del comunicador, cuando la supervisión de la línea telefónica está configurada.

3.2 Esquemas para conectar a la zona del interruptor de llave del panel



Armar / desarmar el panel a través de la zona de interruptor de llave, cuando la supervisión de la línea telefónica no está configurada.



Armar / desarmar el panel a través de la zona del interruptor de llave, cuando la supervisión de la línea telefónica está configurada.

Siga estos esquemas si el panel de control se armará/desarmará con la salida PGM del **E16T_2** activando/desactivando la zona de interruptor de llave del panel.



Nota: El comunicador **E16T_2** tiene 3 terminales de entrada/salida universales que se pueden configurar en un modo de operación OUT (PGM). Las salidas pueden controlar tres áreas del sistema de seguridad. La configuración de gestión de zona se realiza en la aplicación **Protequs**.

3.3 Diagramas para la conexión de entrada

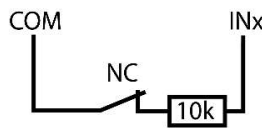
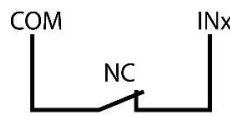
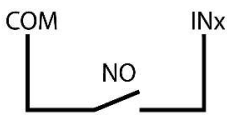
El comunicador tiene 3 terminales de entrada / salida universales que se pueden configurar en el modo de entrada IN. Los circuitos NC, NO, NO / EOL, NC / EOL, NO / DEOL, NC / DEOL pueden conectarse al terminal de entrada. Configuración de entrada I/O2 predeterminada - NO. El tipo de entrada se puede 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.

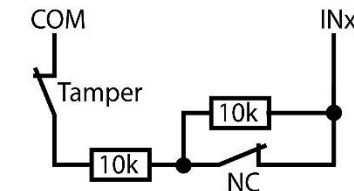
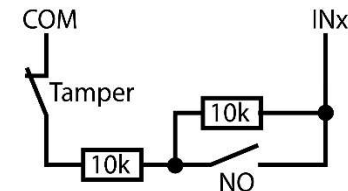
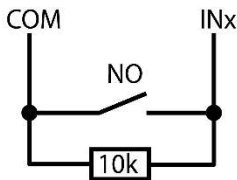
Circuito normalmente cerrado con resistencia 10k de fin de línea (EOL o fin de línea). Short - Alarm; Open - Alarm; 10k - Restore.



Circuito normalmente abierto con resistencia 10k de fin de línea (EOL o fin de línea). Short - Alarm; Open - Alarm; 10k - Restore.

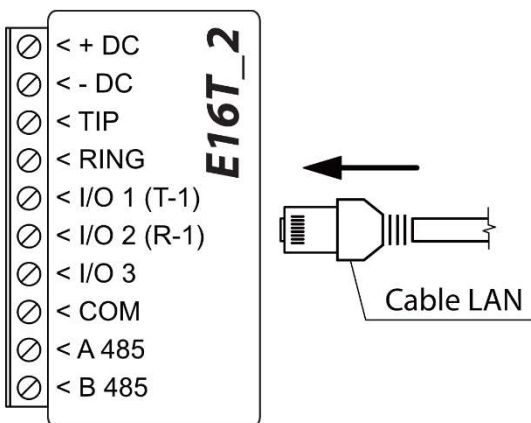
Circuito normalmente abierto con resistencia de fin de línea y reconocimiento de manipulación (NO con EOL y con sabotaje). Short - Tamper; Open - Tamper; 10k - Alarm; 15k-25k - Restore.

Circuito normalmente cerrado con resistencia de fin de línea y reconocimiento de manipulación (NC con EOL y reconocimiento de manipulación). Short - Tamper; Open - Tamper; 10k - Restore; 15k-25k - Alarm.



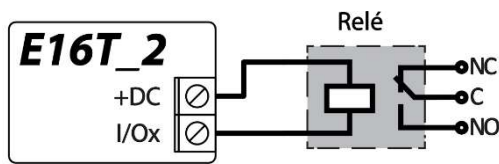
Nota: Si más entradas o salidas necesitan ser conectadas al comunicador, conecte el expansor alámbrico o inalámbrico serie **iO** de TRIKDIS. El método de conexión está descrito en el manual de **iO**.

