

EBS

CREATING A SENSE OF SECURITY
SINCE 1989

CENTRALITA DE ALARMAS

CPX230NWB

Manual de instalador

Versión de firmware:	2.12.3
Versión del EBS Config 2.0:	1.17.2
Versión del servidor OSM:	1.5.01.015

DECLARACIÓN DE CONFORMIDAD

Nosotros, EBS Sp. z o.o., declaramos con plena responsabilidad que este producto cumple todos los requisitos de la Directiva 2014/53/UE del Parlamento Europeo y del Consejo de miércoles, 16 de abril de 2014. La copia de la «Declaración de conformidad» se puede encontrar en www.ebssmart.com.

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: dws@ebssmart.com
Asistencia técnica: support@ebssmart.com
Sitio web: www.ebssmart.com



CREATING A SENSE OF SECURITY
SINCE 1989

1. Introducción.....	6
2. FUNCIONES DE LA CENTRALITA.....	7
2.1. Parámetros funcionales.....	7
2.2. Parámetros técnicos.....	8
2.3. Accesorios y aplicaciones.....	9
3. INSTALACIÓN Y CABLEADO.....	10
3.1. Orden de instalación.....	10
3.2. Descripción de los componentes pcb.....	11
3.3. Descripción de las conexiones por tornillos de la centralita.....	14
3.4. Configuración de las líneas de entrada alámbricas.....	15
3.5. Conexión ejemplar de avisador.....	17
3.5.1. Avisador interno sin propia alimentación.....	17
3.5.2. Avisador externo con propia alimentación.....	18
3.6. Teclado alámbrico KP32.....	19
3.6.1. Descripción de los elementos de teclado.....	19
3.6.2. Características del teclado.....	22
3.6.3. Instalación del teclado.....	22
3.6.4. Direccionamiento de los dispositivos conectados al bus del teclado.....	23
3.7. Teclado inalámbrico KP2W.....	23
3.7.1. Añadir un teclado al sistema.....	24
3.7.2. Descripción de los elementos de teclado.....	24
3.7.3. Características del teclado.....	25
3.7.4. Montaje del dispositivo.....	26
3.7.5. Detector de apertura de puerta.....	26
3.8. Ubicación de la centralita de alarmas.....	27
3.9. Instalación de detectores inalámbricos.....	28
4. MODO DE SERVICIO.....	29
4.1. Activación del modo de servicio.....	30
4.2. Salida del modo de servicio.....	30
4.3. Menú del instalador en el modo de servicio.....	30
4.3.1. Código de instalador.....	31
4.3.2. Desaparición de alimentación.....	31
4.3.3. Restablecimiento de la configuración de fábrica.....	32
4.3.4. Opciones del sistema.....	32
4.3.5. Administración remota de usuarios.....	33
4.3.6. Opciones avanzadas del sistema.....	33
4.3.7. Longitud de los códigos de acceso.....	34
4.3.8. Retraso en la desactivación de la señalización de alarmas históricas.....	35
4.3.9. Tiempo de detección del desvanecimiento de los detectores inalámbricos.....	35
4.3.10. Desactivación de la opción de repetición cíclica de los eventos de desvanecimiento de los detectores.....	36
4.3.11. Opción de repetición cíclica de los eventos de desvanecimiento de los detectores.....	36
4.3.12. Números ACN en la comunicación en formato Contact ID.....	36
4.3.13. Configuración de las líneas de detección (entradas).....	37
4.3.14. Configuración de salidas.....	40
4.3.15. Configuración de particiones.....	41
4.3.16. Configuración de líneas inalámbricas.....	43
4.3.17. Configuración de mandos a distancia.....	45
4.3.18. Configuración de los botones de alarma en el teclado.....	47
4.4. MENSAJES DE TEXTO.....	48
5. PROGRAMA DE CONFIGURACIÓN.....	58
5.1. Notas preliminares.....	58
5.2. Ordenador – requisitos.....	58

