Versión del manual: w1.5
Fecha de edición: 06.05.2019

CREATING A SENSE OF SECURITY
SINCE 1989

CENTRALITA DE ALARMAS

CPX230NWB

Manual de instalador

Versión de firmware:	2.10.0
Versión del Configurador de transmisores GPRS:	1.4.94.2
Versión del servidor OSM:	1.3.71.036

ES

DECLARACIÓN DE CONFORMIDAD

Nosotros, EBS Sp. z o.o., declaramos con plena responsabilidad que este producto cumple todos los requisitos de la Directiva 1999/5/CE del Parlamento Europeo y del Consejo de 9 de marzo de 1999. La copia de la «Declaración de conformidad» se puede encontrar en http://www.ebs.pl/certyfikaty/ .

INFORMACIÓN IMPORTANTE

El símbolo de contenedor tachado significa que en el terreno de la Unión Europea, después de terminar el uso de producto se debe eliminar en un punto destinado especialmente para ello. Esto se refiere al mismo dispositivo y a los accesorios marcados con este símbolo. No se debe tirar estos productos junto con los desechos comunales no sorteados.

El contenido del presente documento está presentado "tal como es — as is". No se otorga ninguna garantía tanto expresada como conjetural, incluyendo, pero sin limitación, cualquier garantía conjetural del uso comercial o utilidad para un objetivo concreto a menos que tales sean requeridas por las leyes vigentes. El fabricante se reserva el derecho a realizar cambios en este documento o retirarlo en cualquier momento sin previo aviso.

El fabricante del dispositivo promociona la política de continuo desarrollo. Se reserva el derecho a introducir cambios y mejoras de todas las funciones del producto descritas en el presente documento sin previo aviso.

La disponibilidad de las respectivas funciones dependerá de la versión del software del dispositivo. Para más detalles, póngase en contacto con el distribuidor más cercano.

En ninguna circunstancia el Fabricante se responsabiliza de cualquier pérdida de datos o ganancias o bien de cualquier especial, casual, resultante o intermedios daños ocasionados por cualquier manera.

FABRICANTE

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa, POLSKA
Correo electrónico: sales@ebs.pl
Asistencia técnica: support@ebs.pl
Sitio web: www.ebs.pl

CREATING A SENSE OF SECURITY
SINCE 1989

ÍNDICE

1. Introducción 7
2. FUNCIONES DE LA CENTRALITA 8
2.1. PARÁMETROS FUNCIONALES 8
2.2. PARÁMETROS TÉCNICOS 9
2.3. ACCESORIOS Y APLICACIONES 10
3. INSTALACIÓN Y CABLEADO 11
3.1. ORDEN DE INSTALACIÓN 11
3.2. DESCRIPCIÓN DE LOS COMPONENTES PCB 12
3.3. DESCRIPCIÓN DE LAS CONEXIONES POR TORNILLOS DE LA CENTRALITA 15
3.4. CONFIGURACIÓN DE LAS LÍNEAS DE ENTRADA ALÁMBRICAS 16
3.5. CONEXIÓN EJEMPLAR DE AVISADOR 18
3.5.1. Avisador interno sin propia alimentación 18
3.5.2. Avisador externo con propia alimentación 19
3.6. TECLADO ALÁMBRICO KP32 20
3.6.1. Descripción de los elementos de teclado 20
3.6.2. Características del teclado 23
3.6.3. Instalación del teclado 23
3.6.4. Direccionamiento de los dispositivos conectados al bus del teclado 24
3.7. TECLADO INALÁMBRICO KP2W 24
3.7.1. Añadir un teclado al sistema 25
3.7.2. Descripción de los elementos de teclado 25
3.7.3. Características del teclado 26
3.7.4. Montaje del dispositivo 27
3.7.5. Detector de apertura de puerta 27
3.8. UBICACIÓN DE LA CENTRALITA DE ALARMAS 28
3.9. INSTALACIÓN DE DETECTORES INALÁMBRICOS 29
4. MODO DE SERVICIO 30
4.1. ACTIVACIÓN DEL MODO DE SERVICIO 31
4.2. SALIDA DEL MODO DE SERVICIO 31
4.3. MENÚ DEL INSTALADOR EN EL MODO DE SERVICIO 31
4.3.1. Código de instalador 32
4.3.2. Desaparición de alimentación 32
4.3.3. Restablecimiento de la configuración de fábrica 33
4.3.4. Opciones del sistema 33
4.3.5. Administración remota de usuarios 34
4.3.6. Opciones avanzadas del sistema 34
4.3.7. Longitud de los códigos de acceso 35
4.3.8. Retraso en la desactivación de la señalización de alarmas históricas 36

4.3.9. Tiempo de detección del desvanecimiento de los detectores inalámbricos 36
4.3.10. Desactivación de la opción de repetición cíclica de los eventos de desvanecimiento de los detectores 37
4.3.11. Opción de repetición cíclica de los eventos de desvanecimiento de los detectores 37
4.3.12. Números ACN en la comunicación en formato Contact ID 37
4.3.13. Configuración de las líneas de detección (entradas) 38
4.3.14. Configuración de salidas 41
4.3.15. Configuración de particiones 42
4.3.16. Configuración de líneas inalámbricas 44
4.3.17. Configuración de mandos a distancia 46
4.3.18. Configuración de los botones de alarma en el teclado 48
4.4. MENSAJES DE TEXTO 49
5. PROGRAMA DE CONFIGURACIÓN 58
5.1. NOTAS PRELIMINARES 58
5.2. ORDENADOR – REQUISITOS 58
5.3. FUNCIONES DE PROGRAMA 58
5.3.1. Menú -> Archivo 59
5.3.2. Menú -> Operaciones 63
5.3.3. Menú -> Ayuda 65
5.4. PROGRAMACIÓN DEL DISPOSITIVO 65
5.4.1. Programación local 65
5.4.2. Programación remota 65
6. PARÁMETROS PROGRAMABLES 68
6.1. ACCESO 68
6.1.1. Parámetros 68
6.1.2. Parámetros del punto de acceso 69
6.1.3. Parámetros del servidor primario 70
6.1.4. Parámetros del servidor secundario 71
6.1.5. Acceso 71
6.2. TRANSMISIÓN 73
6.3. ENTRADAS /SALIDAS 74
6.3.1. Líneas (entradas) 74
6.3.2. Dispositivos inalámbricos 78
6.3.3. Particiones 81
6.3.4. Salidas 82
6.3.5. Mandos 84
6.3.6. Botones de alarma 85
6.4. OPCIONES DEL SISTEMA 86
6.4.1. Aviso de fallos memorizados mediante el parpadeo del diodo SYSTEM 86

6.4.2. Ignorar el fallo ATS 86
6.4.3. Requerir que se confirme el armado (con el botón #) en caso de fallo 87
6.4.4. El acceso al historial requiere autorización 87
6.4.5. Sin visualizar el estado de alarmas y bloqueos 87
6.4.6. Bloqueo temporal del teclado tras tres intentos de acceso fallidos 87
6.4.7. Utilizar un código de coacción 87
6.4.8. Visualizar el modo de armado de la partición en vez de violaciones y bloqueos de entradas 87
6.4.9. Bloqueo de la instalación 87
6.4.10. Bloqueo de restauración de los ajustes predeterminados 88
6.4.11. Bloqueo de los ajustes de comunicación 88
6.4.12. Permitir el armado rápido sin autorización del usuario 88
6.4.13. Desactivar la señalización de alarmas históricas tras el desarmado 89
6.4.14. Retraso en la desactivación de la señalización de alarmas históricas 89
6.4.15. Desactivar la posibilidad de armar mediante el teclado alámbrico durante una violación o un sabotaje de la línea 89
6.4.16. Tiempo de detección del desvanecimiento de los detectores inalámbricos 89
6.4.17. Repetir cada 89
6.4.18. Longitud del código de acceso 90
6.5. USUARIOS 91
6.5.1. Usuarios 91
6.5.2. Categorías 92
6.6. MONITOREO 92
6.6.1. Eventos 92
6.6.2. Modificadores 94
6.7. RESTRICCIONES 96
6.7.1. SMS y módems GSM 96
6.7.2. Comandos remotos 98
6.8. NOTIFICACIONES SMS 99
6.8.1. Teléfonos 99
6.8.2. Comunicaciones 99
6.8.3. Eventos 100
6.8.4. Opciones 101
6.8.5. Desvío de SMS 102
6.9. CONTROL DE COMUNICACIÓN 103
6.9.1. GSM 103
6.9.2. GPRS 103
6.10. FIRMWARE 104
6.11. MONITOR DEL DISPOSITIVO 105
6.12. HISTORIAL DE EVENTOS 107
7. SEÑALIZACIÓN CON DIODOS LED 109

7.1. REGISTRO EN LA RED 109
7.2. ALCANCE DE GSM 109
7.3. TRANSMISIÓN 109
7.4. PROGRAMACIÓN 110
7.5. ACTUALIZACIÓN DE FIRMWARE 110
7.6. NO HAY TARJETA SIM O LA TARJETA SIM ESTÁ DAÑADA 110
7.7. ERROR DEL SISTEMA 111
8. AJUSTES GRADE 2 111
8.1. AJUSTES DEL SISTEMA PARA GRADE 2 111
8.2. COMPORTAMIENTO DEL SISTEMA EN EL MODO DE COMPATIBILIDAD CON GRADE 2 112
9. ADITIVOS 113
9.1. COMANDOS REMOTOS Y PARÁMETROS DE CONFIGURACIÓN 113
9.1.1. Parámetros de configuración 114
9.1.2. Comandos generales 118
9.1.3. Comandos de gestión de usuarios 125
9.1.4. Comandos para administrar particiones, líneas y salidas 133
9.1.5. Comandos para la gestión de dispositivos inalámbricos 142
9.1.6. Comandos para la gestión de la seguridad de la configuración 144
9.2. Glosario de términos 146
10. HISTORIAL DE CAMBIOS 147

1. INTRODUCCIÓN

Agradecemos la selección de la centralita de la empresa EBS.

CPX230NWB es una simple y funcional centralita de alarmas con un módulo de comunicación GSM/GPRS/SMS integrado, destinada para edificios pequeños y medianos. La centralita cuenta con 3 salidas y 7 líneas de entrada alámbricas (hasta 14 para la configuración TEOL) y hasta 32 líneas inalámbricas que pueden dividirse en dos particiones. El teclado dedicado LED KP32 cuenta con un diseño moderno y discreto y discreto. Pequeñas dimensiones, grandes y cómodos botones y una simple instalación es una ventaja indiscutible de nuestro sistema.

2. FUNCIONES DE LA CENTRALITA

2.1. PARÁMETROS FUNCIONALES

ZONAS
- 7 líneas de entrada alámbricas para las siguientes configuraciones: NC / NO / EOL-NC / EOL-NO / DEOL-NC / DEOL-NO / TEOL
- Hasta 14 líneas de entrada alámbricas para la configuración TEOL
- Hasta 32 líneas de entrada inalámbricas
- Líneas de detección: inmediata, temporizada, pánico 24h, rearme/desarme por violación, sabotaje 24h, temporización condicional, pánico con alarma silenciosa 24h, incendio 24h, perimetral, perimetral de salida, gas 24h, inundación 24h, nocturna (deshabilitada de noche), nocturna temporizada, rearme/desarme por cambio de estado

SALIDAS PROGRAMABLES
- 1 salida de alarma con monitoreo, de alta corriente (corriente máx. 1,1A)
- 2 salidas de alarma vigiladas, de baja tensión (corriente máx. 50mA)

SALIDAS DE ALIMENTACIÓN
- 1 salida de avisador (corriente máx. 350mA)
- 1 salida de sensor (corriente máx. 350mA)
- 1 salida de teclado (corriente máx. 100mA)

PARTICIONES
- 2 particiones con posibilidad de atribuirles cualquier número de entradas

TECLADO
- compatibilidad con el teclado LED KP32
- posibilidad de conectar hasta tres teclados KP32
- compatibilidad con el teclado inalámbrico KP2W
- posibilidad de conectar hasta 32 KP2W (cada uno ocupa una de las líneas inalámbricas disponibles)

MANDO
- compatibilidad con el mando RC-10
- posibilidad de agregar hasta 32 mandos RC-10

TRANSMISIÓN
- Transmisión de señales por medio del módulo GPRS/SMS
- Cifrado de los datos enviados a través del estándar AES
- Comunicación con la estación de monitoreo por medio del servidor dedicado OSM.Server que garantiza una transmisión de datos fiable gracias a la función de redundancia
- Control de conexión GSM/GPRS: recuperación automática de la comunicación con la estación de monitoreo o conmutación al servidor de reserva

CONFIGURACIÓN
- Local, por medio del teclado KP32 o del ordenador
- Remota, por medio de GPRS, SMS ó CSD

USUARIOS

- 1 código de servicio (ATS: Alarm Transmission System, es un tipo especial de usuario que representa la estación de monitoreo y que se autentifica mediante el código principal de acceso)
- 1 código de instalador
- 1 código de administrador (principal)
- 31 códigos de usuarios
- Es posible restringir permisos para algunos códigos

OPCIONES DEL SISTEMA

- Diagnóstico automático de los básicos elementos del sistema
- Posibilidad de consultar fallos, memoria de alarmas, búfer de eventos
- Historial de eventos del sistema / eventos técnicos: al menos 5000 eventos

2.2. PARÁMETROS TÉCNICOS

Tensión de alimentación:	18VAC (16-20VAC)
Potencia requerida de transformador:	emplear un transformador con una potencia de 20VA a 60VA.
Módems compatibles:	* **modelo CPX230NWB-5xx**: Cinterion BGS2-W (GSM: 850, 900, 1800, 1900 MHz) * **modelo CPX230NWB-6xx**: Cinterion EHS6 (UMTS: 800, 850, 900, 1900, 2100 MHz; GSM: 850, 900, 1800, 1900 MHz)
Consumo de corriente medio/máximo: (medio para las condiciones: batería completamente cargada, conexión al servidor, teclado, sin detectores)	* Versión con módem BGS2-W Cinterion: 120mA / 180mA @18VAC * Versión con módem EHS6 Cinterion 95mA / 170mA @18VAC
Consumo medio de corriente de la batería a falta de alimentación externa (sin teclado/con teclado): (batería completamente cargada, conexión al servidor, teclado, sin detectores)	* Versión con módem BGS2-W Cinterion 60mA / 85mA @13VDC * Versión con módem EHS6 Cinterion 35mA / 65mA @13VDC
Corriente de carga de la batería (medida con la batería completamente cargada):	máx. 350mA
Tensión de carga:	13.8V
Baterías compatibles:	de plomo y ácido 12V
Tensión de la señalización de bajo nivel de carga:	11V
Tensión de desconexión de batería con demasiado bajo nivel:	por debajo de los 9V
Temperatura de servicio:	-10ºC … +55ºC
Rango de humedad de servicio:	5% … 93%
Dimensiones de la placa:	152 x 78 x 30 mm

2.3. ACCESORIOS Y APLICACIONES

Teclados	Descripción
KP32-0 (negro), KP32-9 (blanco)	Teclado alámbrico LED. Permite configurar y controlar la centralita
KP2W-9 (blanco)	Teclado inalámbrico. Permite controlar la centralita.
RC-10	Mando a distancia por radiofrecuencia con cuatro botones

Detectores	Descripción
MC-10	Detector magnético inalámbrico
PIR-10	Detector de movimiento inalámbrico
PIR-11	Detector de movimiento inalámbrico (PET)
SD-10, SD-20	Detector de humo inalámbrico
MC-11	Detector magnético inalámbrico con entrada adicional
FL-10	Detector de inundación
GS-21	Detector de gas inalámbrico (monóxido de carbono y gas natural)
GS-22	Detector de gas inalámbrico (monóxido de carbono y propano-butano)
MD-10	Detector de desplazamiento inalámbrico
GB-10	Detector de rotura de cristal inalámbrico

Programadores	Descripción
GD-PROG	Programador para centralitas de la gama CPX
SP-PROG	Programador universal
SP-PROG-BT	Programador universal con módulo Bluetooth
MINI-PROG-BT	Programador compacto con módulo Bluetooth para centralitas de la gama CPX

Software	Descripción
Configurador de transmisores GPRS	Aplicación para configurar y monitorear la centralita
OSM	Servidor de comunicación instalado en la estación de monitoreo
AVA INSTALL	Aplicación móvil para configurar y monitorear la centralita (sistema Android)
AVA	Aplicación para controlar la centralita (sistemas Android e iOS)

3. INSTALACIÓN Y CABLEADO

3.1. ORDEN DE INSTALACIÓN

1. Elaborar el esquema de instalación teniendo en cuenta la distribución de la centralita, teclado, sensores y los demás elementos del sistema.
2. Montar la centralita en un lugar de difícil acceso con posibilidad de alimentación continua.
3. Montar el teclado en un lugar fácil para el usuario y conectarlo a la centralita. La instalación del teclado se describe en el capítulo 3.6.3 Instalación del teclado.

ATENCIÓN: La longitud máxima de los cables que conectan la centralita con el teclado (a una sección de conductor de 0,5mm^2) no debe superar los 200 m.

4. Instalar sensores y reed switches de puertas y ventanas. Conectar los elementos montados a la centralita de alarmas. Los ejemplos de configuración de las líneas de entrada se describen en el capítulo 3.4 CONFIGURACIÓN DE LAS LÍNEAS DE ENTRADA ALÁMBRICAS.
5. Montar y conectar los avisadores a la centralita de alarmas. Los ejemplos de esquemas de conexión de los avisadores se dan en el capítulo 3.5 CONEXIÓN EJEMPLAR DE AVISADOR.
6. Realizar las demás conexiones de cables.
7. Conectar la batería a los bornes de tornillo BAT+, BAT- y la alimentación externa 16-20VAC a los bornes de tornillo AC, AC.
8. Programar las funciones de la centralita. El procedimiento de programación está descrito en los siguientes capítulos.

ATENCIÓN: En caso de usar más de un teclado en el sistema, hay que recordar de asignar dirección a cada teclado (véase el punto 3.6.4.).

9. Comprobar el funcionamiento del sistema y de todos sus elementos.

3.2. DESCRIPCIÓN DE LOS COMPONENTES PCB

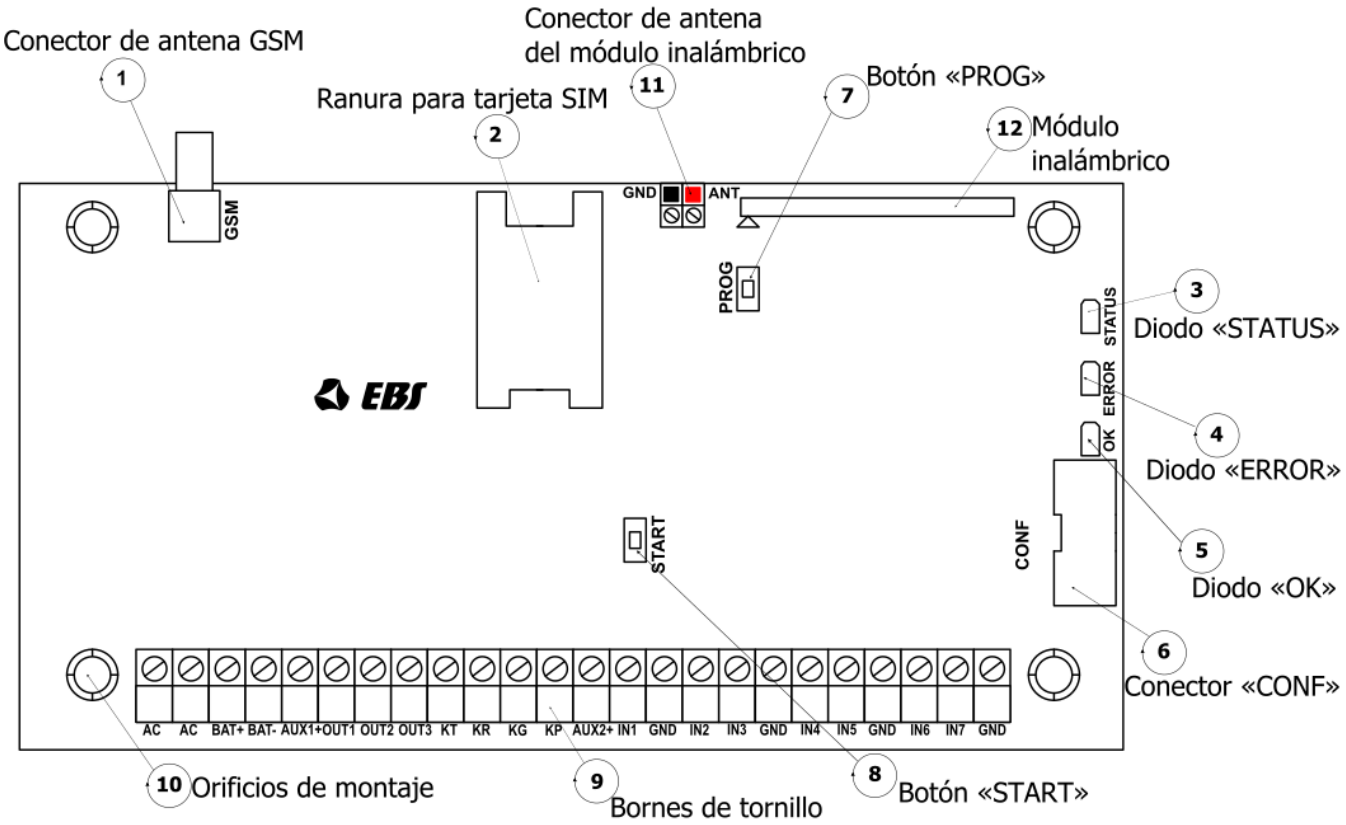


Fig. 1. Descripción de los componentes PCB

1. Conexión de la antena GSM (SMA hembra)

La antena GSM se suministra por separado como uno de los componentes opcionales del sistema. Se recomienda usar la antena con conducto, lo cual permite encontrar la respectiva posición que garantiza la cobertura óptima de GSM. La centralita está compatible con una antena GSM con la conexión SMA macho.

La antena de este tipo (foto al lado) debe colocarse (con adhesivo) sobre un soporte no metálico (plástico, vidrio, etc.) en posición vertical. La instalación a gran altura y en espacios abiertos ayuda a conseguir mejores niveles de señal de la red GSM. No instalar la antena cerca de objetos metálicos (por ejemplo, haces de cables). No instalar la antena dentro de las carcasas (especialmente las metálicas). Tender el cable coaxial evitando curvas cerradas o aplastamientos. No se recomienda extender el cable de la antena.

ATENCIÓN: La antena no debe instalarse sobre la carcasa de la centralita, cerca del receptor del sistema inalámbrico. Tal posición puede reducir significativamente su alcance.

2. Toma de la tarjeta SIM

La centralita está dotada de la transmisora integrada GSM/GPRS/SMS. Para la comunicación con el servidor se necesita una tarjeta SIM con transmisión GPRS activa. Se debe colocar la tarjeta en la ranura indicada en la figura.

ATENCIÓN: Antes de introducir la tarjeta asegúrese de que la tarjeta tiene desactivada la demanda del código secreto PIN o bien fijado el código secreto PIN conforme con el programado en la centralita. El código secreto PIN de la centralita es 1111.

3. Diodo LED «STATUS»

Diodo LED amarillo. La descripción detallada se encuentra en el capítulo 7

4. Diodo LED «ERROR»

Diodo LED rojo. La descripción detallada se encuentra en el capítulo 7.

5. Diodo LED «OK»

Diodo LED verde. La descripción detallada se encuentra en el capítulo 7.

6. Conector del programador «CONF»

El conector IDC10 «CONF» permite configurar la centralita mediante los programadores dedicados que cuentan con tal conector, como **GD-PROG, MINI-PROG-BT, SP-PROG-BT** y cualquier ordenador equipado con un puerto RS232 (GD-PROG), USB (MINI-PROG-BT, SP-PROG-BT) o Bluetooth (MINI-PROG-BT, SP-PROG-BT).

7. Botón «PROG»: restauración de los ajustes predeterminados

Al mantener pulsado este botón durante 10 segundos mientras se conecta la fuente de alimentación de la centralita, se borrarán todos los usuarios y se restaurará el código predeterminado de administrador y de instalador. El código predeterminado de administrador es 1111 y él de instalador es 2222

8. Botón «START»: inicio de la centralita con la batería sin alimentación de red

Cuando ponemos en marcha la centralita en caso de la falta de alimentación, después de conectar la batería se debe apretar este botón.

9. Conectores de tornillos de la centralita

Los conectores de alimentación, de entrada y de salida se describen con detalles en el capítulo 3.3.

10. Agujeros de montaje de la centralita (distancia de agujeros 132x61mm)

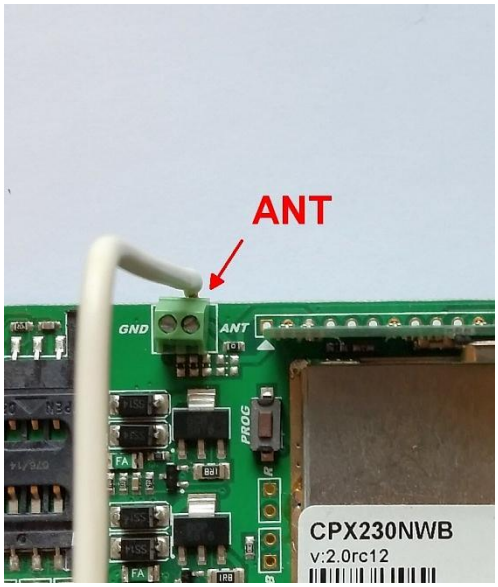
Los agujeros indicados sirven para montar la centralita en la carcasa de cualquier tipo. Opcionalmente, se puede pedir una carcasa dedicada de plástico tipo OBDNA (la carcasa incluye un transformador apropiado de 230VAC/18VAC).

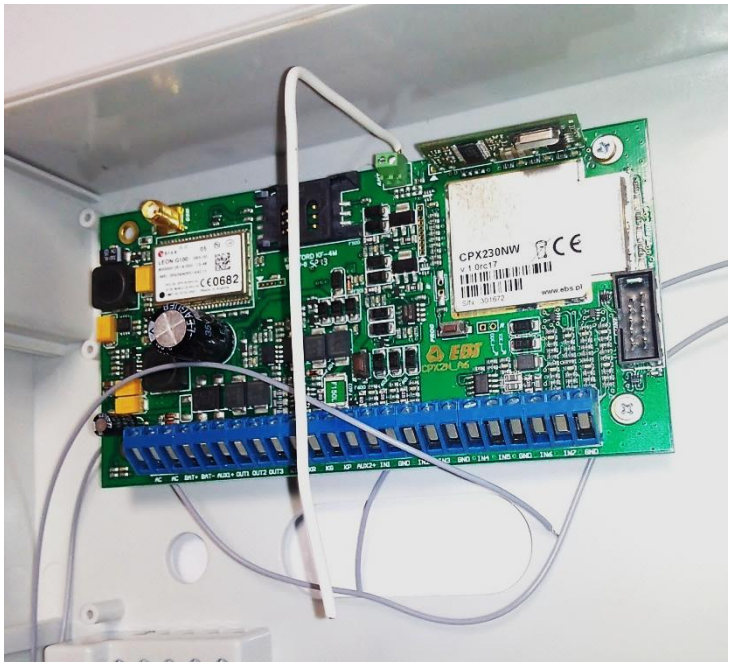
11. Conexión de antena al módulo inalámbrico

El conjunto incluye dos tipos de antenas: interior y exterior tipo dipolo.

Antena interior 433MHz

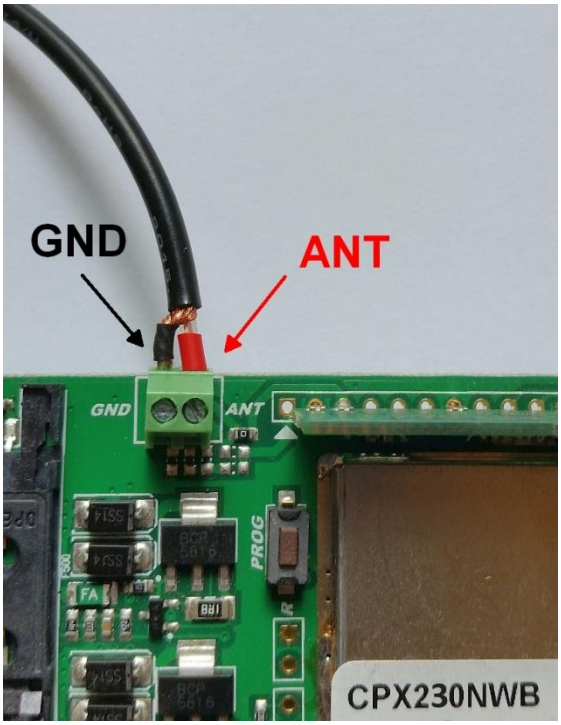
La antena interior (foto al lado) se puede utilizar en cualquier lugar donde se requieren dimensiones compactas y la antena proporciona la cobertura adecuada. Colocar la extremidad desnuda de la antena interior en el borne de potencial de la toma ANT (la polaridad correcta está marcada en rojo en Fig. 1 y en la foto). El borne de masa está tapado con un obturador de plástico (marcado en negro en la figura). La posición correcta de la antena se muestra en la foto de abajo.





Antena dipol externa 433MHz

ATENCIÓN: Para mejorar el alcance de la transmisión de radio en condiciones difíciles, se puede utilizar la antena dipolo externa (foto al lado). Conectar la antena a los bornes GND y ANT según los colores. Antes de apretar, debe retirarse el obturador de la toma GND. La instalación correcta de la antena externa se muestra en la foto de abajo.



12. Módulo inalámbrico

El módulo inalámbrico sirve para recibir las señales de los manos y sensores inalámbricos.

3.3. DESCRIPCIÓN DE LAS CONEXIONES POR TORNILLOS DE LA CENTRALITA

ATENCIÓN: ¡Todos los trabajos de montaje e instalación se deben realizar con la alimentación de red y batería desconectadas!

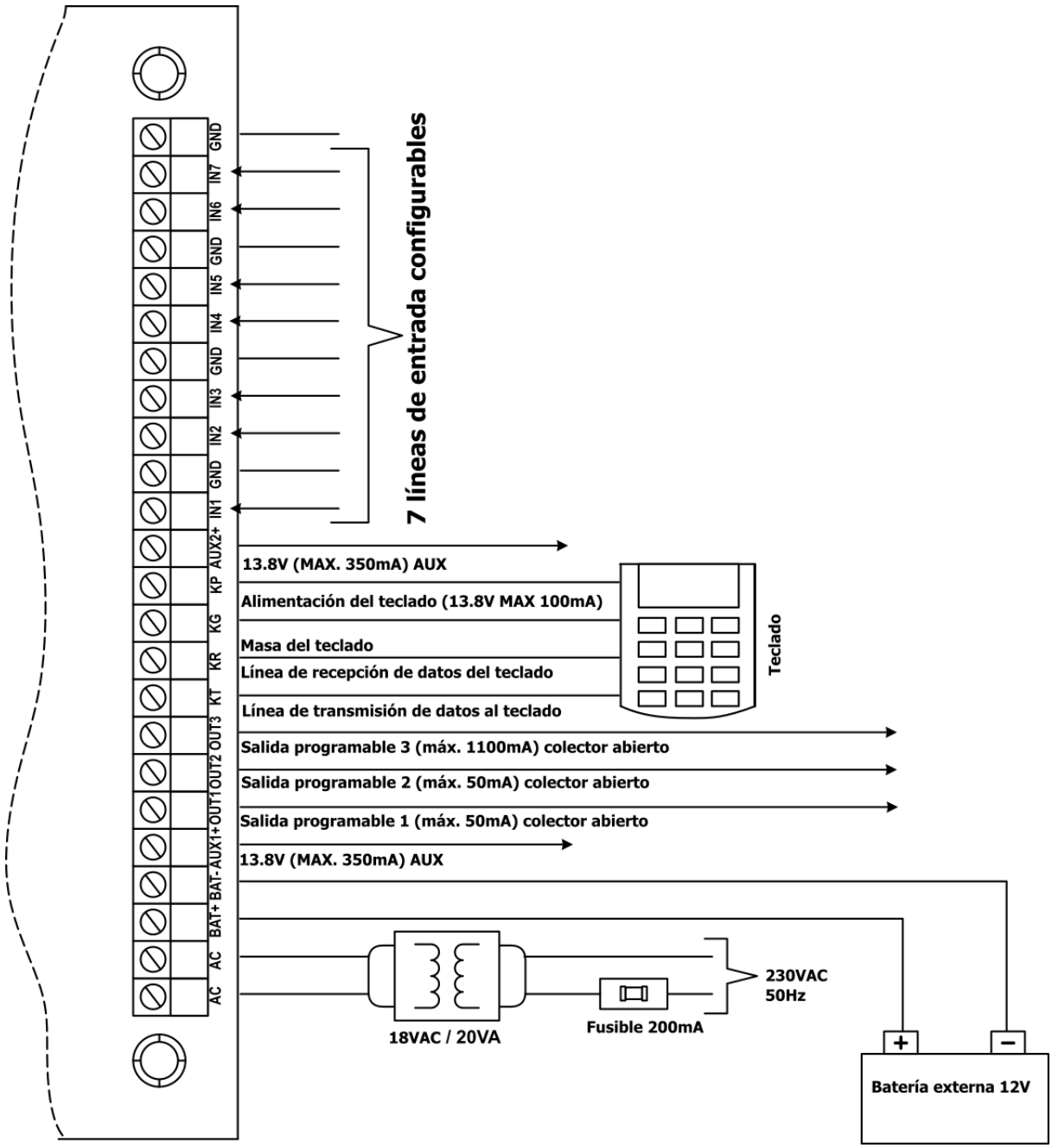


Figura 2. Descripción de las conexiones por tornillos de la centralita

3.4. CONFIGURACIÓN DE LAS LÍNEAS DE ENTRADA ALÁMBRICAS

Todas las líneas de entrada alámbricas son totalmente configurables y pueden funcionar como normalmente cerradas (NC), normalmente abiertas (NO), parametrizadas (EOL-NO o EOL-NC) con resistencias de 2,2kΩ o doblemente parametrizadas (DEOL-NO/DEOL-NC) con resistencias de 1,1kΩ. La configuración TEOL permite duplicar la línea de alarma, es decir conectar dos detectores alámbricos a un borne de la centralita, siendo posible detectar alarmas del detector 1 y del detector 2, ver fig. 3, la señalización de apertura del interruptor de manipulación será común para ambos detectores.
Todos los tipos de resistencias se entregan junto con la centralita. Las diferentes configuraciones de la línea de entrada se muestran en la siguiente figura 3.

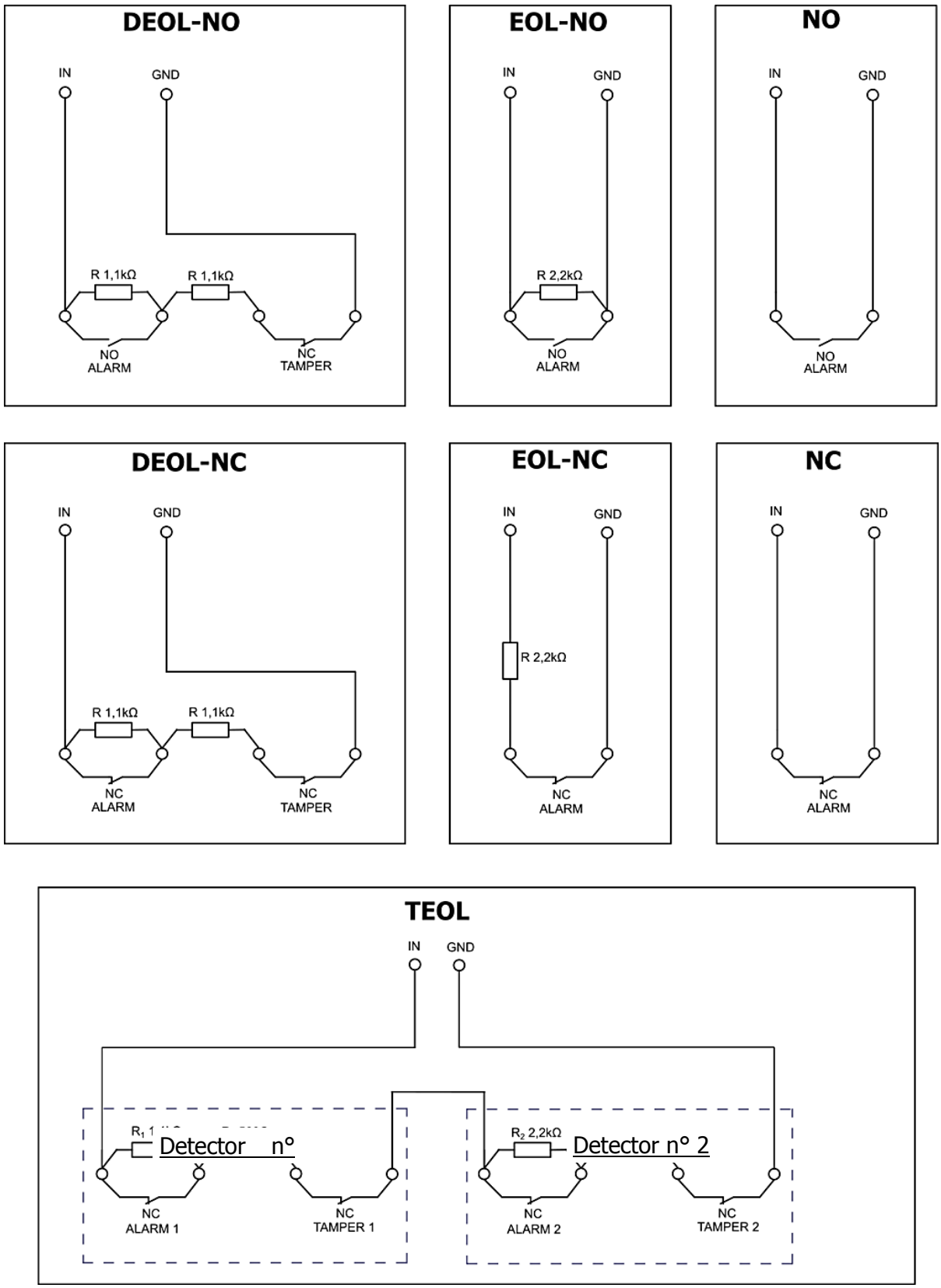


Fig. 3. Configuración de las líneas de entrada

3.5. CONEXIÓN EJEMPLAR DE AVISADOR

3.5.1. Avisador interno sin propia alimentación

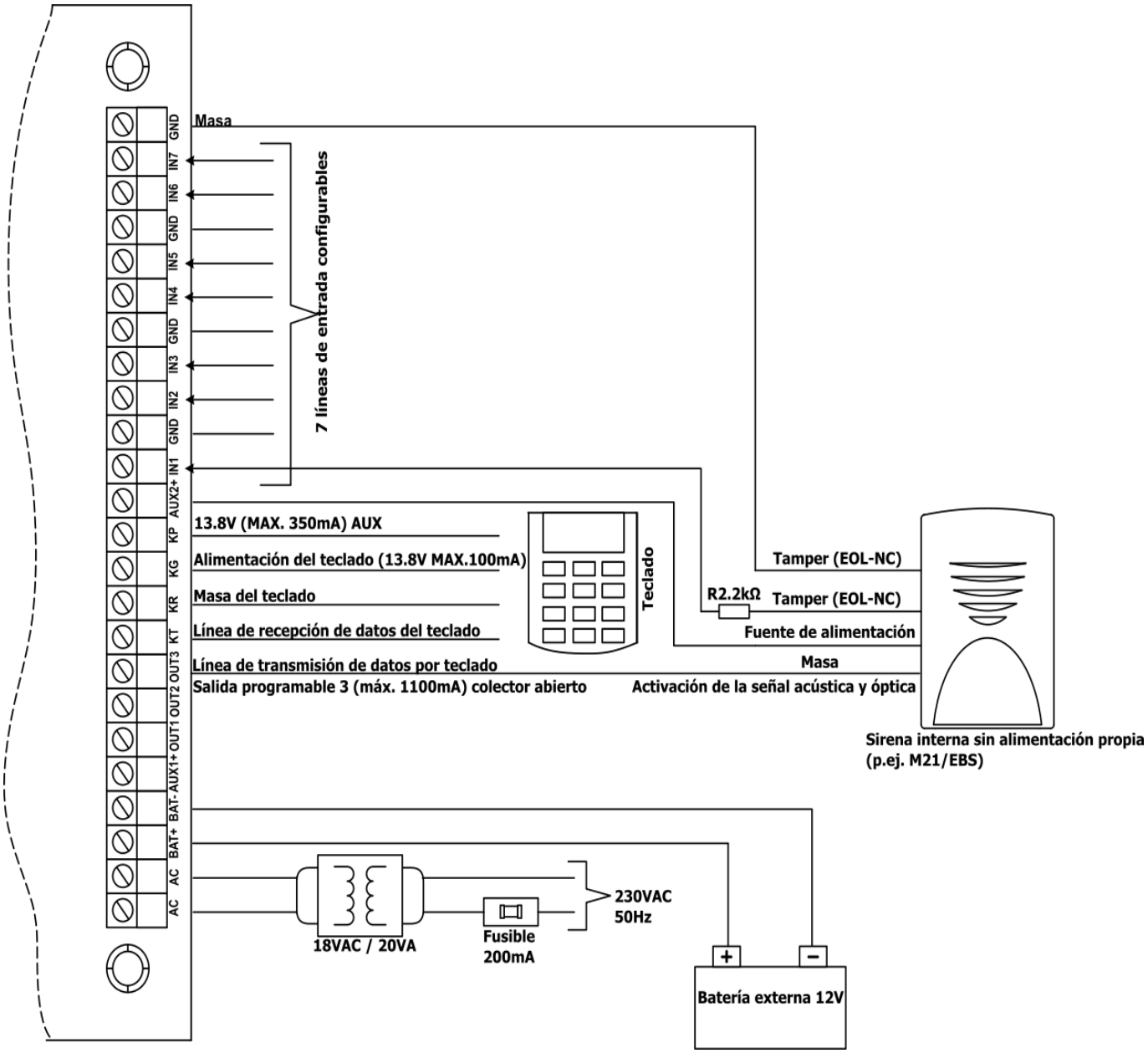


Fig. 4. Conexión ejemplar del avisador interno sin propia alimentación

3.5.2. Avisador externo con propia alimentación

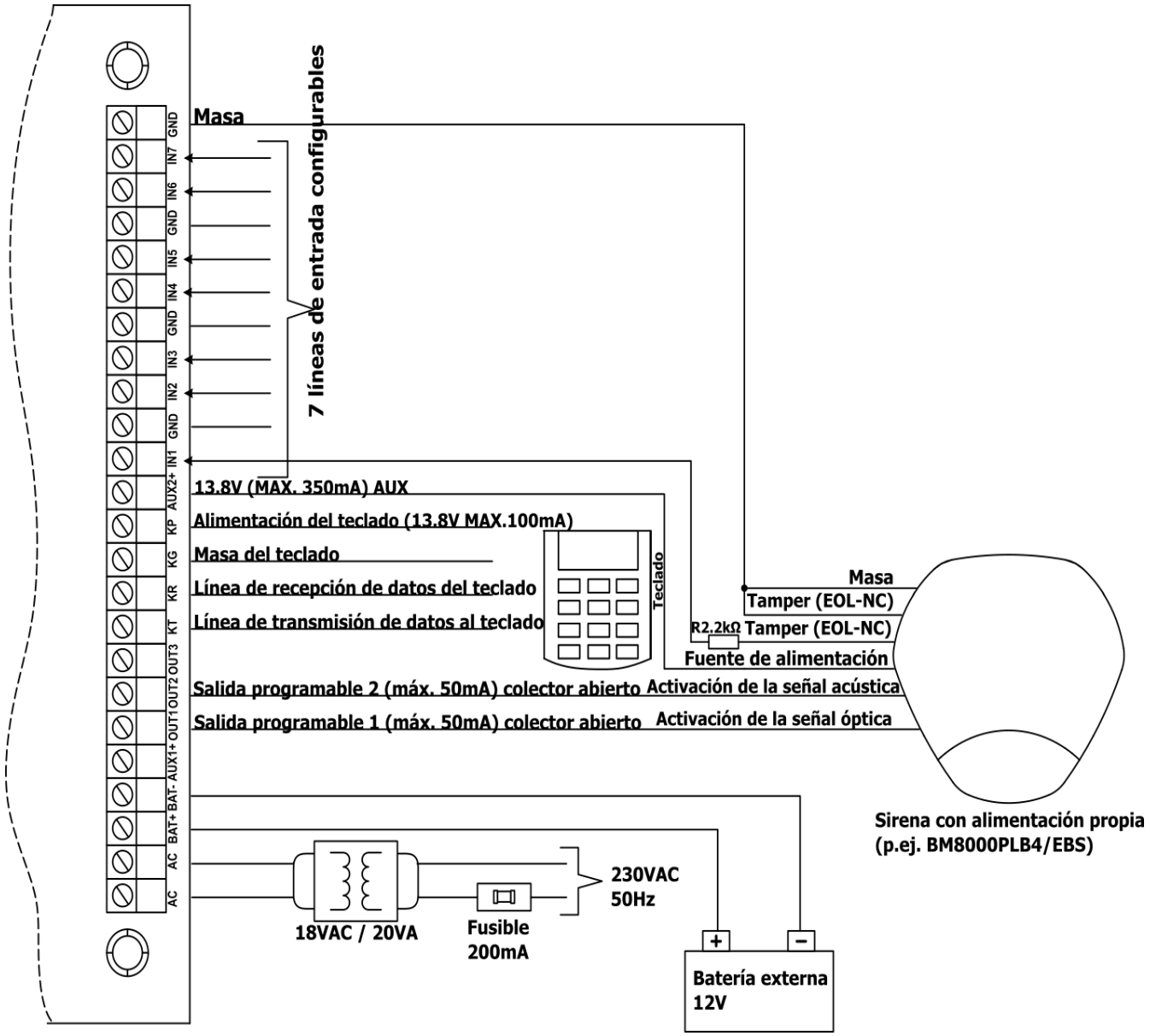


Fig. 5. Conexión ejemplar del avisador externo con propia alimentación

3.6. TECLADO ALÁMBRICO KP32

3.6.1. Descripción de los elementos de teclado

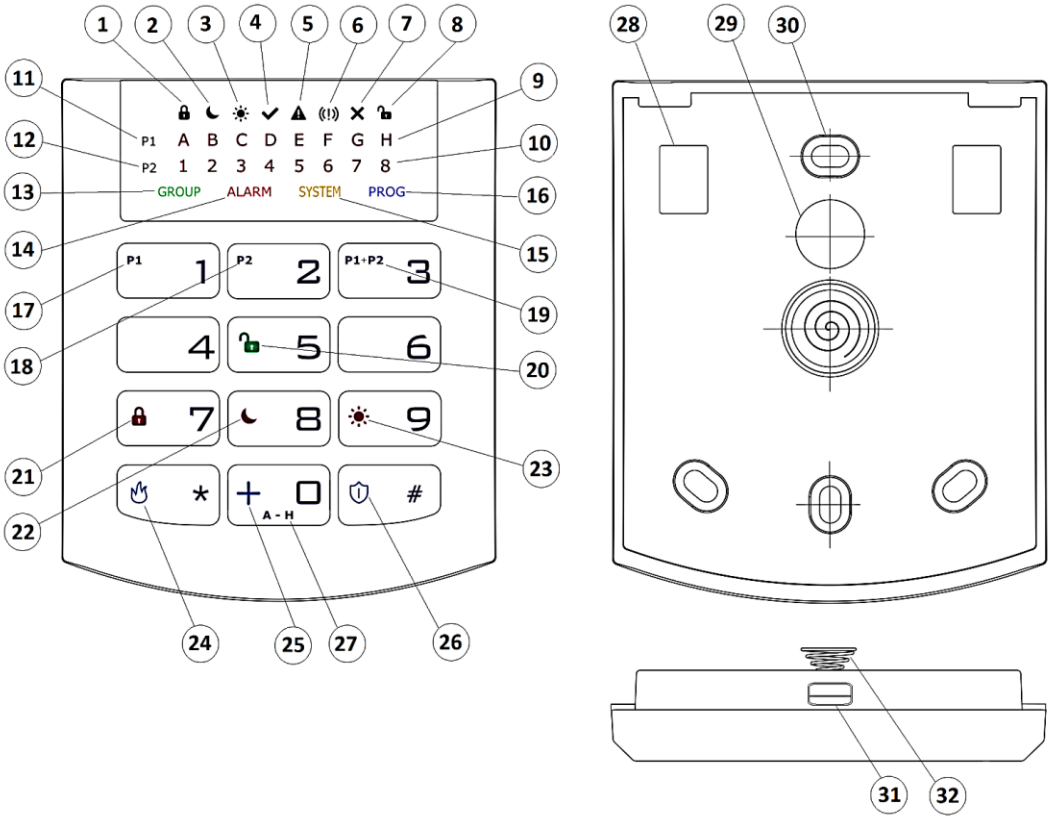


Fig. 6. Teclado KP32

1. **Símbolo de armado en modo completo FULLY ARMED : señalización con diodos A (partición P1) y 1 (partición P2)**

   Parpadeo lento: cuenta regresiva del retardo de salida,
   Parpadeo rápido: cuenta regresiva del retardo de entrada,
   Continuo: partición armada en modo completo,
   Apagado: partición no armada en modo completo.