3.4 Conectar el cable LAN





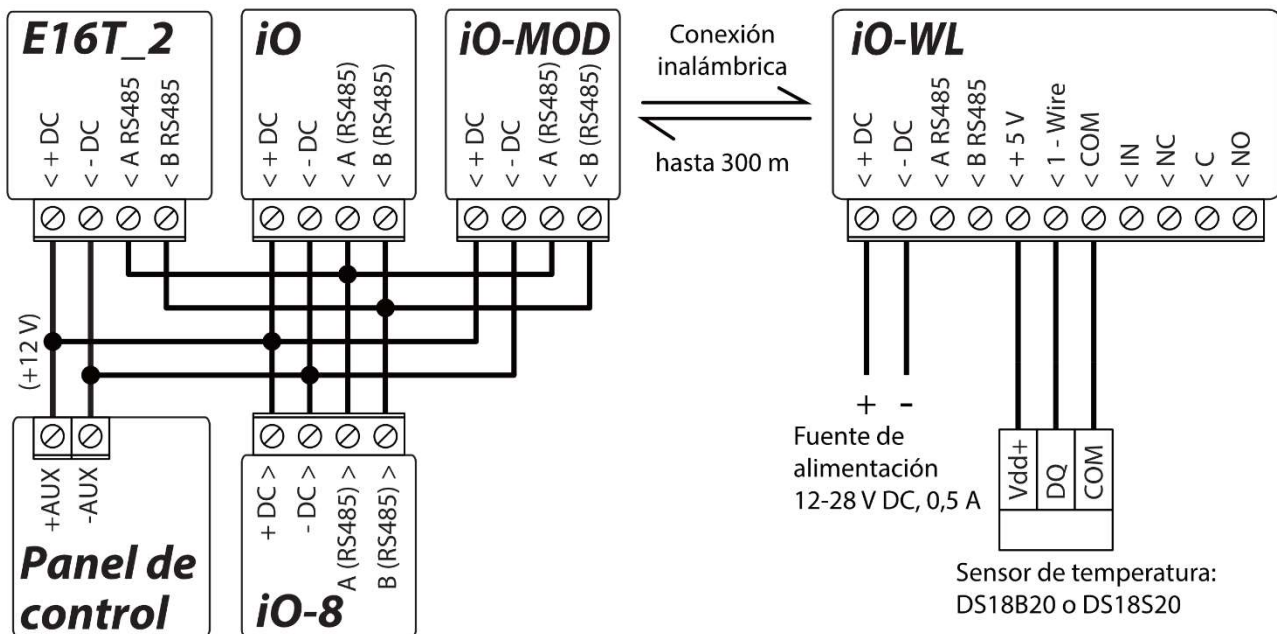
3.5 Esquemas de cableado de un relé



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).

3.6 Esquemas para la conexión de módulos de expansión de la serie de iO

Si es necesario conectar más entradas o salidas al comunicador, o si desea conectar un sensor de temperatura, conecte el expansor de salida inalámbrico o por cable de la serie **TRIKDIS iO**. Configuración de los módulos expansores conectados al **E16T_2** se describe en el capítulo 6.7 "Ventana "RS485 modules".



3.7 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 **E16T_2** debe mostrar:

- El LED de "POWER" se iluminará de color verde cuando se encuentre prendido;
- El LED de "NETWORK" se iluminará de color verde cuando se registre a una red.

Nota: Si la indicación de luz es diferente, consulte la sección 1.4 "LED indicador de operación" para determinar qué sucede. Si la indicación **E16T_2** no está encendida, verifique la fuente de alimentación y las conexiones.

4 Programación 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 estación de monitoreo (se puede utilizar cualquier número de más de 2 dígitos. La **E16T_2** recogerá y responderá cuando la central llame 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 **E16T_2**, 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 **E16T_2** 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 **Protegeus**. véase el capítulo 5.1 “Configuraciones adicionales para armar/desarmar el sistema con la zona keyswitch”.

4.1 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].

4.2 Ajustes especiales para panel de Honeywell Vista 48

Si desea utilizar el comunicador **E16T_2** con el panel Honeywell Vista 48, configure las siguientes secciones como se describe:

Sección	Datos	Sección	Datos	S	Sección	Datos
* 41	111 (# telefónico receptor)	* 60	1		* 69	1
* 42	1111	* 61	1		* 70	1
* 43	1234 (número de cuenta panel)	* 62	1		* 71	1
* 44	1234	* 63	1		* 72	1
* 45	1111	* 64	1		* 73	1
* 47	1	*65	1		* 74	1
* 48	7	* 66	1		* 75	1
* 50	1	* 67	1		* 76	1
* 59	0	* 68	1			

Cuando todos los ajustes necesarios están configurados, es necesario salir del modo de programación. Ingrese *99 en el teclado.

5 Conectado el comunicador a la app Protegeus

Con **Protegeus**, los usuarios podrán controlar su sistema de alarmas de forma remota. Podrán ver el estado del sistema y recibir notificaciones sobre eventos del sistema. **Protegeus** funciona con sistemas de seguridad de otras marcas, que soportan el comunicador **E16T_2**.