5.3.	Smartphone – requisitos	58
5.4.	Instalación	58
5.4.1.	PC.....	59
5.4.2.	Smartphone.....	59
5.5.	Menú principal del programa	59
5.5.1.	Nueva configuración	60
5.5.2.	Abrir 	60
5.5.3.	Guardar 	60
5.5.4.	Estado del dispositivo 	61
5.5.5.	Leer configuración 	62
5.5.6.	Enviar configuración 	62
5.5.7.	Historial de eventos 	63
5.5.8.	Actualización de firmware 	63
5.5.9.	Restablecimiento de la configuración de fábrica 	63
5.5.10.	Configuración de la conexión 	64
5.5.11.	Configuraciones de la aplicación 	65
5.5.12.	EBS Config 2.0 - Información 	65
5.6.	MENÚ DE CONFIGURACIÓN – HARDWARE	65
5.7.	Resumen	66
5.8.	Configuraciones de la central.....	67
5.8.1.	Acceso y autorización	67
5.8.2.	Bloqueos	69
5.8.3.	Pérdida de comunicación con el dispositivo inalámbrico	70
5.8.4.	Alimentación y estabilidad de comunicación.....	71
5.8.5.	Teclado y mando.....	71
5.8.6.	Pitido de las salidas cableadas	73
5.9.	Particiones	74
5.9.1.	Detalles.....	74
5.9.2.	Dispositivos asignados	75
5.10.	Dispositivos.....	75
5.10.1.	Agregación de dispositivos inalámbricos	76
5.10.2.	Dispositivos con líneas	77
5.10.3.	Detectores inalámbricos (familia MC, PIR, GB, SD, MD, FL y GS)	77
5.10.4.	KP2W teclado.....	80
5.10.5.	Sirena exterior BM8000PLx-C3W (compatible a partir de la versión FW 2.11.4).....	81
5.10.6.	Mando a distancia RC-10.....	83
5.10.7.	Entradas de cables	84
5.11.	Usuarios	85
5.12.	Configuraciones de SMS.....	86
5.12.1.	Gestión de SMS.....	87
5.12.2.	Periodos de validez de los mensajes salientes SMS.....	88
5.12.3.	Restricciones.....	88
5.12.4.	Reenvío de SMS	88
5.12.5.	Notificaciones por SMS.....	89
5.12.6.	Contenidos únicos de mensaje.....	90
5.12.7.	Notificaciones de SMS 0/10	90
5.13.	Monitoreo TCP/IP, monitoreo de SMS.....	91
5.13.1.	Seguridad - clave de encriptación	91
5.13.2.	Eventos	91
5.14.	Modificadores de eventos.....	92
5.14.1.	Identificador del contacto (Contact ID).....	93
5.15.	Canales de comunicación	94

5.16.	Red móvil	94
5.16.1.	Servidores	95
5.16.2.	Conexión	96
5.16.3.	Estabilidad de conexión.....	97
5.17.	Modo SMS	97
5.17.1.	Número de teléfono.....	97
5.17.2.	Periodo de prueba de los eventos	98
5.17.3.	Periodo de incidencias rápidas.....	98
6.	SEÑALIZACIÓN CON DIODOS LED.....	99
6.1.	Registro en la red	99
6.2.	Alcance de gsm	99
6.3.	Transmisión	99
6.4.	Programación.....	100
6.5.	Actualización de firmware.....	100
6.6.	No hay tarjeta sim o la tarjeta sim está dañada.....	100
6.7.	Error del sistema	101
7.	AJUSTES GRADE 2	101
7.1.	Ajustes del sistema para Grade 2	101
7.2.	Comportamiento del sistema en el modo de compatibilidad con Grade 2	102
8.	ADITIVOS.....	103
8.1.	Comandos remotos y parámetros de configuración.....	103
8.1.1.	Parámetros de configuración	104
8.1.2.	Comandos generales	108
8.1.3.	Comandos de gestión de usuarios.....	115
8.1.4.	Comandos para administrar particiones, líneas y salidas	123
8.1.5.	Comandos para la gestión de dispositivos inalámbricos.....	132
8.1.6.	Comandos para la gestión de la seguridad de la configuración	134
8.2.	Glosario de términos.....	135
9.	HISTORIAL DE CAMBIOS.....	137