2. **Símbolo de armado en modo nocturno SLEEP : señalización con diodos B (partición P1) y 2 (partición P2)**

   Parpadeo lento: cuenta regresiva del retardo de salida,
   Parpadeo rápido: cuenta regresiva del retardo de entrada,
   Continuo: partición armada en modo nocturno,
   Apagado: partición no armada en modo nocturno.

3. **Símbolo de armado en modo diurno STAY : señalización con diodos C (partición P1) y 3 (partición P2)**

   Parpadeo lento: cuenta regresiva del retardo de salida,
   Parpadeo rápido: cuenta regresiva del retardo de entrada,

Continuo: partición armada en modo diurno,

Apagado: partición no armada en modo diurno.

4. **Símbolo READY ✔: señalización con diodos D (partición P1) y 4 (partición P2)**

   Iluminado cuando todas las líneas (sin la opción «ignorar al armar» habilitada) están en estado normal (no violadas).

5. **Símbolo de sabotaje/fallo de entradas y salidas en una partición determinada ⚠: señalización con diodos E (partición P1) y 5 (partición P2)**

   Parpadeo rápido: hubo un fallo/sabotaje de entradas o salidas asignadas a la partición,

   Continuo: hay un fallo/sabotaje de entradas o salidas asignadas a la partición.

6. **Símbolo de alarma activa/memorizada en una partición determinada ((!)): señalización con diodos F (partición P1) y 6 (partición P2)**

   Parpadeo rápido: había alarmas procedentes de las líneas asignadas a la partición,

   Continuo: hay una alarma procedente de una línea asignada a la partición.

7. **Símbolo de bloqueo de línea ✕: señalización con diodos G (partición P1) y 7 (partición P2)**

   Iluminado cuando al menos una línea de la partición queda bloqueada por el usuario (BYPASS).

8. **Símbolo de desarme de la partición DISARM 🔓: señalización con diodos H (partición P1) y 8 (partición P2)**

   Iluminado cuando la partición determinada está desarmada, es decir en do DISARM.

9. **Diodos A-H (blancos)**

   Fila de diodos que indican el estado de la partición P1 (ejemplo: el diodo «B» iluminado indica que la partición P1 está armada en modo nocturno SLEEP).

10. **Diodos 1-8 (blancos)**

    Fila de diodos que indican el estado de la partición P2 (ejemplo: el diodo «3» iluminado indica que la partición P2 está armada en modo diurno STAY).

11. **Partición 1 («P1»)**

    El símbolo P1 identifica la partición 1 a la que están asignados los diodos de A a H.

12. **Partición 2 («P2»)**

    El símbolo P2 identifica la partición 2 a la que están asignados los diodos de 1 a 8.

13. **Diodo «GROUP»**

    Su iluminación señala la entrada al función de usuario en la que se visualizan líneas o usuarios.

14. **Diodo «ALARM»**

    Su iluminación señala una alarma en todo el sistema (p.ej. sabotaje del teclado, botón ALARMA en el mando) dónde:

    Parpadeo: alarma que ha ocurrido en el pasado,

    Iluminado: alarma actual.

15. **Diodo «SYSTEM»**

    Su iluminación señala un fallo del sistema, por ejemplo: fallo de alimentación, fallo de la batería, fallo de la conexión ATS, fallo de salidas de alimentación, fallo en la hora, sabotaje del teclado.

    Parpadeo: la memoria contiene fallos que ya han desaparecido,

    Iluminado en continuo: en el sistema hay un fallo que no ha sido eliminado,

    Apagado: no hay fallos en el sistema.

16. **Diodo «PROG»**

    Parpadeo lento: está activada la función de servicio (de las funciones de usuario),

    Parpadeo rápido: se introducirán los datos,

    Iluminado en continuo: activado el modo de servicio del instalador.

17. **Botón 1 «P1»**

    Tecla de función para el armado de la partición P1.

18. **Botón 2 «P2»**

    Tecla de función para el armado de la partición P2.

19. **Botón 3 «P1+P2»**

    Tecla de función para el armado de las particiones P1 y P2.

20. **Botón 5** (candado abierto)

    Tecla de función para el desarmado.

21. **Botón 7** (candado cerrado)

    Tecla de función para el armado en modo completo.

22. **Botón 8** (luna)

    Tecla de función para el armado en modo nocturno (SLEEP).

23. **Botón 9** (sol)

    Tecla de función para el armado en modo diurno (STAY).

24. **Botón «*»** (llama)

    Tecla de función INCENDIO que genera una alarma de incendio cuando se mantiene presionada durante unos 3 segundos.

25. **Botón 0 «+»**

    Tecla de función AYUDA que genera una alarma médica cuando se mantiene presionada durante unos 3 segundos.

26. **Botón «#»** (escudo)

    Tecla de función PÁNICO que genera una alarma de pánico cuando se mantiene presionada durante unos 3 segundos.

27. **Botón 0 (A - H)**

    Tecla de función que permite cambiar de grupo.

28. **Conexión por tornillos**

    Conexiones para conectar los conductos que conectan el teclado a la centralita de alarmas.

29. **Orificio para introducir conductos**

    Lugares de introducción de los conductos de conexión.

30. **Orificios de montaje**

    El teclado fue dotado de cuatro orificios ovales de montaje para la adecuada fijación de teclado.

31. **Cierre automático de la carcasa**

    Para abrir la carcasa se recomienda usar un destornillador de 2,5 a 5 mm. Se debe introducirlo en el orificio indicado y realizar un pequeño movimiento de palanca hacia la parte trasera de la carcasa.

32. **Conmutador de sabotaje**

    Después de montar el teclado, el contacto de conmutador está cerrado. El desmontaje no autorizado de teclado ocasionará el envío de información a la centralita de alarmas. Para nivelar las irregularidades del suelo, en la palanca de conmutador fue situado un muelle.

3.6.2. Características del teclado

Alimentación:	10 – 13,8 VDC
Consumo de energía:	nominal 20 mA, máx. 70 mA
Peso del teclado:	70g
Dimensiones:	99 x 82 x 19 mm
Tipo del teclado:	LED, 16 diodos de estatus, 4 diodos de estado (GROUP, ALARM, SYSTEM, PROG)
Distribución de teclas:	Teclado de teléfono estándar 3 x 4 teclas

3.6.3. Instalación del teclado

1. El teclado KP32 está diseñado para su instalación en interiores sobre una superficie seca y plana. Por regla general, se coloca en la pared, cerca de la puerta de entrada, a una altura de 120 a 140 cm del suelo.
2. Abre la carcasa del teclado: introduzca un destornillador plano en el orificio en la parte inferior de la carcasa y apriete el cierre. Luego, con cuidado abre ambas partes de la carcasa, empezando por la parte inferior de la carcasa.
3. Marque y taladre orificios en la pared para montar la parte trasera de la carcasa.
4. Atornille la parte trasera de la carcasa a la pared. Los 4 pernos y tacos adjuntos están diseñados para el hormigón. En el caso de otras superficies, deben seleccionarse los tornillos correspondientes.

5. Conecte los conductos que unen el teclado a la centralita. Los bornes del teclado marcados como: KT, KR, KP, KG, deberán estar conectadas a los bornes KT, KR, KP, KG en la centralita de alarmas (véase fig. 2.)
6. Junte la parte frontal de la carcasa con la parte trasera empezando por la parte superior. Asegúrese de que el teclado está bien montado y el interruptor de sabotaje está apretado.

3.6.4. Direccionamiento de los dispositivos conectados al bus del teclado

Cada teclado conectado a la conducción deberá tener dirección individual de 1 a 3. Las direcciones no pueden repetirse (la centralita no soporta dispositivos con direcciones idénticas). Se recomienda atribuir las siguientes direcciones a partir de 1. En los teclados la dirección se fija de forma programable (por defecto se fija en la dirección 1).

La programación de la dirección de teclado:

1. Quitar el teclado de la pared (el contacto del conmutador de sabotaje deberá estar abierto).
2. Pulsar y mantener al mismo tiempo la tecla 5 y P1 1 o P2 2 o P1+P2 3 hasta que se ilumine el diodo correspondiente (A para la dirección n° 1, B para n° 2 y C para n° 3).
3. Después de unas decenas de segundos, el teclado programado recuperará toda su funcionalidad con nuevas direcciones.

3.7. TECLADO INALÁMBRICO KP2W

El teclado inalámbrico KP2W está diseñado para funcionar con la centralita híbrida CPX230NWB. Se pueden añadir hasta 32 teclados de este tipo, pero cada uno de ellos ocupa una de las líneas de entrada. O sea, después de añadir 5 teclados inalámbrico, quedan 27 líneas disponibles que se pueden utilizar para otros dispositivos (por ejemplo, detectores).

La transmisión por radio entre el teclado y la centralita está protegida por un código variable y encriptada. El dispositivo envía a la centralita una transmisión cíclica de prueba cuya ausencia será señalada como una violación de la línea a la que está asignado el teclado. El teclado detecta y señala la carga baja de la batería, así como la apertura de la carcasa o su separación del soporte.

Además, el teclado cuenta con una entrada tipo NC para la conexión de un detector de apertura de puertas adicional.

Hay que tener en cuenta que el teclado inalámbrico KP2W utiliza una transmisión unidireccional y no puede recibir información de la centralita. Por esta razón, se recomienda que una de las salidas de la centralita esté en modo de señalización de armado/desarmado (el llamado «chirp») y que se conecte una sirena adecuada a esta salida. Esto facilitará la operación de la centralita.

Recomendamos que se instale al menos un teclado alámbrico KP32 en el sistema de alarma para programar los parámetros de la centralita, visualizar el estado del sistema y cambiar los códigos de usuario. Con la centralita CPX230NWB, también recomendamos utilizar la aplicación AVA que facilita la operación.

3.7.1. Añadir un teclado al sistema

El teclado inalámbrico KP2W se registra en el sistema de alarma de una manera similar a los detectores inalámbricos. Hay dos formas de hacerlo:

- mediante el teclado KP32, véase el punto 4.3.16.1. Configuración de detectores inalámbricos,
- Mediante el programa Configurador de transmisores GPRS, véase el punto 6.3.2. Dispositivos inalámbricos.

3.7.2. Descripción de los elementos de teclado

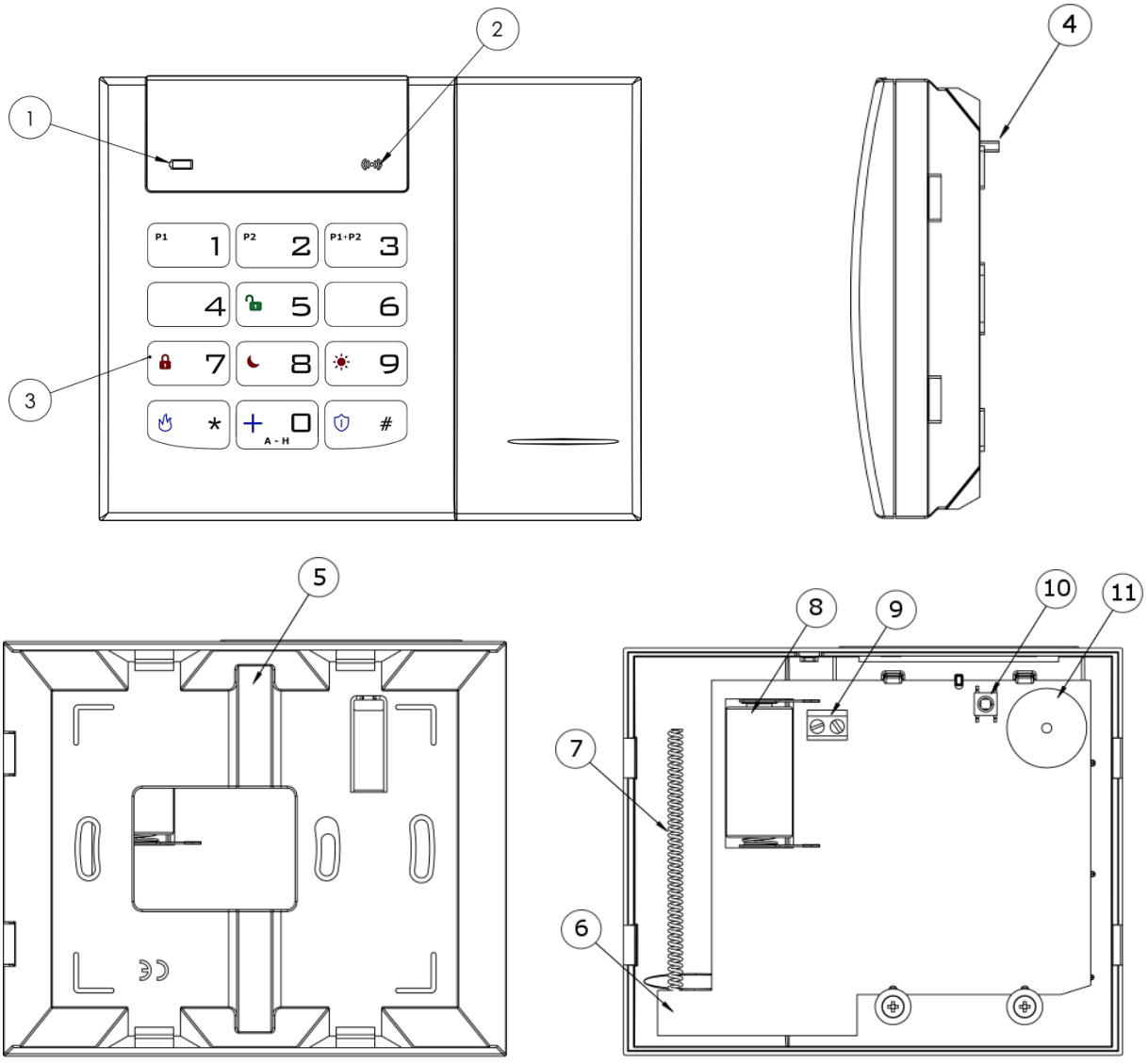


Fig. 7. Vista general y disposición de los elementos del teclado KP2W

1. **<u>Diodo de carga baja de la batería (rojo)</u>**

   Iluminado en continuo: significa que la batería está a punto de descargarse y debe reemplazarse lo antes posible,

   Apagado: batería cargada.

2. **Diodo de transmisión de datos (azul)**

   Iluminado: transmisión de datos en curso,

   Apagado: no hay transmisión de datos.

3. **Botones de teclado**

   Los botones del teclado KP2W tienen las mismas funciones que en el teclado KP32 (véase el capítulo 3.6.1 Descripción de los elementos de teclado: puntos de 17 a 27). Después del primer apriete de cualquier botón el teclado queda iluminado. Pasado el periodo de unos segundos de inercia, la iluminación se apaga automáticamente con fluidez.

4. **Conmutador de sabotaje**

   Después de montar el teclado, el contacto de conmutador está cerrado. El desmontaje no autorizado de teclado ocasionará el envío de información a la centralita de alarmas.

5. **Ranura de cables**

   Para colocar de los cables de conexión.

6. **Placa base del teclado**

7. **Antena de radio 433,92 MHz**

8. **Batería**

   Batería de alimentación tipo CR123A 3V, de litio.

9. **Conector de tornillo**

   Para conectar los cables que conectan el teclado con el detector de apertura de puerta (contacto reed). Si no se utiliza para conectar el detector, debe estar cerrado.

10. **Detector de sabotaje (tamper)**

11. **Avisador acústico (zumbador)**

3.7.3. Características del teclado

Alimentación:	1 batería CR123A 3V
Autonomía:	3 años*
Frecuencia de servicio:	433,92 MHz
Alcance de comunicación por radio (LOS):	hasta 500 metros en campo abierto
Tipo de comunicación:	unidireccional
Consumo medio de energía:	30 µA
Rango de temperatura de funcionamiento:	-10 °C +55 °C
Entradas de alarma:	1 tipo NC
Dimensiones:	125 x 102 x 33 mm
Peso sin batería:	150 g

*Condiciones de servicio: transmisión de prueba cada 15 minutos, uso del teclado (armado/desarmado) 2 veces al día, detector de apertura de puerta cerrado, temperatura ambiente 20 °C.

3.7.4. Montaje del dispositivo

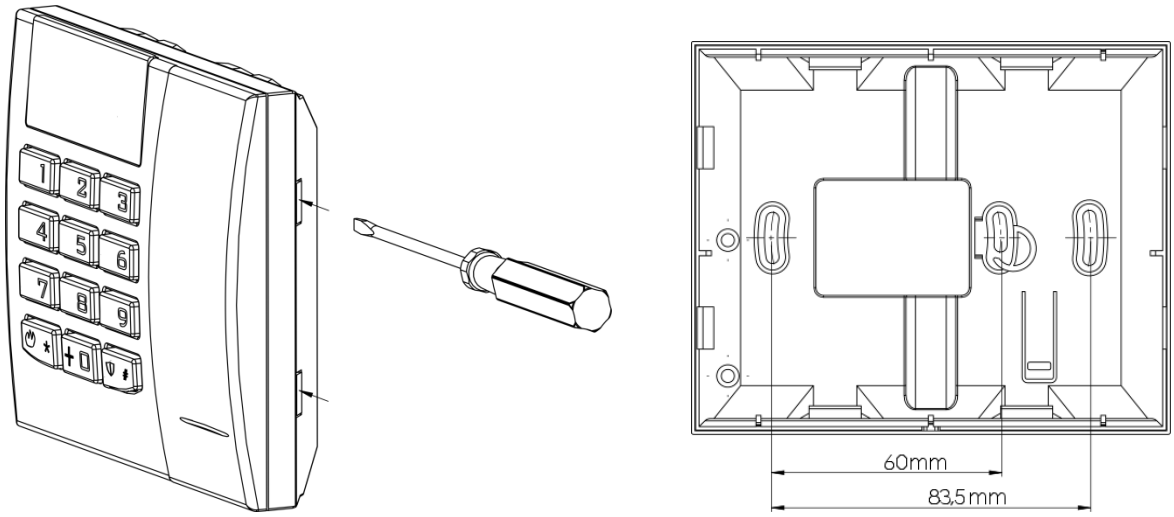


Fig. 8. Cierres de la carcasa y orificios de montaje

El teclado KP2W está diseñado para su instalación en interiores sobre una superficie seca y plana. Por regla general, se coloca en la pared, cerca de la puerta de entrada, a una altura de 120 a 140 cm del suelo.

1. Abre la carcasa del teclado: introduzca un destornillador plano en el orificio en la parte inferior de la carcasa y apriete el cierre. Luego apriete el otro cierre y separe suavemente ambas partes de la carcasa, empezando por su parte inferior.
2. Marque y taladre agujeros en la pared para montar la parte trasera de la carcasa.
3. Atornille la parte trasera de la carcasa a la pared.
4. Coloque la batería CR123A según las marcas en la placa. La instalación incorrecta de la batería impide que el dispositivo se ponga en marcha. Tras colocar la batería, deben de encenderse durante un instante dos diodos LED (el rojo de la batería y el azul de transmisión) y la retroiluminación de las teclas.
5. Junte la parte delantera de la carcasa con la trasera, empezando por la parte superior. Asegúrese de que el teclado está bien montado y el interruptor de sabotaje está apretado.

3.7.5. Detector de apertura de puerta

Al teclado KP2W puede conectarse un contacto reed que puede servir de detector de apertura de puerta.

Si no hay ningún detector conectado, el conector tipo NC (normalmente cerrado) debe estar cerrado. El conector se encuentra en la placa del teclado (n° 9 en la figura 7).

En el sistema de alarma CPX230NWB, este detector tendrá asignado el mismo número de línea que el teclado.

3.8. UBICACIÓN DE LA CENTRALITA DE ALARMAS

La centralita de alarmas con módulo de radio debe estar situada en un lugar adecuado del edificio para garantizar la mejor recepción posible de las señales de los detectores inalámbricos. La centralita debe estar situada en la parte central del edificio. La ubicación central del dispositivo garantiza una buena comunicación con todos los detectores inalámbricos. Véase las figuras 9 y 10.

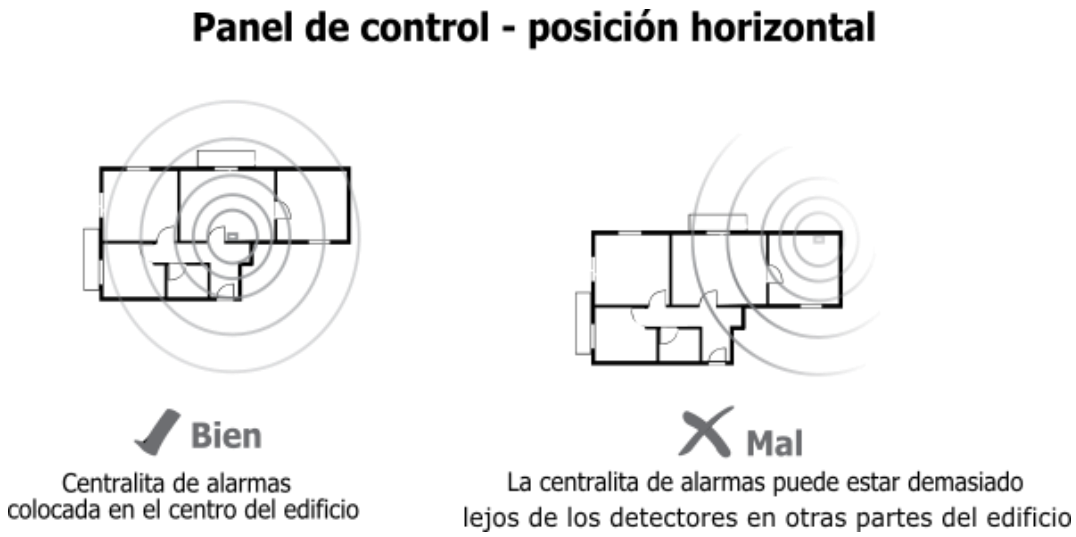


Fig. 9. Situación horizontal de la centralita de alarmas

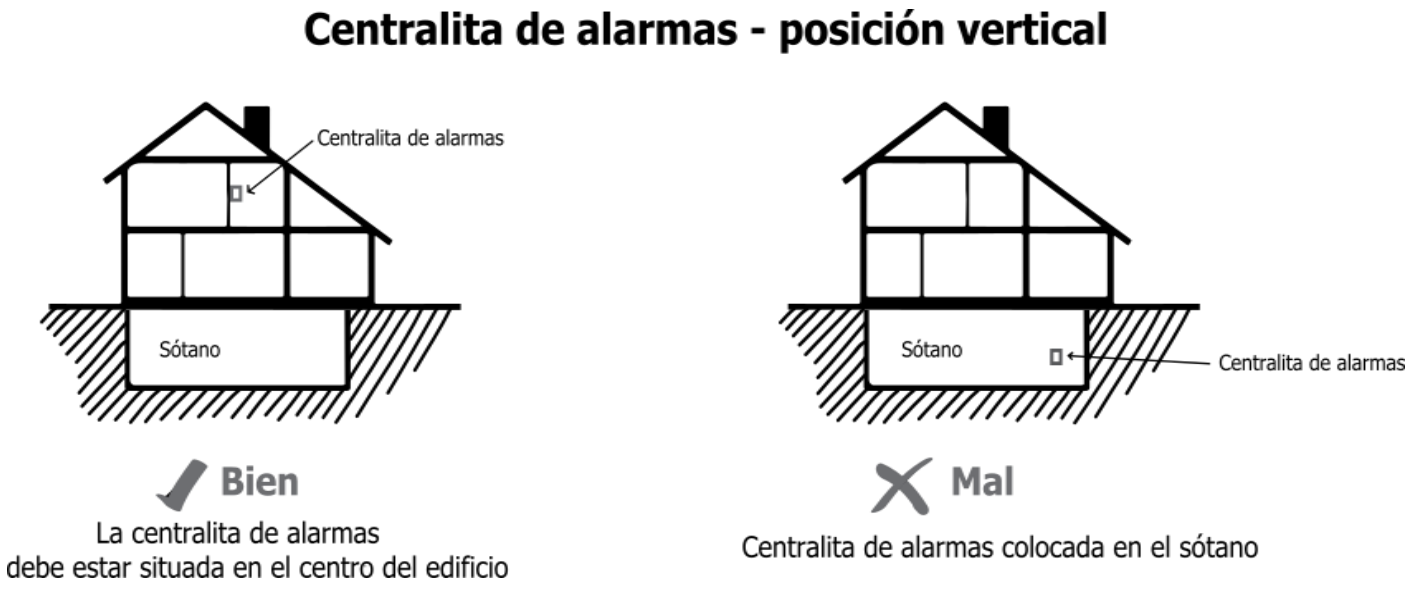


Figura 10. Situación vertical de la centralita de alarmas

También hay que tener en cuenta que las ondas de radio tienen dificultad para atravesar paredes y otros obstáculos. Las paredes de cartón yeso y madera son las más fáciles de atravesar, las de hormigón o ladrillo, más difíciles. Las más difíciles de atravesar son las paredes de hormigón armado o con malla metálica. La figura 11 muestra las pérdidas de señal después de atravesar diferentes materiales estructurales (**NOTA:** esquema simplificado, proporcionado a título informativo, hay que tener en cuenta que las ondas de radio se propagan en varias direcciones).

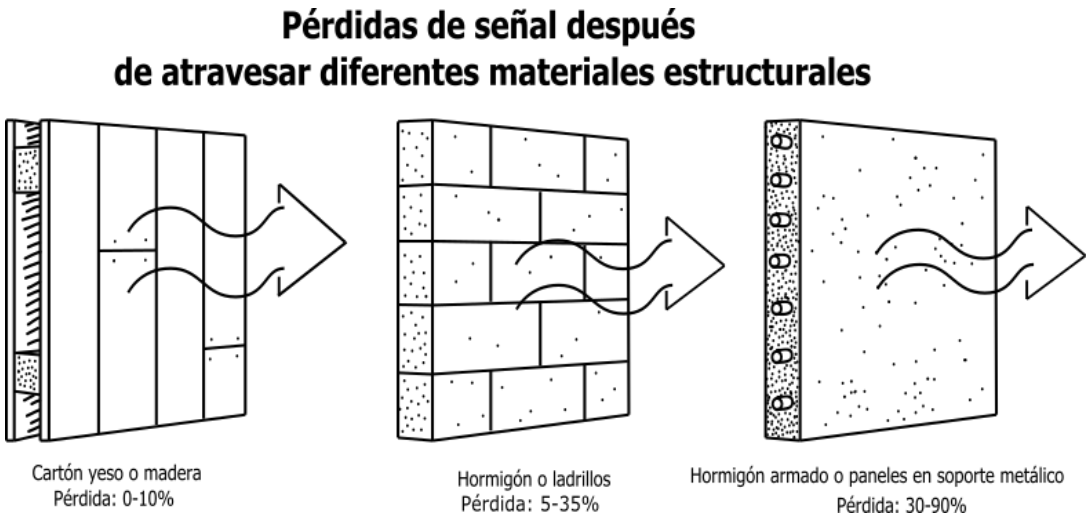


Figura 11. Pérdidas de señal después de atravesar diferentes materiales estructurales

3.9. INSTALACIÓN DE DETECTORES INALÁMBRICOS

Recomendaciones de instalación

Los detectores inalámbricos deben colocarse de tal manera que estén situados en el lado de la antena de radio de la centralita, es decir, en el lado de los componentes electrónicos en la placa de la misma. De este modo se consigue la mejor cobertura posible. Debe evitarse colocar los detectores en el lado trasero de la centralita.

Las recomendaciones de instalación adicionales se proporcionan en la figura 12.

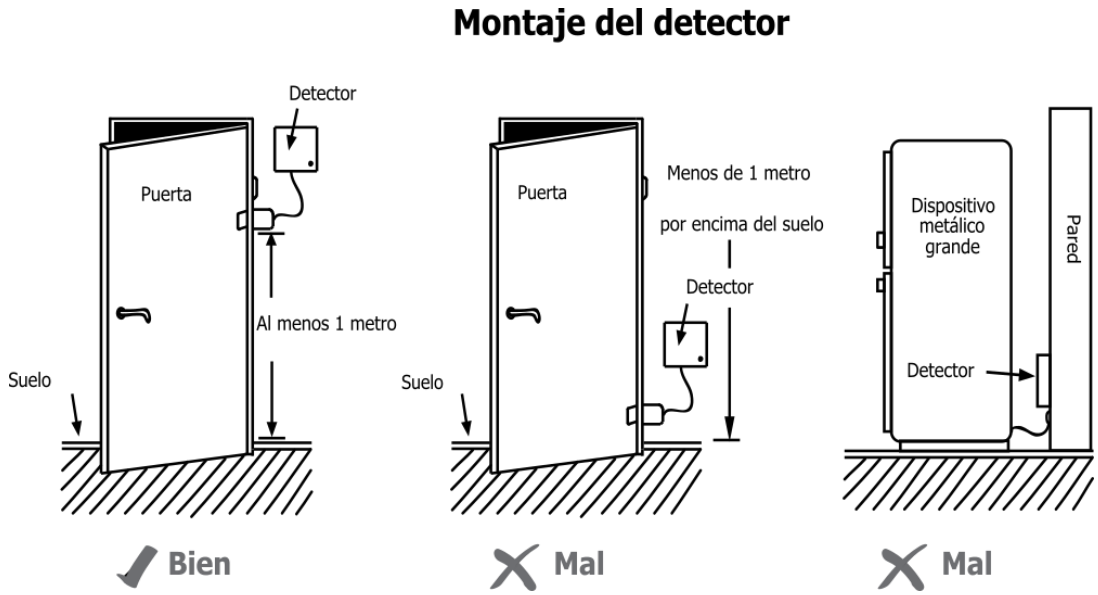


Fig. 12. Montaje del detector

4. MODO DE SERVICIO

Nota: Las siguientes operaciones sólo se pueden realizar con el teclado principal KP32

El modo de servicio sirve para configurar los parámetros básicos relacionados con las entradas, salidas y particiones. Permite de modo manual, por medio del teclado, programar todas las dependencias, necesarias para el trabajo correcto del sistema.
Después de ejecutar el modo de servicio tenemos para seleccionar una serie de las funciones de servicio. La configuración del sistema consta en dar el número de funciones y sus argumentos, dependientes de la función dada, según el siguiente esquema:

<Número de función> [0 #] **<Argumento>** [0 #]

Siendo:

Número de función: número de una de las funciones de servicio disponibles,
Argumento: argumento de la función de servicio determinada (tipo BIN o DEC).

Cada función de servicio acepta argumentos, uno de dos tipos: binario (BIN) o decimal (DEC). A continuación se encuentra la forma de usar los dos tipos de argumentos:

Tipo binario (BIN)
Después de entrar en la función que tiene tipo binario el tipo de argumento, el estado actual de la opción se visualiza por medio de los diodos LED encendidos o apagados que corresponden a la opción dada de la función. El apriete de las teclas de 1 a 9 ocasiona el cambio del estado del diodo LED y de la opción que le corresponde. Las opciones de 10 a 16 se seleccionan manteniendo pulsadas las teclas de 0 a 6 durante un período más largo (aprox. 2s). El instalador puede cambiar del estado de opción cualquier número de veces. Después de ajustar el estado deseado hay que apretar [0 #] para confirmar los valores o bien [*] para salir sin guardar los cambios.

Tipo decimal (DEC)
La función de servicio que aprueba los argumentos de tipo decimal puede aprobar las series de los números decimales de cualquier largo que no supere el máximo definido para la función. La introducción de un símbolo automáticamente hace pasar a la introducción del siguiente símbolo. La tecla [0 #] hacer guardar los cambios actualmente introducidos y abandonar la función de servicio, la tecla [*] hace cancelar los datos introducidos y abandonar la función de servicio. Antes de que se apriete cualquier botón en el teclado, se visualizará el valor del parámetro programado. La presentación se realiza por medio de la visualización de los siguientes dígitos de parámetro entre los cuales existe una corta pausa. Cuando se visualicen todos los dígitos del parámetro hay una pausa larga. Después de apretar el botón numérico, en el teclado se visualiza el último dígito introducido. La forma de presentar los dígitos por medio del teclado está presentada en la siguiente tabla:

Número ingresado	Diodos encendidos
0	**1 2 3 4 5 6 7 8**
1	**1** 2 3 4 5 6 7 8
2	1 **2** 3 4 5 6 7 8
3	1 2 **3** 4 5 6 7 8
4	1 2 3 **4** 5 6 7 8
5	1 2 3 4 **5** 6 7 8
6	1 2 3 4 5 **6** 7 8
7	1 2 3 4 5 6 **7** 8
8	1 2 3 4 5 6 7 **8**
9	**1** 2 3 4 5 6 7 **8**
10	1 **2** 3 4 5 6 7 **8**
11	1 2 **3** 4 5 6 7 **8**
12	1 2 3 **4** 5 6 7 **8**
13	1 2 3 4 **5** 6 7 **8**
14	1 2 3 4 5 **6** 7 **8**
15	1 2 3 4 5 6 **7 8**

4.1. ACTIVACIÓN DEL MODO DE SERVICIO

Para activar el modo de servicio se requiere la autorización con el código de instalador.

9 9 # <Código de instalador> #

La correcta introducción del número de función y del código se confirmará con el tono triple. El diodo PROG encendido informará que nos encontramos en el modo de servicio. Después de entrar en cualquier función de servicio el diodo PROG parpadeará. Después de salir de la función, el diodo PROG volverá a parpadear continuamente y nos avisará de que nos encontramos en el menú principal del modo de servicio.

4.2. SALIDA DEL MODO DE SERVICIO

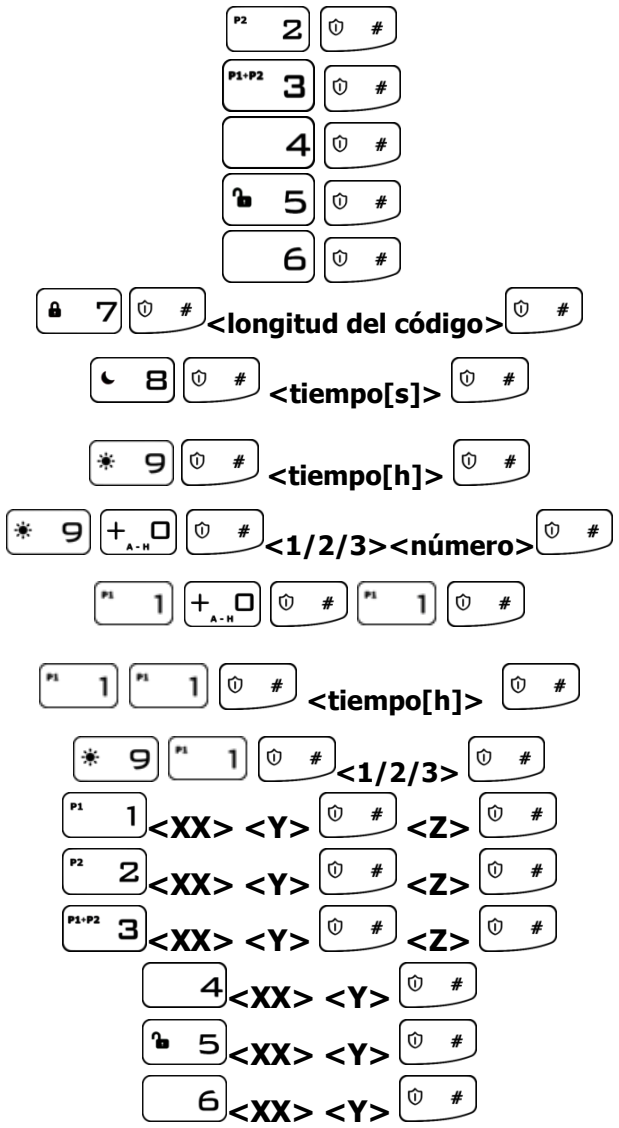
La salida del modo de servicio se realiza después de usar la función + y después de confirmar #. El uso de esta función ocasionará el reinicio de la centralita con el uso de parámetros configurados.

Pasados los 5 minutos de inactividad (sin apretar las teclas) saldremos automáticamente del modo de servicio y reiniciaremos la centralita.

4.3. MENÚ DEL INSTALADOR EN EL MODO DE SERVICIO

Después de entrar en el modo de servicio, el instalador tiene acceso a los parámetros y a la configuración de la centralita:

P1 1 # Cambio del código del instalador



4.3.1. Código de instalador

Esta función permite al instalador cambiar de su código. La función introducida correctamente será confirmada con un tono triple.

1 # **<código del instalador>** # **<código del instalador>** #

Siendo:

Código de instalador: Nuevo código de instalador (de 4 a 7 dígitos).

En cualquier momento puede apretar * para salir sin guardar cambios.

4.3.2. Desaparición de alimentación

Esta función determina el tiempo en segundos después del cual se avisa el fallo de alimentación. El argumento de la función es de tipo decimal. La función introducida correctamente será confirmada con un tono triple.

El cambio/la configuración de este tiempo se realiza de la siguiente forma:

P2 2 # **<Tiempo (s)>** #

Siendo:

***Tiempo*:** tiempo en segundos

En cualquier momento puede apretar * para salir sin guardar cambios.

4.3.3. Restablecimiento de la configuración de fábrica

La activación de esta función ocasionará el restablecimiento de la configuración de fábrica de las funciones que están disponibles desde el nivel del modo de servicio. No se restablecerá la configuración de los detectores inalámbricos y de los mandos a distancia. Esta función también restablece los parámetros predeterminados de las salidas y restaura el código de instalador predeterminado (2222).