1. Descargue y abra la aplicación **Protegeus** o utilice la versión de navegador de internet: www.protegeus.eu/login:



2. Inicie sesión con su nombre de usuario y contraseña o regístrese para crear una nueva cuenta.
3. De clic en agregar un nuevo sistema e ingrese la dirección MAC **E16T_2**. Este número puede ser encontrado en el dispositivo y en la etiqueta del empaque.



Nota: Al agregar **E16T_2** a **Protegus**, revise si:

1. La servicio **Protegus** está activada. Podrá encontrar información sobre como activar la nube en la sección 6.4 Ventana de "Informes para usuario".
2. La fuente de alimentación está conectada (el LED de "POWER" debe iluminarse de color verde);
3. Estar registrado en la red (el LED de "NETWORK" de iluminarse de color verde).

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

Nota: La zona de panel de control, donde la salida del **E16T_2** se encuentra conectada, tiene que ser establecida a modo de keyswitch.

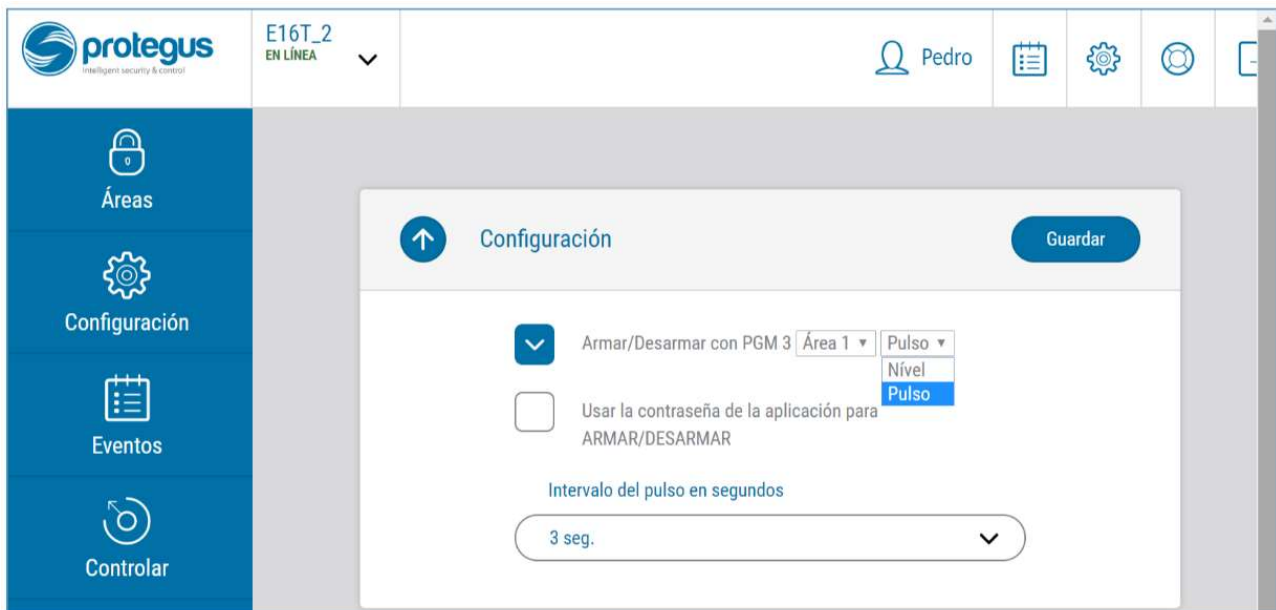
Siga las instrucciones de abajo si el panel de control no será controlado de forma directa, pero con la salida del **E16T_2** PGM, prendiendo/apagando el panel de control de la zona de keyswitch.

1. De clic en "Next" después de ingresar el número "MAC/Unique ID". En la nueva ventana de clic en "Áreas". En la siguiente ventana especifique cuantas áreas de sistema de alarma (1, 2, 3) están en el sistema y presione "Siguiete".

2. En la nueva ventana, identifique cuál es el número para cada una de las áreas especificadas en el sistema y presione "Guardar".