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:	CPX230NWB-5xx: Cinterion BGS2-W (GSM: 850, 900, 1800, 1900 MHz) CPX230NWB-6xx: Cinterion EHS6 (UMTS: 800, 850, 900, 1900, 2100 MHz; GSM: 850, 900, 1800, 1900 MHz) CPX230NWB-A10: Cinterion ELS61-E (LTE: 700, 800, 900, 1800, 2100 MHz; UMTS/HSPA+: 900, 2100 MHz; GSM: 900, 1800 MHz) CPX230NWB-Q30: Quectel EG915U-EU (LTE-FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM/EDGE: B2 / B3 / B5 / B8) CPX230NWB-Q40: Quectel EG915U-LA: LTE-FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM/EDGE: B2 / B3 / B5 / B8)
Consumo de corriente medio/máximo: (medio para las condiciones: batería completamente cargada, conexión al servidor, teclado, sin detectores)	* Versión con módem <u>BGS2-W Cinterion</u>: 120mA / 180mA @18VAC * Versión con módem <u>EHS6 Cinterion</u> 95mA / 170mA @18VAC * Versión con módem <u>ELS61-E Cinterion</u> 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 <u>BGS2-W Cinterion</u> 60mA / 85mA @13VDC * Versión con módem <u>EHS6 Cinterion</u> 35mA / 65mA @13VDC * Versión con módem <u>ELS61-E Cinterion</u> 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:	-10°C ... +55°C
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
BM8000PLx-C3W	Señalizador inalámbrico para exteriores (Nota: se requiere un controlador WLM-C3W adicional para su funcionamiento)

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
EBS Config 2.0	Aplicación para configurar y monitorear la centralita
OSM	Servidor de comunicación instalado en la estación de monitoreo
EBS INSTALL	Aplicación móvil para configurar y monitorear la centralita (sistema Android)
EBS Security	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 0,5mm²) 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