Para protegerse contra la eliminación accidental de configuración, la función deberá ser confirmada, además, con el código de instalador. La función introducida correctamente será confirmada con un tono triple. El uso de esta función ocasionará el reinicio de la centralita con el uso de la configuración de fábrica.

P1+P2 3 # **<Código de instalador>** #

En cualquier momento puede apretar * para salir sin guardar cambios.

4.3.4. Opciones del sistema

La función permite activar y desactivar las opciones adicionales del sistema. El argumento de esta función es de tipo BIN. Por medio de las teclas 1 a 7 se activan o desactivan las respectivas opciones. La función introducida correctamente será confirmada con un tono triple.

4 # **<Opciones>** #

Siendo:

Opciones: número de opción (parámetro de tipo BIN):

- **1** – Activación/desactivación de la señalización del historial de fallos (cuando la opción está desactivada, el diodo SYSTEM no señala los fallos históricos por medio de parpadeo; es posible consultar el historial de fallos después de acceder a la función «memoria de fallos»).
- **2** – Activación/desactivación de la verificación de ATS (sistema de transmisión de alarmas). Cuando la opción está activa, el fallo de ATS no se señala o hace que se deshabilite el armado.
- **3** – Requerir que se confirme el armado en caso de fallo (con el botón #). Cuando esta opción está activa, cualquier fallo en el sistema causará que el armado sea bloqueado: el teclado alámbrico emitirá un pitido continuo, los diodos ALARM y SYSTEM parpadearán lentamente y diodos de 1 a 8 mostrarán códigos de error (véase el capítulo 6.6 Armando el sistema con un fallo en el Manual de usuario). Presionar el botón # para armar el sistema. De lo contrario, la centralita permanecerá desarmada. La información sobre fallos y violaciones estará disponible

después de acceder –desde el teclado alámbrico– a la función de usuario: memoria de fallos y estado actual de las entradas. Cuando la opción no está activa, el bloqueo de armado se omitirá automáticamente si hay un fallo en el sistema.

- **4** – El acceso al historial requiere autorización. Si esta opción está activa, el acceso al historial de alarmas y fallos es posible después de introducir el código de usuario. Active esta opción para mantener la compatibilidad con Grado 2.
- **5** – Sin visualizar el estado de alarmas y bloqueos. Si esta opción está activa, las violaciones y los bloqueos de línea actuales no se muestran en el teclado. Active esta opción para mantener la compatibilidad con Grado 2.
- **6** – Bloqueo del teclado después de 3 intentos de acceso fallidos. Si esta opción está activa, el teclado quedará bloqueado durante 90 segundos después de introducir 3 códigos erróneos. Durante este tiempo, ninguna función de la centralita no estará disponible desde el teclado. Una vez trascurrido el tiempo de bloqueo, el siguiente bloqueo del teclado se producirá después de introducir sucesivamente 3 códigos erróneos. La introducción del código correcto (por ejemplo, después de 2 códigos incorrectos) restablecerá el contador de códigos incorrectos. Active esta opción para mantener la compatibilidad con Grado 2.
- **7** – Código de coacción. El código de coacción (*duress code*) introducido durante el armado/desarmado envía una alarma silenciosa a la estación de monitoreo.

En cualquier momento puede apretar [*] para salir sin guardar cambios.

4.3.5. Administración remota de usuarios

Esta función permite activar o desactivar la administración remota de usuarios. El estado de la opción se conmuta con el botón 1. La función introducida correctamente será confirmada con un tono triple.

[5] [#] **<opción>** [#]

Siendo:

posible valor de la **opción**:

- **1** – Activación/desactivación de la administración remota de usuarios.

En cualquier momento puede apretar [*] para salir sin guardar cambios.

4.3.6. Opciones avanzadas del sistema

Función adicional que permite activar/desactivar las opciones correspondientes. El argumento de esta función es de tipo BIN. La función introducida correctamente será confirmada con un tono triple.

[6] [#] **<Opciones>** [#]

Opciones: número de opción (parámetro de tipo BIN):

- **1 –** Bloqueo de la instalación. Esta función desactiva la posibilidad de armar la centralita. Tras activar esta función, el usuario no podrá armar la instalación de ninguna manera (por ejemplo, SMS/GPRS, control remoto, entrada de armado, horarios, teclado normal, teclado inalámbrico). Sólo sera posible desarmar la centralita. Todo intento de armado será rechazado por la centralita.

- **2 –** Bloqueo de restauración de los ajustes predeterminados. Esta función permite desactivar la posibilidad de restaurar el código de instalador predeterminado. Sin embargo, cuando se restauran los ajustes predeterminados mediante el Configurador, después de seleccionar la opción «Restaurar los ajustes predeterminados», aparecerá una ventana pidiendo el código de instalador o el código de servicio (ATS).

  Tras activar esta función es recomendable cambiar el código de acceso del instalador y el código de servicio (ATS).

  ATENCIÓN: En caso de pérdida de los nuevos códigos, será necesario enviar los dispositivos bloqueados al servicio de EBS.
- **3 –** Permitir el armado rápido sin autorización del usuario. Si esta opción está activa, el sistema puede armarse rápidamente utilizando el teclado sin necesidad de introducir el código de autorización de usuario.
- **4 –** Desactivar la señalización de alarmas históricas tras el desarmado. Si esta opción está activa, tras desarmar el sistema (la partición), las alarmas históricas procedentes de las líneas asignadas a la partición y señaladas mediante el parpadeo del diodo F (partición 1) y del diodo 6 (partición 2) no se visualizarán en el teclado una vez trascurrido el tiempo de retraso ajustado (véase el capítulo 4.3.8). El usuario seguirá teniendo acceso al estado de las alarmas históricas de las entradas mediante la función 3# hasta que se borren. Cuando el sistema está desarmado y se activa una alarma de cualquier línea de 24 horas, el historial de alarmas puede desactivarse armando y desarmando el sistema (sólo si la opción está activada) o accediendo a la función 3# y borrando el historial.
- **5** – Desactivar la posibilidad de armar mediante el teclado alámbrico durante una violación o un sabotaje de la línea. Si esta opción está activa, el armado con el KP32 se bloquea cuando las líneas sean violadas o saboteadas. La violación / el sabotaje de cualquier línea asignada al sistema se señala mediante el apagado del diodo READY: D en el caso de una línea de la partición 1 o 4 en caso de una línea de la partición 2. Si el sistema cuenta con dos particiones, basta con que una de ellas tenga un detector violado/saboteado para que no se pueda armar la centralita. Cuando se intenta armar, el teclado alámbrico emitirá un pitido alto de un segundo y se iluminarán los diodos GROUP, ALARM, SYSTEM y PROG durante unos 4 segundos. Los fallos del sistema no afectan a esta opción.
  ATENCIÓN: Opción disponible a partir de la versión de firmware 2.8.8.

En cualquier momento puede apretar [*] para salir sin guardar cambios.

4.3.7. Longitud de los códigos de acceso

Esta función permite determinar la longitud de los códigos de administrador y de usuarios (la modificación afecta a todos los usuarios). El rango de longitud es de 4 a 7 dígitos. El valor por defecto es 4.

[7] [#] **<longitud del código>** [#]

Siendo:

longitud del código: de 4 a 7 dígitos.

Sólo es posible reducir la longitud si los códigos acortados no resultan ser los mismos.

Ejemplo:

Supongamos que tenemos los siguientes códigos de 5 dígitos en la base CPX: 44440, 44444, 44449. No será posible acortar la longitud del código a 4 dígitos, ya que tendríamos códigos idénticos. No se aceptará el cambio, lo que será indicado por el teclado mediante un pitido continuo de varios segundos. En tal caso la única solución posible es eliminar usuario(s) con códigos similares.

1. **Si el código de usuario en la base de datos CPX es más corto que el valor definido, se agregarán «0» al final del código:**
   Ejemplo: Si hay un código 1234 en la base, tras cambiar la longitud del código a 6 dígitos, este código será 123400.
2. **Si el código de usuario en la base de datos CPX es más largo que el valor definido, se acortará a los «n» primeros dígitos.**
   Ejemplo: Si hay un código 1234567 en la base, tras cambiar la longitud del código a 5 dígitos, este código será 12345.
3. **En el caso de un código de coacción:**
   - **Si hay un código 12345 en la base, tras cambiar la longitud del código a 7 dígitos, este código será 1234500. Por lo tanto, el código de coacción será 1234501**
   - **Si hay un código 12345 en la base, tras cambiar la longitud del código a 4 dígitos, este código será 1234. Por lo tanto, el código de coacción será 1235**

4.3.8. Retraso en la desactivación de la señalización de alarmas históricas

8 # **<tiempo[s]>** #

Esta función sólo es disponible tras activar la opción «Desactivar la señalización de alarmas históricas tras el desarmado». Permite determinar un retraso en segundos, tras el cual ya no se mostrarán las alarmas históricas en el teclado. Cuándo el sistema está armado y suceden violaciones señaladas mediante el parpadeo de los diodos F y 6, los diodos se apagarán una vez el sistema desarmado y trascurrido el tiempo determinado. Todavía se podrán consultar las alarmas mediante la función 3#, hasta que el usuario las borre.

4.3.9. Tiempo de detección del desvanecimiento de los detectores inalámbricos

Esta función permite determinar el tiempo después del cual se enviará el aviso sobre el desvanecimiento de los detectores inalámbricos a la estación de monitoreo.

9 # **<tiempo [h]>** #

Este tiempo se exprime en horas. El valor por defecto es de 6 horas, el mínimo de 2 y el máximo de 24 horas.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.8.8.

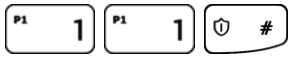
4.3.10. Desactivación de la opción de repetición cíclica de los eventos de desvanecimiento de los detectores

Esta función sólo desactiva la opción de envío cíclico de la información de desvanecimiento de los detectores inalámbricos (véase el capítulo 4.3.11).

ATENCIÓN: Opción disponible a partir de la versión de firmware 2.10.0.

4.3.11. Opción de repetición cíclica de los eventos de desvanecimiento de los detectores

Esta función permite activar el envío cíclico de la información de desvanecimiento de los detectores inalámbricos a intervalos definidos (a partir del primer desvanecimiento) a la estación de monitoreo.

 **<tiempo [h]>** 

Este tiempo se exprime en horas. El valor por defecto es de 6 horas, el mínimo de 2 y el máximo de 24 horas.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.10.0.

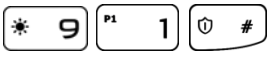
4.3.12. Números ACN en la comunicación en formato Contact ID

En caso de transmisión de datos en formato Contact ID, es posible determinar números de identificación individuales de la cuenta del sistema (ACN0) y de las cuentas de sus subsistemas: partición 1 (ACN1) y partición 2 (ACN2). Esto permite determinar de qué parte del sistema proviene la señal.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.9.0.

4.3.12.1. Registro y modificación de números ACN

Una vez registrado el número ACN0, la información sobre cada evento del sistema enviada a la estación de monitoreo llevará este número. Los eventos del sistema son aquellos que contienen información sobre el mismo, por ejemplo: fallo de alimentación, reinicio del módem, fallo en la hora.
Una vez registrados los números ACN1 y ACN2, la información sobre cada evento no relacionado con el sistema (con identificador de partición 1 y/o 2) llevará el número ACN1 (para la partición 1) o ACN2 (para la partición 2). Los eventos no relacionados con el sistema son aquellos que contienen información sobre las particiones, por ejemplo: armado/desarmado de la partición 1 y/o 2, alarmas de los detectores asignados a la partición.

Para definir los números, presione:

 **<botón 1/2/3> <número>** 

Siendo:

Botón 1: definición o cambio del número ACN1 de la cuenta de la partición 1
Botón 2: definición o cambio del número ACN2 de la cuenta de la partición 2
Botón 3: definición o cambio del número ACN0 de la cuenta del sistema
número: número ACN: cuatro caracteres hexadecimales cualquiera

Los diodos 1, 2 y 3 indican que los números ACN no están configurados. Después de pulsar el botón 3, introducir cuatro caracteres hexadecimales y confirmar con el botón [#], se registra el número ACN0. Del mismo modo se definen los números ACN1 y ACN2. Cuándo los diodos están iluminados, al pulsar los botones 1, 2, 3 se pueden visualizar los números y cambiarlos si es necesario.

ATENCIÓN: Si se configura el número de cuenta para una sola partición, el mismo número se establecerá automáticamente para la otra partición y para el sistema.

4.3.12.2. Supresión de números ACN y cambio de la configuración de opciones

Para suprimir los números o configurar el envío de los eventos del sistema, presione:

[*] [9] [+] [#] **<botón 1/2/3>** [#]

Siendo:
Botón 1: supresión del número ACN0 enviado a la cuenta del sistema
Botón 2: supresión de los números ACN1 y ACN2 enviados a las cuentas de las particiones 1 y 2
Botón 3: configuración del envío de eventos del sistema, siendo:

- diodo 3 apagado: los eventos del sistema se envían solamente a la cuenta del sistema
- diodo 3 iluminado: los eventos del sistema se envían a todas las cuentas

ATENCIÓN: Si se elimina el número ACN0, también se eliminarán los números ACN1 y ACN2.

4.3.13. Configuración de las líneas de detección (entradas)

Las líneas alámbricas e inalámbricas pueden configurarse mediante funciones de servicio que configuran un único parámetro de línea o funciones de servicio compuestas que configuran todos sus parámetros. En las funciones de servicio compuestas, los parámetros de cada línea se ingresan uno tras otro. La configuración de las líneas inalámbricas se describe en el punto 4.3.16.

Los códigos de las funciones de configuración corresponden al siguiente esquema:

[1] **<XX> <Y>** [#] **<Z>** [#]

Siendo:

XX – número de línea de **01** a **32**; los nombres de las líneas y sus números correspondientes se indican en la siguiente tabla:

Nombre	A1	A2	A3	A4	A5	A6	A7	A8	B1	B2	B3	B4	B5	B6	B7	B8	C1	C2	C3	C4	C5	C6	C7	C8	D1	D2	D3	D4	D5	D6	D7	D8
Número	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

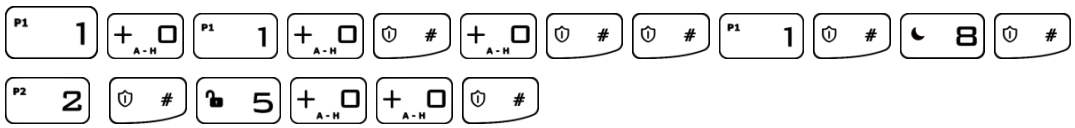
El número **00** permite cambiar los parámetros de todas las líneas del sistema al mismo tiempo,

Y – número del parámetro correspondiente a la línea,

Z – número (o valor) del parámetro siguiente.

- **Para Y=0** – función compuesta cuya activación configurará los siguientes parámetros como el siguiente conjunto de parámetros;

Ejemplo: cambiar múltiples parámetros para la línea A1 simultáneamente usando una función compuesta: queremos configurar la línea A1 como inmediata, en modo NC que se bloqueará después de 8 violaciones, generará una alarma cuando violada después de armar y tendrá una sensibilidad de 500 ms:



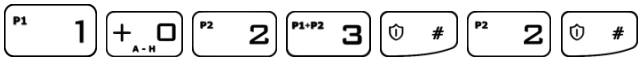
Nota: En caso de una función compuesta (programación de varios parámetros al mismo tiempo), después de introducir el parámetro y confirmarlo con el botón # el parámetro se guarda en la memoria de configuración y se espera a que se introduzca el siguiente parámetro y así hasta introducir todos los parámetros de la función de servicio compuesta. Pulsando el botón * se cancelan sólo los cambios realizados en el parámetro actualmente configurado y se sale de la función de servicio; los parámetros introducidos anteriormente y aceptados con el botón # no se cancelan.

- **Para Y=1** – tipo de respuesta de la línea (parámetro tipo DEC). Las opciones de 10 a 13 se seleccionan manteniendo pulsadas las teclas de 0 a 3 durante un período más largo (aprox. 2s), valores posibles del parámetro **Z**:
  - 0 – línea inmediata
  - 1 – línea temporizada (entradas/salidas)
  - 2 – línea 24H de pánico
  - 3 – línea de rearme/desarme por violación
  - 4 – línea de sabotaje
  - 5 – línea temporizada condicionalmente
  - 6 – línea 24H de pánico con alarma silenciosa
  - 7 – línea 24H de incendio
  - 8 – línea perimetral
  - 9 – línea perimetral de salida
  - 10 – línea 24H de gas

- 11 – línea 24H de inundación
- 12 – línea nocturna (deshabilitada de noche)
- 13 – línea nocturna temporizada
- 14 – línea de rearme/desarme por cambio de estado (a partir de la versión de firmware 2.10.0)

- **Para Y=2** – retraso **Z** en segundos para las líneas con respuesta «atrasada» (parámetro tipo DEC). Para otros tipos de reacciones el parámetro no importa.
- **Para Y=3** – modo de trabajo (parámetro tipo DEC), valores posibles del parámetro **Z**:
  - 0 – línea no usada
  - 1 – modo NC
  - 2 – modo NO
  - 3 – modo EOL/NC
  - 4 – modo EOL/NO
  - 5 – modo DEOL/NC
  - 6 – modo DEOL/NO
  - 7 – modo inalámbrico
  - 8 – modo TEOL

Ejemplo: cambio del modo de trabajo de la línea A2 al modo NO:



- **Para Y=4** – número de alarmas **Z** después de las cuales la línea quedará automáticamente bloqueada hasta el rearme (parámetro tipo DEC). En caso de 0, la línea no estará bloqueada;
- **Para Y=5** – opciones de la línea (parámetro tipo DEC), valores posibles del parámetro **Z**:
  - 1 – línea omitida durante el rearme, es decir, puede ser violada durante el rearme de la partición (por ejemplo, las líneas temporizadas deberán tener esta opción activa)
  - 2 – genera una alarma cuando violada después de rearmar
  - 3 – bloqueo de la línea cuando violada durante el armado (parámetro «Después del retardo de salida»)
  - 4: activación/desactivación de la función de timbre. Durante una violación, el teclado emite una señal sonora (cuando el sistema está desarmado) sin enviar el informe de alarma a la estación de monitoreo.
- **Para Y=6** – sensibilidad de la línea **Z** en milisegundos, es decir el tiempo después del cual el sistema considera que la línea ha cambiado de estado, valor por defecto del parámetro **Z**: 400 ms;

Ejemplo: Cambio de sensibilidad de todas las líneas a 200 milisegundos:

Nota: Para las líneas inalámbricas, la función compuesta 1XX0 no puede contener la opción (función) 6: sensibilidad de entrada. La función 1XX3 (modo de trabajo) para las líneas inalámbricas indica el valor 7: modo inalámbrico. Este valor no se puede modificar.

4.3.14. Configuración de salidas

Las salidas y entradas pueden configurarse mediante funciones de servicio que configuran un único parámetro de salida o funciones de servicio compuestas que configuran todos sus parámetros. En las funciones de servicio compuestas, los parámetros de cada salida se ingresan uno tras otro.

Los códigos de las funciones de configuración de la salida corresponden al siguiente esquema:

[P2 2] **<XX> <Y>** [# ⏻] **<Z>** [# ⏻]

Siendo:

XX – determina el número de salida de **01** a **03**; el uso del número **00** ocasionará el cambio de parámetros para todas las salidas en el sistema,

Y – número del parámetro correspondiente a la salida,

Z – número (o valor) del parámetro siguiente.

- **Para Y=0** – función compuesta cuya activación configurará los siguientes parámetros como el siguiente conjunto de parámetros;

Ejemplo: Cambiar múltiples parámetros para la salida 1 simultáneamente usando una función compuesta: queremos configurar la salida 1 como aviso de alarma con el tiempo de respuesta de 120 segundos:

[P2 2] [+ A-H 0] [P1 1] [+ A-H 0] [# ⏻] [P1 1] [# ⏻] [P1 1] [P2 2] [+ A-H 0] [# ⏻]

Nota: En caso de una función compuesta (programación de varios parámetros al mismo tiempo), después de introducir el parámetro y confirmarlo con el botón [# ⏻] el parámetro se guarda en la memoria de configuración y se espera a que se introduzca el siguiente parámetro y así hasta introducir todos los parámetros de la función de servicio compuesta. Pulsando el botón [* 🔥] se cancelan sólo los cambios realizados en el parámetro actualmente configurado y se sale de la función de servicio; los parámetros introducidos anteriormente y aceptados con el botón [# ⏻] no se cancelan.

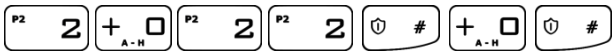
- **Para Y=1** – tipo de salida (parámetro tipo DEC), valores posibles del parámetro **Z**:
  - 0 – no usado,
  - 1 – aviso de alarma,
  - 2 – estado de armado,
  - 3 – fallo de alimentación,
  - 4 – fallo ATS – falta de comunicación con el servidor de recepción.
  - 5 – indicador de interferencia de la señal GSM
  - 6 – señalización chirp en el rearme/desarme
  - 7 – señalización chirp en el rearme/desarme y señalización de alarma

Ejemplo: Cambio de tipo de la salida número 3 a activación en caso de fallo de alimentación:

[P2 2] [+ A-H 0] [P1•P2 3] [P1 1] [# ⏻] [P1•P2 3] [# ⏻]

- **Para Y=2** – tiempo de funcionamiento de la salida **Z** en segundos (parámetro tipo DEC); en caso de ajustar a 0, la salida funcionará en modo biestable;

Ejemplo: Cambio del modo de trabajo de la salida número 2 a modo de trabajo biestable:



La señalización chirp se configura mediante dos comandos:

- **Para Y=3** – duración de la señal chirp **Z** en milisegundos;

Ejemplo: Ajustar la duración de la señal chirp a 600 milisegundos para todas las líneas:

- **Para Y=4** – intervalo **Z** entre las señales en milisegundos en caso de chirp doble;

Ejemplo: Ajustar el intervalo a 500 ms para todas las líneas:

Nota: La configuración chirp es común para todas las salidas.
Los valores por defecto para ambos parámetros son 250 ms

4.3.15. Configuración de particiones

Al igual que las líneas y las salidas, las particiones pueden configurarse mediante funciones de servicio que configuran un único parámetro de partición o funciones de servicio compuestas que configuran todos sus parámetros. En las funciones de servicio compuestas, los parámetros de cada partición se ingresan uno tras otro.

Los códigos de las funciones de configuración de la partición corresponden al siguiente esquema:

Siendo:

XX – determina el número de partición de **01** a **02**; el uso del número 00 ocasionará el cambio simultáneo de parámetros para ambas particiones,

Y – número del parámetro correspondiente a la partición,

Z – número (o valor) del parámetro siguiente.

- **Para Y=0** – función compuesta cuya activación configurará los siguientes parámetros como el siguiente conjunto de parámetros;
- **Para Y=1** – líneas de la partición (parámetro tipo BIN). El diodo parpadeante (de A a D) representa el grupo actual. Los diodos iluminados en continuo representan los grupos con líneas asignadas a la partición determinada. Los diodos apagados representan los grupos sin líneas asignadas a la partición determinada. Pulsando los botones de 1 a 8 se asignan las líneas del grupo a la partición determinada. El botón  permite cambiar de grupo. No hay parámetro **Z**;
- **Para Y=2** – salidas de la partición (parámetro tipo BIN), no hay parámetro **Z**;
- **Para Y=3** – retardo de salida de la partición **Z** en milisegundos (parámetro tipo DEC);

- **Para Y=4** – tiempo de alarma en la partición **Z** en segundos (parámetro tipo DEC);
- **Para Y=5** – opciones de la partición (parámetro tipo BIN), valores posibles del parámetro **Z**:
  - 1 – señalización silenciosa del retardo de entrada (no sonará el zumbador del teclado durante la cuenta regresiva del retardo de entrada)
  - 2 – señalización silenciosa del retardo de la salida (no sonará el zumbador del teclado durante la cuenta regresiva del retardo de salida)
- **Para Y=6** – hora del armado automático **Z** de la partición (parámetro tipo DEC, tiempo en formato HHMM de 24 horas);
- **Para Y=7** – configuración del armado automático de la partición (parámetro tipo BIN), valores **Z** posibles:
  - 1 – activación/desactivación del armado
- **Para Y=8** – hora del desarmado automático **Z** de la partición (parámetro tipo DEC, tiempo en formato HHMM de 24 horas);
- **Para Y=9** – configuración del desarmado automático de la partición (parámetro tipo BIN), valores posibles del parámetro **Z**:
  - 1 – activación/desactivación del desarmado

Observaciones:

Al activar la función compuesta 3006 (tiempo de armado para todas las particiones) se copiará el indicador de activación/desactivación del cronograma de armado de la primera a la segunda partición.

Al activar la función compuesta 3007 (activación/desactivación del cronograma de armado para todas las particiones) se copiará el tiempo de armado de la primera a la segunda partición.

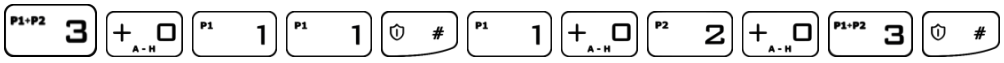
Al activar la función compuesta 3008 (tiempo de desarmado para todas las particiones) se copiará el indicador de activación/desactivación del cronograma de desarmado de la primera a la segunda partición.

Al activar la función compuesta 3009 (activación/desactivación del cronograma de desarmado para todas las particiones) se copiará el tiempo de desarmado de la primera a la segunda partición.

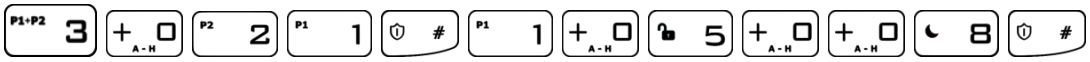
Si la hora del sistema se adelanta (por ejemplo, al cambiar la hora de invierno a verano), se omitirán los eventos de armado/desarmado programados durante este tiempo. Por ejemplo: si el armado automático está programado para las 02:30, al cambiar la hora de invierno a verano (de 2:00 a 3:00), no se armará la centralita.

<u>Ejemplos:</u>

a) cambio de un solo parámetro: asignación de las líneas A1, B2, C3 a la primera partición:

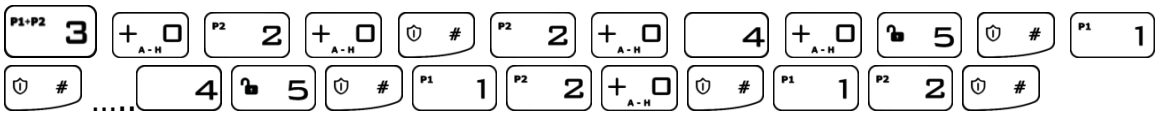


b) cambio de un solo parámetro: asignación de las líneas A1, B5, D8 a la segunda partición:



c) cambio del retardo de salida en ambas particiones a 60 segundos:

d) cambiar múltiples parámetros para la partición 2 simultáneamente usando una función compuesta: queremos asignar las líneas A2, B4, C5 y la salida 1 a la partición 2, ajustar el retardo de salida de la partición a 45 segundos, el tiempo de alarma en la partición 2 a 120 s, y ajustar la señalización silenciosa de entrada y salida:



Nota: En caso de una función compuesta (programación de varios parámetros al mismo tiempo), después de introducir el parámetro y confirmarlo con el botón # el parámetro se guarda en la memoria de configuración y se espera a que se introduzca el siguiente parámetro y así hasta introducir todos los parámetros de la función de servicio compuesta. Pulsando el botón * se cancelan sólo los cambios realizados en el parámetro actualmente configurado y se sale de la función de servicio; los parámetros introducidos anteriormente y aceptados con el botón # no se cancelan.

4.3.16. Configuración de líneas inalámbricas

4.3.16.1. Configuración de detectores inalámbricos

Las líneas inalámbricas pueden configurarse mediante funciones de servicio que configuran un único parámetro de línea o funciones de servicio compuestas que configuran todos sus parámetros. En las funciones de servicio compuestas, los parámetros de cada línea se ingresan uno tras otro. Los códigos de las funciones de configuración de las líneas inalámbricas corresponden al siguiente esquema:

Siendo:

XX – número de línea inalámbrica de **01** a **32**, los nombres de las líneas y sus números correspondientes se indican en la siguiente tabla:

Nombre	A1	A2	A3	A4	A5	A6	A7	A8	B1	B2	B3	B4	B5	B6	B7	B8	C1	C2	C3	C4	C5	C6	C7	C8	D1	D2	D3	D4	D5	D6	D7	D8
Número	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

El número **00** permite cambiar los parámetros de todas las líneas del sistema al mismo tiempo,

Y – número del parámetro correspondiente a la línea,

Para Y=0 – función compuesta cuya activación configurará los siguientes parámetros como el siguiente conjunto de parámetros

Para Y=1 – Eliminar el detector. Después de seleccionar esta función, puede confirmar la eliminación del detector con la tecla [#] o cancelar la eliminación con la tecla [*].

Ejemplo:

a) eliminación del detector B2 (número 10, véase la tabla anterior):

[4] [P1 1] [+ A-H] [P1 1] [#] [#]

Para Y=2 – Añadir un detector. Después de seleccionar este parámetro se debe apretar el botón de sabotaje en el sensor. Tras detectar la transmisión desde el detector se visualizará automáticamente el número de serie en el teclado (valor hexadecimal). Una vez aprobado, el detector se guardará.

Ejemplo:

b) registro del detector B3 (número 11, véase la tabla anterior):

[4] [P1 1] [P1 1] [P2 2] [#] (botón de sabotaje sobre el detector) [#]

Para Y=3 – Tipo del detector inalámbrico (sólo lectura)

0 – falta de sensor
1 – sensor PIR-10
2 – sensor MC-10
4 – sensor SD-10
5 – sensor PIR-11
6 – sensor SD-20
7 – teclado KP2W
8 – sensor MC-11
9 – sensor FL-10
12 – sensor GS-21
13 – sensor GS-22
14 – sensor MD-10 (a partir de la versión de firmware 2.9.2)
15 – sensor GB-10 (a partir de la versión de firmware 2.9.2)

Para Y=4 – Intensidad de la señal de los detectores inalámbricos. Esta función permite comprobar la intensidad de la señal de radio de los detectores inalámbricos. Los diodos 1 a 8 indican la intensidad de la señal procedente de esta línea. Todos los diodos apagados indican que no hay señal.

1 diodo: 12 % de señal
2 diodos: 25 % de señal
3 diodos: 37% de señal
4 diodos: 50% de señal
5 diodos: 62 % de señal
6 diodos: 75% de señal
7 diodos: 88% de señal
8 diodos: 100% de señal

Al mismo tiempo, el teclado indica la intensidad de la señal mediante pitidos. 1 pitido indica 25 % de señal, 2 pitidos 50 % de señal, 3 pitidos 75 % de señal, 4 pitidos 100 % de señal.

Para salir de la función, pulse la tecla [*] (o [#] si no hay ningún número de línea seleccionado).

Nota: Al añadir un nuevo detector al sistema (parámetro 2), debe quitarse su tapa. Es recomendable añadir detectores inalámbricos individualmente. Durante este procedimiento sólo se debe quitar la carcasa de un detector para eliminar las transmisiones accidentales de otros detectores.

4.3.16.2. Eliminación de detectores inalámbricos

Para eliminar todos los detectores inalámbricos del sistema, introduzca la siguiente función:

[4] [+ A-H] [+ A-H] [P1 1] [#]

Después de entrar en la función, el diodo PROG parpadea y los demás diodos permanecen apagados. Presionando la tecla [#] se borrarán todos los detectores inalámbricos, se generarán 3 pitidos cortos y se saldrá de la función. Pulsando la tecla [*] se saldrá de la función sin borrar los detectores.

4.3.17. Configuración de mandos a distancia

4.3.17.1. Configuración de mandos a distancia

Los mandos a distancia pueden configurarse mediante funciones de servicio que configuran un único parámetro de mando o funciones de servicio compuestas que configuran todos sus parámetros. En las funciones de servicio compuestas, los parámetros de cada mando se ingresan uno tras otro.

Los códigos de las funciones de configuración del mando corresponden al siguiente esquema:

[5] **<XX> <Y>** [#] **<Z>** [#]

Siendo:

XX – número de mando de **01** a **32**; los nombres de los mandos y sus números correspondientes se indican en la siguiente tabla:

Nombre	A1	A2	A3	A4	A5	A6	A7	A8	B1	B2	B3	B4	B5	B6	B7	B8	C1	C2	C3	C4	C5	C6	C7	C8	D1	D2	D3	D4	D5	D6	D7	D8
Número	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Y – número del parámetro correspondiente al mando,

Z – número (o valor) del parámetro siguiente.

Para Y=0 – función compuesta cuya activación configurará los siguientes parámetros como el siguiente conjunto de parámetros;

Para Y=1 – Eliminar el mando. Después de seleccionar esta función, puede confirmar la eliminación del mando con la tecla [#] o cancelar la eliminación con la tecla [*].

Para Y=2 – Añadir un mando. Después de seleccionar este parámetro se debe apretar cualquier botón del mando. La detección de la transmisión desde el mando ocasionará automáticamente la visualización del número de serie en el teclado (valor hexadecimal). Tras aprobar, se guardará el mando; no hay parámetro **Z**.

Para Y=3 – Tipo del mando (sólo lectura); no hay parámetro **Z**:
0 – Falta de mando
2 – Mando RC-10

Para Y=4 – Usuario al que está asignado el mando

Para Y=5, 6, 7 y 8 – Asignación de funciones a las teclas del mando, donde el número 5 corresponde a la tecla - , 6 - , 7 - , 8 - ; valores **Z** posibles:
0 – Falta de función
1 – Armar (en modo completo)
2 – Desarme
3 – Alarma
4 – Alarma silenciosa
5 – Active la salida 1
6 – Active la salida 2
7 – Active la salida 3
8 – Desactive la salida 1
9 – Desactive la salida 2
10 – Desactive la salida 3
11 – Asistencia médica (disponible a partir de la versión de firmware 2.8.8)
12 – armar inmediatamente (disponible a partir de la versión de firmware 2.10.0)

Nota:

La función «Alarm» significa la generación de una alarma con aviso sonoro.

La función «Alarma silenciosa» significa una alarma sin aviso sonoro.

Las funciones de activación/desactivación de las salidas 1, 2 y 3 permiten controlar dispositivos externos.

La función «Asistencia médica» funciona de la misma manera que el botón «AYUDA» en el teclado, es decir, genera una alarma médica.

La función «Armar inmediatamente» permite el armado inmediato del sistema sin esperar el retardo de salida ajustado.

Los alarmas del mando a distancia funcionan independientemente de si la partición apropiada está armada o no. Para ambos tipos de alarma puede enviarse un mensaje al centro de monitoreo, dependiendo de la configuración de la centralita.

Ejemplos:

a) eliminar el mando n° 1:
[5] [+ A-H] [P1 1] [P1 1] [#]

b) añadir el mando n° 1:

5 + A-H 0 P1 1 P2 2 # (cualquier botón del mando) #

4.3.17.2. Eliminar todos los mandos

Para eliminar todos los mandos del sistema, introduzca la siguiente función:

5 + A-H 0 + A-H 0 P1 1 #

Después de entrar en la función, el diodo PROG parpadea y los demás diodos permanecen apagados. Presionando la tecla # se eliminarán todos los mandos, se generarán 3 pitidos cortos y se saldrá de la función. Pulsando la tecla * se saldrá de la función sin eliminar los mandos.

4.3.18. Configuración de los botones de alarma en el teclado

El funcionamiento de los botones de alarma se configura como sigue:

6 **<XX> <Y>** # **<Z>** #

Siendo:

XX – botón de alarma:

- **00** – cambiar el ajuste de todos los botones de alarma
- **01** – botón INCENDIO que genera una alarma de incendio
- **02** – botón AYUDA que genera una alarma médica
- **03** – botón PÁNICO que genera una alarma de pánico

Y – número del parámetro correspondiente al botón

Z – número (o valor) del parámetro siguiente.

- **Para Y=0** – función compuesta cuya activación configurará los siguientes parámetros como el siguiente conjunto de parámetros.
- **Para Y=1** – Configuración del botón de alarma, valores posibles del parámetro **Z**:
  - 1: activación/desactivación del botón
  - 2: salida 1
  - 3: salida 2
  - 4: salida 3

Después de confirmar la opción deseada, se visualizarán los números de salidas asignadas al botón de alarma en cuestión. Con los botones numerados de 2 a 4, puede cambiar el estado de las salidas que se activarán después de que se active una alarma mediante un botón de función configurable. No se cambiarán las salidas para las funciones que activan o desactivan el funcionamiento de todos los botones.

Ejemplo:

a) desactivación del funcionamiento de todos los botones de alarma:

6 + A-H 0 + A-H 0 P1 1 # P1 1 #

b) activación de la función «pánico» (mantenga pulsado el botón #) y cambio de estado de las salidas 2 y 3 (activación, si están desactivadas; los diodos encendidos señalan la activación de las opciones):

6 + A-H 0 P1+P2 3 P1 1 # P1 1 P1+P2 3 4 #

4.4. MENSAJES DE TEXTO

Para que la configuración de los mensajes de texto sea posible desde el nivel de instalador, el administrador primero deberá permitir acceso al instalador. El comando que sirve para ello es: [5] [2] [#] **<código de administrador>** [#]

Ahora se puede activar o desactivar los permisos de instalador para configurar los mensajes de texto con la tecla [1]. Cuando los permisos estén activos encenderá el diodo 1. Cuando no estén activos – el diodo 1 quedará apagada. La selección de permisos debe confirmarse con la tecla [#]

La cantidad máximo de números a los cuales puede enviar mensajes es 10. La cantidad máxima de mensaje para configurar es 32. Cuando por cualquier razón el dispositivo no pueda enviar mensaje, será enviado en el momento de recuperar la comunicación a la red, sin embargo, no más tarde que a 1 día después de la existencia del evento que ha generado el mensaje (entonces los mensajes caducan y se eliminan).

Nota: El contenido de mensaje no deberá contener caracteres fuera del alfabeto inglés. Además, cuando el contenido del mensaje incluye espacio, se debe cerrar entre comillas (" ") el contenido del mensaje desde el signo de igualdad (=) hasta el último carácter.

Nota: Algunos componentes de los comandos se presentan entre corchetes [...]. Esto significa que se trata de campos opcionales.

Configuración del número de teléfono	
Formato de comando	XXXX SETTELNUM=ID,NUMBER
Descripción de comando	Configuración de teléfono en el índice indicado en el listado de números XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio ID – índice del número de teléfono en el listado, se puede tomar el valor de 1 a 10 NUMBER – número de teléfono al que se enviarán los mensajes *Ejemplo: 1234 SETTELNUM=3,600987654*
Descripción del mensaje de retorno	SETTELNUM:OK - el comando fue aprobado SETTELNUM:ERROR – el comando fue rechazado por el sistema

Descarga del número de teléfono	
Formato de comando	XXXX GETTELNUM=ID
Descripción de comando	Descarga del número de teléfono desde el índice indicado XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio ID – índice del número de teléfono del listado *Ejemplo: 1234 GETTELNUM=2*
Descripción del mensaje de retorno	GETTELNUM=ID,NUMBER – información sobre el número de teléfono GETTELNUM:ERROR – el comando fue rechazado por el sistema

Configuración del contenido de mensaje	
Formato de comando	XXXX SETMESSAGE=ID,MESSAGE_sin_espacios XXXX SETMESSAGE="ID,MESSAGE_con_espacios"
Descripción de comando	Configuración del contenido del mensaje en el índice dado. XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio ID – índice de mensaje, se puede aprobar el valor de 1 a 32 MESSAGE – contenido de mensaje *Ejemplo: 1234 SETMESSAGE=4,efraccion*
Descripción del mensaje de retorno	SETMESSAGE:OK – el comando fue aprobado SETMESSAGE:ERROR – el comando fue rechazado por el sistema

Descarga del contenido de mensaje	
Formato de comando	XXXX GETMESSAGE=ID
Descripción de comando	Descarga del contenido de mensaje del índice dado. XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio ID – índice de mensaje, se puede aprobar el valor de 1 a 32 *Ejemplo: 1234 GETMESSAGE=30*
Descripción del mensaje de retorno	GETMESSAGE=ID,MESSAGE – información sobre el contenido de mensaje GETMESSAGE:ERROR – el comando fue rechazado por el sistema

Asignación del contenido de mensaje y los números de teléfonos a los eventos	
Formato de comando	XXXX SETUSERSMS=EVENT,TELNUM,MSG_ID
Descripción de comando	Asignación al evento el contenido de mensaje y el número de teléfono al que se enviará este mensaje XXXX – – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio EVENT – nombre simbólico de evento, el listado de eventos está disponible al final de este capítulo TELNUM – serie de ceros y unos compuesta de diez elementos. Los siguientes dígitos (de izquierda) corresponden a los índices de los números de teléfonos, es decir, el primer dígito corresponde al primer número de teléfono, el segundo dígito corresponde al segundo número, etc. 0 – el mensaje no se enviará a este número 1 – el mensaje se enviará a este número MSG_ID – índice de mensajes que se enviará cuando ocurre un evento *Ejemplo:* 1234 SETUSERSMS=ARM1,1000000110,6 significa que al evento ARM1 (rearme de la partición 1) se asignaron los números de teléfonos de los índices 1,8 y 9 y el contenido del mensaje del índice 6.