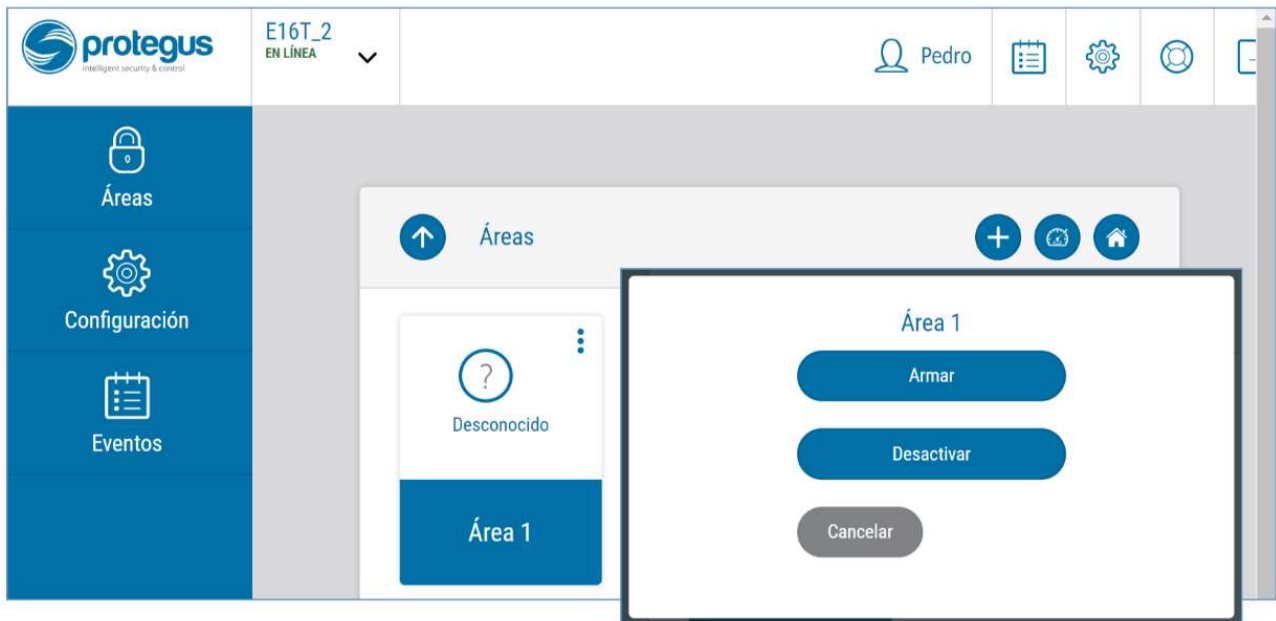


3. En el menú lateral, presione “Configuración” y en la nueva ventana presione “Configuración”. Seleccione la casilla de “Armadado/Desarmado con PGM” y especifique que área de salir será controlada. Una salida PGM puede controlar sólo un área (PGM 1 – Área 1, PGM 2 – Área 2, PGM 3 - Área 3).
4. Seleccione el Nivel o Pulso, dependiendo del tipo de la zona keyswitch del panel de control. También puede cambiar la duración o intervalo de pulso si es requerido para el panel de control conectado.
5. Para mayor seguridad, puede seleccionar "Usar la contraseña de la aplicación para ARMAR/DESARMAR". Luego, al presionar el botón de armar/desarmar se abrirá la ventana de solicitud de ingreso de contraseña de la aplicación.



5.2 Control del sistema con Protegeus

1. Para controlar el sistema, vaya a la ventana de “Área”.
2. En la ventana de “Área” de clic en el botón de área. En la nueva ventana seleccione la acción (Armar o Apagar el área de sistema de seguridad).
3. Si es solicitado, ingrese el código de usuario o la contraseña de **Protegeus**.



6 Descripción de la ventana de TrikdirConfig

6.1 Barra de Estado

Después de conectar **E16T_2** y haciendo clic en **Leer [F4]**, **TrikdirConfig** proporcionará información sobre el dispositivo conectado en la barra de estado.

MAC/ID única: 801F126244E7						
Estado: lectura finalizada	Dispositivo: E16T_2000	SN: 001009	BL: 1.00	FW: 1.10	HW: 0.01	Estado: HID Administrado

Barra de Estado

Nombre	Descripción
Identificación única	Número MAC del dispositivo
Estado	Estado de acción
Dispositivo	Tipo de dispositivo (E16T_2)
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)

Después de pulsar **Leer [F4]**, el programa leerá y mostrará los ajustes, que se establecen en **E16T_2**. Establecerá los ajustes necesarios de acuerdo con las descripciones de las ventanas del **TrikdirConfig** las cuales se dan a continuación.