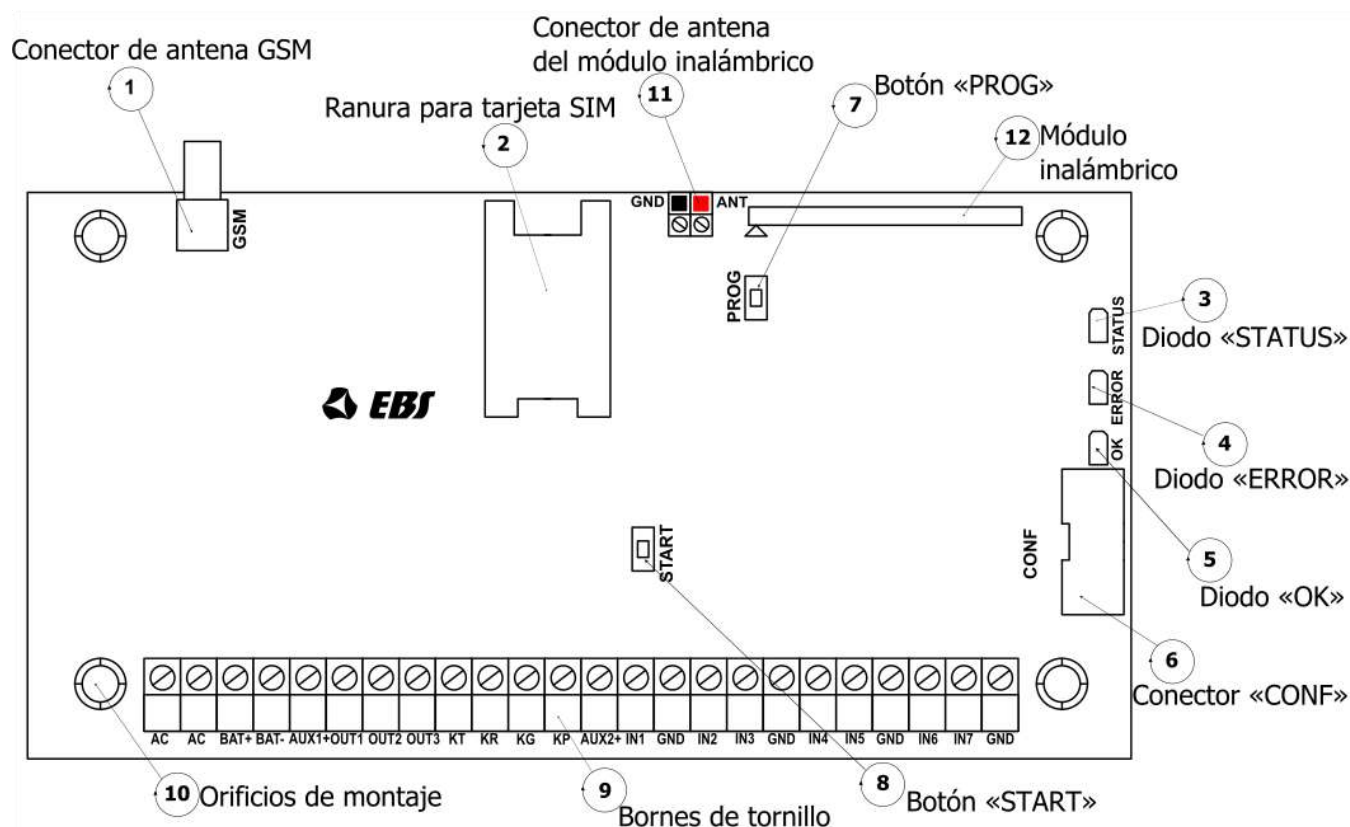


Fig. 1. Descripción de los componentes PCB

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 6

4. Diodo LED «ERROR»

Diodo LED rojo. La descripción detallada se encuentra en el capítulo 6.

5. Diodo LED «OK»

Diodo LED verde. La descripción detallada se encuentra en el capítulo 6.

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 el 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).

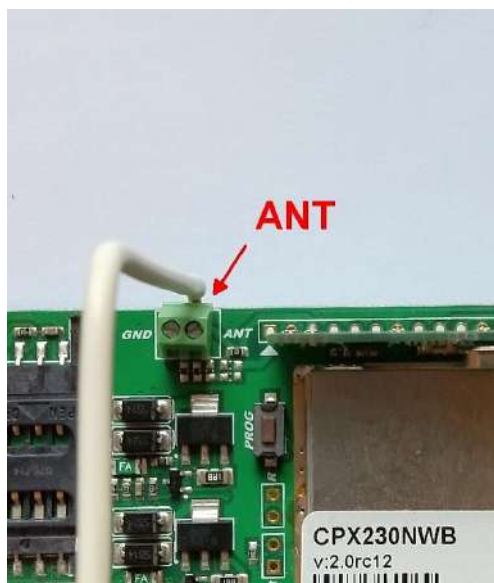
11. Conexión de antena al módulo inalámbrico

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

Antena interior 433MHz

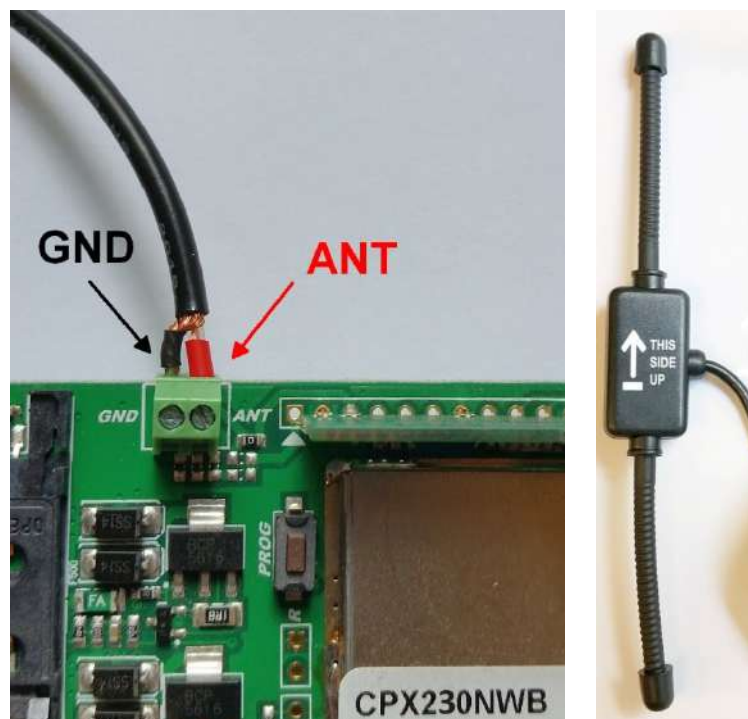


La antena interior (foto al lado) se puede utilizar en cualquier lugar donde se requieren dimensiones compactas y la antena proporciona la cobertura adecuada. Colocar la extremidad desnuda de la antena interior en el borne de potencial de la toma ANT (la polaridad correcta está marcada en rojo en Fig. 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!