Descripción del mensaje de retorno	SETUSERSMS=EVENT,TELNUM,MSG_ID:OK - el comando fue aprobado SETUSERSMS=EVENT,TELNUM,MSG_ID:ERROR – el comando fue rechazado por el sistema

Recuperación del contenido de los mensajes y de los números de teléfono asignados a los eventos	
Formato de comando	XXXX GETUSERSMS=EVENT
Descripción de comando	Descarga de los índices de teléfonos y del contenido de mensajes asignados al evento indicado XXXX – – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio EVENT – nombre simbólico de evento, el listado de eventos está disponible al final de este capítulo
Descripción del mensaje de retorno	GETUSERSMS=EVENT:TELNUM,MSG_ID – información sobre los mensajes asignados al evento y el número de teléfono GETUSERSMS=EVENT:ERROR – el comando fue rechazado por el sistema

Descarga de información sobre los estados de particiones	
Formato de comando	XXXX GETARMED
Descripción de comando	Descarga de información sobre el rearme/desarme de la partición. XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio. *Ejemplo: 1234 GETARMED*

Descripción del mensaje de retorno	PARTITION1:X, PARTITION2:Y – información sobre el armado de la partición. PARTITION1,PARTITION2 – nombres predeterminados de la partición, pueden ser modificados por medio del comando SETNAME X,Y – estados de particiones, tienen los siguientes valores: 0-desarmada 1-armada GETARMED:ERROR – comando rechazado por el sistema

Descripción de las particiones, líneas de entrada, salidas, usuarios y objetos	
Formato de comando	XXXX SETNAME=ELEMENT,[NR],VALUE_sin_espacios XXXX SETNAME=”ELEMENT,[NR],VALUE_con_espacios”
Descripción de comando	Configuración del nombre (posición VALUE) del elemento (valores posibles a continuación) n°. XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio Valores posibles de la posición **ELEMENT**: PARTITION – nombre de la partición; números 1 y 2 ZONE – nombre de la línea de entrada correspondiente al número determinado; números de 1 a 32 OUTPUT – nombre de la salida correspondiente al número determinado; números de 1 a 3 USER– nombre del usuario con el número determinado; números de 1 a 32 SYSTEM – nombre del edificio en el que funciona la centralita y el sistema de alarma. Nota: para este elemento no se especifica el campo n°. *Ejemplo 1:* *1234 SETNAME=PARTITION,1,Sótano* *Ejemplo 2:* *1234 SETNAME=”PARTITION,2,Cuarto de niños”*
Descripción del mensaje de retorno	SETNAME:OK – comando aceptado SETNAME:ERROR-PERMISSION – el usuario no tiene permiso para ejecutar este comando SETNAME:ERROR-FORMAT – formato de comando incorrecto SETNAME:ERROR-VALUE – valores erróneos SETNAME:ERROR-PERMISSION – comando rechazado; otros errores

Recuperación de la descripción de las particiones, líneas de entrada, salidas, usuarios y objetos	
Formato de comando	XXXX GETNAME=ELEMENT,[NR]
Descripción de comando	Recuperación de la descripción del elemento con el número indicado. Es un comando complementario a SETNAME, donde se describen los valores permitidos de los diferentes campos, véase la tabla «Nombres de particiones, líneas de entrada, salidas, usuarios y objetos». XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio Valores posibles de la posición ELEMENT: PARTITION – recupera la descripción de la partición; números 1 y 2 ZONE – recupera la descripción de la línea de entrada correspondiente al número determinado; números de 1 a 32 OUTPUT – recupera la descripción de la salida correspondiente al número determinado; números de 1 a 3 USER– recupera la descripción del usuario con el número determinado; números de 1 a 32 SYSTEM – recupera la descripción del edificio en el que funciona la centralita y el sistema de alarma. Nota: para este elemento no se especifica el campo n°. *Ejemplo 1:* *1234 GETNAME=PARTITION,1* – recupera la descripción de la partición 2
Descripción del mensaje de retorno	GETNAME=ELEMENT,[NR],VALUE – comando ejecutado con éxito, descripción recuperada (NOTA: Si el nombre no se ha cambiado (sigue siendo el predeterminado), no se dará en respuesta) GETNAME:ERROR-PERMISSION – el usuario no tiene permiso para ejecutar este comando GETNAME:ERROR-FORMAT: formato de comando incorrecto GETNAME:ERROR-VALUE: valores erróneos GETNAME:ERROR-PERMISSION: comando rechazado; otros errores

Listado de eventos soportados por los comandos SETUSERSMS y GETUSERSMS	
Nombre simbólico	Explicación
ARM1	Armado completo de la partición 1
ARMSTAY1	Armado de la partición 1 en modo perimetral
ARM2	Armado completo de la partición 2
ARMSTAY2	Armado de la partición 2 en modo perimetral
DISARM1	Desarme de la partición 1
DISARM2	Desarme de la partición 2
INPUT1 (a INPUT32)	Violación de la línea 1…32
INPUT1-OFF (a INPUT32-OFF)	Final de la violación de la línea 1…32
INPUT1-TAMPER (a INPUT32-TAMPER)	Sabotaje de la línea 1…32
INPUT1-TAMPEREND (a INPUT32-TAMPEREND)	Final del sabotaje de la línea 1…32
INPUT1-LOCK (a INPUT32-LOCK)	Bloqueo de la línea 1...32
INPUT1-UNLOCK (a INPUT32-UNLOCK)	Final del bloqueo de la línea 1…32
OUTPUT1-ON (a OUTPUT3-ON)	Las salidas activadas 1…3
OUTPUT1-OFF (a OUTPUT3-OFF)	Salidas desactivadas 1…3
OUTPUT1-TAMPER (a OUTPUT3-TAMPER)	Fallo de la salida 1…3
OUTPUT1-TAMPEREND (a OUTPUT3-TAMPEREND)	Final del fallo de la salida 1…3
POWER-FAIL	Fallo de alimentación
POWER-OK	Final del fallo de alimentación
BATTERY-FAIL	Fallo de batería
BATTERY-OK	Final del fallo de batería
AUX1-FAIL	Fallo de la salida de alimentación AUX1
AUX2-FAIL	Fallo de la salida de alimentación AUX2

AUX1-OK	Final del fallo de la salida de alimentación AUX1
AUX2-OK	Final del fallo de la salida de alimentación AUX2
KEYPAD1-LOST (a KEYPAD3-LOST)	Fallo del teclado 1…3
KEYPAD1-OK (a KEYPAD3-OK)	Final del fallo del teclado 1…3
KEYPAD1-TAMPER (a KEYPAD3-TAMPER)	Sabotaje de teclado 1…3
KEYPAD1-TAMPEREND (a KEYPAD3-TAMPEREND)	Final de sabotaje de teclado 1…3
KEYPAD-FIRE-BEGIN	Alarma «Incendio» activada desde el teclado
KEYPAD-HELP-BEGIN	Alarma «Ayuda» activada desde el teclado
KEYPAD-SILENTALARM-BEGIN	Alarma «Pánico» activada desde el teclado
KEYPAD-FIRE-END	Alarma «Incendio» finalizada
JAMMING-BEGIN	Interferencia GSM
JAMMING-END	Final de interferencia GSM
DETECTOR1-LOST (a DETECTOR32-LOST)	Desaparición de la comunicación al detector inalámbrico 1…32
DETECTOR1-OK (a DETECTOR32-OK)	Final de la desaparición de comunicación al detector inalámbrico 1…32
DETECTOR1-PWR (a DETECTOR32-PWR)	Bajo nivel de batería en el detector inalámbrico 1…32
DETECTOR1-PWROK (a DETECTOR32-PWROK)	Final del nivel bajo de batería en el detector inalámbrico 1…32

Listado de errores enviados en los mensajes de retorno	
Nombre simbólico	Explicación
ERROR-PERMISSION	Falta de permisos para realizar el comando
ERROR-FORMAT	Formato de comando incorrecto
ERROR-VALUE	Valor de parámetro incorrecto
ERROR-EMPTY	Falta del valor de parámetro
ERROR	Otro error

5. PROGRAMA DE CONFIGURACIÓN

5.1. NOTAS PRELIMINARES

El software **Configurador de los transmisores GPRS** se puede descargar desde la página www.ebs.pl (usuario: ebs, contraseña: ebs). Se debe activar la opción de instalador que pasa por el proceso de instalación de programa. Por defecto se instala en la carpeta C:\Program Files\EBS\. El instalador puede crear también los atajos al programa en el pupitre y en el menú del sistema Windows.

Cuando el dispositivo ha de ser usado por primera vez, primero se debe programar por medio del software arriba mencionado y, luego, se puede colocar la tarjeta SIM en el dispositivo. En caso contrario la tarjeta SIM puede estar bloqueada en caso de introducir el código PIN incorrecto. Una solución alternativa es usar la tarjeta SIM con el código PIN desactivado.

En caso de programar de forma remota existe la necesidad de situar la tarjeta SIM antes de empezar a enviar la configuración. En tal caso se debe o bien usar las tarjetas SIM con el código PIN desactivado o bien, antes de su introducción modificar el código PIN por medio del teléfono móvil.

5.2. ORDENADOR – REQUISITOS

Los requisitos mínimos para el ordenador PC en que instalar el software de configuración están presentados abajo:

Equipo:

- Procesador 1 GHz o más rápido, 32 bits (x86) o 64 bits (x64),
- 1 GB de RAM (versión de 32 bits) o 2 GB de RAM (versión de 64 bits)
- 4,5 GB de espacio en el disco duro,

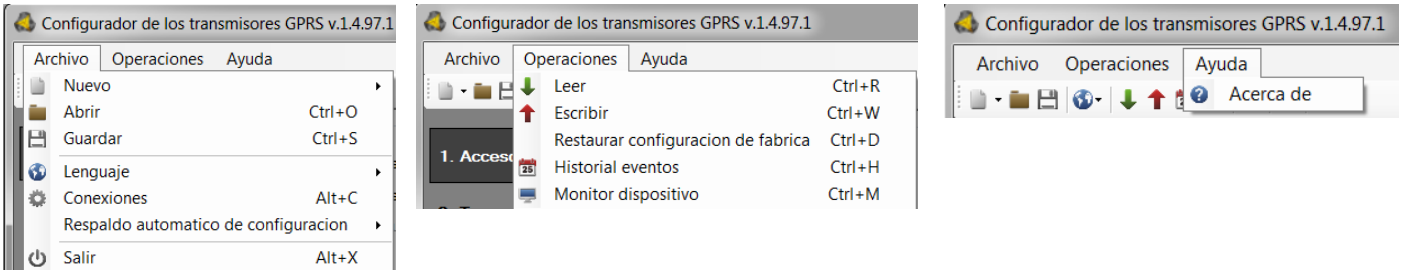
Software:

- Sistema Operativo: Windows 7 o posterior,
- Programa .NET Framework 4.5 o posterior.

5.3. FUNCIONES DE PROGRAMA

Después de instalar y ejecutar el programa en la pantalla aparecerá su ventana principal. Desde este nivel tenemos acceso tanto a las funciones de programa como a los parámetros programables del dispositivo (véase el capítulo 6.).
La ventana principal del programa está dividida entre unas zonas.
Menú principal: situado en la parte superior de la ventana, incluye la opción de control y configuración de programa.

El contenido del menú principal es el siguiente:

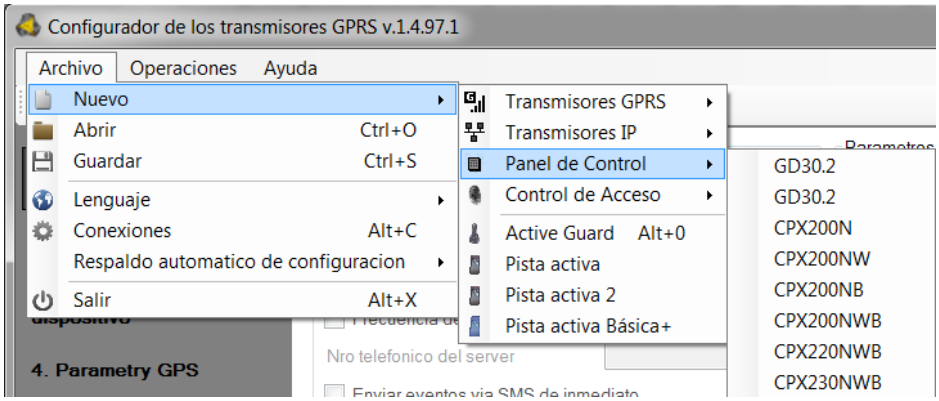


El menú principal es reflejado también en forma de iconos, en la barra de acceso rápido:

5.3.1. Menú -> Archivo

5.3.1.1. Archivo -> Nuevo

Abre un nuevo conjunto de parámetros. Basándose en esta opción se pueden editar los parámetros de configuración del dispositivo.



Se debe seleccionar el tipo del dispositivo: CPX230NWB

5.3.1.2. Archivo -> Abrir

Si tiene un archivo con la configuración guardada, estos datos se pueden utilizar para programar el siguiente dispositivo. Primero seleccione el directorio donde se guardó el archivo y luego especifique el nombre del archivo. La colección de datos conseguida puede ser modificada por el usuario. Para que los cambios sean efectivos, deben enviarse al dispositivo.

5.3.1.3. Archivo -> Guardar

Si programa varios dispositivos en configuraciones diferentes, no tiene que recordar cada una de ellas. Se pueden guardar en el disco duro todas las configuraciones del dispositivo con el nombre determinado y cargarse posteriormente. Esta función guarda en el disco toda la información desde las ventanas de configurador. Después de llamar la función aparecerá la ventana de diálogo con la petición de introducir el nombre de archivo. Por defecto, los datos se guardan con la extensión **.cmi**.

5.3.1.4. Archivo -> Idioma

Esta opción nos permitirá seleccionar uno de los idiomas disponibles (definidos en los archivos externos de idiomas).

5.3.1.5. Archivo -> Conexiones

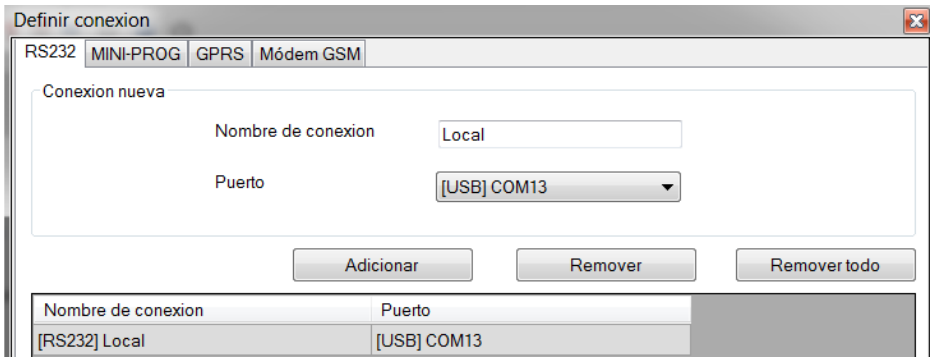
Antes de programar los dispositivos, es necesario definir el tipo de conexión que se desea utilizar.
Tendremos dos métodos de programación: local y remoto.

5.3.1.5.1. Conexión local

La conexión local significa que el software de configuración (en realidad, el ordenador en el que está instalado) está directamente conectado al conector de la central mediante un cable de programación especial utilizando el puerto serie RS-232 (GD-PROG) o el puerto USB o Bluetooth (MINI-PROG-BT, SP-PROG-BT). Cada canal de conexión (también USB y Bluetooth) "abre" los puertos COM serie virtuales utilizados en la comunicación entre la centralita de alarmas y el configurador.

Para poder programar el dispositivo o realizar otras actividades (por ejemplo, leer la configuración del dispositivo, cambiar de firmware, etc.) primero se deben definir los parámetros de la conexión.

Para ello, utilice la siguiente ventana disponible después de activar la opción Archivo en el Menú Principal y seleccionar la función Conexiones o después de hacer clic en el icono  en la barra de acceso rápido y abrir a la pestaña RS232.

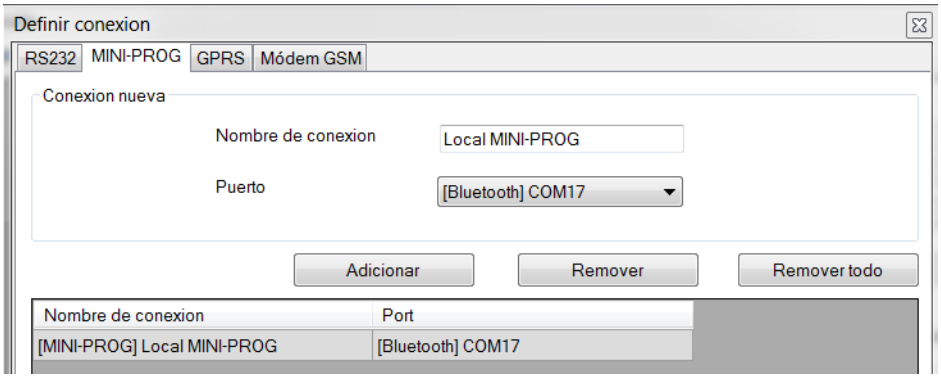


Determinamos:

- Nombre de la conexión, por ejemplo, Local
- Elegimos el puerto serie apropiado asignado al programador conectado, por ejemplo, COM13

Con el clic de botón [Añadir] confirmamos la configuración. La conexión se memoriza (y se sitúa en la tabla). A partir de este momento el programa nos permite una conexión por cable al dispositivo y permitirá leer y guardar los parámetros en la memoria del dispositivo.

En la siguiente pestaña "MINI-PROG" (el nombre que viene del programador) también se deben definir los parámetros de conexión.



Las actividades son análogas a las de la pestaña "RS232". Especifique el nombre, el puerto COM apropiado y agregue la conexión.

Los programadores MINI-PROG-BT y SP-PROG-BT tienen un conector microUSB, gracias al cual se pueden conectar a un PC/ portátil mediante el puerto USB, pero también tienen una interfaz Bluetooth incorporada que permite la comunicación.

Después de la conexión (ya sea a través de USB o Bluetooth), encuentre el puerto COM apropiado para el dispositivo y selecciónelo.

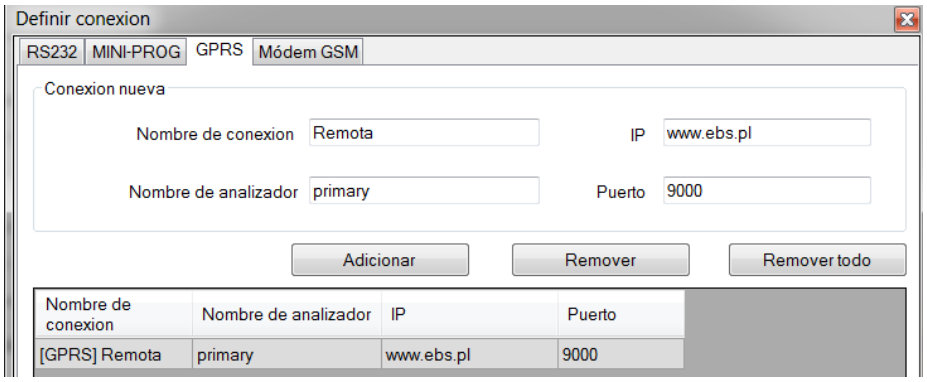
5.3.1.5.2. Conexión remota

Como se ha mencionado anteriormente, el dispositivo y el software permiten una configuración completa a través de la conexión GPRS o el canal CSD. Para tal modo de programación se deben definir adecuadamente los parámetros de las conexiones.

Conexión GPRS

Para configurar este modo, debe activar la opción Archivo del Menú Principal, seleccionar la función Conexiones (o hacer clic en el icono  de la barra de acceso rápido) y abrir la pestaña GPRS.

En la pantalla aparecerá la siguiente ventana.



Determinamos:

- Nombre de la conexión, por ejemplo, Remota
- Seleccionamos el nombre de analizador, por ejemplo, primary
- Introducimos la dirección del analizador, por ejemplo, www.ebs.pl
- Introducimos el puerto, en el que el analizador escucha los comandos, por ejemplo, 9000

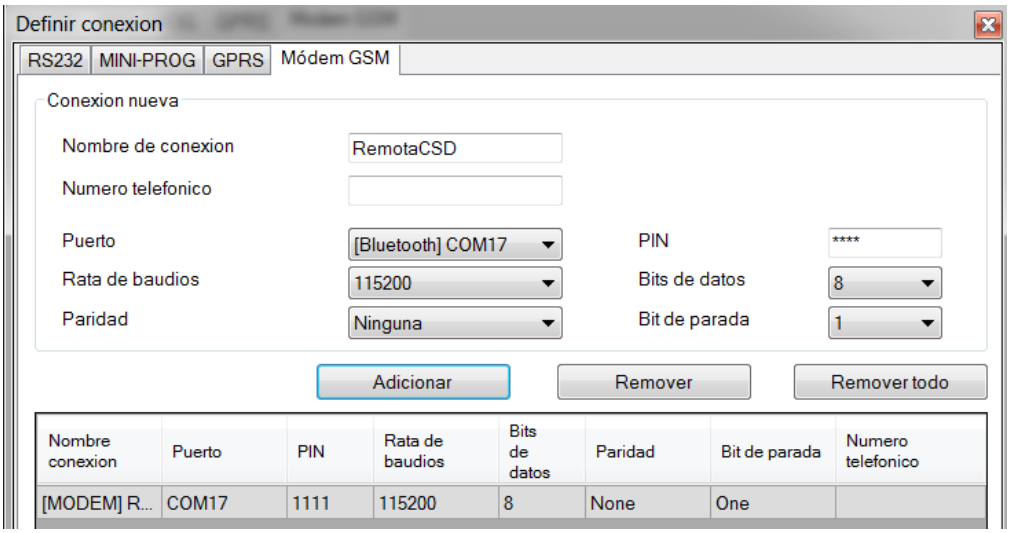
Con el clic de botón [Añadir] confirmamos la configuración. La conexión se memoriza (y se sitúa en la tabla). A partir de este momento el programa nos permite una conexión remota al dispositivo y permitirá leer y guardar los parámetros en la memoria del dispositivo.

ATENCIÓN: Los parámetros: nombre del analizador, dirección del analizador, puerto se refieren a los ajustes del receptor del sistema de monitoreo OSM.Server. La programación remota está disponible solamente en caso de usar el dispositivo arriba mencionado (software).

Conexión CSD

Para configurar este modo, debe activar la opción Archivo del Menú Principal, seleccionar la función Conexiones (o hacer clic en el icono de la barra de acceso rápido) y abrir la pestaña Módem GSM.

- En la pantalla aparecerá la ventana, donde determinaremos:
- Nombre de la conexión, por ejemplo RemotaCSD
- Puerto serie (por ejemplo COM17) al que está conectado un módem GSM como Wavecom Fastrack
- Código PIN de la tarjeta SIM instalada en el módem GSM, por ejemplo, 1111
- Parámetros del puerto en serie: Número de bits/seg. (por ejemplo, 115200), Bits de datos (8), Paridad (falta), Bits de stop (1).



Con el clic de botón [Añadir] confirmamos la configuración. La conexión se memoriza (y se sitúa en la tabla). A partir de este momento el programa nos permite una conexión remota al dispositivo y permitirá leer y guardar los parámetros en la memoria del dispositivo.

ATENCIÓN: La configuración remota con canal CSD sólo es posible cuando el servicio de datos CSD está activo tanto para la tarjeta SIM del dispositivo como para la tarjeta SIM instalada en el módem GSM. Además, la centralita debe tener activada la autorización para recibir las conexiones CSD – véase el punto 6.7.1.2. Números de los módems

GSM autorizados**.**

La programación a través de la conexión CSD también es posible cuando tenemos instalado el sistema OSM.Server, al que está conectado al menos un módem GSM. Si el dispositivo está registrado en la lista de servidores (número de serie y número de teléfono de la tarjeta SIM, ver el manual de OSM.Server), podemos usar la conexión vía OSM. La condición para esto es la falta de conexión GPRS con el dispositivo. La prueba de programación (a través de la conexión GPRS – véase arriba) terminará con la pregunta si queremos usar el módem conectado al servidor. Cuando contestemos de forma positiva el procedimiento seguirá como en caso de otros canales de programación.

5.3.1.6. Archivo -> Archivar

Todas las configuraciones del configurador tanto las leídas de los dispositivos como las guardadas en el dispositivo se guardan automáticamente en el disco duro. Si los directorios no se modificaron durante la instalación del configurador, los archivos se pueden encontrar, por ejemplo, en esta ubicación:

C:\Program Files\EBS\KonfiguratorLX\configs\CPX230NWB_20000\

La carpeta CPX230NWB_20000 contiene todos los archivos relacionados con la programación del dispositivo CPX230NWB con el número de fábrica 20000. El nombre de archivos incluye la fecha y la hora de la operación y su tipo (escritura / lectura). Los archivos tienen la extensión cmi.

5.3.1.7. Archivo -> Fin

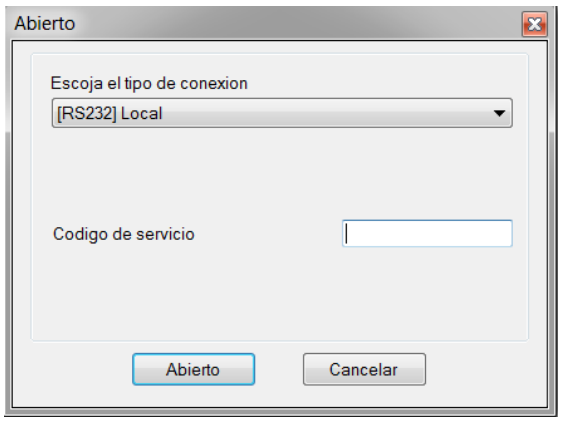
Termina la actividad del programa.

5.3.2. Menú -> Operaciones

5.3.2.1. Operaciones -> Lectura

Esta función lee los datos guardados en la memoria del módulo GPRS. El intercambio de los datos se realiza en el puerto seleccionado en la sección "Seleccionar el tipo de conexión" (véase la descripción de la opción "Configuración" abajo). La lectura correcta se confirmará con el respectivo mensaje. Los datos recuperados del dispositivo pueden guardarse en un archivo (véase el punto 5.3.1.3) y usarse para otros dispositivos.

El uso de esta función requiere volver a definir el tipo y los parámetros de la conexión. Por ejemplo, para la conexión local aparecerá la siguiente ventana:



donde:

Tipo de conexión: la forma de conectarse al dispositivo.

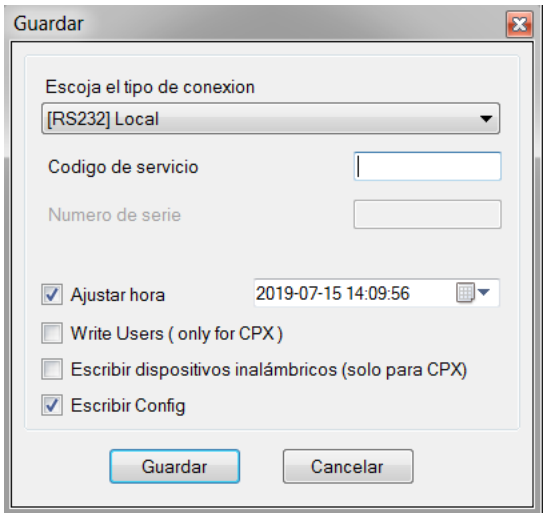
Código de servicio o de instalador: código de acceso al dispositivo.

Para una descripción detallada de cómo configurar las conexiones, consulte el punto 5.3.1.5.

5.3.2.2. Operaciones -> Enviar

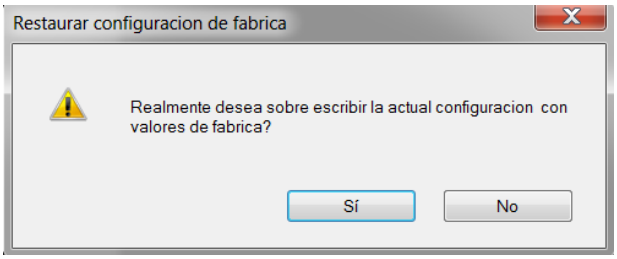
Esta función es análoga a la anterior, pero nos permite guardar los datos en la memoria del dispositivo. También es posible configurar el reloj interno del dispositivo. Para ello es necesario marcar el campo "Fijar el tiempo" e introducir la respectiva fecha junto con la hora. La escritura correcta se confirmará con el respectivo mensaje.

Para guardar todos los cambios de configuración, los usuarios añadidos y los dispositivos inalámbricos, deben enviarse utilizando esta función – campos: «Guardar usuarios (solo CPX)», «Guardar disp. inalámbricos (solo CPX)» y «Guardar configuración».



5.3.2.3. Operaciones -> Restablecer la configuración predeterminada

En caso cuando la operación "Lectura" termine con la indicación de error (por ejemplo, en caso de desconocer el código de acceso) se podrá realizar la operación de retorno a la configuración predeterminada. Para ello se debe seleccionar esta función. En la pantalla aparecerá el mensaje «¿Desea sobreescribir los parámetros del dispositivo con la configuración predeterminada?». Después de confirmarlo aparecerá la ventana de la definición de la conexión:



Esta operación es posible sólo en caso de la conexión local. Después de terminar, se restablecerán los parámetros de fábrica.

5.3.2.4. Operaciones -> Historial de eventos

Esta función permite visualizar los últimos eventos guardados en la memoria del dispositivo. Véase el capítulo 6.12.

5.3.2.5. Operaciones -> Monitor del dispositivo

Esta función permite controlar el estado del dispositivo en tiempo real. Véase el capítulo 6.11.

5.3.3. Menú -> Ayuda

Después de seleccionar esta función se visualizará la información adicional sobre el programa.

5.4. PROGRAMACIÓN DEL DISPOSITIVO

Para programar se debe abrir la conexión al dispositivo. En función del modo de conexión existen dos formas posibles de programar.

5.4.1. Programación local

Para realizar la programación local del dispositivo se debe:

- Conectar un cable de servicio, por ejemplo, GD-PROG, SP-PROG-BT o MINI-PROG-BT en el modo PROG entre el conector CONF (en la PCB del dispositivo) y el puerto COM del ordenador definido en la opción Conexiones -> RS-232 o MINI-PROG (para el programador del mismo nombre).
- Conectar la alimentación a la centralita. Después de conectar la alimentación y detectar el conducto de programación, el módulo avisará este hecho con los diodos LED: el verde iluminará y el rojo empezará a parpadear.
- Lanzar el Configurador y definir las opciones del dispositivo (véase el capítulo 6.).

ATENCIÓN: Introduzca el código PIN correcto para la tarjeta SIM.

- Seleccione la función Enviar. Aparecerá la ventana donde se debe seleccionar la conexión local previamente definida (capítulo 5.3.1.5.1). Copie la configuración en la memoria del dispositivo.
- Desactive la alimentación y desconecte el cable de programación o cambie el programador al modo DEBUG (MONITOR) para monitorear el funcionamiento del dispositivo.
- Introduzca la tarjeta SIM.
- Vuelve a conectar la alimentación.
- El dispositivo está listo para usar.

5.4.2. Programación remota

La programación remota del dispositivo es posible en dos casos:

- El usuario usará el Configurador de las emisoras GPRS y el módem GSM conectado al ordenador.

- El usuario trabaja con el receptor del sistema de monitoreo OSM.Server.

En el primer caso, la programación remota se realiza en el canal CSD y el procedimiento es análogo a la programación local, con la diferencia de que en las opciones de conexión debe seleccionare «Módem GSMM (véase el capítulo 5.3.1.5.2. – Conexión CSD).

ATENCIÓN: La configuración remota con canal CSD sólo es posible cuando el servicio de datos CSD está activo tanto para la tarjeta SIM del dispositivo como para la tarjeta SIM instalada en el módem GSM.

En el segundo caso, como se describe en el capítulo 5.3.1.5.2. – Conexión GPRS, debe definirse una conexión remota basada en los parámetros de OSM Server. Como OSM.Server recibe (y envía) la información exclusivamente de los dispositivos que tiene guardados en su base de datos, la primera actividad en la programación remota será el registro adecuado del dispositivo. El procedimiento está descrito en el manual de OSM.Server.

5.4.2.1. Primera programación del dispositivo

Dado que el dispositivo no tiene parámetros de acceso definidos tanto para GPRS como para OSM.Server, la programación debe iniciarse introduciéndolos. Independientemente de la forma de realizar tal introducción, primero se debe realizar el registro del dispositivo en la base de datos OSM.Server.

Antes de proceder a la programación remota, asegúrese de que el dispositivo esté equipado con una tarjeta SIM (con reservas indicadas en el capítulo 6.1.5.3.) y conectado a la fuente de alimentación. El usuario deberá conocer el número de fábrica del dispositivo y el número de teléfono de la tarjeta SIM.

El procedimiento de programación es el siguiente:

- En caso de usar la consola OSM.Server, indique con el cursor el dispositivo adecuado en la pestaña Dispositivos.
- Haga clic en la opción «Config» e indique la función «Set configuration». Aparecerá el listado de parámetros.
- Introduzca la dirección de servidor, el puerto de servidor y el APN. Después de hacer clic en OK, el sistema enviará los parámetros introducidos al dispositivo (SMS).
- Espere hasta que el dispositivo conteste al servidor (en la pestaña Dispositivos estará marcado en verde).
- Active el software y defina las opciones del dispositivo (la descripción se encuentra en el capítulo 6.).
- Seleccione la función Enviar. Aparecerá la ventana en la que habrá que seleccionar la conexión remota previamente definida (capítulo 5.3.1.5.2.). Copie la configuración en la memoria del dispositivo.
- Después de guardar cierre el programa de configurador.
- El dispositivo está preparado para la transmisión de datos.

5.4.2.2. Reprogramación del dispositivo

Dado que el dispositivo tiene parámetros de acceso definidos tanto para GPRS como para OSM.Server, la programación se puede realizar en cualquier momento.

Cuando el dispositivo está instalado en el edificio protegido, es decir, está dotado de la tarjeta SIM y conectado a la alimentación, el procedimiento de programación será el siguiente:

- Inicie el software de configuración y defina las opciones del dispositivo (véase la descripción en el capítulo 6.).
- Seleccione la función Enviar. Aparecerá la ventana en la que habrá que seleccionar la conexión remota previamente definida (capítulo 5.3.1.5.2.). Copie la configuración en la memoria del dispositivo.
- Después de guardar cierre el programa de configurador.
- El dispositivo está preparado para la transmisión de datos conforme con la nueva configuración.

6. PARÁMETROS PROGRAMABLES

Los parámetros disponibles en el programa de configuración están divididos entre grupos: Acceso, Transmisión, Entradas/Salidas, Opciones del sistema, Usuarios, Monitoreo, Restricciones, Notificaciones SMS, Control de conexión, Firmware. Cada uno de los grupos se describirá detalladamente en la siguiente parte del manual.

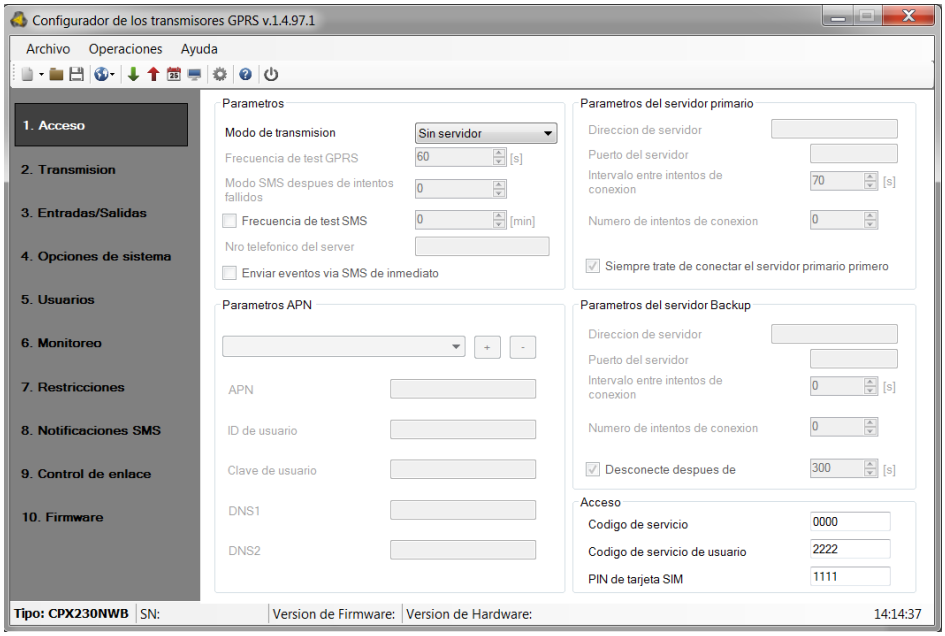
6.1. ACCESO

6.1.1. Parámetros

6.1.1.1. Modo de trabajo del dispositivo

En función de las preferencias del usuario, el dispositivo puede funcionar en uno de los 4 modos (selección del listado despegable):

- GPRS & SMS: por regla general, transmisión GPRS (protocolo TCP/IP) y en caso de problemas con esta conexión pasará automáticamente al modo SMS
- SMS: Transmisión únicamente en el modo SMS, sin intentar establecer una conexión GPRS.
- GPRS: por regla general, transmisión GPRS (protocolo TCP/IP). En caso de problemas con esta conexión se perderá la comunicación remota.
- Sin servidor: sin transmisión al servidor, la comunicación remota al usuario es posible solamente a través de las notificaciones SMS.



6.1.1.2. Periodo de la prueba GPRS

El dispositivo envía, con el intervalo determinado, la señal «Prueba» que informa a la estación de monitoreo que el dispositivo está funcionando. En este campo se determina cada cuántos segundos se enviará tal mensaje.

6.1.1.3. Modo SMS después de la cantidad de pruebas fallidas

Definimos la cantidad de pruebas de conectarse al servidor. Si no se puede establecer la conexión, el dispositivo pasará al modo SMS después del número de intentos configurado. En este modo el dispositivo seguirá tratando de conectarse al servidor, según el intervalo definido en el punto 6.1.3.3.

6.1.1.4. Periodo de prueba SMS

Esta función es análoga a la de GPRS. Se refiere a los problemas con la transmisión GPRS. Cuando el dispositivo pase automáticamente al modo SMS (se refiere también al modo de trabajo únicamente en forma de SMS). Normalmente, no se recomienda enviar el texto en forma de SMS con tanta frecuencia como en caso de la transmisión GPRS. Este parámetro permite prolongar bastante la distancia entre las pruebas (tiempo en minutos) o desactivar por completo esta opción.

6.1.1.5. Número de teléfono del servidor

Si un módem GSM está conectado a la aplicación del servidor (por ejemplo, OSM.Server), introduzca su número aquí. A este número se enviarán los mensajes SMS en caso de problemas con la transmisión GPRS.

Si este campo se deja vacío o sólo se introduce un dígito (incluyendo 0), el dispositivo no pasará al modo SMS y solo funcionará en modo GPRS.

ATENCIÓN: El campo estará inactivo cuando el modo de trabajo del dispositivo está definido como GPRS.

6.1.1.6. Envíe inmediatamente los eventos SMS

En caso de perder la conexión GPRS, la información sobre los eventos entrantes se enviará por mensaje SMS inmediatamente, incluso cuando el dispositivo no ha pasado aún al modo SMS.

6.1.2. Parámetros del punto de acceso

6.1.2.1. APN

El parámetro depende del operador de la red GSM, cuyos servicios GPRS usaremos. Determina el nombre del punto de acceso a la red GPRS. Existe la posibilidad de conseguir el punto de acceso privado. En tal caso su nombre se da por el operador concreto de la red GSM.

6.1.2.2. ID Usuario

En caso de usar el APN público no es requerido. Para el APN privado este parámetro debe ser conseguido del operador (sin él no se conseguirá acceso a la red GPRS).

6.1.2.3. Contraseña de usuario

En caso de usar el APN público no es requerido. Para el APN privado este parámetro debe ser conseguido del operador (sin él no se conseguirá acceso a la red GPRS).

ATENCIÓN: El uso del privado APN aumenta la seguridad del sistema.

6.1.2.4. DNS1 y DNS2

Determina la dirección del DNS primario y secundario (sistema del nombre de dominios). Cuando la dirección del servidor se introduzca en forma de dominio debemos introducir al menos una dirección DNS.

6.1.3. Parámetros del servidor primario

6.1.3.1. Dirección IP del servidor

Es la dirección IP del receptor del sistema de monitoreo (OSM.Server) o del ordenador en el que está instalado el programa «Servidor de Comunicación», por ejemplo, 89.123.115.8. Se puede introducir esta dirección también en forma del nombre de dominio del servidor, por ejemplo, modul.gprs.com. En tal caso, se requiere introducir al menos una dirección del servidor DNS.

6.1.3.2. Puerto de servidor

Determina el puerto del servidor destinado para recibir los datos del dispositivo.

6.1.3.3. Distancia entre las siguientes pruebas de conectarse al servidor

El dispositivo programado y dotado de la tarjeta SIM tratará automáticamente de conectarse al servidor. En este lugar vamos a definir las distancias de tiempo (en segundos), después del que la prueba de conectarse se renovará con tal de que no haya terminado con éxito.

6.1.3.4. Número de pruebas de conectarse al servidor

Determinamos cuántas veces el dispositivo tratará de conectarse al servidor. En caso de las siguientes faltas de éxito. Después de realizar el determinado número de intentos, el dispositivo empezará el procedimiento de conectarse al servidor secundario. Esta opción será activa solamente cuando definamos los parámetros del servidor secundario.

6.1.3.5. Orden de conectarse a los servidores

Si selecciona esta casilla, el dispositivo intentará conectarse primero al servidor primario, independientemente de los parámetros del servidor secundario (en especial, del número de intentos de conexión).

6.1.4. Parámetros del servidor secundario

6.1.4.1. Dirección IP del servidor

Es la dirección IP del segundo receptor (secundario) del sistema de monitoreo (OSM.Server) o del ordenador en el que está instalado el programa «Servidor de Comunicación», por ejemplo, 89.130.125.82. Se puede introducir esta dirección también en forma del nombre de dominio del servidor, por ejemplo, monitor.gprs.com. En tal caso, se requiere introducir al menos una dirección del servidor DNS.

6.1.4.2. Puerto de servidor

Determina el puerto del servidor destinado para recibir los datos del dispositivo.

6.1.4.3. Distancia entre las siguientes pruebas de conectarse al servidor

Si el dispositivo no puede conectarse al servidor principal, después del número de intentos definido, iniciará el procedimiento de conexión al servidor secundario. En este lugar vamos a definir las distancias de tiempo (en segundos), después del que la prueba de conectarse se renovará con tal de que no haya terminado con éxito.

6.1.4.4. Número de pruebas de conectarse al servidor

Determinamos cuántas veces el dispositivo tratará de conectarse al servidor secundario. En caso de los siguientes fallos, después de realizar el número determinado de pruebas, volverá al procedimiento de conectarse al servidor primario.

6.1.4.5. Desconexión después del tiempo

Si selecciona esta casilla, el dispositivo se desconectará del servidor secundario después de un período de tiempo definido. El siguiente paso depende de la definición del parámetro Secuencia de conexión (véase el punto 6.1.3.5). Cuando la opción está activa, el dispositivo tratará de conectarse al servidor primario. Cuando la opción no está activa, el dispositivo primero terminará el procedimiento de conectarse al servidor secundario y cuando termine con fracaso, pasará a la prueba de conectarse al servidor primario.

6.1.5. Acceso

6.1.5.1. Código de servicio

Su papel es proteger el dispositivo contra el acceso no autorizado. Es usado tanto en el proceso de programar el dispositivo como en su control remoto (en el modo TCP/IP ó SMS). Por defecto, está fijado el código 0000. Debe cambiarse durante la primera activación (programación) del dispositivo. Puede contener de cuatro a siete dígitos.

6.1.5.2. Código de instalador

El código de instalador se utiliza en el proceso de programación del dispositivo con el teclado KP32. Por defecto, el código está fijado en el valor 2222. Debe cambiarse

durante la primera activación (programación) del dispositivo. El código puede contener de cuatro a siete caracteres.

El código de servicio de instalador podrá ser leído y modificado de forma remota desde la consola de OSM.Server o bien por medio de un comando SMS. En caso de leer el código de servicio del instalador desde la consola de OSM.Server se debe enviar cualquier comando con el contenido:

GETPARAM=3,1

la respuesta con el código aparecerá en la parte inferior de la ventana de consola.

La modificación del código de servicio de instalador podrá realizarse desde la consola de OSM.Server enviando cualquier comando con el contenido:

SETPARAM=3,1,nuevo_código

donde *nuevo_código* será una secuencia de 4 a 7 dígitos.

6.1.5.3. PIN de la tarjeta SIM

Dado que el dispositivo utiliza una red GSM para su funcionamiento, necesitará una tarjeta SIM de su operador de red móvil. El PIN de la tarjeta SIM, destinado para el trabajo en un dispositivo concreto, deberá ser programado antes de su primer uso. Es necesario para activar el sistema automáticamente. En caso de tener una tarjeta sin el código PIN, en el campo podrá introducirse cualquier valor, por ejemplo, 0000.