6.2 Ventana de “Ajustes del sistema”

TrikidisConfig 1.66.34 E16T_2000

Programa Acción Acerca de

Leer [F4] Escribir [F5] Abrir [F8] Guardar [F9] Desconectar

Ajustes del sistema

CRA informes

Informes para usuario

Ajustes de Ethernet

IN/OUT

RS485 modules

Resumen del incidente

Firmware

Recordar contraseña

Mostrar contraseña

General

Número de objeto 1111

Usar ID de cuenta del panel de control

Esperar confirmación de CRA

Tipo de panel 2. INTERFACE DTMF

Frecuencia del tono de marcado 425 Hz

Supervisión de línea

Tiempo de sincronización Servicio PROTEGUS

Acceso

Código de administrador

Código de instalador

Sólo un administrador puede restaurar

Permitir que el instalador cambie

Número de cuenta

CRA informe

Informes para el usuario

Ajustes de Ethernet

Resumen del incidente

Grupo de opciones “General”

- **Número de objeto** - si van a enviar los eventos al CRA (Central Receptora de Alarmas), introduzca el número de cuenta proporcionado por el CRA (4 caracteres número hexadecimal, 0-9, A-F. **No utilice números de objeto FFFE, FFFF.**).
- **Usar ID de cuenta del panel de control** - Si se selecciona la casilla, el comunicador enviará con eventos no con el valor establecido en el campo ID de objeto, pero la ID de cuenta ingresada en el panel.
- **Esperar confirmación de CRA** - Si se selecciona la casilla, después de enviar cada evento, el comunicador esperará el recibo del receptor de IP, que ha recibido correctamente el mensaje de evento. Si el comunicador no recibe la señal de recibo, no formará la señal de finalización de la comunicación (kiss-off). Después de no recibir el mensaje de Kiss-off, el comunicador telefónico del panel de control transmitirá repetidamente el mensaje del evento.
- **Tipo de panel** - activar/desactivar la interfaz de línea fija DTMF en el comunicador.
- **Frecuencia de tono de marcado** - Frecuencia en la que el **E16T_2** comunica con el comunicador telefónico de panel de control.
- **Supervisión de línea**- si se selecciona esta casilla, se supervisará la conexión de línea fija entre el panel de control y comunicador. Para la supervisión de trabajo, el comunicador telefónico del panel de control tiene que estar conectado con el **E16T_2** con 4 hilos (véase el capítulo 3.1 “Cableado del comunicador al panel de control de seguridad”).
- **Tiempo de sincronización** - seleccionar qué servidor utilizara para la sincronización de tiempo.

Grupo de opciones de “Acceso”

Al configurar el comunicador **E16T_2** hay dos niveles de acceso para el administrador e instalador:

- **Código de administrador** – permite el acceso a los campos de configuración.
- **Código de instalador** – acceso limitado para configurar el comunicador.
- **Sólo un administrador puede restaurar** - si esta casilla ha sido seleccionada, las configuraciones de fábrica pueden ser restauradas con tan sólo ingresar el código del administrador.
- **Permitir que el instalador cambie** – puede especificar que opciones pueden ser cambiadas por el instalador.

Nota: Los códigos de Administrador y de Instalador deben consistir de 6 dígitos o caracteres en latín.



6.3 Ventana de “CRA informes”

Pestaña de parámetros “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 a los software de monitoreo:

- **Para conectarse a través de IP** – software receptor IPcom Windows/Linux, hardware IP/SMS receptor RL14 o receptor multicanal RM14.

Grupo de opciones del “Canal de comunicación principal”

- **Modo** – seleccione que método de conexión será usado: IP.
- **Protocolo** – seleccione en que tipo de código serán enviados los eventos: TRK (a receptor TRIKDIS); DC-09_2007 o DC-09_2012 (a receptores universales); TL150 (a receptor SUR-GARD).
- **Clave de cifrado TRK** – Ingrese la llave de encriptación que está establecida en el receptor.
- **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 “Segundo canal”