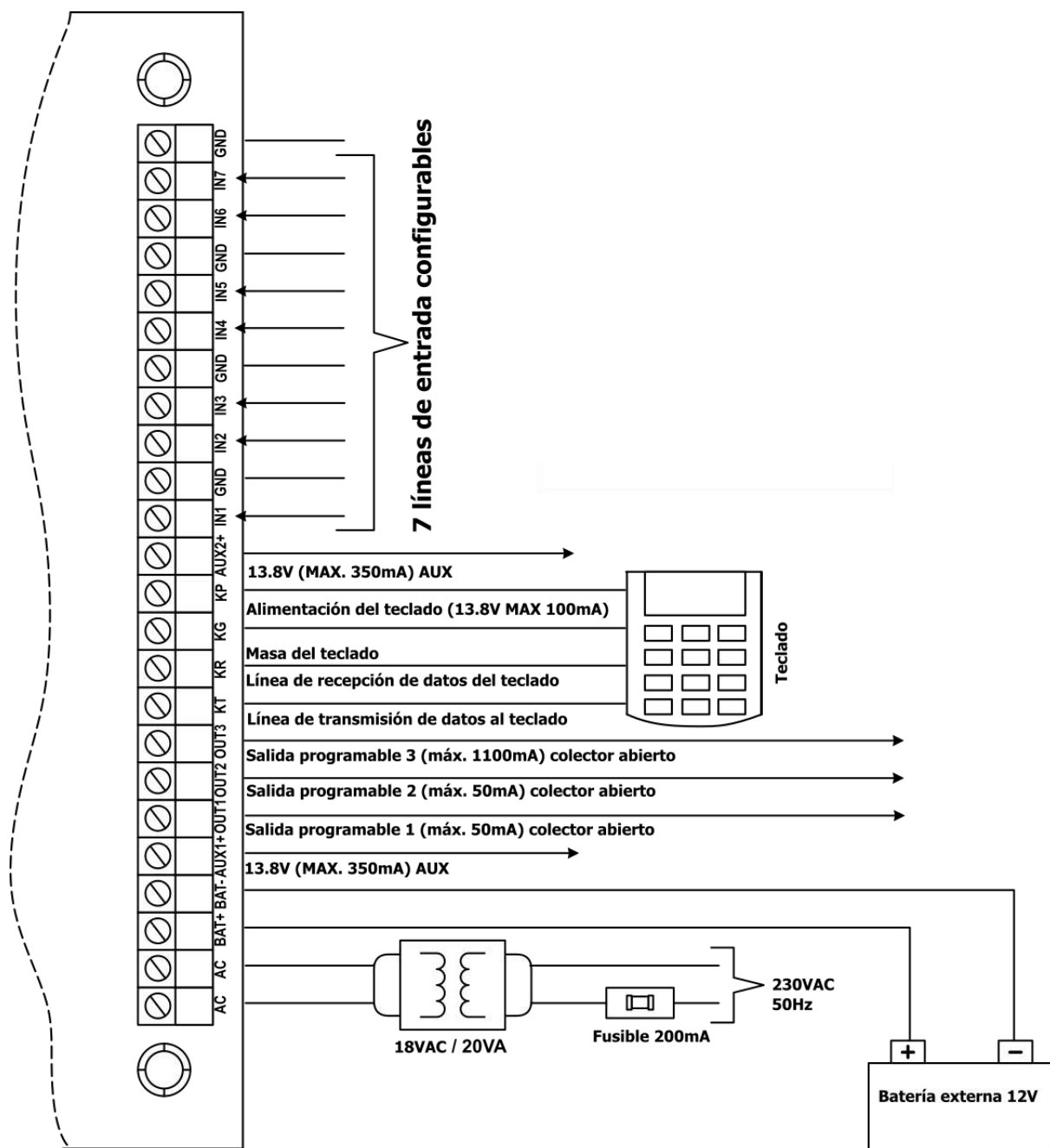


Figura 2. Descripción de las conexiones por tornillos de la centralita

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.