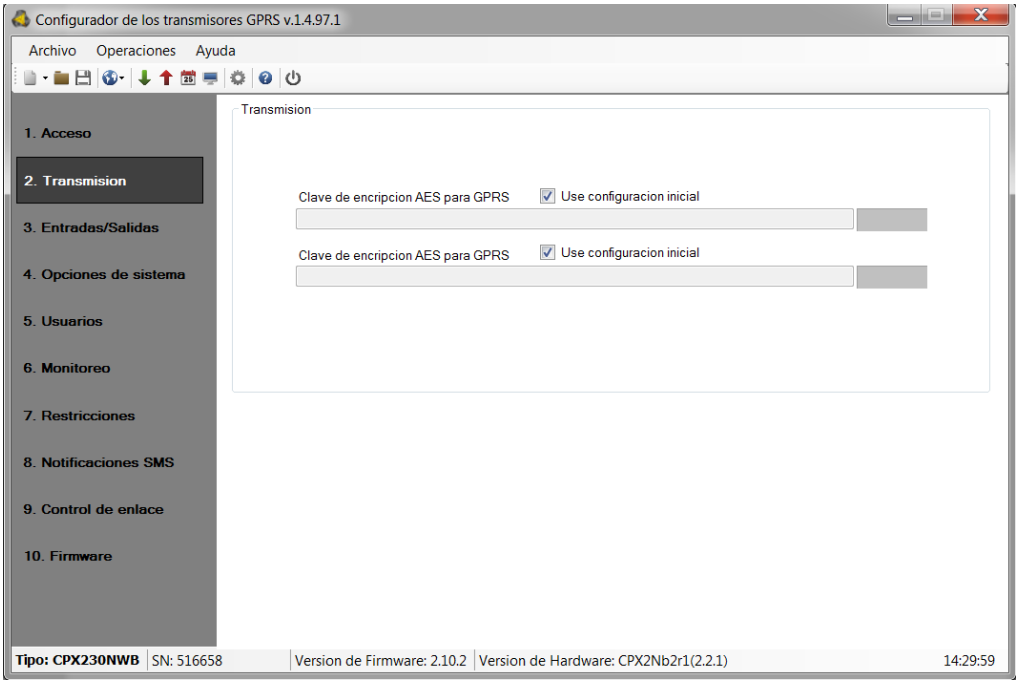
Cuando el número PIN se introduzca incorrectamente, después de introducir la tarjeta y activar la alimentación, el sistema no se activará y el uso de la tarjeta será posible después de introducir el número PUK (con el uso de cualquier teléfono GSM).

Por defecto, en el dispositivo se guardó el número PIN en la siguiente forma: 1111.

6.2. TRANSMISIÓN

Para garantizar la máxima seguridad de los datos transmitidos, se ha introducido el cifrado de datos con la clave AES. Esta opción puede ser empleada tanto para la transmisión GPRS como para SMS.

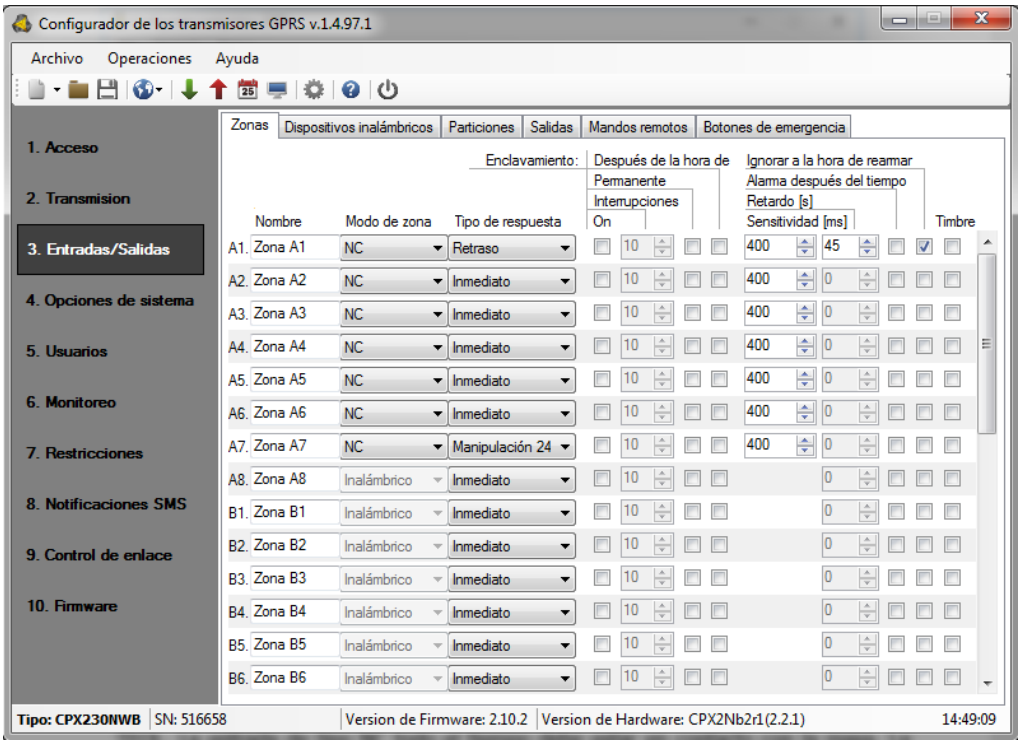
Después de seleccionar la transmisión codificada se puede introducir su propia clave de codificación (256 bits – caracteres 0-9 y A-F) o bien usar la configuración predeterminada.



6.3. ENTRADAS /SALIDAS

La centralita cuenta con 32 líneas de detección (entradas) totalmente configurables y 3 salidas controladas por software. Estas líneas se pueden asignar libremente entre dos particiones. Cada línea y cada salida tiene una serie de parámetros programables que se describen a continuación.

6.3.1. Líneas (entradas)



6.3.1.1. Modo de entrada

Este parámetro nos permite determinar el estado estable de entrada. La modificación de este estado ocasionará el envío de la información sobre la alarma. La entrada alámbrica puede ser de tipo NO o NC. Para seleccionar tenemos los siguientes tipos de configuración: NO / NC / EOL-NO / EOL-NC / DEOL-NO / DEOL-NC / Inalámbrico / TEOL. La entrada de tipo NC todo el tiempo debe estar en contacto con la masa. La excitación ocurre después de su desaparición (apertura). La entrada de tipo NO se queda en el estado abierto. Se activa después de conectar a masa. Las versiones EOL y DEOL (parametrizadas y doblemente parametrizadas) difieren en el número de resistencias y tienen la ventaja de poder distinguir entre alarma y sabotaje. La configuración TEOL permite duplicar la línea de alarma, es decir conectar dos detectores alámbricos a un borne de la centralita, siendo posible detectar alarmas del detector 1 y del detector 2, la señalización de apertura del interruptor de manipulación será común para ambos detectores. Los esquemas eléctricos para todos los tipos de configuración se presentan en el capítulo 3.4 CONFIGURACIÓN DE LAS LÍNEAS DE ENTRADA ALÁMBRICAS

6.3.1.2. Tipo de reacción

- **Inmediata** – La violación de la línea causa una alarma inmediata, cuando el sistema está armado.
- **Temporizada** – Este tipo de línea suele usarse para los detectores en las entradas al edificio. La línea pasa al estado de alarma después de pasar el tiempo programado para entrar. Cuando el sistema está armado, la activación de esta línea ocasiona la activación del retardo de entrada para la partición seleccionada. Para evitar que el sistema dispare una alarma, debe desarmarse antes de que haya transcurrido el tiempo programado.
- **Pánico 24h** – Esta línea dispara una alarma inmediata, independientemente de si el sistema está armado o no.
- **De rearme/desarme por violación** – La línea puede ser usada para rearmar o desarmar el sistema. En caso de inducir la línea con el sistema desarmado, se armará la partición que corresponda a esta línea. La inducción de esta línea con el sistema rearmado desarmará la partición que corresponda a esta línea.
  Nota: Para las líneas con cable es recomendable configurar la salida como NC o NO para este tipo de respuesta.
- **Sabotaje 24h** – Esta línea se puede utilizar para conectar los circuitos de sabotaje de los detectores. Cuando el sistema no está armado, la violación de la línea de sabotaje 24h generará un evento de violación de la entrada sin generar una alarma. Cuando el sistema está armado, la violación de la línea de sabotaje 24h generará un evento de violación de la y disparará una alarma.
- **Temporizada condicionalmente** – Esta línea se puede utilizar si el teclado del sistema no se encuentra en la primera zona violada al acceder al teclado. Cuando la línea atrasada condicionalmente se viole, el sistema comprueba que la partición a la cual pertenece la línea, cuenta atrás el retardo de entrada. Cuando se cuenta el retardo de entrada, la línea se comportará como temporizada, en caso contrario se comportará como inmediata.
- **Pánico 24h con alarma silenciosa** – La violación de la línea causa el envío de la información sobre el evento, independientemente de si el sistema está armado o no. La violación de la línea no ocasiona la activación de la salida y aviso de teclado.
- **Incendio 24h** – Funciona de forma similar a la línea de pánico 24h.
- **Perimetral** – Línea armada en el modo perimetral. De este modo se definen los detectores que protegen la entrada al edificio (puertas y ventanas). Toda violación de esta línea durante la cuenta del retardo de salida generará inmediatamente una alarma.
- **Perimetral de salida** – Si el sistema se arma usando un código sin seleccionar el modo de armado, toda violación de esta línea durante la cuenta del retardo de salida causará el armado del sistema en modo completo. En el caso de que no se viole la línea durante la cuenta del retardo de salida, la centralita se armará en modo perimetral. Si el sistema se arma seleccionando un modo, se ignorará la violación de la línea durante la cuenta del retardo de salida y el sistema se armará en el modo seleccionado por el usuario. Está línea tiene asignado un

retraso y se comporta como una línea temporizada normal cuando el sistema está armado.

- **Gas 24h** – Funciona de forma similar a la línea de pánico 24h.
- **Inundación 24h** – Funciona de forma similar a la línea de pánico 24h.
- **Nocturna (desactivada de noche)** – Esta línea se utiliza para los detectores instalados en aquellas zonas donde las personas circulan de noche. La violación de una línea nocturna no generará una alarma cuando el sistema está armado en modo nocturno. Cuando el sistema está armado en modo completo, esta línea se comporta como una línea inmediata.
- **Nocturna temporizada** – Cuando el sistema está armado en modo nocturno, la violación de esta línea iniciará la cuenta del retardo de entrada. Para evitar que se genere una alarma, es necesario desarmar el sistema (o armarlo en modo diurno, si hay personas dentro del edificio). Cuando el sistema está armado en modo completo, esta línea se comporta como una línea inmediata. Cuando el sistema está armado en modo perimetral, se ignorará la violación.
- **Rearme/desarme por cambio de estado** – La violación de la línea provoca el armado de la partición a la que está asignada. Una vez que la violación ha terminado, se desarma. Si el sistema está armado y se viola la línea, la partición a la que está asignada se volverá a armar (señalando la cuenta atrás del retardo de salida configurado). Una vez que la violación ha terminado, se desarma la partición.
  Nota: Para las líneas alámbricas es recomendable configurar la salida como NC o No para este tipo de respuesta.

  La línea de rearme/desarme por cambio de estado está disponible a partir de la versión de firmware 2.10.0.

6.3.1.3. Bloqueo

Esta opción permite bloquear cualquier línea, lo cual hace que los cambios de estado se ignoren y no se avisen a la estación de monitoreo.

Se puede bloquear la entrada de modo permanente o activar el bloqueo después de un número determinado de violaciones.

Seleccionando la opción «Después del retardo de salida» se bloqueará la línea de entrada si fue violada en el momento del armado. También se generará un evento de bloqueo, lo que permite informar la estación de monitoreo sobre el fallo. Este bloqueo permanece activo hasta que se desarme la partición. Si también se marca la opción «alarma después del retardo de salida», la opción «bloqueo después del retardo de salida» tiene prioridad, es decir que la línea se bloqueará sin generar una alarma.

Si está activa la opción «Después del retardo de salida» y sucede una violación o un sabotaje después del retardo, se bloqueará automáticamente (se activará la función bypass). Las líneas con bloqueo automático (opción «bloqueo después del retardo de salida» o después de «n» violaciones) se desbloquean automáticamente una vez desarmada la partición a la que están asignadas.

6.3.1.4. Sensibilidad

Este parámetro indica el tiempo mínimo que debe durar un cambio en una entrada de línea para que el transmisor lo detecte. El valor por defecto del parámetro son 400ms.

6.3.1.5. Retraso

El parámetro está activo solamente para las líneas temporizadas. Especifica el tiempo de retardo –a partir del momento en que se detecte una violación de la línea– tras el cual se generará una alarma.

6.3.1.6. Alarma después del retardo de salida

Si está activa la opción «Alarma después del retardo de salida», se generará una alarma en el caso de violación una vez trascurrido el tiempo de retardo para la partición a la que está asignada la línea (es decir, la línea se vuelve supervisada).

Si la opción no está activa, no se generará una alarma en el caso de violación una vez trascurrido el tiempo de retardo.

La primera alarma de la línea puede generarse cuando la línea se cierra y se viola de nuevo.

6.3.1.7. Ignorar a la hora de rearmar

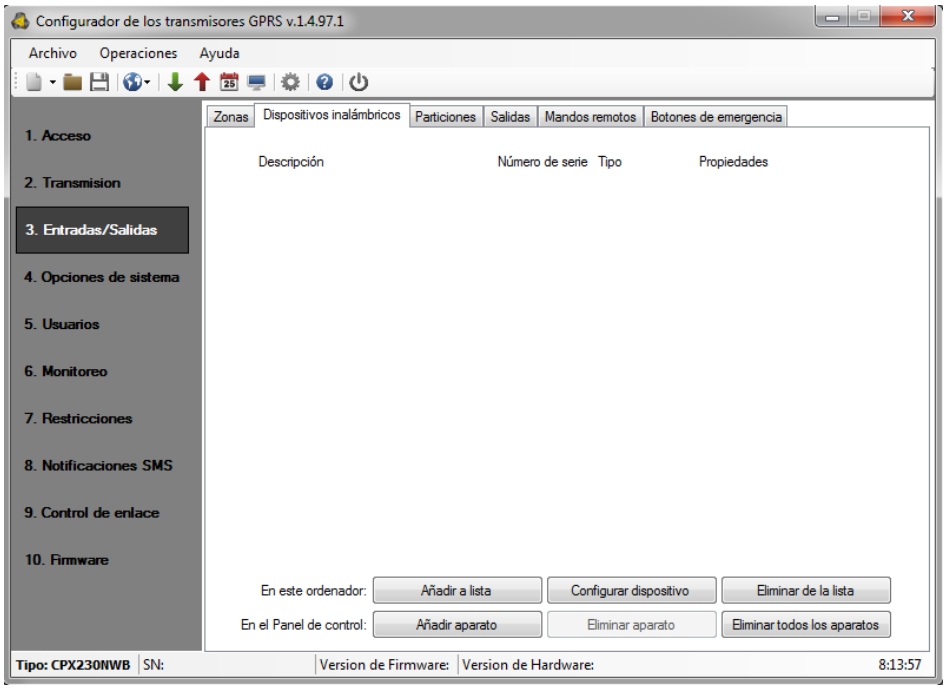
La línea de entrada puede ser violada durante el rearme de la partición (por ejemplo, las líneas de tipo atrasado deberán tener esta opción fijada).

6.3.1.8. Timbre

La función Timbre se utiliza para informar a las personas en el edificio sobre la violación de las líneas de entrada (por ejemplo, al abrir una puerta de entrada). Durante una violación, el teclado emite una señal sonora (cuando el sistema está desarmado) sin enviar el informe de alarma a la estación de monitoreo.

Si el sistema cuenta con más de un teclado, todos ellos sonarán cuando la línea esté violada (se aplica sólo a los teclados con cable).

6.3.2. Dispositivos inalámbricos

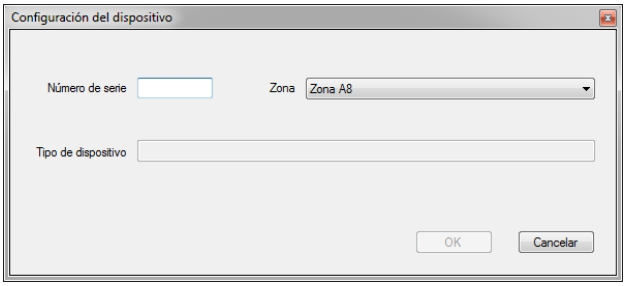


El dispositivo permite añadir hasta 32 detectores inalámbricos de A1 a A8, de B1 a B8, de C1 a C8 y de D1 a D8.

Hay dos maneras de añadir detectores (descritas a continuación).

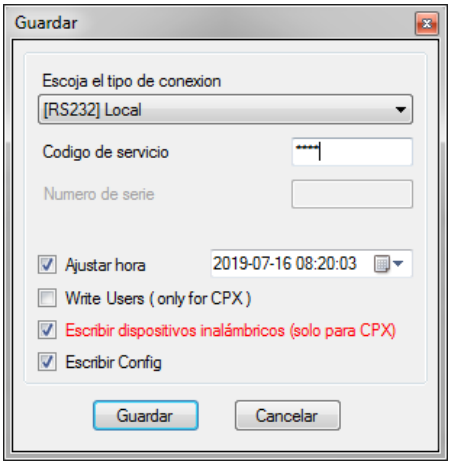
La primera es añadir a la lista en el ordenador (introduciendo el número de serie) en el que está instalado el Configurador y, a continuación, enviar todos los dispositivos añadidos a la centralita.

Después de hacer clic en «Añadir a la lista» aparecerá la ventana:



Introduzca el número de serie S/N que figura en la etiqueta del detector. El campo al lado corresponde al número de entrada que se puede asignar. El tipo de dispositivo aparecerá automáticamente después ingresar los dos primeros dígitos. Después de ingresar los datos, presione el botón *OK*.

En este caso, para que el detector pueda comunicarse con la centralita, es necesario enviar esta información, por ejemplo, pulsando *Enviar* en la barra de acceso rápido (u *Operaciones -> Enviar*). Aparecerá la ventana:

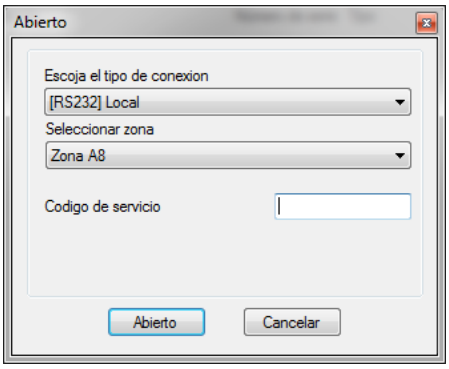


donde debe marcar la tercera casilla «Guardar disp. inalámbricos (solo CPX)» y «Guardar». Esto permite establecer la comunicación correcta entre el detector y la centralita.

ATENCIÓN: Para que la centralita reciba señales del detector, es necesario introducir un número de serie válido.

La segunda manera es registrar el detector directamente en la centralita.

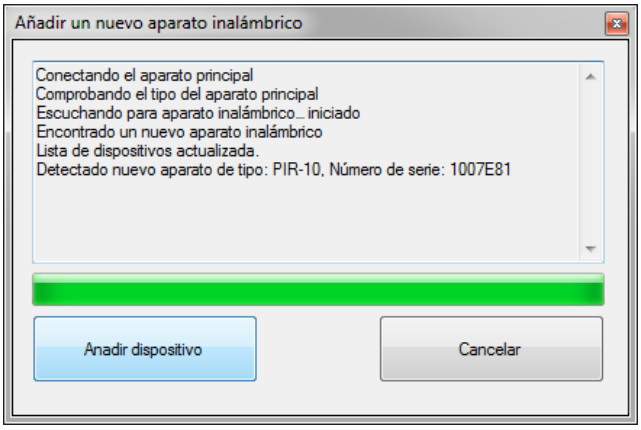
Para añadir un detector inalámbrico, pulse el botón «Registrar dispositivo».



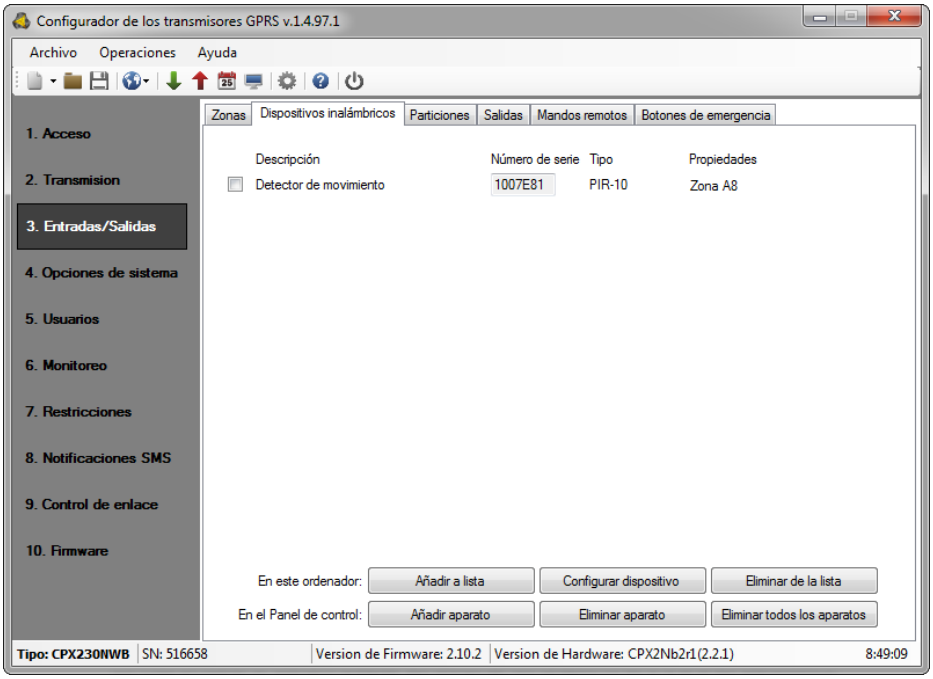
En esta ventana se debe seleccionar el tipo de conexión, es decir, el puerto serie, al que está conectado el dispositivo CPX230NWB. Seleccione el número de línea para el nuevo detector inalámbrico, introduzca el código de servicio y pulse «Leer».

Aparecerá otra ventana informando de que se ha comenzado a buscar los dispositivos inalámbricos.

El programa esperará la llegada de la señal del detector inalámbrico. En este momento, se debe apretar durante un instante el botón de sabotaje del detector. Es recomendable añadir detectores inalámbricos individualmente. Durante este procedimiento sólo se debe quitar la carcasa de un detector para eliminar las transmisiones accidentales de otros detectores. La centralita detectará la comunicación e informará al usuario sobre este hecho, visualizando información sobre el tipo de dispositivo y su número de serie.

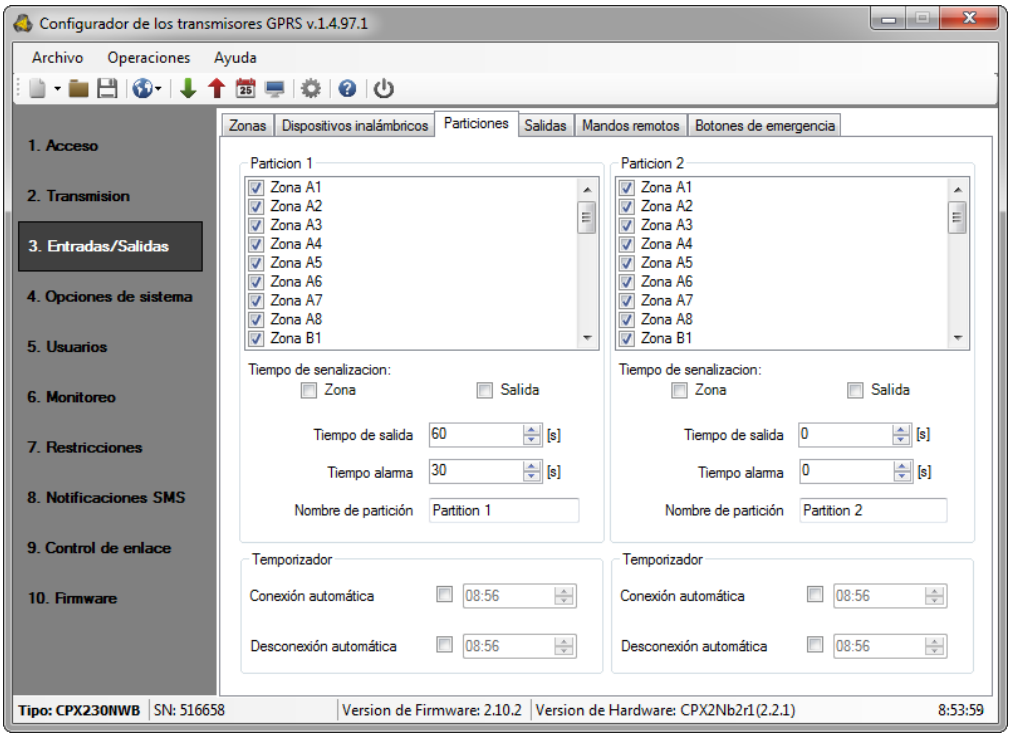


Ahora se puede conectar el dispositivo detectado a la centralita pulsando el botón «Añadir dispositivo». El nuevo sensor aparecerá en el listado de entradas inalámbricas:



A cada detector se le puede asignar un tipo de respuesta y se pueden seleccionar otros parámetros (en la pestaña «Entradas»), excepto la sensibilidad.

6.3.3. Particiones



6.3.3.1. P1 – Partición 1, P2 – Partición 2

En esta pestaña se pueden asignar las líneas de los grupos A, B, C y D a las particiones. Cuando la línea no está asignada a ninguna partición (y no es de tipo 24H), se ignorarán los eventos (violación/retorno) generados por la misma.

6.3.3.2. Entrada / Salida

Este parámetro permite desactivar la señalización del retardo de entrada/salida que muestra el teclado KP32.

6.3.3.3. Retardo de salida

Retardo de salida de la partición. Las líneas pertenecientes a la partición estarán activas (monitoreadas) cuando transcurra el tiempo especificado, contando desde el momento de la violación de la línea de armado.

6.3.3.4. Tiempo de alarma

Este parámetro determina la duración de la alarma en el teclado KP32.

6.3.3.5. Nombre de la partición

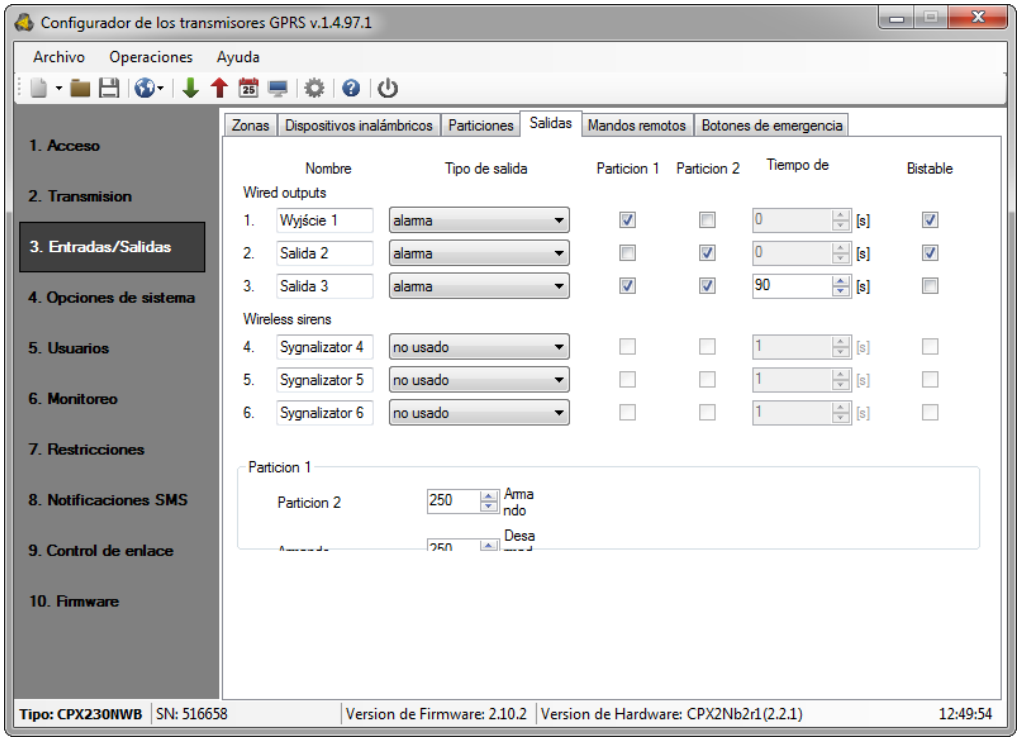
Este parámetro permite dar el nombre a la partición.

6.3.3.6. Temporizador

En esta sección se pueden configurar los parámetros de armado y desarmado automático de la partición.

Además de configurar la hora de armado/desarmado, se puede activar y desactivar cada hora por separado. Para activar o desactivar el armado/desarmado automático, haga clic en la casilla. Si la hora de armado/desarmado no está activa, el campo se vuelve inactivo y se vuelve gris.
Cuando la partición se arma/desarma automáticamente, a la estación de monitoreo se enviará el número de usuario 253.
A la hora de armado establecida, comienza la cuenta atrás del retardo de salida –el usuario puede anual el armado en cualquier momento ingresando el código– en tal caso el sistema no se armará y no se enviará ningún mensaje a la estación de monitoreo.
Los posibles fallos del sistema no impiden el armado (al igual que un comando remoto o el mando a distancia).
Para cada entrada está disponible la opción «bloqueo de línea después del retardo de salida»: en el caso de armado con una línea violada, una vez trascurrido este tiempo, se generará un evento de bloqueo. La entrada permanecerá bloqueada hasta que se desarme la partición (véase el punto 6.3.1.3. Bloqueo).
Cuando se establece el mismo tiempo de armado y desarmado, el sistema se desarma primero y luego se arma inmediatamente.
Si la hora del sistema se adelanta (por ejemplo, al cambiar la hora de invierno a verano), se omitirán los eventos de armado/desarmado programados durante este tiempo. Por ejemplo: si el armado automático está programado para las 02:30, al cambiar la hora de invierno a verano (de 2:00 a 3:00), no se armará la centralita.

6.3.4. Salidas



6.3.4.1. Salidas 1 / 2 / 3

Tipos de salidas:

- **No usadas** – La salida es inactiva.

- **Alarma** – La salida se activa en el momento de detectar una alarma.
- **Estado de armado**: La salida se activa después del armado en cada modo (completo, nocturno y perimetral) de cualquier partición a la que esté asignada.
- **Fallo de alimentación** – La salida se activa cuando se detecte un fallo de alimentación.
- **Fallo de comunicación** – La salida se activa cuando no es posible enviar información al servidor.
- **Interferencia de la señal GSM** – La salida se activa durante la interferencia de GSM.
- **Chirp** – La salida se activa durante el rearme (1 chirp) o desarme (2 chirps). El tiempo mínimo de duración de la señal chirp que se puede ajustar mediante el configurador es de 40 ms. En el caso de particiones con el retardo de salida configurado, el chirp sólo se generará después de armar. Del mismo modo, si se ajusta el retardo de entrada, se generarán chirps después del desarmado.
- **Alarma y Chirp** – La salida se activa después de detectar una alarma y durante el rearme o desarme.

6.3.4.2. Partición 1 (P1) y 2 (P2)

El parámetro permite asignar las respectivas particiones a las salidas.

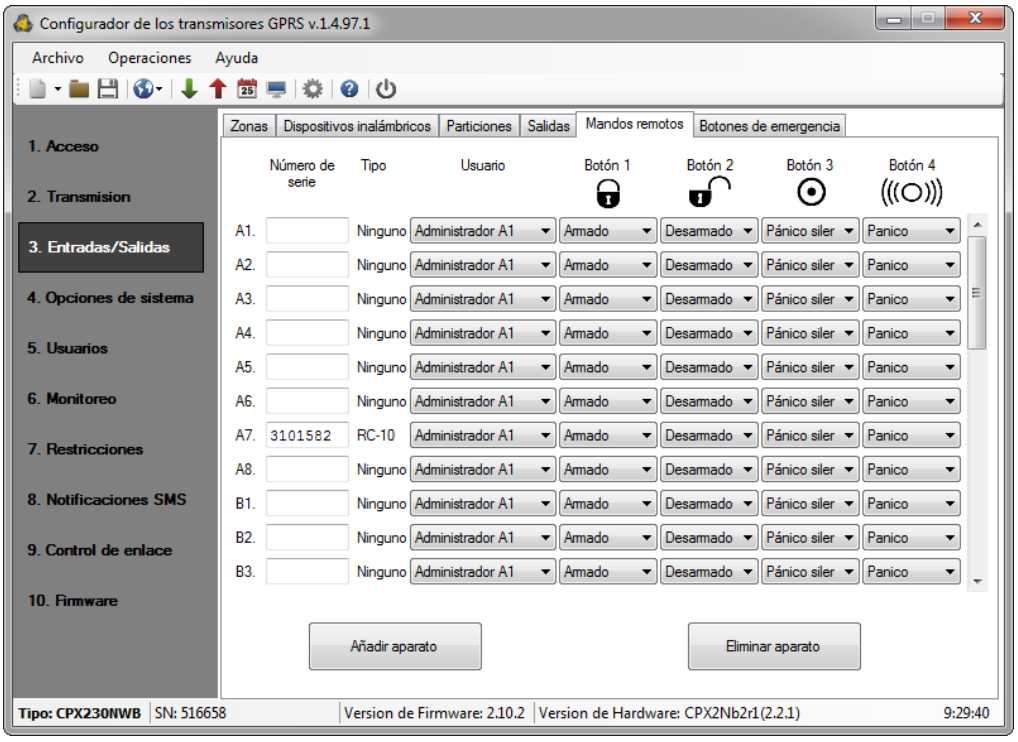
6.3.4.3. Duración

Parámetro que determina el tiempo durante el cual debe estar activada la salida.

6.3.4.4. Biestable

Este parámetro permite activar el modo biestable de la salida. Esto significa que la salida estará activa mientras dure el estado indicado en el campo «Tipo de salida».
Si el tipo es «No usada», el estado solo puede cambiarse mediante un comando remoto.

6.3.5. Mandos



El configurador permite añadir y configurar los mandos para el control inalámbrico de la centralita. El procedimiento en caso de añadir el mando es análogo como en caso de añadir la entrada inalámbrica. Se debe seleccionar la línea que corresponde a uno de los mandos, apretar el botón *Añadir*, seleccionar el puerto serie correspondiente, introducir el código de servicio y hacer clic en OK. Luego, después de aparecer la ventana de espera en el mensaje, se debe apretar uno de los botones del mando. Cuando la centralita detecte un nuevo mando, presentará información sobre el nombre y el número de serie. Ahora se puede emparejar con el dispositivo haciendo clic en el botón *Añadir*. El nuevo mando aparecerá en la línea seleccionada antes en el listado de mandos.

Ahora se debe configurar el nuevo mando, seleccionando el usuario al que se desea asignar – columna *Usuario*. Además, deben configurarse las acciones a realizar por la centralita después de pulsar los botones del mando: Columnas de *Botón 1* a *Botón 4* (para mandos a distancia con menos botones, basta con configurar los botones disponibles y en los demás campos seleccionar *Ninguno)*.

ATENCIÓN: Tenga en cuenta que el número de usuario debe ser activado por el Administrador (se debe generar un código de acceso para este número).

La función «Armar» es para armar la centralita en modo completo.

La función «Desarmar» es para desarmar la centralita.

La función «Alarm» significa la generación de una alarma con aviso sonoro.

La función «Alarma silenciosa» significa una alarma sin aviso sonoro.

Las funciones de activación/desactivación de las salidas 1, 2 y 3 permiten controlar dispositivos externos.

La función «Asistencia médica» funciona de la misma manera que el botón «AYUDA» en el teclado, es decir, genera una alarma médica.

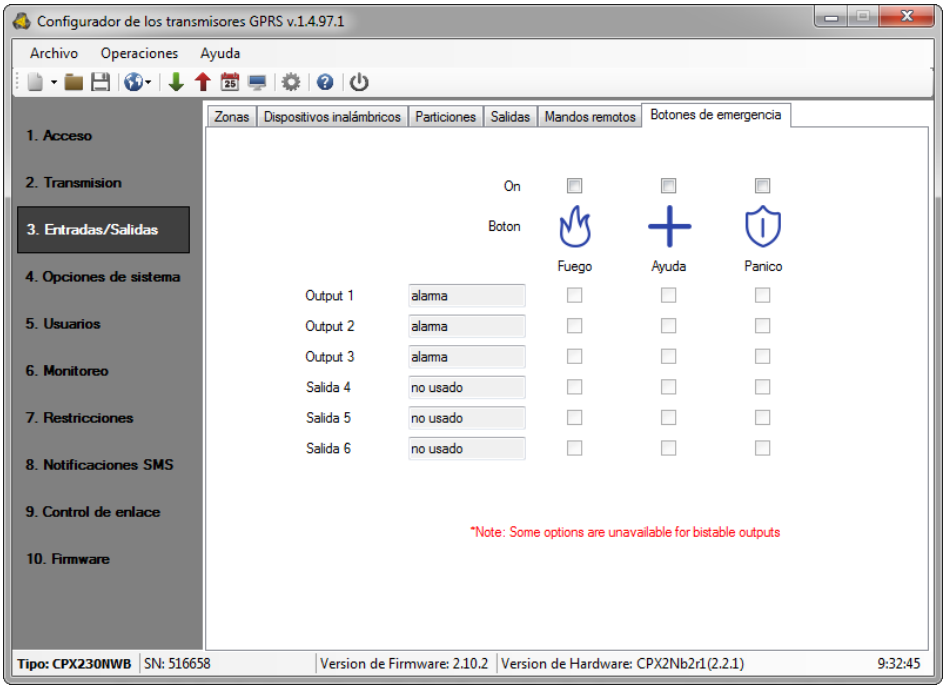
La función «Armar inmediatamente» permite el armado inmediato del sistema sin esperar el retardo de salida ajustado.

Los alarmas del mando a distancia funcionan independientemente de si la partición apropiada está armada o no. Para ambos tipos de alarma puede enviarse un mensaje al centro de monitoreo, dependiendo de la configuración de la centralita.

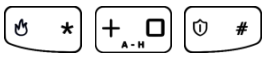
El fabricante recomienda asignar el botón con el símbolo  a una alarma normal, y el botón  a una alarma silenciosa. Dado que la centralita permite asignar teclas del mando a distancia a diferentes funciones, es posible activar una alarma con otra tecla.

La información sobre la configuración de los mandos a distancia debe enviarse automáticamente a la centralita. Sin embargo, el fabricante recomienda que después de añadir y configurar el mando o mandos a distancia, la información se envíe pulsando la flecha roja «Enviar» en la barra de acceso rápido (u «Operaciones» -> «Enviar»). Aparecerá una ventana como en el capítulo sobre los detectores inalámbricos. Marque la tercera casilla «Guardar disp. inalámbricos (solo CPX)», introduzca el código de servicio y pulse «Guardar».

6.3.6. Botones de alarma



6.3.6.1. Iconos

Los símbolos  corresponden a las teclas de función  en el teclado. Para habilitar una tecla, marque la opción «Act.» en la línea correspondiente.

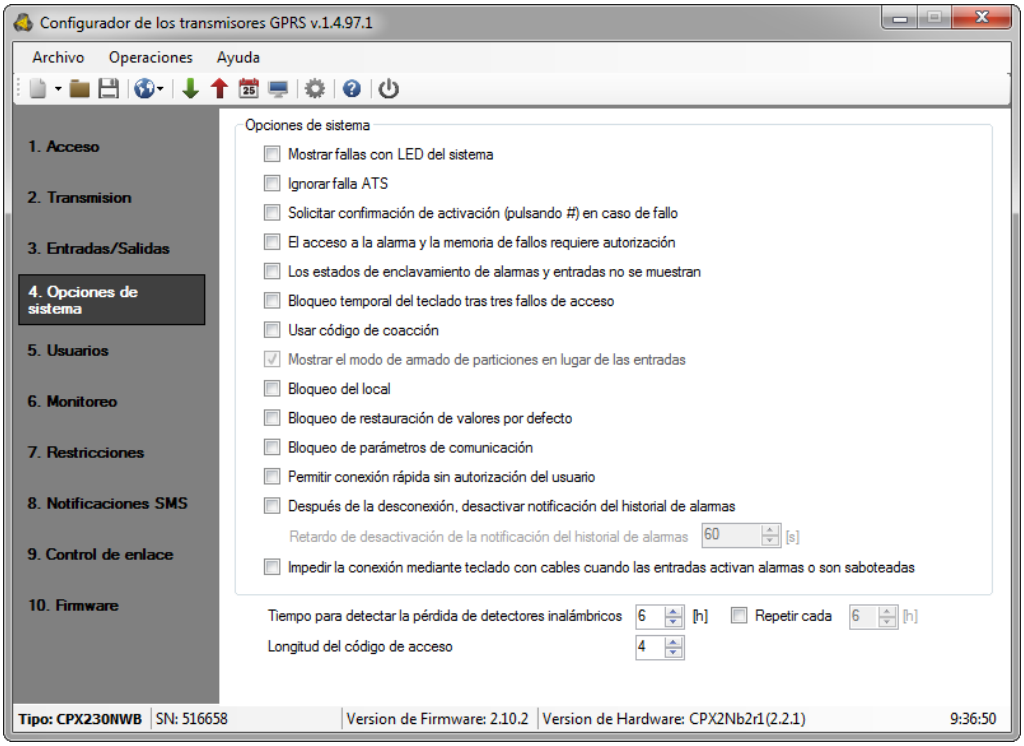
La estación de monitoreo recibirá la información sobre el uso de la función de alarma, independientemente de si alguna salida ha sido activada o no.

Los eventos correspondientes a los botones de alarma se enviarán siempre que hayan sido seleccionados en la pestaña «Monitoreo» del programa de configuración (véase el capítulo 6.6.).

6.3.6.2. Salidas

El usuario puede seleccionar las salidas que se activarán cuando se active la función (pulsando y manteniendo la tecla de función durante 3 segundos).
Para cada salida está disponible una descripción del comportamiento configurado en la pestaña «Salidas».

6.4. OPCIONES DEL SISTEMA



6.4.1. Aviso de fallos memorizados mediante el parpadeo del diodo SYSTEM

Después de seleccionar esta opción, la información sobre la ocurrencia y terminación de fallos en el sistema se señalizará mediante el parpadeo del diodo SYSTEM en el teclado KP32 hasta que se borre la memoria de fallos.

6.4.2. Ignorar el fallo ATS

Al seleccionar esta opción se desactivará la señalización de pérdida de comunicación con el servidor en el teclado KP32.

6.4.3. Requerir que se confirme el armado (con el botón #) en caso de fallo

Si se selecciona esta opción, el usuario recibirá una alerta adicional sobre los fallos al armar el sistema. El teclado alámbrico emitirá un pitido continuo, los diodos ALARM y SYSTEM parpadearán lentamente y los diodos de 1 a 8 mostrarán códigos de error (véase el capítulo 6.6 Armando el sistema con un fallo en el Manual de usuario). Presionar el botón # para armar el sistema. De lo contrario, la centralita permanecerá desarmada.

La información sobre fallos y violaciones estará disponible después de acceder –desde el teclado alámbrico– a la función de usuario: *memoria de fallos* y *estado actual de entradas*.

6.4.4. El acceso al historial requiere autorización

Al seleccionar esta opción se restringe el acceso al historial de alarmas y fallos. Para acceder al historial, es necesario ingresar el código de usuario. Active esta opción para mantener la compatibilidad con Grado 2.

6.4.5. Sin visualizar el estado de alarmas y bloqueos

Si esta opción está activa, las violaciones y los bloqueos de línea actuales no se muestran en el teclado. Active esta opción para mantener la compatibilidad con Grado 2.