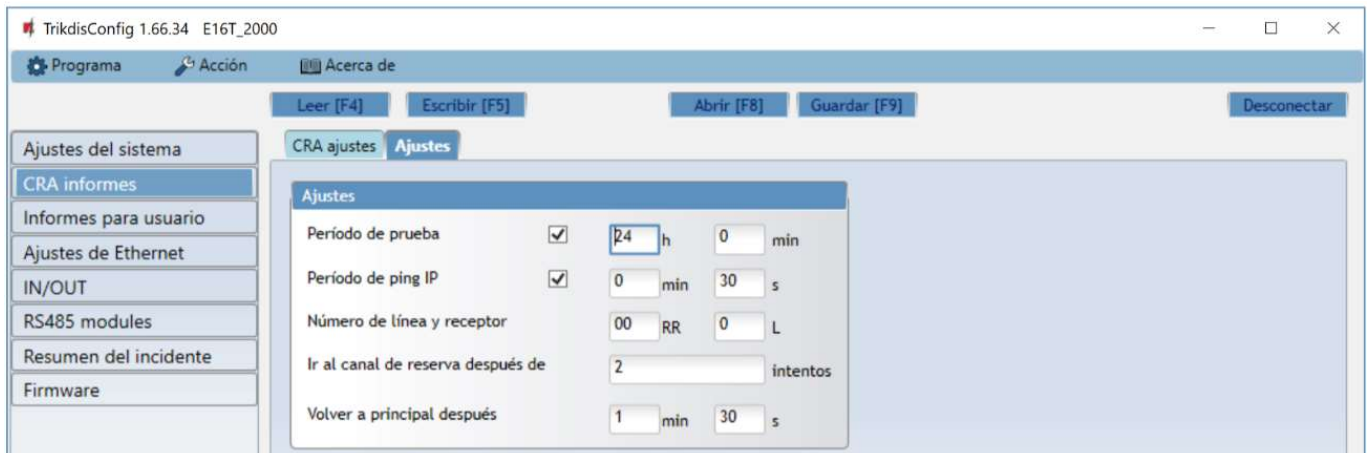
Los eventos de este canal son transmitidos en paralelo con el primer canal. Cuando el segundo canal es habilitado, los eventos pueden ser enviados de forma simultánea por dos receptores (por ejemplo., estaciones de monitoreo local y centralizado) Las opciones del canal paralelo son las mismas que las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

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.



Pestaña de “Ajustes”



Grupo “Ajustes”

- **Periodo de prueba** – el periodo de evento de PRUEBA para la prueba de la conexión. Los eventos de prueba son enviados como mensajes de Contacto ID y son reenviados al software de monitoreo.
- **Periodo de ping IP** – periodo para enviar corazonadas PING internas. El receptor no reenviara los mensajes PING al software de monitoreo para evitar sobre cargarlo. Las notificaciones sólo serán enviadas al software de monitoreo si el receptor falla en recibir los mensajes PING del dispositivo dentro de un lapso de tiempo establecido.
Por defecto, la notificación de “Conexión perdida” será transmitida al software de monitoreo si el mensaje PING no es recibido en el receptor en tiempos mayores al establecido en el dispositivo. Por ejemplo, si el PING es establecido para 3 minutos, el receptor transferirá la notificación de “Conexión perdida” si no recibe un PING en los próximos 9 minutos.
Las corazonadas de PING mantienen la sesión activa de comunicación entre el dispositivo y el receptor. Una sesión activa es requerida para conexiones remotas, control y configuración del dispositivo. Recomendamos establecer un periodo de PING no mayor a 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** – tiempo en el que después el **E16T_2** intentará reconectarse y transmitir mensajes a través de un canal Primario.

Grupo de opciones de “Configuración DC-09”

Las opciones son mostradas cuando el protocolo DC-09_2007 o DC-09_2012 es establecido en el campo de Protocolo del canal de comunicación para enviar eventos a los receptores universales.

- **ID de objeto en DC-09** – ingrese el número del objeto. Si la codificación DC-09 es seleccionada, el número del objeto ingresado en el campo será usado. Se puede ingresar un número hexadecimal de 3 a 16 caracteres. El número es provisto por el centro de recibimiento de alarmas.
- **Núm. de línea DC-09** – ingrese el número de línea en el receptor.
- **Núm. de receptor DC-09** - ingrese el número del receptor.



6.4 Ventana de “Informes para usuario”

Pestaña de la “Servicio Protegus”



- **Activar conexión** – permita que el comunicador se conecte a la nube de **Protegus**.
- **Código de acceso a Protegus** – aquí puede cambiar la contraseña para conectarse al servidor de **Protegus** (por defecto esta es – 123456). Si la contraseña ha sido cambiada usted tendrá que reingresarla cuando agregue el sistema en la app de **Protegus**. Esta es una medida de seguridad adicional.

6.5 Ventana de “Ajustes de Ethernet”



Grupo de opciones de “Ajustes de Ethernet”

- **Usar DHCP** – marque la casilla para que el comunicador se registre automáticamente en la red. Si el registro automático falla, deberá ingresarlo manualmente:
 - **IP estática** – dirección IP del comunicador.
 - **Máscara de subred** – máscara de subred.
 - **Por defecto gateway** – para conectarse a internet.
 - **DNS1, DNS2** – (Sistema de Nombre de Dominio) identifica el servidor que especifica la dirección IP del dominio. Usada cuando el dominio está establecido en el campo de canal de comunicación de Dominio o IP (no dirección IP). Las opciones por defecto son direcciones de servidores DNS establecidas por Google.