6.4.6. Bloqueo temporal del teclado tras tres intentos de acceso fallidos

Esta opción habilita el bloqueo del teclado. El teclado quedará bloqueado durante 90 segundos después de introducir 3 códigos erróneos. Durante este tiempo, ninguna función de la centralita no estará disponible desde el teclado. Una vez trascurrido el tiempo de bloqueo, el siguiente bloqueo del teclado se producirá después de introducir sucesivamente 3 códigos erróneos. La introducción del código correcto (por ejemplo, después de 2 códigos incorrectos) restablecerá el contador de códigos incorrectos. Active esta opción para mantener la compatibilidad con Grado 2.

6.4.7. Utilizar un código de coacción

El código de coacción (*duress code*) introducido durante el armado/desarmado envía una alarma silenciosa a la estación de monitoreo.

6.4.8. Visualizar el modo de armado de la partición en vez de violaciones y bloqueos de entradas

Opción no disponible en CPX230NWB.

6.4.9. Bloqueo de la instalación

La función «Bloqueo de la instalación» permite deshabilitar la posibilidad de armar la centralita. Tras activar esta función, el usuario no podrá armar la instalación de ninguna manera (por ejemplo, SMS/GPRS, control remoto, entrada de armado, horarios, teclado normal, teclado inalámbrico). Sin embargo, será posible desarmar el sistema.

Todo intento de armado será rechazado por la centralita: el teclado alámbrico emitirá cuatro pitidos entre los cuales se iluminarán simultáneamente los diodos GROUP, ALARM, SYSTEM y PROG. La información de que el sistema no ha sido armado debido a la función de bloqueo habilitada figurará en los registros del Configurador y de OSM.Server.

6.4.10. Bloqueo de restauración de los ajustes predeterminados

Esta función permite desactivar la posibilidad de restaurar el código de instalador predeterminado. Sin embargo, al restaurar los ajustes por defecto, después de seleccionar la opción «Restaurar los ajustes por defecto», aparecerá una ventana solicitando el código de instalador o el código de servicio (ATS).

Tras activar esta función es recomendable cambiar el código de acceso del instalador y el código de servicio (ATS).

ATENCIÓN: En caso de pérdida de los nuevos códigos, será necesario enviar los dispositivos bloqueados al servicio de EBS.

6.4.11. Bloqueo de los ajustes de comunicación

Tras activar esta opción, para restablecer la configuración de fábrica y para cambiar los siguientes parámetros:

- código de servicio (ATS),
- número de teléfono del servidor,
- APN, ID de usuario, contraseña de usuario,
- puerto del servidor primario,
- Puerto del servidor secundario,
- clave de encriptación SMS,
- clave de encriptación GPRS,
- direcciones de servidores DNS,
- números a los que se reenviarán los SMS entrantes,
- activar/desactivar la opción «Bloqueo de los ajustes de comunicación»,

iserá necesario conocer el código de servicio (ATS)! Esto impide el registro no autorizado de la centralita en otra estación de monitoreo.

El instalador podrá:

- cambiar los parámetros relacionados con los usuarios, las entradas y salidas, los dispositivos inalámbricos, las particiones, los mandos a distancia, el monitoreo y algunas opciones del sistema,
- enviarlos a la centralita,
- actualizar el firmware,
- leer los ajustes almacenados en el dispositivo,
- guardar los ajustes de la centralita en un archivo con la extensión emi,

El código de servicio (ATS) por defecto es 0000, es recomendable cambiar este código por otro, preferiblemente de 7 dígitos. En caso de pérdida de este código será necesario enviar el dispositivo a la sede de EBS.

6.4.12. Permitir el armado rápido sin autorización del usuario

Si esta opción está activa, el sistema puede armarse rápidamente utilizando el teclado sin necesidad de introducir el código de autorización de usuario.

6.4.13. Desactivar la señalización de alarmas históricas tras el desarmado

Si esta opción está activa, tras desarmar el sistema (la partición), las alarmas históricas procedentes de las líneas asignadas a la partición y (parpadeo del diodo F – partición 1 y del diodo 6 – partición 2) no se visualizarán en el teclado una vez trascurrido el tiempo de retraso ajustado (véase el capítulo 6.4.14). El usuario seguirá teniendo acceso al estado de las alarmas históricas de las entradas mediante la función 3# hasta que se borren. Cuando el sistema está desarmado y se activa una alarma de cualquier línea de 24 horas, el historial de alarmas puede desactivarse armando y desarmando el sistema (sólo si la opción está activada) o accediendo a la función 3# y borrando el historial.

6.4.14. Retraso en la desactivación de la señalización de alarmas históricas

Esta función sólo es disponible tras activar la opción «Desactivar la señalización de alarmas históricas tras el desarmado». Permite determinar un retraso en segundos, tras el cual ya no se mostrarán las alarmas históricas en el teclado. Cuándo el sistema está armado y suceden violaciones señaladas mediante el parpadeo de los diodos F y 6, los diodos se apagarán una vez el sistema desarmado y trascurrido el tiempo determinado. Todavía se podrán consultar las alarmas mediante la función 3#, hasta que el usuario las borre.

6.4.15. Desactivar la posibilidad de armar mediante el teclado alámbrico durante una violación o un sabotaje de la línea

Si esta opción está activa, el armado con el KP32 se bloquea cuando las líneas sean violadas o saboteadas. La violación / el sabotaje de cualquier línea asignada al sistema se señala mediante el apagado del diodo READY: D en el caso de una línea de la partición 1 o 4 en caso de una línea de la partición 2. Si el sistema cuenta con dos particiones, basta con que una de ellas tenga un detector violado/saboteado para que no se pueda armar la centralita. Cuando se intenta armar, el teclado alámbrico emitirá un pitido alto de un segundo y se iluminarán los diodos GROUP, ALARM, SYSTEM y PROG durante unos 4 segundos. Los fallos del sistema no afectan a esta opción.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.8.8.

6.4.16. Tiempo de detección del desvanecimiento de los detectores inalámbricos

Esta función permite determinar el tiempo después del cual se enviará el aviso sobre el desvanecimiento de los detectores inalámbricos a la estación de monitoreo.
Este tiempo se exprime en horas. El valor por defecto es de 6 horas, el mínimo de 2 y el máximo de 24 horas.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.8.8.

6.4.17. Repetir cada

Esta función permite activar el envío cíclico de la información de desvanecimiento de los detectores inalámbricos a intervalos definidos (a partir del primer desvanecimiento) a la estación de monitoreo.

Este tiempo se exprime en horas. El valor por defecto es de 6 horas, el mínimo de 2 y el máximo de 24 horas.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.10.0.

6.4.18. Longitud del código de acceso

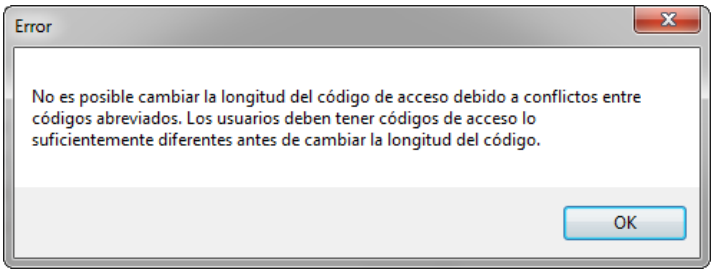
Esta función permite determinar la longitud de los códigos de administrador y de usuarios (la modificación afecta a todos los usuarios). El rango de longitud es de 4 a 7 dígitos. El valor por defecto es 4.

Sólo es posible reducir la longitud si los códigos acortados no resultan ser los mismos.

Si quiere acortar la longitud del código, es recomendable eliminar y volver a configurar los usuarios para evitar conflictos.

Ejemplo:

Supongamos que tenemos los siguientes códigos de 5 dígitos en la base CPX: 44440, 44444, 44449. No será posible acortar la longitud del código a 4 dígitos, ya que tendríamos códigos idénticos. No se aceptará el cambio y aparecerá una ventana de aviso:

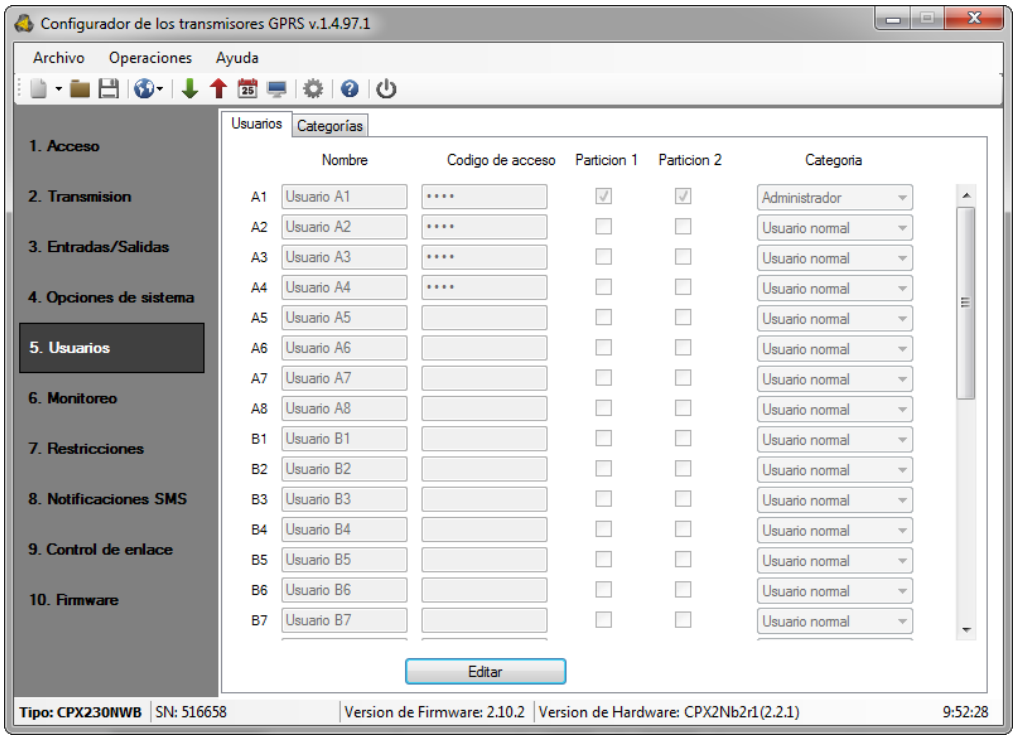


En tal caso la única solución posible es eliminar usuario(s) con códigos similares.

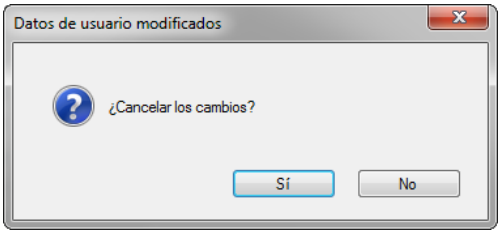
1. **Si el código de usuario en la base de datos CPX es más corto que el valor definido, se agregarán «0» al final del código.**
   Ejemplo: Si hay un código 1234 en la base, tras cambiar la longitud del código a 6 dígitos, este código será 123400.
2. **Si el código de usuario en la base de datos CPX es más largo que el valor definido, se acortará a los «n» primeros dígitos.**
   Ejemplo: Si hay un código 1234567 en la base, tras cambiar la longitud del código a 5 dígitos, este código será 12345.
3. **En el caso de un código de coacción:**
   - **Si hay un código 12345 en la base, tras cambiar la longitud del código a 7 dígitos, este código será 1234500. Por lo tanto, el código de coacción será 1234501**
   - **Si hay un código 12345 en la base, tras cambiar la longitud del código a 4 dígitos, este código será 1234. Por lo tanto, el código de coacción será 1235**

6.5. USUARIOS

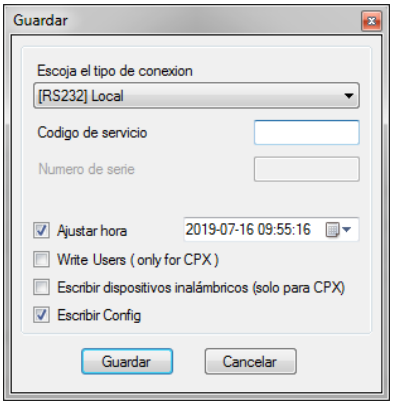
6.5.1. Usuarios



Esta pestaña se utiliza para gestionar usuarios. Para hacerlo, pulse el botón «Editar» e introduzca la contraseña de administrador actual. Una vez que el sistema haya aceptado la contraseña, podrá cambiar las contraseñas de los usuarios, sus permisos para la partición y seleccionar una categoría (confiable no autorizado). Una vez finalizada la edición de los usuarios, pulse el botón «Aceptar cambios» para guardar los datos en el Configurador. Para deshacer los datos introducidos, pulse el botón «Cancelar cambios». Aparecerá una ventana de pregunta:

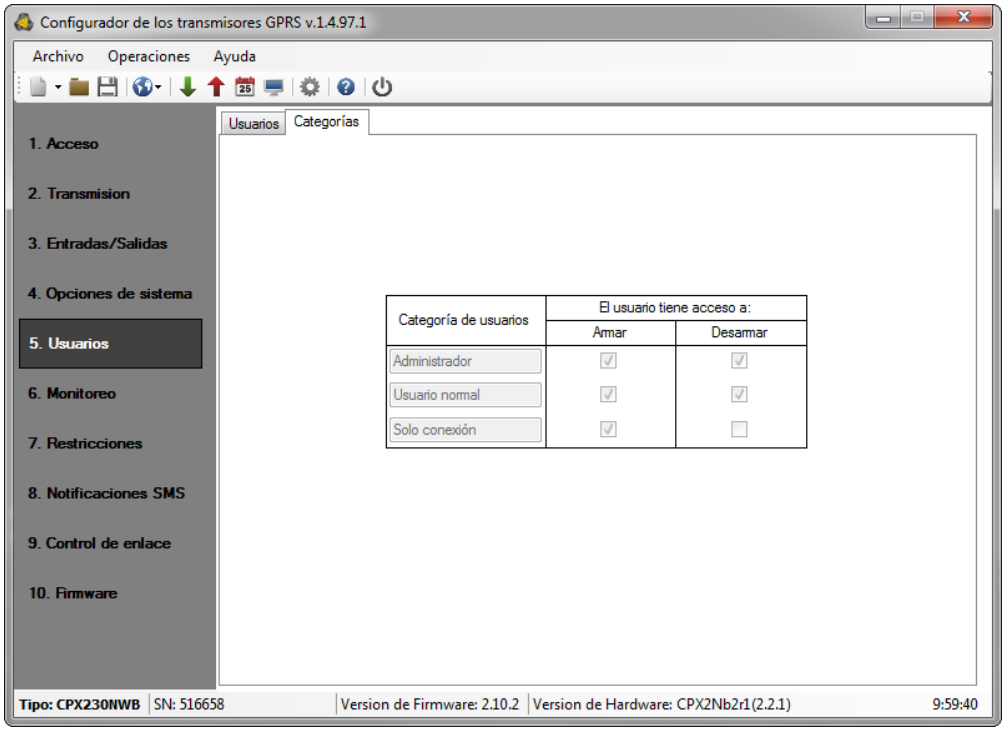


Tenga en cuenta que una vez realizados los cambios, cuando los usuarios se cargan en la centralita, debe estar marcada la opción «Guardar usuarios»:



La configuración de usuarios sólo se puede cambiar con el cable de programación. No es posible editar los usuarios de forma remota a través de GPRS.

6.5.2. Categorías



Existen 3 categorías de usuarios con diferentes niveles de acceso a las funcionalidades del sistema:

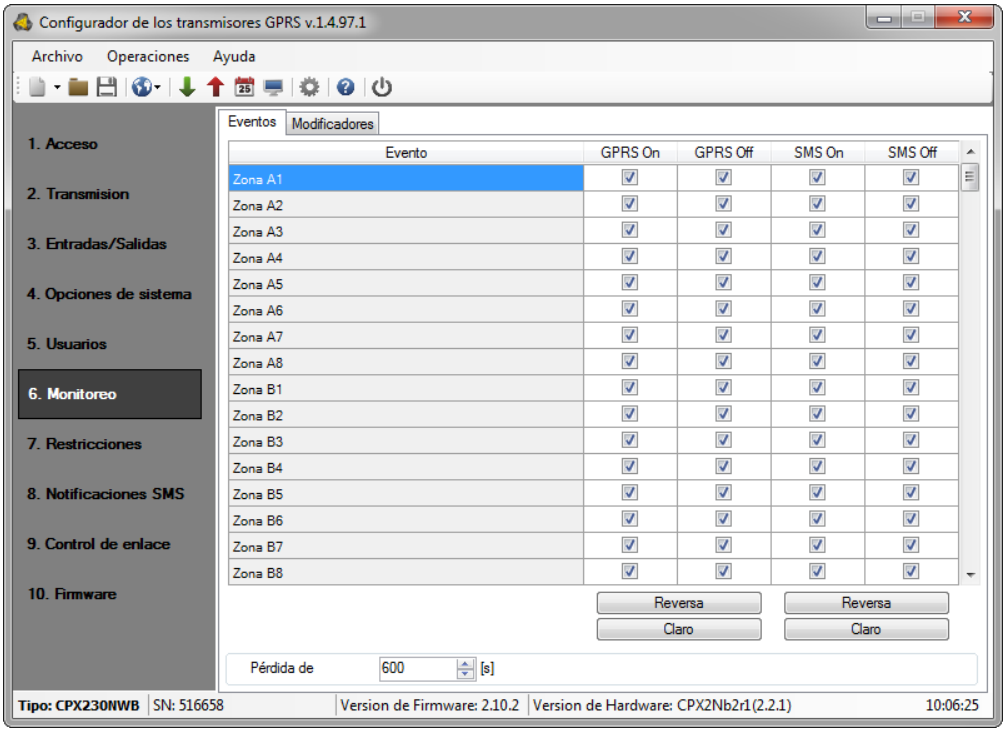
1. Administrador: usuario con el acceso más amplio. Puede armar y desarmar el sistema y acceder y editar todas las funciones de usuario. El administrador es un usuario A1 y no se pueden cambiar sus permisos.
2. Confiable: un usuario que puede armar y desarmar el sistema y tiene acceso al historial de alarmas y fallos, estados de entradas y bloqueo de entradas, puede cambiar su código y examinar entradas y salidas,
3. No autorizado: un usuario que sólo puede armar el sistema. No tiene acceso a ninguna función que requiera la introducción de código. Si la opción «*Acceso al historial requiere autorización*» no ha sido activada durante la configuración, el usuario tiene acceso a las funciones a las que se aplica esta opción (ver capítulo 9).

6.6. MONITOREO

6.6.1. Eventos

Esta opción permite determinar cuáles de las señales disponibles, generados por el dispositivo, se trasmitirán a la estación de monitoreo.

ATENCIÓN: El evento «Cambio de configuración» se referirá al cambio de configuración a través del mensaje SMS o bien a través de los comandos GPRS.



6.6.1.1. Anexo GPRS / Desact. GPRS

En estas columnas definimos las señales que deben avisarse a la estación de monitoreo con el uso de la transmisión GPRS. Tenemos la posibilidad de enviar la información tanto sobre los alarmas (cambio del estado de la entrada del de descanso al activo) como sobre los retornos al estado de las entradas del activo al de descanso (normalización). Para que se transmita una señal, basta con seleccionarla (haciendo clic en la casilla a la derecha).

El botón [Borrar] eliminará todas las señales marcadas.

El botón [Revertir] ocasionará el cambio de las selecciones al revés.

6.6.1.2. Anexo SMS / Desact. SMS

En estas columnas definimos las señales que deben ser avisados a la estación de monitoreo con el empleo del mensaje SMS – cuando el dispositivo no tenga conexión al servidor a través de GPRS. Tenemos la posibilidad de enviar la información tanto sobre los alarmas (cambio del estado de la entrada del de descanso al activo) como sobre los retornos al estado de las entradas del activo al de descanso (normalización). Para que una señal determinada sea transmitida, basta con seleccionarla (haga clic en la casilla correspondiente a la derecha).

El botón [Borrar] eliminará todas las señales marcadas.

El botón [Revertir] ocasionará el cambio de las selecciones al revés.

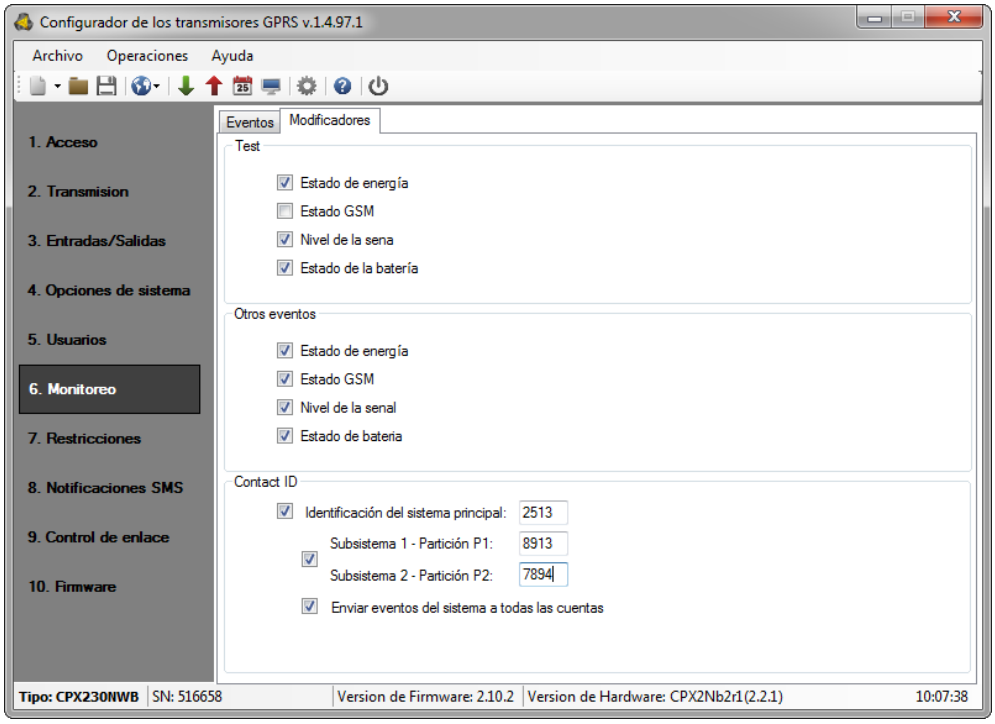
6.6.1.3. Desaparición de alimentación

Una de las opciones adicionales del dispositivo es controlar la existencia de la tensión de alimentación. Como unas cortas desapariciones de la alimentación de red pueden existir en algunos edificios, se puede evitar el aviso introduciendo el tiempo, después del cual se envíe la información. El valor de este parámetro significa que la falta de

alimentación debe durar un tiempo definido para que el dispositivo considere que efectivamente es falta de alimentación y que se envíe la información adecuada.

6.6.2. Modificadores

En esta pestaña se puede especificar el tipo de información adicional que será transmitida a la estación de monitoreo por GPRS/SMS junto con la señal. Esta información puede ser una apreciable fuente de datos sobre las condiciones de trabajo del dispositivo, sin embargo, en poco grado aumentará el número de los datos enviados por medio de la red GSM.



6.6.2.1. Modificadores para pruebas y otros eventos

Es posible definir dos conjuntos separados: para la señal de prueba (enviado en forma cíclica según la configuración en la pestaña Acceso) y para los demás eventos. Si marca la casilla, la información de este tipo se transmitirá al software receptor. Si no se selecciona, no se envía ninguna información de este tipo a la estación de monitoreo.

Parámetros para configurar:

- Tensión de alimentación – información sobre el cargador conectado y el estado de carga de la batería
- Estado GSM – estado de la conexión con la red GSM, tipo de conexión con el servidor (GPRS/SMS), información sobre las llamadas telefónicas actuales
- Nivel de señal – calidad de la señal de conexión a la red GSM
- Tensión de la batería – valor de la tensión de la batería de alimentación en milivoltios

6.6.2.2. Contact ID

En caso de transmisión de datos en formato Contact ID, en esta sección es posible determinar números de identificación individuales de la cuenta del sistema (ACN0) y de

las cuentas de sus subsistemas: partición 1 (ACN1) y partición 2 (ACN2). Esto permite determinar de qué parte del sistema proviene la señal.
ATENCIÓN: Opción disponible a partir de la versión de firmware 2.9.0.

ATENCIÓN: Los números ACN0, ACN1 y ACN2 son cuatro caracteres hexadecimales.

6.6.2.2.1. Número ACN0

Una vez ingresado el número ACN0, la información sobre cada evento del sistema enviada a la estación de monitoreo llevará este número. Los eventos del sistema son aquellos que contienen información sobre el mismo, por ejemplo: fallo de alimentación, reinicio del módem, fallo en la hora.

6.6.2.2.2. Números ACN1 y ACN2

Una vez ingresados los números ACN1 y ACN2, la información sobre cada evento no relacionado con el sistema (con identificador de partición 1 y/o 2) llevará el número ACN1 (para la partición 1) o ACN2 (para la partición 2). Los eventos no relacionados con el sistema son aquellos que contienen información sobre las particiones, por ejemplo: armado/desarmado de la partición 1 y/o 2, alarmas de los detectores asignados a la partición.

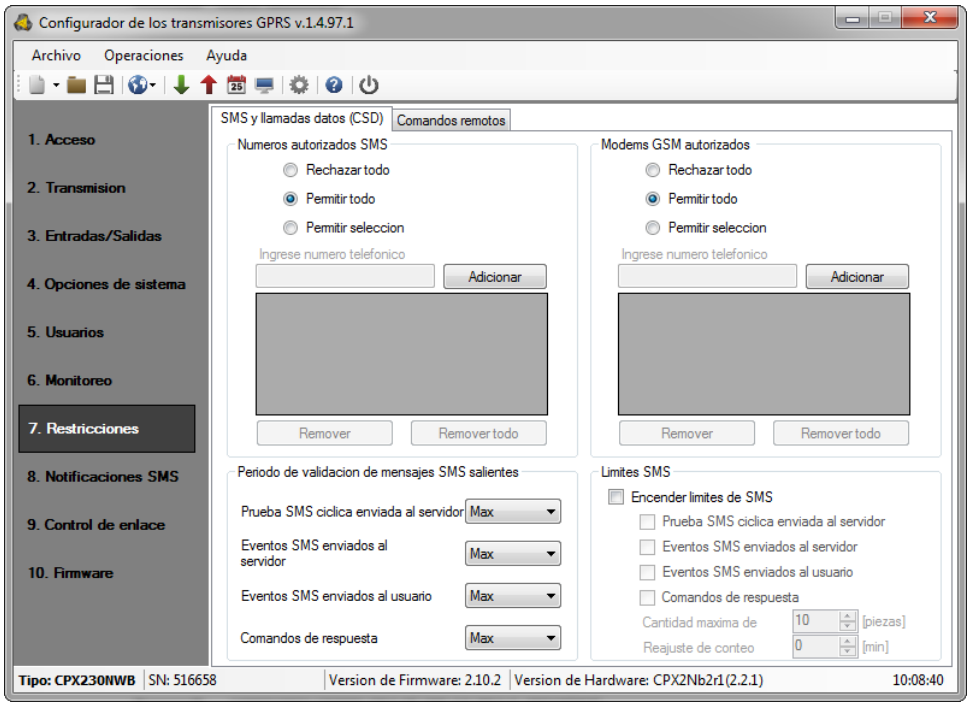
ATENCIÓN: Si introduce un número de cuenta para una sola partición, no será posible enviar la configuración a la centralita. Deben introducirse ambos números (ACN1 y ACN2).

6.6.2.2.3. Enviar los eventos del sistema a todas las cuentas

Si se selecciona esta opción, los eventos del sistema se enviarán a todas las cuentas, es decir, cuenta de sistema, cuenta de partición P1 y cuenta de partición P2.

6.7. RESTRICCIONES

6.7.1. SMS y módems GSM



6.7.1.1. Teléfonos autorizados para SMS

El usuario podrá restringir el acceso remoto al dispositivo (por medio de SMS) sólo para los determinados números de teléfonos. El listado creado de números (hasta 5) significa que solamente de estos números será posible controlar el dispositivo.

Las opciones disponibles son:

- Restringir a todos: Significa falta de la posibilidad de comunicación.
- Permitir a todos: Significa que la comunicación es posible desde cualquier número de teléfono.
- Permitir a los seleccionados: Significa que la comunicación sólo es posible con los números de teléfono de la lista. Se admite definir hasta 5 números.

Tras seleccionar «Permitir seleccionados» se accede al campo de edición. Los números subsiguientes se ingresan en el campo y agregan a la tabla de abajo haciendo clic en el botón «Agregar». Al situar el cursor en la línea dada con el número y al clicar el botón "Eliminar" ocasionaremos la eliminación del número de la tabla.

La opción "Eliminar todos" borrará todo el contenido de la tabla.

ATENCIÓN: La autorización del mensaje SMS entrante consta en comparar el número desde el que vino con los que se encuentran en la tabla. Se admite la versión de registro en la tabla de tan solamente un fragmento de número, por ejemplo 1234. Entonces se autorizarán todos los números que contengan la secuencia especificada, por ejemplo, 600**1234**56 **o** 60**1234**567**.**

ATENCIÓN: Si utiliza un módem conectado al servidor OSM.Server para enviar SMS, su número de teléfono debe estar incluido en la lista anterior.

6.7.1.2. Números de los módems GSM autorizados

Para las conexiones en el canal CSD el usuario podrá limitar el acceso remoto al dispositivo desde los módems GSM. El listado creado de números (hasta 5) significa que solamente de estos números será posible la comunicación con el dispositivo.

Las opciones disponibles son:

- Restringir a todos: Significa falta de la posibilidad de comunicación.
- Permitir a todos: Significa que la comunicación es posible desde cualquier número de teléfono.
- Permitir a los seleccionados: Significa que la comunicación sólo es posible con los números de teléfono de la lista. Se admite definir hasta 5 números.

Después de la selección Permitir seleccionados se consigue el acceso al campo de edición. Los siguientes números deben introducirse en el campo y, luego, al clicar el botón [Añadir] trasladaremos el número a la tabla abajo. Al situar el cursor en la línea dada con el número y al clicar el botón "Eliminar" ocasionaremos la eliminación del número de la tabla.

La opción "Eliminar todos" borrará todo el contenido de la tabla.

ATENCIÓN: La autorización de la conexión entrante CSD consta en comparar el número desde el que vino con los que se encuentran en la tabla. Se admite la versión de registro en la tabla de tan solamente un fragmento de número, por ejemplo 1234. Entonces se autorizarán todos los números que contengan la secuencia especificada, por ejemplo, 600**1234**56 **o** 60**1234**567**.**

ATENCIÓN: Si utilizar un módem conectado al servidor OSM.Server para una llamada entrante CSD, su número de teléfono debe estar en la lista anterior.

6.7.1.3. Periodos de validez de los mensajes salientes SMS

El usuario podrá determinar el tiempo que el dispositivo tiene para transferir la información en forma del mensaje SMS. La validez se define por separado para los siguientes grupos de información:

- Pruebas de SMS al servidor
- Eventos SMS enviados al servidor
- Eventos SMS enviados al usuario
- Respuestas a los comandos

La selección se realiza por entre los valores se encuentran en el listado desplegable por medio de clicar en la flecha al lado del campo de selección. Hay opciones disponibles: 5, 10, 15, 30 minutos; 1, 2, 6, 12 horas; 1, 7 días; MAX (significa falta del periodo de validez).

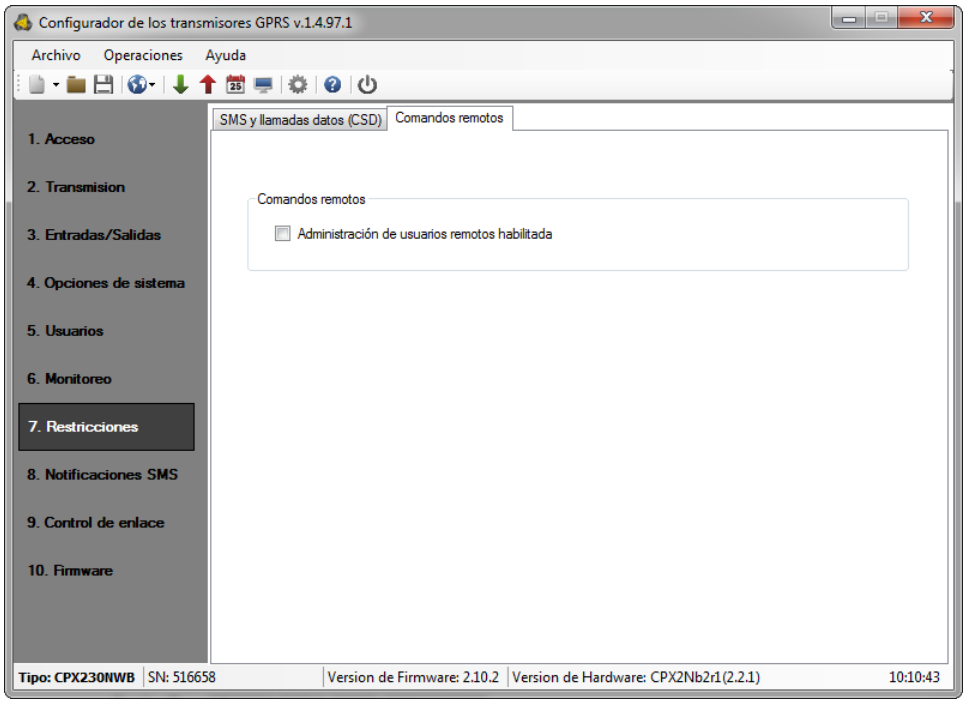
6.7.1.4. SMS salientes

El usuario puede limitar la cantidad de los mensajes SMS que enviará el dispositivo. Dado que la forma básica de transmisión debe ser GPRS, esta limitación es importante, principalmente por razones económicas.

Al marcar el campo [Activar restricciones SMS] activaremos el acceso a los grupos de información que estarán restringidos:

- Pruebas de SMS al servidor
- Eventos SMS enviados al servidor
- Eventos SMS enviados al usuario
- Respuestas a los comandos
- Estas restricciones se definen por medio de introducir dos valores:
- Cantidad máxima de mensajes SMS: Determina la cantidad máxima de los mensajes SMS enviados por una unidad de tiempo (véase el parámetro Puesta a cero del contador). Esta opción protege al usuario contra el envío de demasiados mensajes, por ejemplo, en caso de fallo.
- Puesta a cero de contador: Este parámetro determina el tiempo (en minutos), en que debe ponerse a cero el contador de los mensajes SMS enviados.

6.7.2. Comandos remotos



6.7.2.1. Permitir la administración remota de usuarios

Al seleccionar la opción permitimos la configuración remota de las cuentas de los usuarios del sistema de alarmas.

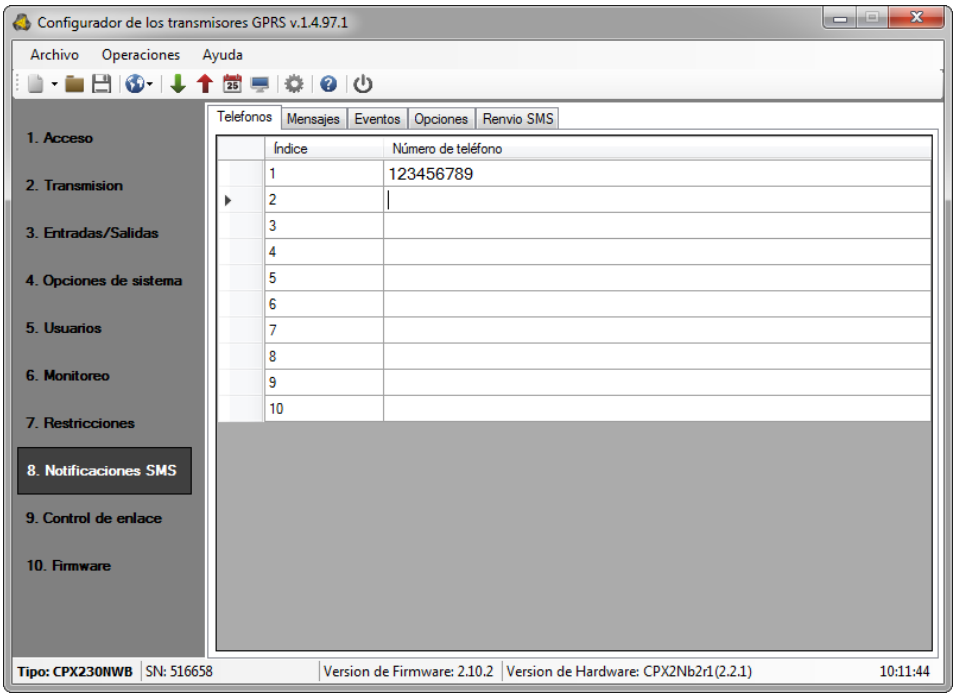
ATENCIÓN: Si el usuario desea utilizar la aplicación móvil AVA, esta opción debe estar habilitada.

6.8. NOTIFICACIONES SMS

6.8.1. Teléfonos

El dispositivo es capaz de avisar al usuario sobre la existencia de diferentes eventos por medio de los mensajes SMS. Antes de enviar un mensaje, se puede intentar realizar una llamada de voz (véase el capítulo 6.8.4. Opciones).

Para añadir el número de usuario al listado de números a los que se enviarán los mensajes, se debe introducir este número en uno de los índices. El dispositivo soporta como máximo 10 números.

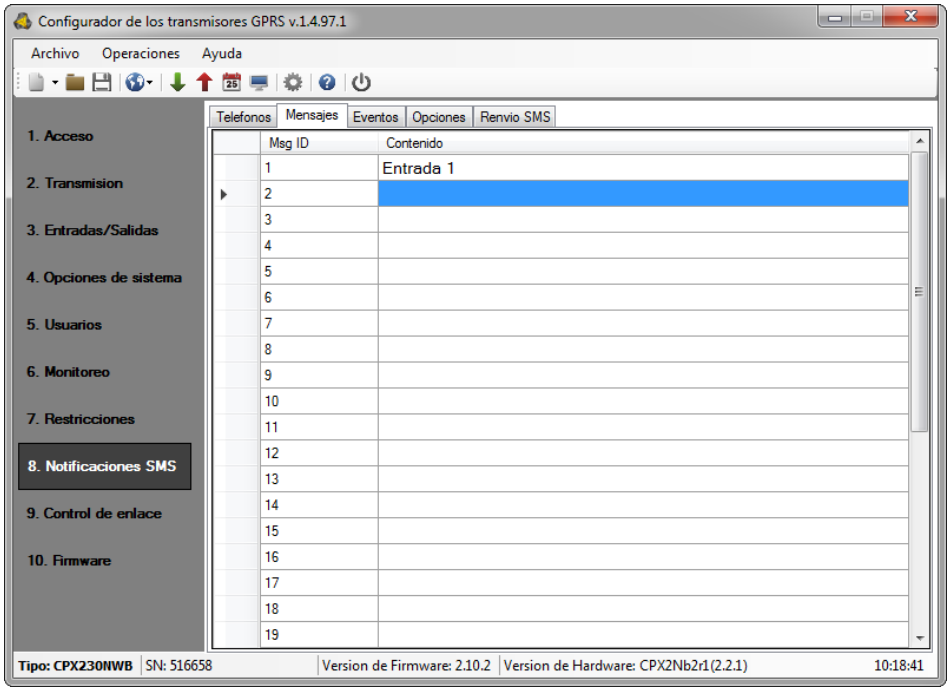


6.8.2. Comunicaciones

El contenido de los respectivos mensajes se debe introducir en las líneas de la pestaña Comunicaciones. Estos mensajes se podrán asignar a los eventos disponibles en la pestaña Eventos. Es posible definir como máximo 32 mensajes. Antes de enviar un mensaje, se puede intentar realizar una llamada de voz (véase el capítulo 6.8.4. Opciones).

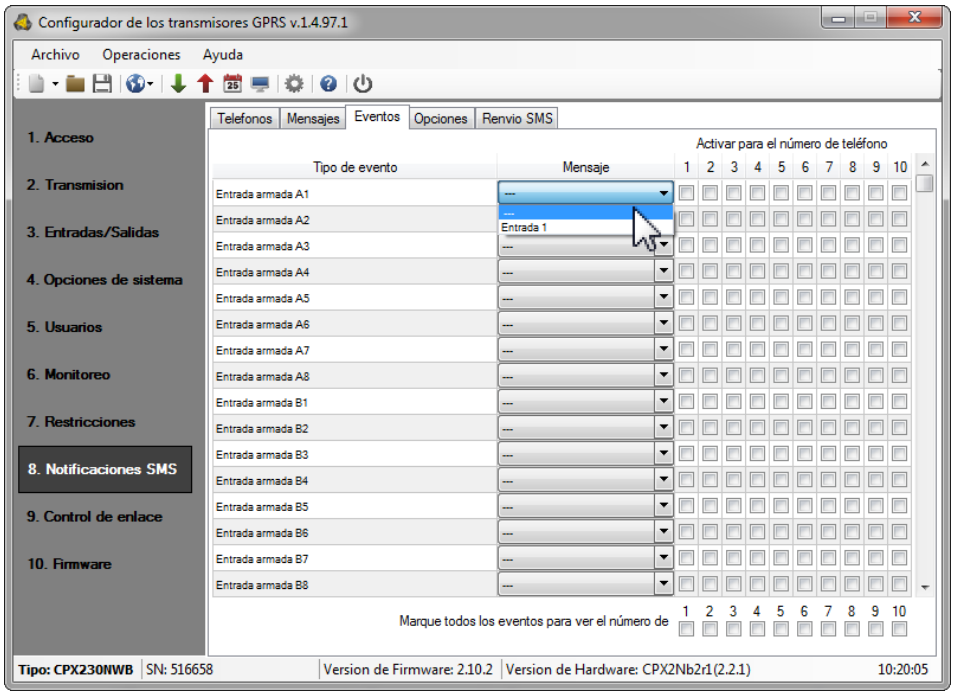
NOTA

Los mensajes sólo pueden contener caracteres alfanuméricos y: - ! @ # $ % " < > & * ( ) + : ? ` ; ' = , . / y espacio.



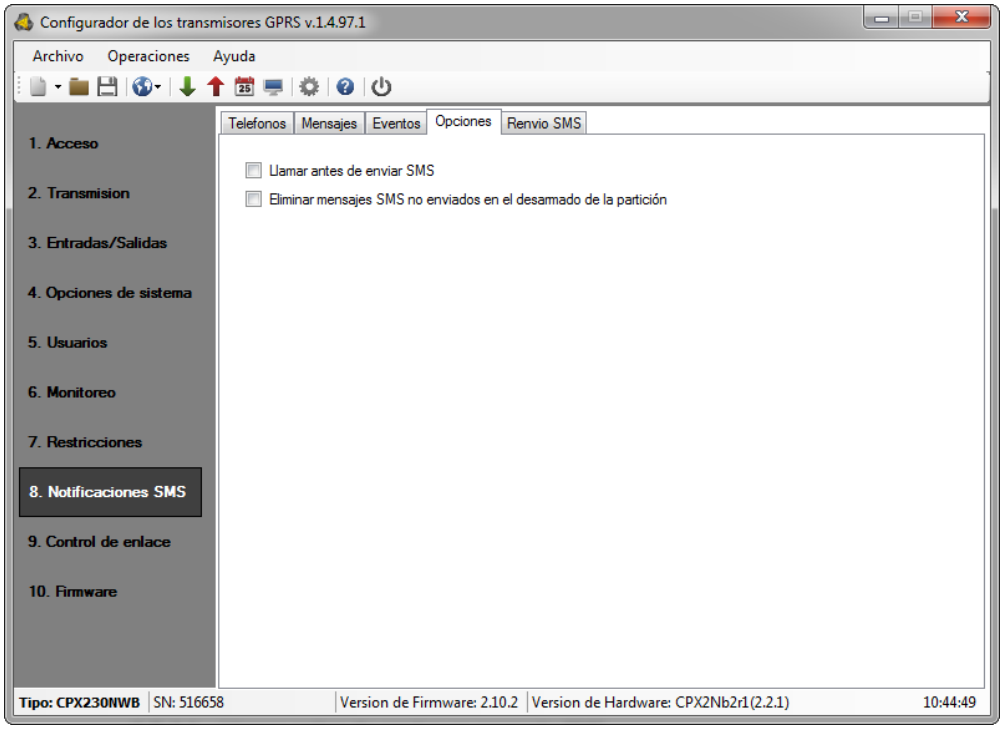
6.8.3. Eventos

Para asignar un mensaje al evento, es necesario desplegar el menú de la columna Comunicación y seleccionar uno de los mensajes previamente definidos. A continuación, seleccione los números de teléfono a los que se debe enviar el mensaje cuando se produzca el evento. Antes de enviar un mensaje, se puede intentar realizar una llamada de voz (véase el capítulo 6.8.4. Opciones).



6.8.4. Opciones

En esta sección se pueden habilitar opciones adicionales relacionadas con el envío de mensajes SMS.



6.8.4.1. Llamar antes de enviar un mensaje SMS

Seleccione la opción «Llamar antes de enviar un mensaje SMS» si desea recibir información adicional sobre un mensaje SMS entrante. Si esta opción está activa, el dispositivo llama al número de teléfono del usuario antes de enviarle un SMS para informarle sobre un mensaje SMS entrante.

La llamada puede durar varias docenas de segundos, el usuario puede rechazar o contestar la llamada. Cuando contesta la llamada, el dispositivo se desconecta. Independientemente de lo que haga el usuario, tras la llamada se enviará el mensaje SMS. Después de enviar el mensaje al primer usuario (primer número de teléfono definido), se intenta llamar al siguiente usuario y enviarle un mensaje.

Si hay más mensajes que enviar, las llamadas de voz se realizarán con una frecuencia mínima de 15 minutos.

6.8.4.2. Eliminar los mensajes SMS no enviados al desarmar la partición

Si esta opción está activa, después de desarmar el sistema, se eliminarán de la cola todos los mensajes SMS no relacionados con la partición que aún está armada.

En otras palabras, después de desarmar, se borrarán los mensajes SMS relacionados con la partición desarmada y todo el sistema (excepto la partición armada).

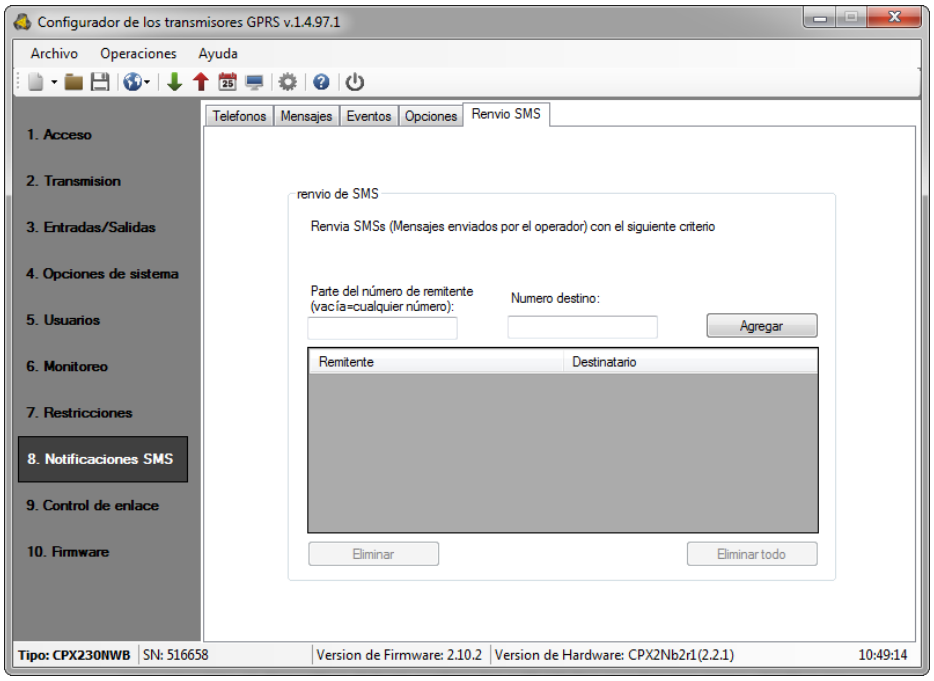
Si el usuario desarma ambas particiones, se eliminarán todos los mensajes SMS pendientes.

Todos los mensajes SMS relacionados con nuevos eventos que ocurran después de desarmar la partición se almacenarán en la memoria del dispositivo y se enviarán lo antes posible.

Nota: El fabricante no recomienda utilizar esta opción, ya que reduce la seguridad del sistema. Para uso exclusivo de usuarios avanzados.

6.8.5. Desvío de SMS

El dispositivo es capaz de transmitir los mensajes recibidos SMS a los determinados números de teléfonos según las reglas configuradas. Esta función puede resultar necesaria, por ejemplo, en caso de las notificaciones SMS sobre el estado de la cuenta. En la ventana se podrá introducir hasta 2 reglas para desviar las comunicaciones SMS.

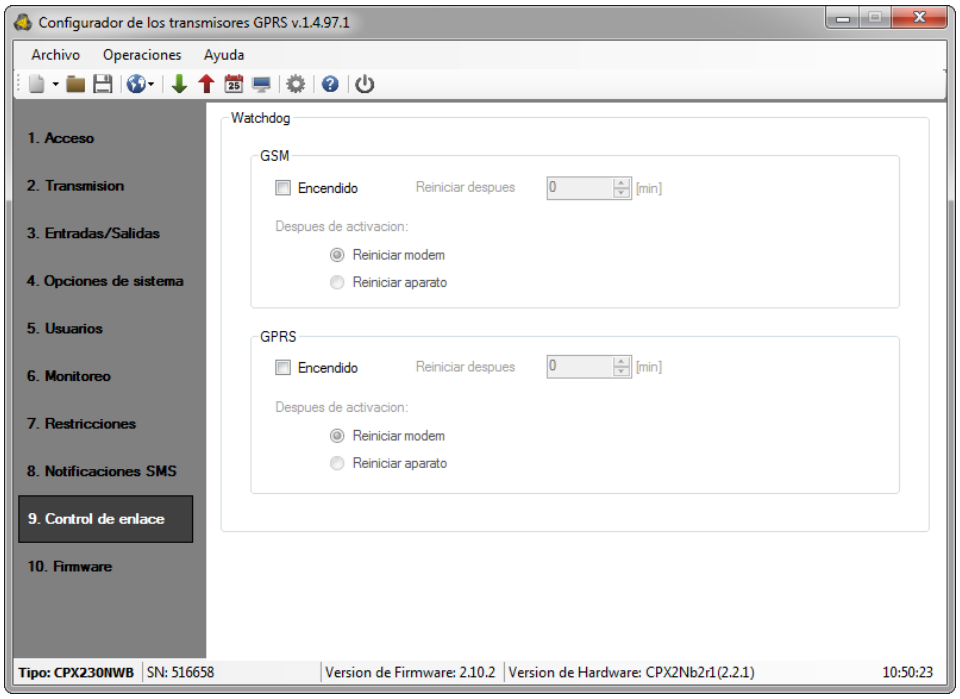


Cada regla está compuesta de la pareja: fragmento del número de teléfono del remitente y del número de teléfono correcto de destinatario. El fragmento del número de teléfono del remitente puede constar en un caso extremo de una serie vacía, lo cual significa el ajuste a cualquier número de teléfono. El tratamiento de las reglas se realiza según el orden encargado desde el principcio hasta el final, es decir, el resultado del tratamiento de la regla no influye en el tratamiento de las reglas siguientes. Asimismo, esto quiere decir que el mensaje dado SMS puede ser enviado a unos números de teléfonos o bien el mismo mensaje puede ser enviado unas veces al mismo número de teléfono. Tal caso tiene lugar cuando exista la condición puesta en el número de teléfono del remitente para al menos dos reglas que tengan el mismo número de destinatario.

ATENCIÓN: El usuario se responsabiliza de la correcta introducción de los números, gracias a los cuales no se creará un bucle en el envío de los mensajes SMS.

6.9. CONTROL DE COMUNICACIÓN

Estas opciones permiten que el dispositivo reaccione automáticamente si se interrumpe la comunicación con la estación de monitoreo. Esto se aplica a la situación cuando el dispositivo ha perdido la comunicación con la red GSM o la transmisión GPRS es imposible.



6.9.1. GSM

La activación de esta función (marcar en la casilla [Activar]) hace que tengamos acceso a los parámetros que determinan la reacción del dispositivo después de la salida de la red GSM.

Determinamos el tiempo, después del cual, contando desde la pérdida de comunicación, el dispositivo deberá realizar las actividades que tengan como objetivo su restablecimiento. La selección del tiempo se realiza en el campo [Reinicio después del tiempo] y se expresa en minutos.

El siguiente paso es determinar qué debe hacer el dispositivo. La selección se realiza por medio de marcar la respectiva casilla en caso de describir la reacción:

- Reinicio de módem
- Reinicio del dispositivo

En caso de la falta de comunicación a la red GSM, el dispositivo tras comprobar este hecho, esperará el periodo definido y, luego, realizará las tareas previstas.

6.9.2. GPRS

La activación de esta función (al marcar en la casilla [Activar]) hará que tengamos acceso a los parámetros que determinan la reacción del dispositivo después de perder la comunicación al servidor.

Determinamos el tiempo, después del cual, contando desde la pérdida de comunicación, el dispositivo deberá realizar las actividades que tengan como objetivo su

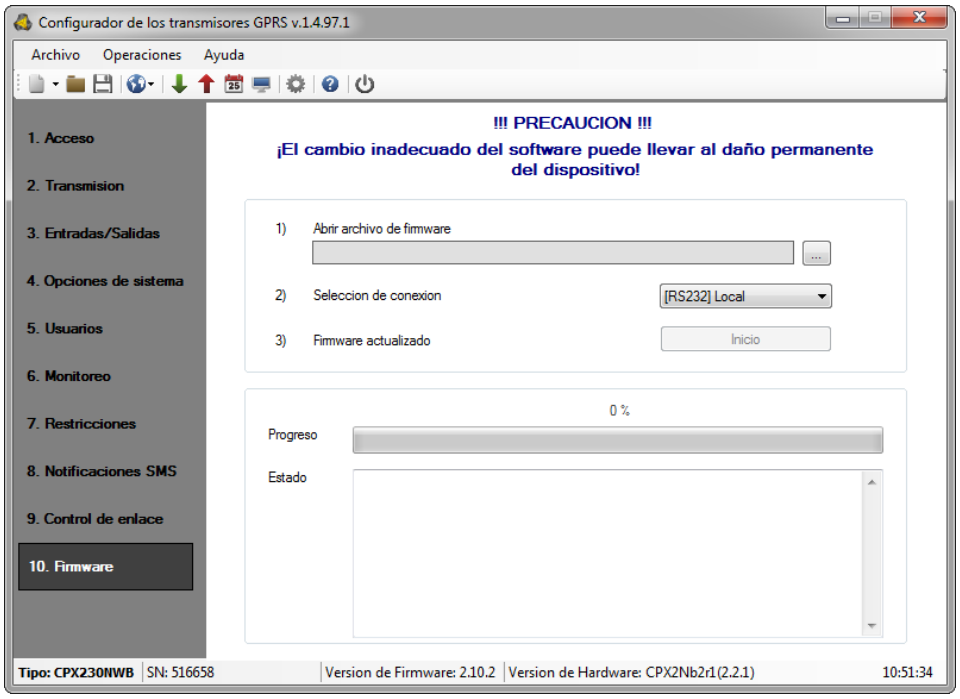
restablecimiento. La selección del tiempo se realiza en el campo [Reinicio después del tiempo] y se expresa en minutos.

El siguiente paso es determinar qué debe hacer el dispositivo. La selección se realiza por medio de marcar la respectiva casilla en caso de describir la reacción:

- Reinicio de módem
- Reinicio del dispositivo

En caso de la falta de comunicación GPRS, el dispositivo tras comprobar este hecho, esperará el periodo definido y, luego, realizará las tareas previstas.

6.10. FIRMWARE



El dispositivo cuenta con un cargador de arranque incorporado que permite actualizar el software del módulo. Durante la programación se visualizará toda la información sobre el transcurso de esta operación.

Se debe realizar las siguientes actividades:

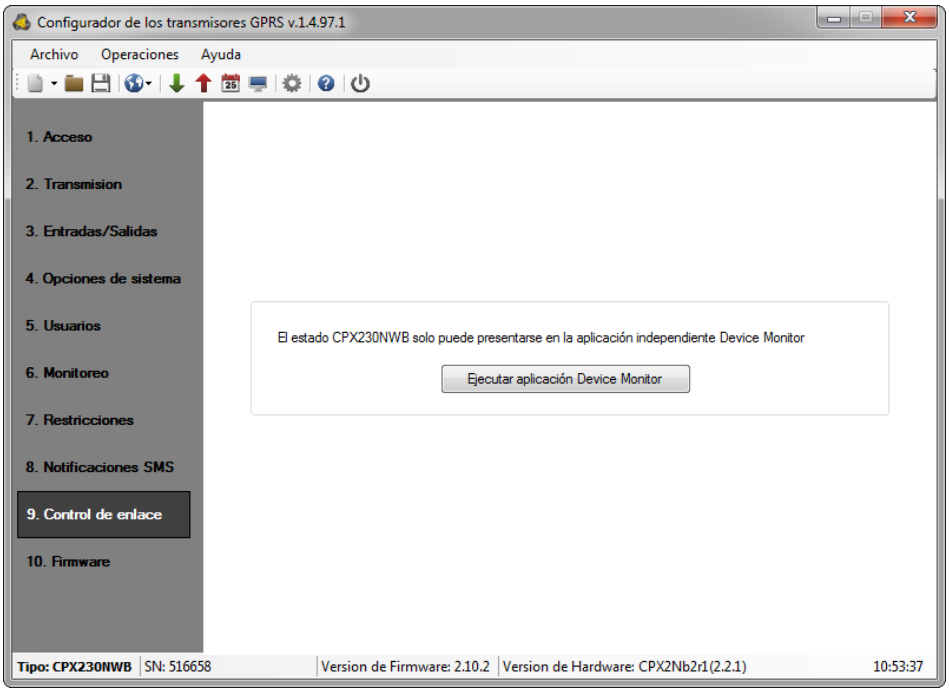
- Poner en marcha el programa de configuración,
- Pasar a la opción "Firmware" del configurador,
- Abrir el archivo con el nuevo firmware (el botón [Abrir] nos permite indicar el lugar donde se encuentra el archivo adecuado),
- Seleccionar el método de transmisión de archivos: local,
- Hacer clic en el botón [Inicio]. Se iniciará el procedimiento de sustitución del software,
- El proceso de grabación se muestra en una ventana especial del programa,
- Cerrar el programa después de completar la grabación,
- Espere más de diez segundos hasta que vuelva a iniciar el dispositivo.

A partir de ahora, el dispositivo funcionará bajo el control de un nuevo firmware.

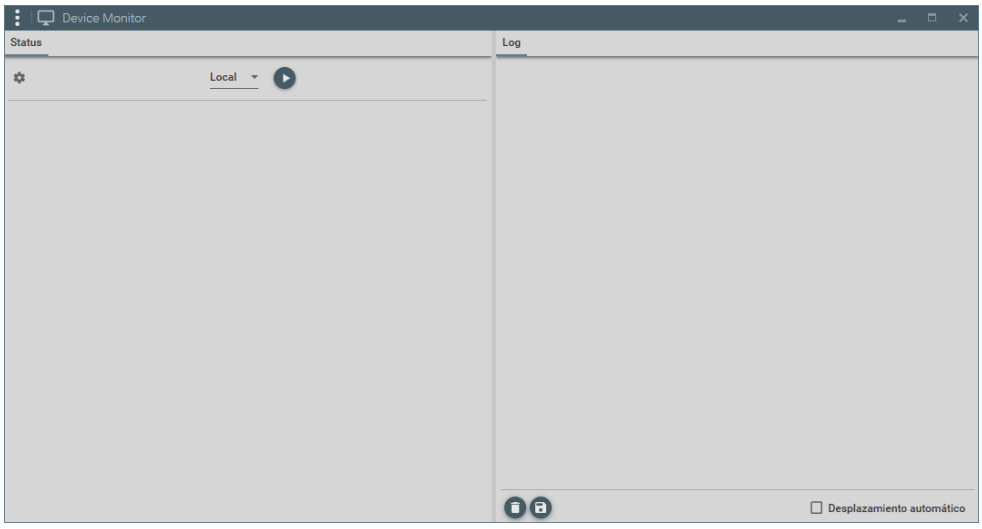
ATENCIÓN: El procedimiento de actualización del firmware debe llevarse a cabo con especial cuidado, ya que la ejecución incorrecta del procedimiento puede impedir que el dispositivo funcione correctamente.

6.11. MONITOR DEL DISPOSITIVO

La opción de monitoreo del dispositivo está disponible desde el menú principal (pestaña Operaciones -> Monitor del dispositivo) o desde el menú de acceso rápido: icono de monitor. Tras seleccionar esta opción, aparecerá un mensaje pidiendo que se ejecute el programa externo Device Monitor.

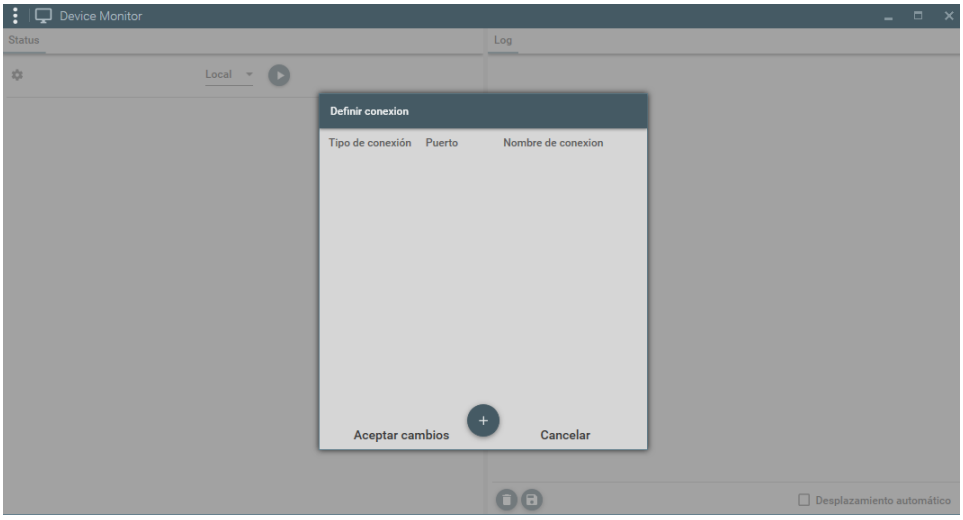


Este programa se instala por defecto junto con el Configurador de transmisores GPRS.

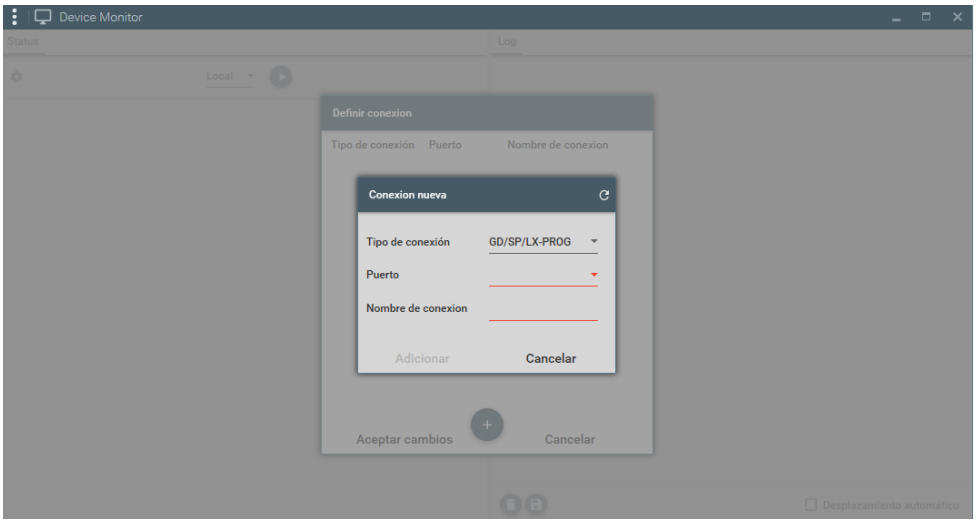


Para utilizar esta funcionalidad, conecte la centralita a un ordenador PC utilizando el cable de programación GD-PROG, SP-PROG/SP-PROG-BT o MINI-PROG-BT en el modo DEBUG

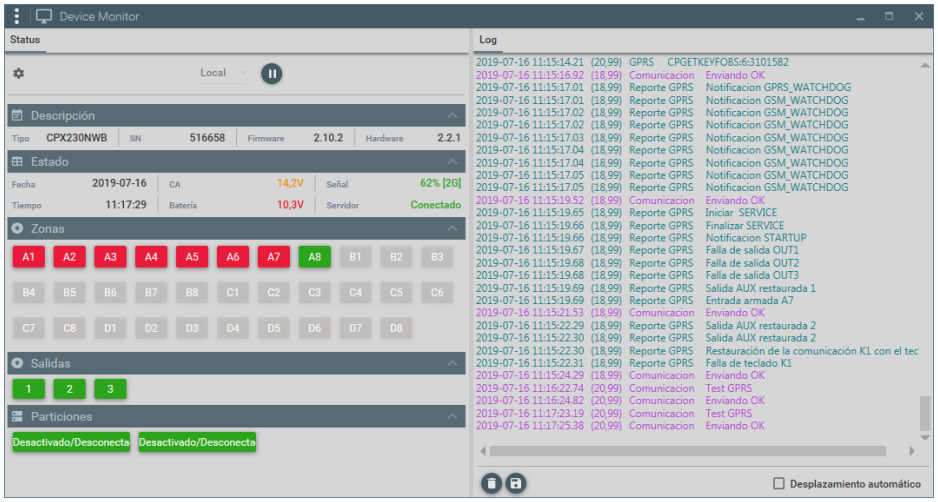
(MONITOR). A continuación, defina la conexión haciendo clic en (esquina superior izquierda). Aparecerá la ventana:



después de pulsar «+» y definir el tipo, puerto y nombre de la conexión, podrá añadir una nueva conexión.



Una vez aceptados los cambios, en el campo «Port» aparecerá la conexión definida. Selecciónela y pulse «Play». El monitor muestra información sobre el tipo de dispositivo, el número de serie, la versión de firmware y del circuito impreso, y la hora ajustada en el dispositivo:



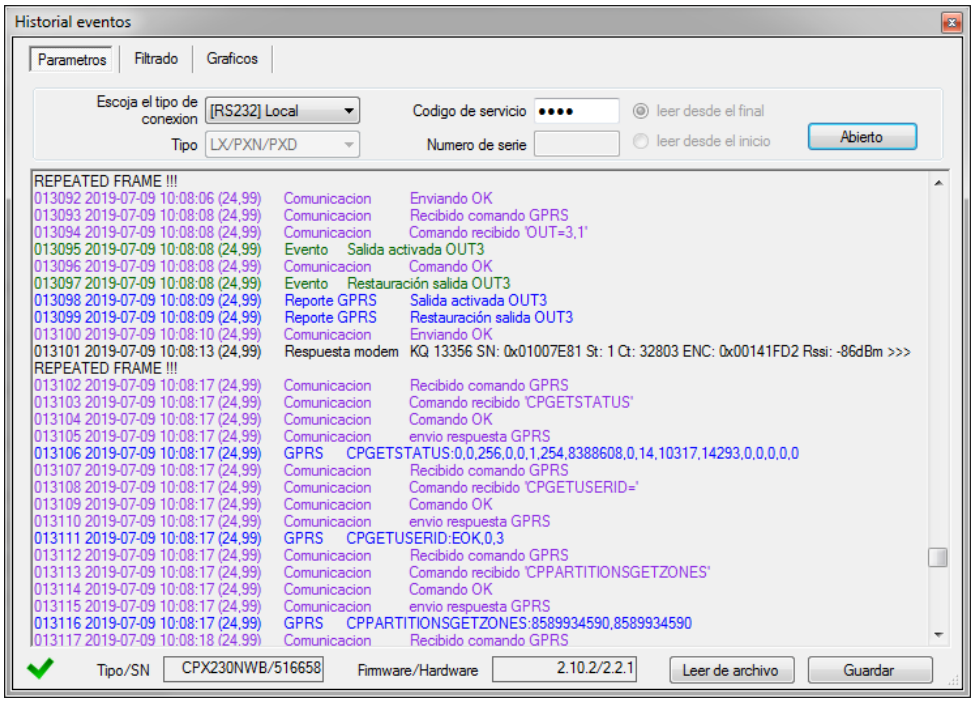
Device Monitor también permite controlar los siguientes parámetros en tiempo real:

- Estado de la alimentación de red
- Nivel de señal de red GSM
- Estado de la conexión al servidor OSM.Server (estación de monitoreo)
- Estado de las líneas (entradas) alámbricas e inalámbricas: al desplazar el cursor sobre la línea, aparece información adicional, como por ejemplo:
    - Modo de entrada, por ejemplo alámbrico (NO)
    - Número de serie
    - Tipo de respuesta, por ejemplo inmediata, sabotaje 24h
    - Nivel de señal
    - Estado: no violado, alarma, sabotaje o no utilizado (detector do asignado a ninguna partición)
- Estado de salidas
- Estado de armado

Además, bajo cada bloque con número de línea aparece el nivel de señal RSSI del detector.

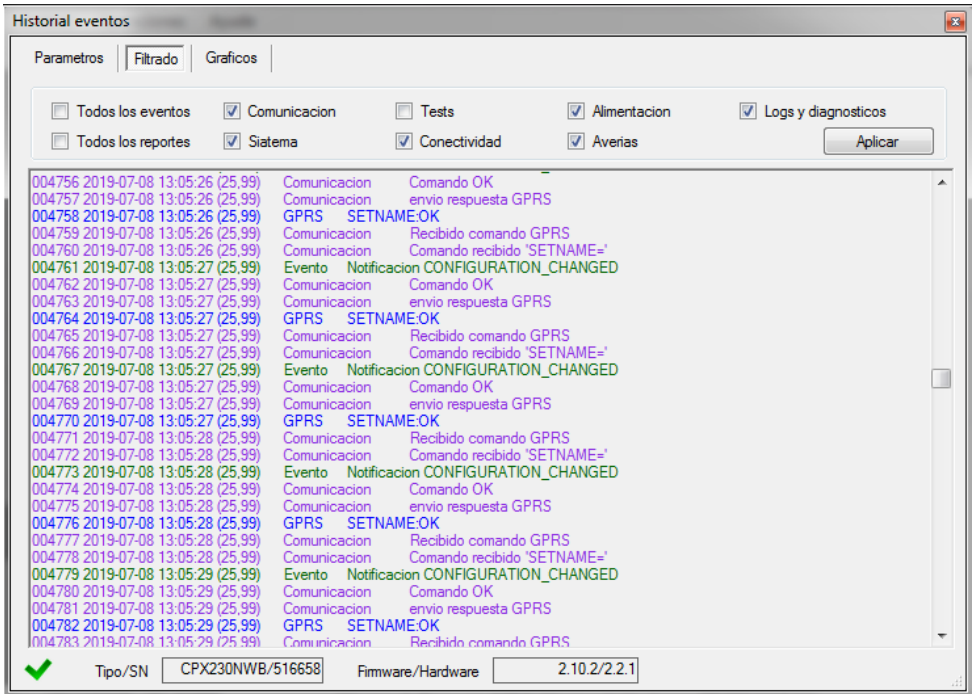
Los cambios de todos los parámetros son visibles también en forma de texto en el campo Log.

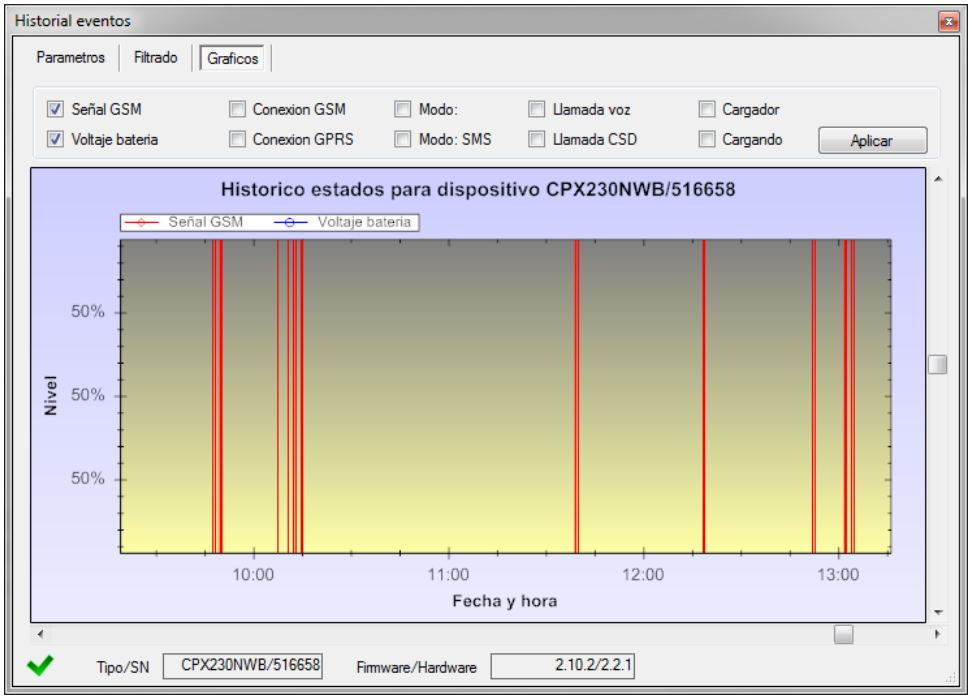
6.12. HISTORIAL DE EVENTOS



La función permite leer los últimos eventos guardados en la memoria del dispositivo. El transmisor tiene la memoria destinada para registrar los eventos, lo cual permite memorizar unos 5 mil últimos eventos técnicos. Es posible la lectura del historial tanto por medio de la conexión GPRS como RS232. En el segundo caso, en primer lugar se debe conectar el dispositivo al ordenador PC por medio del cable GD-PROG. Luego, en la

ventana «Historial de eventos» se debe seleccionar el respectivo puerto RS232 o bien la comunicación GPRS, introducir el código de acceso y hacer clic en «Lectura». Después de la lectura correcta será posible el acceso a tales funciones como «Filtrado» y «Diagramas» gracias a los cuales podremos diagnosticar rápidamente el dispositivo.





7. SEÑALIZACIÓN CON DIODOS LED

El dispositivo indica el estado actual por medio de los 3 diodos LED, montados directamente en la placa impresa.

7.1. REGISTRO EN LA RED

Al introducir la tarjeta SIM en el dispositivo y al activar la alimentación tendrá lugar una prueba de registro en la red GSM.

Descripción	Diodos LED		
	Aceptar (verde)	ERROR (rojo)	ESTADO (amarillo)
Prueba de registro en la red GSM			

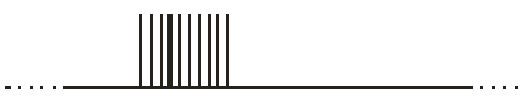
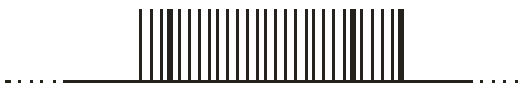
7.2. ALCANCE DE GSM

La fuerza de la señal GSM se indica mediante el parpadeo del diodo verde (1-8 parpadeos). El modo de trabajo del dispositivo se avisa por medio de iluminación durante unos 2 segundos del diodo verde después de mostrar la cobertura. Si, después de mostrar el rango, el diodo no se enciende durante 2 segundos, esto significa el modo SMS del dispositivo. La señalización de la cobertura está interrumpida durante la transmisión de datos y, luego, después de enviar los datos se vuelve a enseñar la cobertura GSM.

Descripción	Diodos LED		
	Aceptar (verde)	ERROR (rojo)	ESTADO (amarillo)
Cobertura GSM = 8 **Modo GPRS**			
Cobertura GSM = 6 **Modo SMS**			

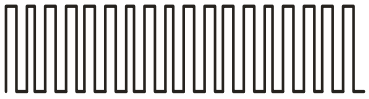
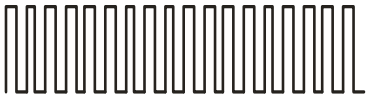
7.3. TRANSMISIÓN

Durante la transferencia de datos el diodo verde señala la transmisión.

Descripción	Diodos LED		
	Aceptar (verde)	ERROR (rojo)	ESTADO (amarillo)
Transmisión GPRS			
Transmisión SMS			

7.4. PROGRAMACIÓN

Después de detectar el modo de programación, los diodos empiezan a señalar el estado de programación.

Descripción	Diodos LED		
	Aceptar (verde)	ERROR (rojo)	ESTADO (amarillo)
Conectado conducto de servicio			
Programación en el modo CSD			

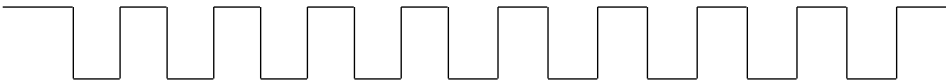
7.5. ACTUALIZACIÓN DE FIRMWARE

Durante la programación se señala el funcionamiento de bootloader. Si se produce un error durante la actualización, el cargador de arranque que permanece en el dispositivo permite volver a programarlo.

Descripción	Diodos LED		
	Aceptar (verde)	ERROR (rojo)	ESTADO (amarillo)
Falta de programa en el dispositivo			
Actualización de software			
Descodificación de firmware recibido			

7.6. NO HAY TARJETA SIM O LA TARJETA SIM ESTÁ DAÑADA

En caso de problemas con la tarjeta SIM el dispositivo lo va a señalar con el diodo rojo ERROR y verde OK.

Diodo LED	Señalización
OK (verde)	
ERROR (rojo)	

7.7. ERROR DEL SISTEMA

Pueden producirse errores durante el funcionamiento. La existencia del error se señala al iluminar para siempre el diodo rojo y con más frecuencia significa el problema de comunicación con el módem o con la tarjeta SIM.

8. AJUSTES GRADE 2

8.1. AJUSTES DEL SISTEMA PARA GRADE 2

Para cumplir con los requisitos de la norma EN 50131 para el Grade 2:

- Ajustar el retardo de entrada a no más de 45 segundos.
- Las salidas de señalización de alarma deben configurarse de forma que la duración de los avisos sonoros no sea inferior a 90 segundos ni superior a 15 minutos.
- Ajustar la sensibilidad de la línea a 400 ms como máximo.
- El número de violaciones antes del bloqueo debe ser de 3 a 10.
- El tiempo después del cual se informa de un fallo de alimentación no debe ser superior a 60 minutos (véase el capítulo 4.3.2. Desaparición de alimentación y el punto 6.6.1.3. Desaparición de alimentación).
- Utilizar códigos de usuarios con una longitud mínima de 5 caracteres.
- Conectar la centralita a une fuente de alimentación de emergencia (batería de 12 V). La capacidad de la batería debe garantizar una autonomía mínima de 12 horas.
- En el Configurador (véase el capítulo 6.4. OPCIONES DEL SISTEMA) o en el menú de instalador (véase el capítulo 4.3.4. Opciones del sistema), configurar las siguientes opciones del sistema:

  – habilitar la opción «Aviso de fallos memorizados mediante el parpadeo del diodo SYSTEM»,

  – deshabilitar la opción «Ignorar fallo ATS»,

  – habilitar la opción «Confirmar el armado en caso de fallo (botón #)»,

  – habilitar la opción «Acceso al historial requiere autorización»,

  – habilitar la opción «Sin visualizar el estado de alarmas y bloqueos»,

  – habilitar la opción «Bloqueo temporal del teclado tras tres intentos de acceso fallidos».
- En el Configurado, en la opción Monitoreo (véase el capítulo 6.6.1.), habilitar el monitoreo de eventos (seleccionar las columnas: Act. GPRS, Desact. GPRS, Act. SMS, Desact. SMS):

  – Líneas A1 – D8,

  – Sabotaje de líneas A1 – D8,

  – Sabotaje de salida 1 – 3,

  – Alimentación,

  – Batería,

– Interferencias,
– Fallo de alimentación del teclado,
– Fallo de la salida de alimentación AUX1,
– Fallo de la salida de alimentación AUX2,
– Pérdida de comunicación con el teclado,
– Sabotaje del teclado,
– Alimentación del teclado demasiado baja,
– Fallo en la hora.

8.2. COMPORTAMIENTO DEL SISTEMA EN EL MODO DE COMPATIBILIDAD CON GRADE 2

En el modo de compatibilidad con los requisitos de la norma EN 50131 para el Grado 2, el sistema funciona de la siguiente manera:

- el acceso a la consulta del estado de línea sólo es posible después de la autorización,
- el acceso a la consulta de alarmas sólo es posible después de la autorización,
- el acceso a la consulta de alarmas históricas sólo es posible después de la autorización,
- el acceso a la consulta de fallos sólo es posible después de la autorización,
- el acceso a la consulta de fallos históricos sólo es posible después de la autorización,
- el armado sólo es posible después de la autorización,
- antes del armado se comprueba que no hay condiciones que impidan el armado,
- los códigos de usuarios deben tener al menos 5 caracteres,
- después de introducir el código incorrecto tres veces, todos los teclados del sistema se bloquean durante 90 segundos.

9. ADITIVOS

9.1. COMANDOS REMOTOS Y PARÁMETROS DE CONFIGURACIÓN

La centralita recibe los mensajes SMS en la forma especialmente preparada para ella. Cuando el mensaje SMS recibido por el dispositivo no sea correcto, será eliminado inmediatamente y el dispositivo no empezará ninguna actividad. Se aprueba el siguiente formato de mensaje que permite por medio de un mensaje SMS enviar unos comandos y cada uno de ellos debe estar separado del anterior con el ESPACIO:

CÓDIGO DE ACCESO COMANDO/PARÁMETRO COMANDO/PARÁMETRO .....

donde:

CÓDIGO DE ACCESO – código de autorización, puede ser el código de servicio (enviado por ATS), el código de usuario o de administrador. Cuando el comando requiera autorización con el código de administrador (por ejemplo CPGETUSERS), este código se debe introducir solamente una vez o bien como código de acceso o bien como parámetro de comando. En otras palabras, cuando el código de acceso no es código de administrador y el comando llamado lo requiera, entonces el código de administrador deberá ser introducido como su parámetro.

– espacio

COMANDO/PARÁMETRO – comando o parámetro de configuración (véase las tablas a continuación)

El parámetro nuevamente enviado se tendrá en cuenta en el momento cuando la centralita quiera usarlo, lo cual significa que se requiere el reinicio del dispositivo. Sin embargo, hay parámetros cuyo cambio sólo se detectará en casos especiales; por ejemplo, si se ha cambiado la dirección del servidor y el dispositivo está actualmente en línea, se debe desconectar la conexión. Después de volver a conectar, el dispositivo se conectará al servidor con la dirección fijada por el usuario.

Para borrar el parámetro, se debe introducir en el mensaje el nombre de parámetro y, luego, el símbolo de igualdad (=). Por ejemplo, para eliminar el número de teléfono al que se envían los mensajes SMS, se debe enviar el mensaje «XXXX SMS=», siendo XXXX el código de servicio del dispositivo.

ATS (Alarm Transmission System) es un tipo especial de usuario que representa la estación de monitoreo. Este usuario se autentifica mediante el código de acceso principal (el mismo que debe ingresarse para leer la configuración con un cable) o mediante las claves de encriptación de la transmisión: si el comando se envía por vía encriptada, el código de acceso no es necesario.

Usuario – (usuario normal) puede armar y desarmar las particiones para las que tiene permisos y realizar otras operaciones descritas en el manual de usuario. Puede haber varios usuarios normales en el sistema.

Administrador – Usuario especial con permisos para añadir y eliminar otros usuarios del sistema de alarma.

Nota: Algunos componentes de los comandos se presentan entre corchetes […]. Esto significa que se trata de campos opcionales.

9.1.1. Parámetros de configuración

9.1.1.1. APN

Formato:	APN=nombre_apn
Restricciones:	Número de caracteres - 31, es posible cambiar solamente a través de ATS
Descripción	Configura APN por medio del que se envían los datos por medio de GPRS.

9.1.1.2. UN

Formato:	UN=username
Restricciones:	Número de caracteres - 31, es posible cambiar solamente a través de ATS
Descripción	Fija el nombre de usuario para APN

9.1.1.3. PW

Formato:	PW=password
Restricciones:	Número de caracteres - 31, es posible cambiar solamente a través de ATS
Descripción	Fija la contraseña para APN

9.1.1.4. SERVER

Formato:	SERVER=direccion_servidor
Restricciones:	Número de caracteres - 31, es posible cambiar solamente a través de ATS
Descripción	Fija la dirección del servidor OSM con el que el dispositivo intercambia los datos. La direccion_servidor puede introducirse en forma de dominio, por ejemplo, .device.miempresa.com o bien la dirección IP, por ejemplo, 1.2.3.4

9.1.1.5. PORT

Formato:	PORT=puerto
Restricciones:	Número del intervalo 1-65535, es posible modificar solamente por medio de ATS
Descripción	Fija el puerto del servidor OSM con el que el dispositivo intercambia los datos

9.1.1.6. DNS1

Formato:	DNS1=dns1
Restricciones:	Dirección IPv4 correcta en forma numérica (hasta 15 caracteres), modificable sólo por ATS
Descripción	Determina la dirección del DNS primario (requerido solamente cuando SERVER está guardado en forma del nombre de dominio).

9.1.1.7. DNS2

Formato:	DNS2=dns2
Restricciones:	Dirección IPv4 correcta en forma numérica (hasta 15 caracteres), modificable sólo por ATS
Descripción	Determina la dirección del DNS secundario (requerido solamente cuando SERVER está guardado en forma del nombre de dominio).

9.1.1.8. SMS

Formato:	SMS=número_teléfono
Restricciones:	Número de caracteres - 15, es posible cambiar solamente a través de ATS
Descripción	Fija el número de teléfono al que se enviarán los mensajes SMS con los eventos en caso de la falta de comunicación GPRS. Cuando el número no esté configurado, el envío de los mensajes SMS no estará disponible. número_teléfono puede contener el prefijo del país.

9.1.1.9. SMSPERIOD

Formato:	SMSPERIOD=tiempo_en_minutos
Restricciones:	Cadena de caracteres que indica un número, sólo modificable por ATS
Descripción	Fija el periodo de pruebas SMS, el tiempo se da en minutos.