6.6 Ventana de “IN/OUT”

Terminal	Propósito	Tipo
1	Apagado	
2	IN	NO
3	OUT	

Incidente	Código del incidente del ID de contacto			Código del restauración del ID de contacto						
	Activar	E/R	CID	Part.	Zona	Activar	E/R	CID	Part.	Zona
IN2_ALARM	<input checked="" type="checkbox"/>	Incidenti	130	99	002	<input checked="" type="checkbox"/>	Restaura	130	99	002
IN2_TAMPER	<input checked="" type="checkbox"/>	Incidenti	144	99	002	<input checked="" type="checkbox"/>	Restaura	144	99	002

El comunicador tiene 3 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, que se enviará a CRA y **Protequs**.

- **Activar** – verifique los campos del evento donde se enviarán los mensajes a CRA y **Protequs**.
- **E/R** – especifique la condición de envío del evento interno del comunicador (Evento o Restablecimiento).
- **CID** – código de evento.
- **Part.** – ingrese el número de área que se enviará cuando ocurra el evento interno y se reinicie el sistema.
- **Zona** - ingrese el número de zona que se enviará cuando ocurra el evento interno y el sistema se reinicie.

6.7 Ventana de “RS485 modules”

El comunicador se puede conectar a un expansor de la serie **iO** para agregar entradas adicionales, salidas controladas y un bus para sensores de temperatura. Los extensores conectados deben incluirse en la tabla Lista de módulos.

ID	Tipo de módulo	Serial Núm.
1	No disponible	
2	No disponible	
3	expansor iO	
4	expansor iO-WL	

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 caja 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** e **iO**.

Ventana de ajustes del expansor iO-8

Código del incidente del ID de contacto						Código del restauración del ID de contacto						
Incidente	Activar	E/R	CID	Part.	Zona	Activar	E/R	CID	Part.	Zona	Númerc	Tipo de e
BUS_FAULT	<input checked="" type="checkbox"/>	Incidenti	333	91	001	<input checked="" type="checkbox"/>	Restaura	333	91	001		
INPUT1	<input checked="" type="checkbox"/>	Incidenti	130	91	001	<input checked="" type="checkbox"/>	Restaura	130	91	001		NO
INPUT2	<input checked="" type="checkbox"/>	Incidenti	130	91	002	<input checked="" type="checkbox"/>	Restaura	130	91	002		NO
INPUT3	<input checked="" type="checkbox"/>	Incidenti	130	91	003	<input checked="" type="checkbox"/>	Restaura	130	91	003		NO

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

- **Recuento de entradas** - 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 **Protegeus**. 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 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 **Protegeus**.

Código del 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** - asigne un código de evento de ID de contacto a la entrada.
- **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 del 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** - asigne un código de restauración del ID de contacto a la entrada.
- **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 o NC).



Ventana de ajustes del expansor iO

Código del incidente del ID de contacto						Código del restauración del ID de contacto					
Incidente	Activar	E/R	CID	Part.	Zona	Activar	E/R	CID	Part.	Zona	
INPUT	<input checked="" type="checkbox"/>	Incidenti	130	91	001	<input checked="" type="checkbox"/>	Restaura	130	91	001	
HIGH_TEMPERATURE	<input checked="" type="checkbox"/>	Incidenti	158	91	001	<input checked="" type="checkbox"/>	Restaura	158	91	001	
LOW_TEMPERATURE	<input checked="" type="checkbox"/>	Incidenti	159	91	001	<input checked="" type="checkbox"/>	Restaura	159	91	001	
BUS_FAULT	<input checked="" type="checkbox"/>	Incidenti	333	91	001	<input checked="" type="checkbox"/>	Restaura	333	91	001	

El expansor iO dispone de: terminales para 1 entrada, 1 salida (contactos de relé) y bus serie 1-Wire para la conexión de sensores de temperatura.

- **Tipo de entrada IN** - ajuste el tipo de entrada (NO o NC).
- **Max °C (T1)** - cuando la temperatura es superior a esta configuración, se genera un mensaje de evento. Para que se genere un mensaje de evento, éste debe estar habilitado en la tabla.
- **Min °C (T2)** - cuando la temperatura es inferior a esta configuración, se genera un mensaje de evento. Para que se genere un mensaje de evento, éste debe estar habilitado en la tabla.

En la tabla se pueden asignar entradas de eventos de Contacto ID y códigos de restauración. Después de que se activa una entrada, el comunicador enviará un evento con el código de evento establecido al receptor en el CRA y a la aplicación **ProteguS**. Ajuste la configuración como se describe en la página anterior acerca de la **Ventana de ajustes del expansor iO-8**.