9.1.1.10. RLIMIT

Formato:	RLIMIT
Restricciones:	Sólo ejecutable por el ATS.
Descripción	Ocasiona la eliminación de los bloqueos temporales de todas las entradas
Formato:	RLIMIT=máscara_entrada
Restricciones:	Sólo ejecutable por el ATS.

Descripción	Elimina los bloqueos temporales de las entradas seleccionadas. El parámetro es un número decimal creado a partir de una palabra de 17 bits: A17,A16… A2, A1, donde A1=0, A2 = entrada 1, A3 = entrada 2, A17 = entrada 16. EJEMPLO RLIMIT=6 (00000000000000110) elimina el bloqueo de las entradas: IN1, IN2 RLIMIT=2 ocasiona la eliminación de bloqueo de la entrada IN1

9.1.1.11. DT

Formato:	DT=YY/MM/DD,hh:mm
Restricciones:	Longitud de datos hasta 14 caracteres, es posible cambiar solamente por medio de ATS o por el administrador
Descripción	Fija la fecha y la hora

9.1.1.12. SETMASK

Formato:	SETMASK=id_tipo,índice,máscara
Restricciones:	*id_tipo* puede tomar valores de 0, 1 o 2, modificable sólo por ATS
Descripción	Es un comando de bajo nivel que afecta directamente a la memoria de configuración del dispositivo. Este comando no genera ningún evento: tras habilitar una función, se recibe la información de que se ha modificado la configuración del dispositivo. PARA: SETMASK=2,19,0x100 Activación de la función ***Bloqueo de la instalación*** que impide al usuario armar la centralita. Tras activar esta función, el usuario no podrá armar la instalación de ninguna manera (por ejemplo, SMS/GPRS, control remoto, entrada de armado, horarios, teclado normal, teclado inalámbrico). Sin embargo, será posible desarmarla. Todo intento de armado será rechazado por la centralita. SETMASK=2,19,0x200 Activación de la función ***Bloqueo de restauración de los ajustes predeterminados*** que impide que se restaure el código de instalador predeterminado. Tras activar esta función es recomendable cambiar el código de acceso del instalador y el código de servicio (ATS). **ATENCIÓN: En caso de pérdida de los nuevos códigos, será necesario enviar los dispositivos bloqueados al servicio de EBS.** SETMASK=2,19,0x400 Activación de la función ***Permitir el armado rápido sin autorización del usuario*** que permite armar el sistema sin necesidad de introducir el código de acceso.

9.1.1.13. CLEARMASK

Formato:	CLEARMASK=id_tipo,índice,máscara
Restricciones:	*id_tipo* puede tomar valores de 0, 1 o 2, modificable sólo por ATS
Descripción	Es un comando de bajo nivel que afecta directamente a la memoria de configuración del dispositivo. Este comando no genera ningún evento: tras habilitar una función, se recibe la información de que se ha modificado la configuración del dispositivo. PARA: CLEARMASK=2,19,0x100 Desactivación de la función ***Bloqueo de la instalación***. Después de desactivar esta función, el usuario podrá armar y desarmar la centralita. CLEARMASK=2,19,0x200 Desactivación de la función ***Bloqueo de restauración de los ajustes predeterminados***. Después de desactivar esta función, será posible restablecer el código de instalador predeterminado con el botón «PROG» situado en la centralita o desde el Configurador. CLEARMASK=2,19,0x400 Desactivación de la función ***Permitir el armado rápido sin autorización del usuario***. Después de desactivar esta función, solo será posible armar el sistema introduciendo el código de acceso.

9.1.2. Comandos generales

Estos comandos permiten realizar remotamente diferentes acciones o consultar ciertos parámetros. Cuando el comando se envíe por SMS, la respuesta será reenviada al número de teléfono desde el que vino el comando. No envíe varios comandos de este conjunto en un SMS o marco, ya que sólo se ejecutará un comando, y no tiene que ser necesariamente el primer comando de la lista.

9.1.2.1. DISC

Formato:	DISC
Restricciones:	Sólo ejecutable por el ATS
Descripción	Desconecta la conexión TCP del servidor OSM

9.1.2.2. KILL

Formato:	KILL
Restricciones:	Sólo ejecutable por el ATS
Descripción	Provoca reinicio del módem GSM en el dispositivo. Ocasiona la interrupción de la sesión GPRS y el deregistro de la red GSM, y después de reiniciar el módem vuelve a registrarse en la red GSM y GPRS

9.1.2.3. RESET

Formato:	RESET
Restricciones:	Sólo ejecutable por el ATS
Descripción	Provoca reinicio del dispositivo. Interrumpe la sesión GPRS y se desconecta de la red GSM; después de reiniciar el dispositivo y el módem, se registra de nuevo en la red GSM y GPRS

9.1.2.4. DESC

Formato:	DESC
Restricciones:	Sólo ejecutable por el ATS
Descripción	Devuelve la descripción del dispositivo que incluye la versión de firmware y el número de serie.

9.1.2.5. GETCFG

Formato:	GETCFG
Restricciones:	Devuelve un máximo de 160 caracteres, ejecutable sólo por el ATS
Descripción	Descarga la configuración actual y básica del dispositivo. Los parámetros se devuelven en el siguiente orden: SERVER:PORT, _APN_UN_PW,_DNS0 Siendo: _ – símbolo de espacio *SERVER* – dirección del servidor OSM *PORT* – puerto del servidor OSM *APN* – nombre de apn con el que se establece la sesión GPRS *UN* – nombre de usuario APN *PW* – contraseña APN *DNS0* – Dirección del servidor DNS

9.1.2.6. OUT

Formato:	OUT=o,s,[tiempo]
Restricciones:	Es posible realizar solamente por medio de ATS o por el administrador

Descripción	Ajusta el estado «s» en la salida «o». *o* – número de salida (1–3) *s* – estado de destino(1 – activo, 0 – inactivo) *tiempo* – en caso de activación de la salida, se puede especificar la duración de la activación en segundos. 0 significa el modo biestable. Si no se especifica este parámetro, la salida se activará durante el tiempo especificado durante la configuración. La salida puede desactivarse en cualquier momento mediante un comando remoto, independientemente de su tipo y modo de funcionamiento. Ejemplos: OUT=2,1 – activación de la salida 2 durante el tiempo configurado OUT=2,0 – desactivación de la salida 2 OUT=1,1,0 – activación de la salida 1 en modo biestable OUT=3,1,10 – activación de la salida 3 durante 10 segundos

9.1.2.7. FLUSH

Formato:	FLUSH=x
Restricciones:	x es igual a 0 o 1, sólo ejecutable por ATS
Descripción	Para x = 0 borra la cola de eventos pendientes de enviar al servidor OSM. Provoca la pérdida de los eventos pendientes – el dispositivo genera un evento que informa de ello. Para x = 1 borra el historial de eventos del dispositivo.

9.1.2.8. SENDSMS

Formato:	SENDSMS=nº_teléfono,text_sin_espacios SENDSMS=”nº_teléfono,text_sin_espacios”
Restricciones:	El comando no funciona cuando se envía por SMS, ejecutable sólo por el ATS
Descripción	Permite enviar un mensaje SMS al número de teléfono especificado (n°_teléfono) con el contenido especificado. El comando permite conseguir información sobre el número de teléfono de la tarjeta SIM instalada en el dispositivo cuando éste está conectado al servidor OSM por medio de GPRS.

9.1.2.9. GETSTATUS

Formato:	GETSTATUS
Restricciones:	Es posible de realizar por medio de ATS, administrador o usuario.
Descripción	Descarga el estado actual del dispositivo. Los datos devueltos tienen el siguiente formato: líneas,particiones,salidas,tensión_batería,tensiónAC,0x0,0x0, bloqueos_líneas Siendo: *líneas* – estado actual de línea. Es el vector de bits, siendo el bit 1 (contando desde 0) significa la línea 1, el bit 2 la línea 2, etc. En caso de violar la línea, el bit está fijado (igual a 1) *particiones* – estado actual de las particiones. Es el vector de bits siendo el bit 0 la partición 1, y el bit 1 – la partición 2 (de otra forma que para la línea y para las salidas siendo el bit 1 la línea/salida 1). Cuando la partición está rearmada o se realiza la cuenta a atrás hasta la salida, está fijado el respectivo bit. *salidas* – estado actual de las salidas. Es el vector de bits siendo el bit 1 (contando desde 0) la salida 1, el bit 2 – la salida 2, y el bit 3 – la salida 3. Cuando la salida está activada, el bit está fijado *tensión_batería* – tensión de la batería en mV (12000 = 12V). Cuando la batería no está conectada, las lecturas pueden ser incorrectas y ser unos 9V (9000) *tensión_CA* – tensión CA en los bornes CA CPX230NWB (detrás del transformador) en mV (18000 = 18V) *bloqueo_líneas* – estado actual de bloqueo de las líneas. Es el vector de bits, siendo el bit 1 (contando desde 0) significa la línea 1, el bit 2 la línea 2, etc. En caso de bloquear la línea, el bit está fijado.

9.1.2.10. CPGETALARMSHOWTIME

Formato:	CPGETALARMSHOWTIME
Restricciones:	Es posible de realizar por medio de ATS, administrador y usuario
Descripción	Este comando se utiliza para recuperar los ajustes del tiempo después del cual se desactiva la señalización de alarmas históricas. El tiempo se cuenta desde el desarmado de la partición. El comando devuelve: CPGETALARMSHOWTIME:delay – si la función «Desactivar la señalización de alarmas históricas tras el desarmado» está activa, *delay* es el tiempo en segundos CPGETALARMSHOWTIME:OFF – si la función «Desactivar la señalización de alarmas históricas tras el desarmado» no está activa

9.1.2.11. CPSETALARMSHOWTIME

Formato:	CPSETALARMSHOWTIME=delay
Restricciones:	Ejecutable por el ATS, el administrador o el instalador, siempre y cuando tenga permisos de servicio
Descripción	Este comando se utiliza para establecer el tiempo después del cual se desactiva la señalización de alarmas históricas. El tiempo se cuenta desde el desarmado de la partición. Esta funcionalidad también se puede deshabilitar. El parámetro *delay* es el valor de retardo en segundos (0-9999999) o el texto *OFF* para deshabilitar la funcionalidad (la señalización no se desactiva). Con el valor cero, la señalización de alarmas de desactiva en el momento de desarmado. El comando devuelve: CPSETALARMSHOWTIME:EOK – ejecución correcta CPSETALARMSHOWTIME:EEFORMAT – formato de comando o rango del parámetro *delay* incorrectos Ejemplos: CPSETALARMSHOWTIME=20 – tiempo de retardo 20 segundos CPSETALARMSHOWTIME=OFF – si la función «Desactivar la señalización de alarmas históricas tras el desarmado» no está activa

9.1.2.12. CPGETACN

Formato:	CPGETACN
Disponible a partir de la versión:	2.8.8
Restricciones:	Ejecutable por el ATS o el instalador, siempre y cuando tenga permisos de servicio
Descripción	Este comando se utiliza para recuperar la configuración del número de cuenta para el protocolo Contact ID. El comando devuelve: CPGETACN:EOK,system[,acn_id:acn_value]… Siendo: *system* – valor ALL (para eventos del sistema enviados a todas las cuentas) o ACN0 (para eventos del sistema enviados a la cuenta ACN0) *acn_id* – identificador de la cuenta ACN, 0 para ACN0, 1 para ACN1, 2 para ACN2. *acn_value* – número de cuenta en formato hexadecimal Son posibles 3 pares (acn_id:acn_value), uno para cada cuenta. Ejemplos de valores devueltos: CPGETACN:EOK:ALL,0:0x1234,1:0x1235,2:0x1236

9.1.2.13. CPSETACN

Formato:	CPSETACN=system[,acn_id:acn_value]…
Disponible a partir de la versión:	2.8.8
Restricciones:	Ejecutable por el ATS o el instalador, siempre y cuando tenga permisos de servicio
Descripción	Este comando se utiliza para cambiar la configuración del número de cuenta para el protocolo Contact ID. Permite ajustar o eliminar todos los números ACN. *system* – valor ALL (para eventos del sistema enviados a todas las cuentas) o ACN0 (para eventos del sistema enviados a la cuenta ACN0) *acn_id* – identificador de la cuenta ACN, 0 para ACN0, 1 para ACN1, 2 para ACN2 acn_value – número de cuenta de dos bytes (de preferencia en formato hexadecimal: 0xFFFF) Son posibles 3 pares (acn_id:acn_value), uno para cada cuenta. **ATENCIÓN:** • Si sólo se especifica ACN0, se eliminarán los números ACN1 y ACN2. • Los números de cuenta pueden ser idénticos, por ejemplo, ACN2 puede ser el mismo que ACN1, y ACN1 puede ser el mismo que ACN0. • Es recomendable especificar todos los tres números ACN. De lo contrario, pueden tomar los valores de otros números de cuenta proporcionados en los parámetros. • La centralita considera las siguientes tres situaciones como correctas y acepta una de ellas según los argumentos del comando: o Ningún número de cuenta o Solo la cuenta principal (ACN0) o Todos los números de cuenta (ACN0, ACN1, ACN2) El comando devuelve: CPSETACN:EOK – ejecución correcta CPSETACN:EFORMAT – formato de comando incorrecto CPSETACN:ERROR-VALUE – rango de acn_value erróneo CPSETACN:EID – rango de acn_id erróneo Ejemplos: CPSETACN=ALL,0:0x1234,1:0x1235,2:0x1236 CPSETACN=ACN0,0:1237

9.1.3. Comandos de gestión de usuarios

9.1.3.1. CPGETUSERS

Formato:	CPGETUSERS[= adminPassword]
Restricciones:	El comando funciona solamente en caso de enviar por vía codificada, se requiere saber la contraseña de administrador (usuario con id == 0). El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador. Es posible realizar solamente por medio de ATS o por el administrador. En el caso de que se ejecute el comando por el ATS, debe introducirse *adminPassword*
Descripción	Recupera la lista de usuarios definidos en el dispositivo. *adminPassword* es la contraseña del administrador del sistema. El comando devuelve: CPGETUSERS:id:name:partitions,… Siendo *id* el número de usuario, *name* el nombre de usuario (puede estar vacío), *partitions* el vector de bits que determina las particiones para las que el usuario tiene permisos: el bit 0 corresponde a la partición 1, el bit 1 a la partición 2. Usuario con id = 0 es el administrador CPGETUSERS:EPERMISIONS Cuando la contraseña de administrador dada es incorrecta CPGETUSERS:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPGETUSERS:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.3.2. CPGETUSERID

Formato:	CPGETUSERID=password
Restricciones:	El comando funciona solamente cuando enviado por vía codificada y está activa la opción "Permitir la administración remota de usuarios" en el Configurador. Sólo ejecutable por el ATS
Descripción	Verifica el código de usuario dado como argumento de comando – comprueba que el usuario del código dado existe. *Password* es la contraseña del usuario, *id* es el número del usuario, *partitions* son las particiones para las que el usuario tiene permisos – el bit 0 corresponde a la partición 1, el bit 1 a la partición 2. El comando devuelve: CPGETUSERID:EOK,id,partitions Cuando el usuario del código dado exixte CPGETUSERID:EPERMISIONS Cuando la contraseña es incorrecta CPGETUSERID:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPGETUSERID:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.3.3. CPSETUSERPARTITIONS

Formato:	CPSETUSERPARTITIONS=id,partitions[,adminPassword]
Restricciones:	El comando sólo funciona cuando se envía cifrado, se requiere la contraseña de administrador (usuario con id = 0), id del rango de 1 a 31 inclusive. El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador. Es posible realizar solamente por medio de ATS o por el administrador. En el caso de que se ejecute el comando por el ATS, debe introducirse *adminPassword*
Descripción	Fija los permisos del usuario a la partición. *Id* es el número del usuario al que modificamos los permisos, *partitions* es un vector de bits con particiones para las que el usuario tendrá permisos: el bit 0 corresponde a la partición 1, el bit 1 a la partición 2, *adminPassword* es la contraseña del administrador del sistema. El comando devuelve: CPSETUSERPPARTITIONS:EOK,id,partitions Cuando el cambio de asignación a la partición ha terminado con éxito CPSETUSERPARTITIONS:ENOT_EXISTS,id,partitions Cuando el usuario no existe CPSETUSERPARTITIONS:EPERMISIONS,id,partitions Cuando la contraseña de administrador dada es incorrecta CPSETUSERPARTITIONS:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPSETUSERPARTITIONS:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.3.4. CPSETUSERPASSWORD

Formato:	CPSETUSERPASSWORD=id,password[,adminPassword]
Restricciones:	El comando sólo funciona cuando se envía cifrado, se requiere la contraseña de administrador (usuario con id = 0), id del rango de 1 a 31 inclusive. El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador. Es posible realizar solamente por medio de ATS o por el administrador. En el caso de que se ejecute el comando por el ATS, debe introducirse *adminPassword*
Descripción	Cambia la contraseña del usuario. *Id* es identificador del usuario cuya contraseña se cambia, *password* es su nueva contraseña y *adminPassword* es la contraseña del administrador del sistema. El comando devuelve: CPSETUSERPASSWORD:EOK,id Cuando el comando ha terminado con éxito CPSETUSERPASSWORD:ENOT_EXISTS,id Cuando el usuario no existe CPSETUSERPASSWORD:EPERMISIONS,id Cuando la contraseña de administrador dada es incorrecta CPSETUSERPASSWORD:ELENGTH,id Cuando la contraseña es demasiado corta o larga o no está compuesta de dígitos CPSETUSERPASSWORD:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPSETUSERPASSWORD:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.3.5. CPADDUSER

Formato:	CPADDUSER=id,partitions,password[,category][,adminPassword]
Restricciones:	El comando sólo funciona cuando se envía cifrado, se requiere la contraseña de administrador (usuario con id = 0), id del rango de 1 a 31 inclusive. El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador. Es posible realizar solamente por medio de ATS o por el administrador. En el caso de que se ejecute el comando por el ATS, debe introducirse *adminPassword*
Descripción	Añade a un nuevo usuario. *Id* es número de usuario, *partitions* son particiones para las que el usuario tendrá permisos – bit 0 corresponde a la partición 1, bit 1 a la partición 2, *password* es contraseña del nuevo usuario, *category* – toma valor *NODISARM* – si se especifica, el usuario no podrá desarmar la partición (disponible a partir de la versión de firmware 2.8.8) , *adminPassword* – si el comando se envía a través de ATS, debe inhgresarse la contraseña de administrador. El comando devuelve: CPADDUSER:EOK,id,partitions En caso de añadir al usuario CPADDUSER:EALREADY_EXISTS,id,partitions Cuando el usuario dado ya existe CPADDUSER:EID,id,partitions Cuando la identificación del usuario dado es incorrecta CPADDUSER:EPERMISIONS,id,partitions Cuando no se puede crear a un usuario porque la contraseña es incorrecta (de administrador o de usuario) CPADDUSER:ELENGTH,id Cuando la contraseña es demasiado corta o larga o no está compuesta de dígitos CPADDUSER:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPADDUSER:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.3.6. CPDELUSER

Formato:	CPDELUSER=id[,adminPassword]
Restricciones:	El comando sólo funciona cuando se envía cifrado, se requiere la contraseña de administrador (usuario con id = 0), id del rango de 1 a 31 inclusive. El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador. Es posible realizar solamente por medio de ATS o por el administrador. En el caso de que se ejecute el comando por el ATS, debe introducirse *adminPassword*
Descripción	Elimina al usuario. *Id* es número de usuario, *adminPassword* es la contraseña del administrador del sistema. El comando devuelve: CPDELUSER:EOK,id Cuando el usuario esté eliminado CPDELUSER:ENOT_EXISTS,id Si el usuario especificado no existe o si se intenta eliminar el administrador o instalador CPDELUSER:EPERMISIONS,id Cuando no se pueda eliminar al usuario porque la contraseña de administrador es incorrecta CPDELUSER:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPDELUSER:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.3.7. CPSETADMINPASSWORD

Formato:	CPSETADMINPASSWORD=newPassword
Restricciones:	El comando sólo funciona cuando se envía cifrado, no se requiere la contraseña de administrador (usuario con id = 0). El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador. Es posible realizar solamente por medio de ATS o por el administrador.
Descripción	Modifica la contraseña del usuario principal – administrador del sistema. Este comando permite restaurar la contraseña olvidada de forma remota (por el personal de la estación de monitoreo). *newPassword* es la nueva contraseña del usuario principal. El comando devuelve: CPSETADMINPASSWORD:EOK CPSETADMINPASSWORD:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPSETADMINPASSWORD:ELENGTH Cuando la contraseña es demasiado corta o larga o no está compuesta de dígitos CPSETADMINPASSWORD: EPERMISIONS Cuando la contraseña no puede ser modificada porque está en uso por otro usuario. Cuando la contraseña introducida actualmente es la de administrador, el comando devuelve EOK.

9.1.3.8. CPGETUSERRIGHTS

Formato:	CPGETUSERRIGHTS=id
Restricciones:	Comando disponible a partir de la versión de firmware 2.8.8. Sólo funciona cuando se envía cifrado, se requiere la contraseña de administrador (usuario con id = 0), id se cuenta a partir de 1. El comando requiere fijar la opción activa "Permitir la administración remota de usuarios" en el Configurador.
Descripción	Recupera los permisos del usuario. El parámetro *id* es el número de usuario. El comando devuelve: CPGETUSERRIGHTS:EOK,id,category[,…] Si el usuario existe. Posibles valores del campo *category*: *USER* para un usuario típico, *NODISARM* para un usuario sin derechos de desarme CPGETUSERRIGHTS:ENOT_EXISTS,id Cuando el usuario no existe CPGETUSERRIGHTS:EPERMISIONS,id Contraseña de administrador incorrecta CPGETUSERRIGHTS:ENOT_ALLOWED Cuando el comando fue enviado por SMS público o la configuración no permite la administración remota de usuarios CPGETUSERRIGHTS:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.4. Comandos para administrar particiones, líneas y salidas

9.1.4.1. CPGETSTATUS

Formato:	CPGETSTATUS[=password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	password es contraseña de administrador del sistema o de usuario. El comando devuelve: CPGETSTATUS:Ready,CurrentPartitionAlarms,alarmHistory, otherAlarmHistory,zoneTampers,keypadTampers,zones, zonesLock,partitions,outputs,batteryVoltage,powerSupplyVoltage, silentAlarms,zonesComFailures,zonesPowerFailures,partitionsStay, partitionsNight Siendo: *Ready* toma el valor de 1 si el sistema está listo para el armado, 0 si no lo está. *CurrentPartitionAlarms* es un vector de bits que indica si las particiones están actualmente en estado de alarma. El bit 0 corresponde a la primera partición, el bit 1 corresponde a la segunda partición. *alarmHistory* es un vector de bits que define la memoria de alarmas desde el último armado. El bit 1 (contando desde 0) corresponde a la línea A1, … el bit 7 corresponde a la línea A7. *otherAlarmHistory* es un vector de bits que determina la memoria de alarmas adicionales desde el último armado. El bit 1 (contando desde 0) corresponde al sabotaje del teclado 1, el bit 2 corresponde al sabotaje del teclado 2, el bit 3 corresponde al sabotaje del teclado 3, el bit 7 significa una alarma del mando a distancia. *zoneTampers* es un vector de bits que indica los sabotajes de las líneas. El bit 1 (contando desde 0) corresponde a la línea A1. *keypadTampers* es un vector de bits que indica los sabotajes de los teclados. El bit 0 significa el teclado 1. *zones* – indica el estado actual de las líneas. Es un vector de bits donde el bit 1 (contando desde 0) corresponde a la línea A1, el bit 2 a línea A2, etc. Si se viola la línea, se activa el bit. *zonesLock* – estado actual del bloqueo de líneas. Es el vector de bits, siendo el bit 1 (contando desde 0) significa la línea 1, el bit 2 la línea 2, etc. En caso de bloquear la línea, el bit está fijado. *partitions* – estado actual de las particiones. Es el vector de bits siendo el bit 0 la partición 1, y el bit 1 – la partición 2 (de otra forma que para la línea y para las salidas siendo el bit 1 la línea/salida 1). Cuando la partición está rearmada o se realiza la cuenta a atrás hasta la salida, está fijado el respectivo bit. *outputs* – estado actual de las salidas. Es el vector de bits siendo el bit 1 (contando desde 0) la salida 1, el bit 2 – la salida 2, y el bit 3 – la salida

	3. Cuando la salida está activada, el bit está fijado. *batteryVoltage* – tensión de la batería en mV (12000 = 12V). Cuando la batería no está conectada, las lecturas pueden ser incorrectas y ser unos 9V (9000). *powerSupplyVoltage* – tensión CA en los bornes CA CPX230NWB (detrás del transformador) en mV (18000 = 18V). *silentAlarms* es un vector de bits que define la memoria de alarmas silenciosas desde el último armado (el armado borra la memoria). El bit 1 (contando desde 0) corresponde a la línea A1, … el bit 7 corresponde a la línea A7. *zonesComFailures* – es un vector de bits que indica en qué líneas se perdió la comunicación con el detector (inalámbrico). El bit 1 (contando desde 0) corresponde a la línea A1, … el bit 32 corresponde a la línea D8. *zonesPowerFailures* – es un vector de bits que indica en qué líneas hay problema con alimentación del detector (bajo nivel de batería). El bit 1 (contando desde 0) corresponde a la línea A1, ... el bit 32 corresponde a la línea D8. *partitionsStay* – un vector de bits en el que 1 significa un modo de armado perimetral, 0 significa uno de los demás modos. El bit 0 significa la partición 1. El bit 1 significa la partición 2. *partitionsNight* – un vector de bits en el que 1 significa un modo de armado nocturno, 0 significa uno de los demás modos. El bit 0 significa la partición 1. El bit 1 significa la partición 2. CPGETSTATUS:EPERMISIONS Cuando la contraseña es incorrecta CPGETSTATUS:ENOT_ALLOWED Cuando el comando fue enviado por el mensaje SMS público CPDELUSER:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.4.2. CPGETFAILURES

Formato:	CPGETFAILURES[= password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	*password* es la contraseña de administrador del sistema o de usuario El comando devuelve: CPGETFAILURES:outFailures,powerOutFailures,powerInFailures,keypadCommFailures,keypadPowerFailures,otherFailures Siendo: *outFailures* es un vector de bits que indica los fallos de las salidas. El bit 1 (contando desde 0) significa la salida 1. *powerOutFailures* es un vector de bits que indica los fallos de las salidas de alimentación. El bit 0 significa la salida KPOUT, el bit 1 significa la salida AUX1, el bit 2 la salida AUX2. *powerInFailures* es un vector de bits que indica los fallos de alimentación. El bit 0 significa el fallo de alimentación de red, el bit1 significa el fallo de batería. *keypadCommFailures* es un vector de bits que indica los fallos de comunicación con los teclados. El bit 0 significa el teclado 1. *keypadPowerFailures* es un vector de bits que indica los fallos de alimentación avisados por los teclados. El bit 0 significa el teclado 1. *otherFailures* es un vector de bits que indica los fallos actuales del sistema. El significado de los bits es el siguiente: bit 0 – pérdida de reloj bit 1 – fallo de la memoria de configuración CPGETFAILURES:EPERMISIONS Cuando la contraseña es incorrecta CPGETFAILURES:ENOT_ALLOWED Cuando el comando fue enviado por el mensaje SMS público CPDELUSER:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.4.3. CPSETPARTITIONS

Formato:	CPSETPARTITIONS=[STAY/SLEEP]partitions[,delay][,password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	Rearma las particiones determinadas. *partitions* es un vector de bits que indica cuáles particiones queremos armar. El bit 0 es partición 1, el bit 1 es partición 2. La configuración de bit significa la partición que queremos rearmar. Enviar el comando con el argumento *partitions* igual a cero no tiene mucho sentido, porque nada cambiará: si *partitions* es 0, la contraseña de usuario no se comprobará y el estado devuelto por el comando será igual a EOK. El parámetro *delay* puede tomar el valor *NOW* (armar inmediatamente la partición definida sin esperar el retardo de salida configurado) o *DEFAULT* (armar la partición después del retardo de salida). *Password* es el código del usuario que realiza el armado. De id de usuario al que pertenece el código se realizará el rearme de las particiones dadas. Los frases *STAY* y *SLEEP* antes del vector con particiones son opcionales. *STAY* significa que las particiones se armarán en modo perimetral y *SLEEP* en modo nocturno. Los modos de armado pueden conmutarse libremente. Sin embargo, no es posible armar en modo perimetral una partición sin líneas perimetrales. El comando devuelve: CPSETPARTITIONS=[STAY/SLEEP]partitionsList:EOK – cuando el comando ha sido enviado con el parámetro *NOW* y ejecutado CPSETPARTITIONS=[STAY/SLEEP]partitionsList:EOK,x,y – cuando el comando ha sido enviado con el parámetro *DEFAULT* y ejecutado; x, y – retardos de salida (en segundos) para la partición 1 y 2 respectivamente partitionList es listado de particiones armadas mediante un comando (*partitionList* puede ser diferente del campo *partitions* del comando, si el usuario no tiene permisos para todas las particiones que desea armar). Si se envía un comando para armar ambas particiones (CPSETPARTITIONS=3), independientemente de si una partición (o particiones) está(n) armada(s) o no, se recibe un mensaje sobre el armado de ambas particiones (CPSETPARTITIONS=3:EOK – sólo si el comando ha sido enviado por un usuario que tiene permiso para ambas particiones). CPSETPARTITIONS=[STAY,]partitions:ENOT_ALLOWED cuando se intenta armar en modo perimetral una partición sin líneas perimetrales o cuando se intenta armar durante una alarma. CPSETPARTITIONS=[STAY/SLEEP]partitions,password:EFORMAT – cuando el formato de los datos es incorrecto (*partitions,password* son argumentos del comando) CPSETPARTITIONS=[STAY/SLEEP]partitions:EPERMISIONS – cuando el usuario con la contraseña dada no existe

9.1.4.4. CPUNSETPARTITIONS

Formato:	CPUNSETPARTITIONS=partitions[,password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	Desarma las particiones determinadas. *partitions* es un vector de bits que indica las particiones a desarmar. El bit 0 es partición 1, el bit 1 es partición 2. La configuración de bit significa la partición que queremos desarmar. Enviar el comando con el argumento *partitions* igual a cero no tiene mucho sentido, porque nada cambiará: si *partitions* es 0, la contraseña de usuario no se comprobará y el estado devuelto por el comando será igual a EOK. *Password* es el código del usuario que realiza el desarmado. De id de usuario al que pertenece el código se realizará el desarme de las particiones dadas. El comando devuelve: CPUNSETPARTITIONS =partitionsList:EOK – cuando se ejecutó el comando. *partitionList* es una lista de particiones que han sido desarmadas mediante comando (*partitionList* puede ser diferente del campo *partitions* del comando si el usuario no tiene permisos para todas las particiones que desea desarmar) Si se envía un comando para desarmar ambas particiones (CPUNSETPARTITIONS=3), independientemente de si una partición (o particiones) está(n) desarmada(s) o no, se recibe un mensaje sobre el desarmado de ambas particiones (CPUNSETPARTITIONS=3:EOK – sólo si el comando ha sido enviado por un usuario que tiene permiso para ambas particiones). CPUNSETPARTITIONS=partitions:ENOT_ALLOWED cuando se intenta desarmar la centralita con una alarma activa (se desactivará la alarma). CPUNSETPARTITIONS=partitions,password:EFORMAT – cuando el formato de los datos es incorrecto (*partitions,password* son argumentos del comando) CPUNSETPARTITIONS=partitions:EPERMISIONS – cuando el usuario con la contraseña dada no existe

9.1.4.5. CPZONESLOCK

Formato:	CPZONESLOCK=zones[,password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	Bloquea permanentemente las líneas dadas. Genera eventos *INPUTx_LOCK*. *zones* es un vector de bits que indica las líneas que queremos bloquear. El bit 1 (contando desde 0) significa la línea 1. Enviar comandos con el argumento *zones* igual a 0 no tiene mucho sentido porque nada cambiará. *Password* es la contraseña de administrador del sistema o del usuario que tiene permisos para la partición con las líneas a bloquear. El comando devuelve: CPZONESLOCK:EOK,zones – en caso de realizar el comando CPZONESLOCK:ENOT_ALLOWED Cuando el comando fue enviado por el mensaje SMS público CPZONESLOCK:EFORMAT Cuando el formato del comando enviado sea incorrecto CPZONESLOCK:EPERMISIONS Cuando el usuario no tiene permisos a la respectiva partición CPZONESLOCK:ENOT_EXISTS Cuando el usuario con la contraseña dada no existe

9.1.4.6. CPZONESUNLOCK

Formato:	CPZONESUNLOCK=zones[,password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	Elimina el bloqueo permanente y temporal de las líneas dadas. Genera eventos *INPUTx_UNLOCK*. *zones* es un vector de bits que indica las líneas que queremos desbloquear. El bit 1 (contando desde 0) significa la línea 1. Enviar comandos con el argumento *zones* igual a 0 no tiene mucho sentido porque nada cambiará. *Password* es la contraseña de administrador del sistema o de usuario. El comando devuelve: CPZONESUNLOCK:EOK,zones – en caso de realizar el comando CPZONESUNLOCK:ENOT_ALLOWED Cuando el comando fue enviado por el mensaje SMS público CPZONESUNLOCK:EFORMAT Cuando el formato del comando enviado sea incorrecto CPZONESUNLOCK:EPERMISIONS Cuando el usuario no tiene permisos a la respectiva partición CPZONESUNLOCK:ENOT_EXISTS Cuando el usuario con la contraseña dada no existe

9.1.4.7. CPPARTITIONSGETZONES

Formato:	CPPARTITIONSGETZONES[= password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	*password* es la contraseña de administrador del sistema o de usuario Devuelve el listado de las líneas asignadas a la partición en el formato CPPARTITIONSGETZONES:P1Zones,P2Zones Donde *P1Zones*, *P2Zones* son vectores de bits que indican cuáles líneas están asignadas a la primera y segunda partición respectivamente. El bit 1 (contando desde 0) significa la línea 1. El comando devuelve: CPPARTITIONSGETZONES:EPERMISIONS Cuando la contraseña es incorrecta CPPARTITIONSGETZONES:ENOT_ALLOWED Cuando el comando fue enviado por el mensaje SMS público CPPARTITIONSGETZONES:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.4.8. CPPARTITIONSGETOUTPUTS

Formato:	CPPARTITIONSGETOUTPUTS[= password]
Restricciones:	Se requiere saber la contraseña de administrador o de usuario. Es posible de realizar por medio de ATS, administrador o usuario. Si el comando proviene del ATS y no ha sido autorizado por un código, hay que introducir *password*
Descripción	*password* es la contraseña de administrador del sistema o de usuario Devuelve el listado de las salidas asignadas a la partición en el formato CPPARTITIONSGETOUTPUTS:P1Outputs,P2Outputs Donde *P1Outputs,P2OUtputs* son vectores de bits que indican cuáles entradas están asignadas a la primera y segunda partición respectivamente. El bit 1. (contando desde 0) es la salida 1. El comando devuelve: CPPARTITIONSGETOUTPUTS:EPERMISIONS Cuando la contraseña es incorrecta CPPARTITIONSGETOUTPUTS:ENOT_ALLOWED Cuando el comando fue enviado por el mensaje SMS público CPPARTITIONSGETOUTPUTS:EFORMAT Cuando el formato del comando enviado sea incorrecto

9.1.5. Comandos para la gestión de dispositivos inalámbricos

9.1.5.1. CPGETKEYFOBS/CPGETDETECTORS

Formato:	CPGETKEYFOBS CPGETDETECTORS
Restricciones:	Ejecutable por el ATS
Descripción	El comando devuelve un listado de dispositivos inalámbricos: mandos a distancia (CPGETKEYFOBS) o detectores inalámbricos (CPGETDETECTORS). El comando devuelve: CMD:id:SERIALNO[,id:SERIALNO,...] Donde *id* es el número de dispositivo contado desde 0. Para los mandos a distancia es el número del mando menos 1 (o sea id=0 corresponde al mando n° 1, id=1 al mando n° 2, etc.), para los detectores inalámbricos es el número de la línea menos 1 (id=0 corresponde al detector n° 1, id=1 al detector n° 2, etc.), *SERIALNO* es el número de serie hexadecimal del dispositivo (caracteres 0-9 y A-F) de 7 dígitos CMD:EEMPTY Cuando la base de dispositivos de este tipo está vacía -EBADSOURCE y NAK a nivel de protocolo, Cuando el comando ha sido enviado por un usuario sin permiso para hacerlo

9.1.5.2. CPDETECTORLOST

Formato:	CPDETECTORLOST=? CPDETECTORLOST=hours
Disponible a partir de la versión:	2.8.8
Restricciones:	Ejecutable por el ATS y el instalador, siempre y cuando tenga permisos de servicio
Descripción	EL comando devuelve o ajusta el tiempo (en horas) después del cual se informa del desvanecimiento de los dispositivos inalámbricos. *hours* es el número de horas antes de enviar la información. El valor mínimo es de 2 h, el máximo es de 24 h, el valor por defecto es de 6 h. El comando devuelve: CPDETECTORLOST=minutes – para el comando CPDETECTORLOST=? devuelve el tiempo configurado en la centralita CPDETECTORLOST=:EOK – cuando el comando ha sido ejecutado correctamente CPDETECTORLOST=:EPERMISIONS – cuando no hay permisos o el código es incorrecto CPDETECTORLOST=:EID – cuando el rengo de datos es incorrecto CPDETECTORLOST=:EFORMAT – cuando el formato del comando es incorrecto

9.1.6. Comandos para la gestión de la seguridad de la configuración

9.1.6.1. SETATSPWD

Formato:	SETATSPWD=oldpwd,newpwd
Disponible a partir de la versión:	2.8.3
Restricciones:	Sólo ejecutable por el ATS
Descripción	El comando cambia el código de servicio (ATS) de *oldpwd* a *newpwd*. El comando devuelve: SETATSPWD:EOK – cuando el código se ha cambiado correctamente SETATSPWD:EPERMISIONS – cuando el comando se ha enviado con permisos distintos de ATS o cuando el código de servicio antiguo (ATS) es incorrecto SETATSPWD:ELENGTH – cuando la longitud del nuevo código es incorrecta (menos de 4 o más de 7 caracteres) o cuando el código contiene caracteres no válidos (por ejemplo, espacios, #, etc.) SETATSPWD:EFORMAT - cuando el formato del comando es incorrecto.

9.1.6.2. SETCOMMLOCK

Formato:	SETCOMMLOCK=state,ats_password
Disponible a partir de la versión:	2.8.3
Restricciones:	state puede ser igual a 0 o 1; Sólo ejecutable por el ATS
Descripción	El comando habilita (si *state* igual a 1) o deshabilita (si *state* igual a 0) la opción «Bloqueo de los ajustes de comunicación». Para que el comando funcione, como argumento *ats_password* debe proporcionarse un código de servicio válido (ATS). El comando devuelve: SETCOMMLOCK:state,EOK – cuando se elimina o activa el bloqueo (state indica la operación realizada) SETCOMMLOCK:EPERMISIONS – cuando el comando se ha enviado con permisos distintos de ATS o cuando el código de servicio (ATS) es incorrecto SETCOMMLOCK:EFORMAT – cuando el formato del comando es incorrecto

9.1.6.3. GETCOMMLOCK

Formato:	GETCOMMLOCK
Disponible a partir de la versión:	2.8.3
Restricciones:	Sólo ejecutable por el ATS
Descripción	El comando recupera el estado de la opción «Bloqueo de los ajustes de comunicación» El comando devuelve: GETCOMMLOCK:0 – opción deshabilitada (bloqueo inactivo) GETCOMMLOCK:1 – opción habilitada (bloqueo activo) GETCOMMLOCK:EPERMISIONS cuando se ha enviado con permisos distintos de ATS

9.2. GLOSARIO DE TÉRMINOS

ATS (Alarm Transmission System) – es un tipo especial de usuario que representa la estación de monitoreo y que se autentifica mediante el código principal de acceso.

P1 y P2 – partición 1 y 2 respectivamente, áreas supervisadas por sus líneas (detectores).

AES (Advanced Encryption Standard) – un esquema de cifrado simétrico por bloques, uno de los más populares del mundo. Fue publicado en 1997 por Vincent Rijmen y Joan Daemen y adoptado como un estándar de cifrado por el gobierno de los Estados Unidos en 2002.

NO – una configuración de la línea de entrada que permite identificar dos estados: normal (stadby): relé NO abierto y alarma (violación): relé NO cerrado.

NC – una configuración de la línea de entrada que permite identificar dos estados: normal (stadby): relé NC cerrado y alarma (violación): relé NC abierto.

EOL – configuración paramétrica de la línea de entrada que permite identificar tres estados: normal (standby), alarma (violación) y fallo gracias a una resistencia de fin de línea de 2,2 kΩ.

EOL – configuración paramétrica doble de la línea de entrada que permite identificar cuatro estados: normal (standby), alarma (violación), sabotaje y fallo (por ejemplo cortocircuito del cable) gracias a una doble resistencia de fin de línea de 1,1 kΩ.

TEOL – configuración de la línea de entrada que permite duplicar la línea, es decir conectar dos detectores con cable a un borne de la centralita. Esta configuración permite detectar de qué detector proviene la alarma, la información de sabotaje es compartida. Para cada detector son necesarias dos resistencias.

Chirp – es un sonido corto emitido por una sirena de alarma conectada a una de las salidas OUT de la centralita. Puede ser único (por ejemplo, al armar) o múltiple (por ejemplo, al desarmar).

RS-232 – un estándar de transmisión de datos en serie. Se utiliza en la comunicación entre diferentes dispositivos mediante los puertos COM.

TAMPER – un botón de sabotaje que señala una perturbación deliberada del funcionamiento del sistema de alarma, por ejemplo, la apertura de la carcasa de un detector.

Fallo en la hora – un evento que indica el restablecimiento del reloj que ocurre cuando se apaga la alimentación y se reinicia el sistema.

Alarmas históricas – son alarmas que ocurrieron en el pasado y que ya no están activas.

Watchdog – una opción que permite la respuesta automática del dispositivo cuando se interrumpe la conexión a la estación de monitoreo

10. HISTORIAL DE CAMBIOS

Fecha / Versión / Firmware	Descripción
2017.09.22/ w1.0 / 2.8.7	Primera versión del manual
2017.10.20/ w1.1 / 2.8.7	Información actualizada sobre el Device Monitor y el comando CPSETPARTITIONS
2018.02.12 / 1.2 / 2.9.1	Información añadida sobre la nueva función para los mandos a distancia; información actualizada sobre el direccionamiento de dispositivos; comando CPADDUSER actualizado; nueva función «Usuarios sin permiso de desarme» y comando remoto relacionado CPGETUSERRIGHT; nueva función «Tiempo de detección del desvanecimiento de los detectores inalámbricos» y comando remoto relacionado CPDETECTORLOST; posibilidad de definir números ACN para las cuentas del protocolo Contact ID y comandos remotos relacionados CPSETACN y CPGETACN; opciones del sistema ampliadas;
2018.07.27 / 1.3 / 2.10.0	Añadido nuevo tipo de respuesta para líneas (entradas), añadida información sobre el nuevo método de armado con mando a distancia y la función de envío cíclico de la información de desvanecimiento de los detectores inalámbricos
2018.11.20 / 1.4 / 2.10.0	Información actualizada en el capítulo 6.4.1. Bloqueo de los ajustes de comunicación
2019.05.06 / 1.5 / 2.10.0	Añadida información sobre los detectores MD-10 y GB-10