6.8 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.

Código del incidente del ID de contacto						Código del restauración del ID de contacto					
Incidente	Activar	E/R	CID	Part.	Zona	Activar	E/R	CID	Part.	Zona	
COMMUNICATION	<input type="checkbox"/>	Incidenti	350	99	999	<input type="checkbox"/>	Restaura	350	99	999	
POWER	<input checked="" type="checkbox"/>	Incidenti	302	99	999	<input checked="" type="checkbox"/>	Restaura	302	99	999	
REMOTE_FINISHED	<input checked="" type="checkbox"/>	Incidenti	412	99	999	<input type="checkbox"/>	Incidenti				
REMOTE_STARTED	<input checked="" type="checkbox"/>	Incidenti	411	99	999	<input type="checkbox"/>	Incidenti				
START	<input checked="" type="checkbox"/>	Incidenti	700	99	999	<input type="checkbox"/>	Incidenti				
TEST	<input checked="" type="checkbox"/>	Incidenti	602	99	999	<input type="checkbox"/>	Incidenti				

- **COMMUNICATION** – mensaje de falla de comunicación entre el panel de control y **E16T_2**.
- **POWER** – aviso de baja tensión de red.
- **REMOTE_FINISHED** – mensaje sobre desconexión de configuración remota con **TrikidisConfig**.
- **REMOTE_STARTED** – mensaje de inicio de sesión remoto para configurar **E16T_2** con **TrikidisConfig**.
- **START** – mensaje sobre la conexión del **E16T_2** a la red.
- **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 Contact ID para cada evento, así como el número de zona y área que se informará.

6.9 Restablecer la configuración de fábrica

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

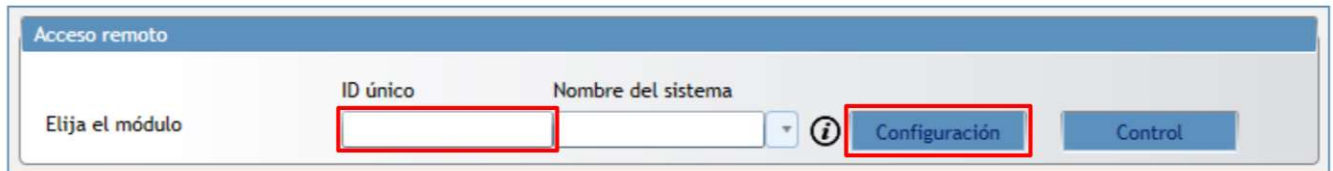


7 Configuración Remota

Nota: La configuración remota sólo funcionará si:

1. La servicio **Protegius** está activada. Podrá encontrar información sobre como activar la nube en la sección 6.4 Ventana de "Informes para usuario".
2. La fuente de alimentación está conectada (el LED de "POWER" debe iluminarse de color verde);
3. Estar registrado en la red (el LED de "NETWORK" de iluminarse de color verde).

1. En su PC abra el software de configuración de *TrikdisConfig*.
2. En la sección de acceso remoto ingrese la dirección MAC del comunicador. Este dirección 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]**.
6. A petición, ingrese el código del administrador o instalador. Para guardar la contraseña, seleccione "Recordar contraseña" en la ventana principal.
7. 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:

Genere un evento:

1. Asegúrese de que la alimentación esté encendida.
2. Verifique la conexión de red (el indicador de NETWORK es verde).
3. Generar un evento:
 - Armando y desarmando sistemas de seguridad;
 - Activando una alarma de zona cuando el sistema de seguridad esté armado.
4. Verifique que los eventos hayan sido recibidos por la Central Monitoring Station y / o el dispositivo **Protegius**.



5. Para probar la entrada del comunicador, ajuste el comunicador y verifique que los destinatarios reciban los mensajes correctos.
6. Para probar las salidas del comunicador, enciéndalas de forma remota y verifique su funcionamiento.
7. Si usa un panel de control remoto, active y desactive el modo de control del panel de forma remota con el applet **Protegius**.

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 existe una versión más nueva del firmware, el software ofrecerá descargar el archivo de la versión más nueva del firmware.
3. Seleccione la parte de Firmware del menú.



4. Presione **Abrir firmware** y seleccione el archivo de firmware requerido. Si no tiene el archivo, el archivo de la versión más nueva del firmware puede ser descargado por usuario registrado desde www.trikdis.com, bajo la sección de descargar del comunicador **E16T_2**.
5. Presione **Actualizar [F12]**.
6. Espere a que se complete la actualización.



10 Anexo

El comunicador puede funcionar con un receptor SUR-GARD. El comunicador recibidos desde panel de alarma 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"