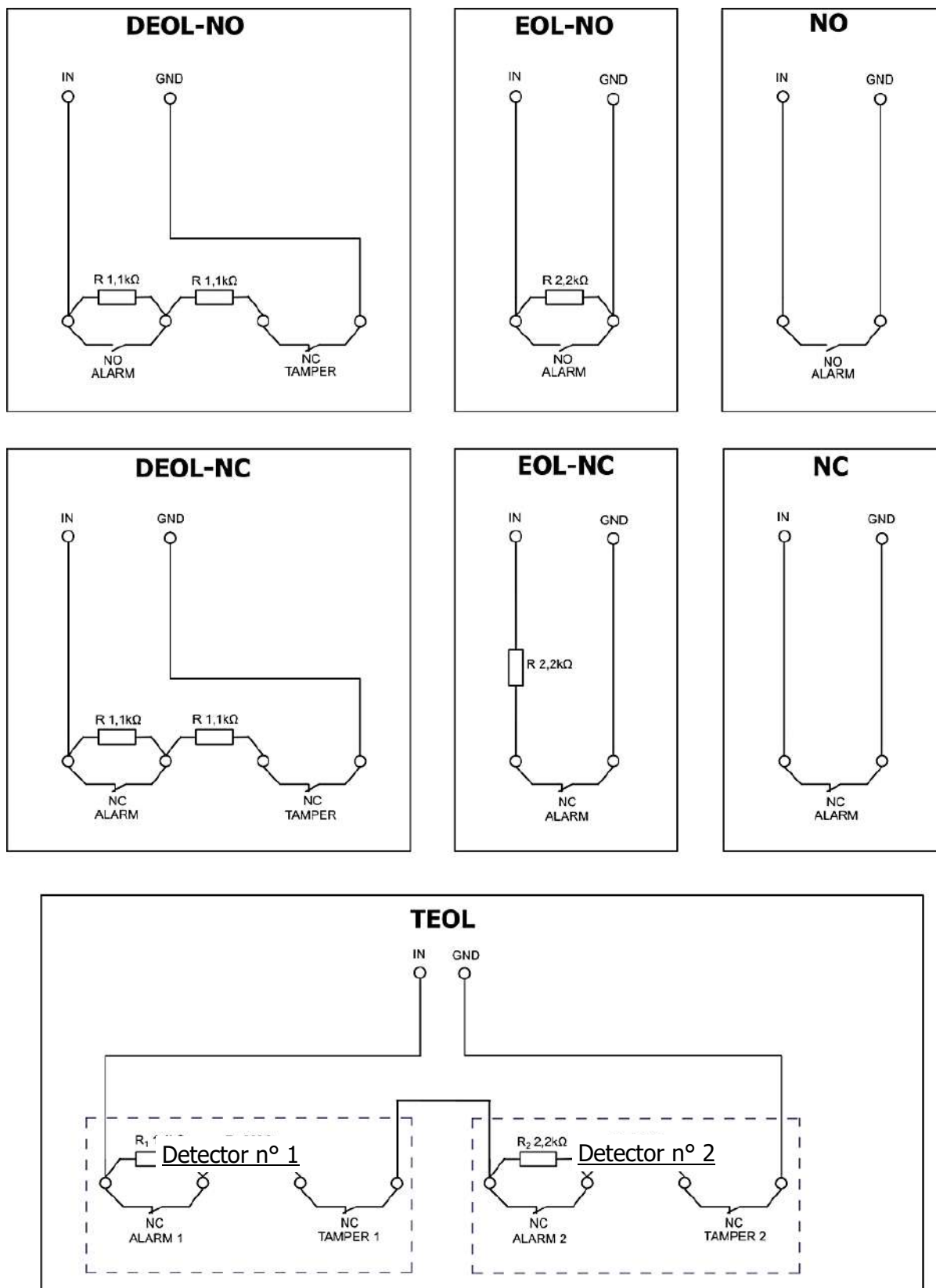


Fig. 3. Configuración de las líneas de entrada

3.5. CONEXIÓN EJEMPLAR DE AVISADOR

3.5.1. Avisador interno sin propia alimentación

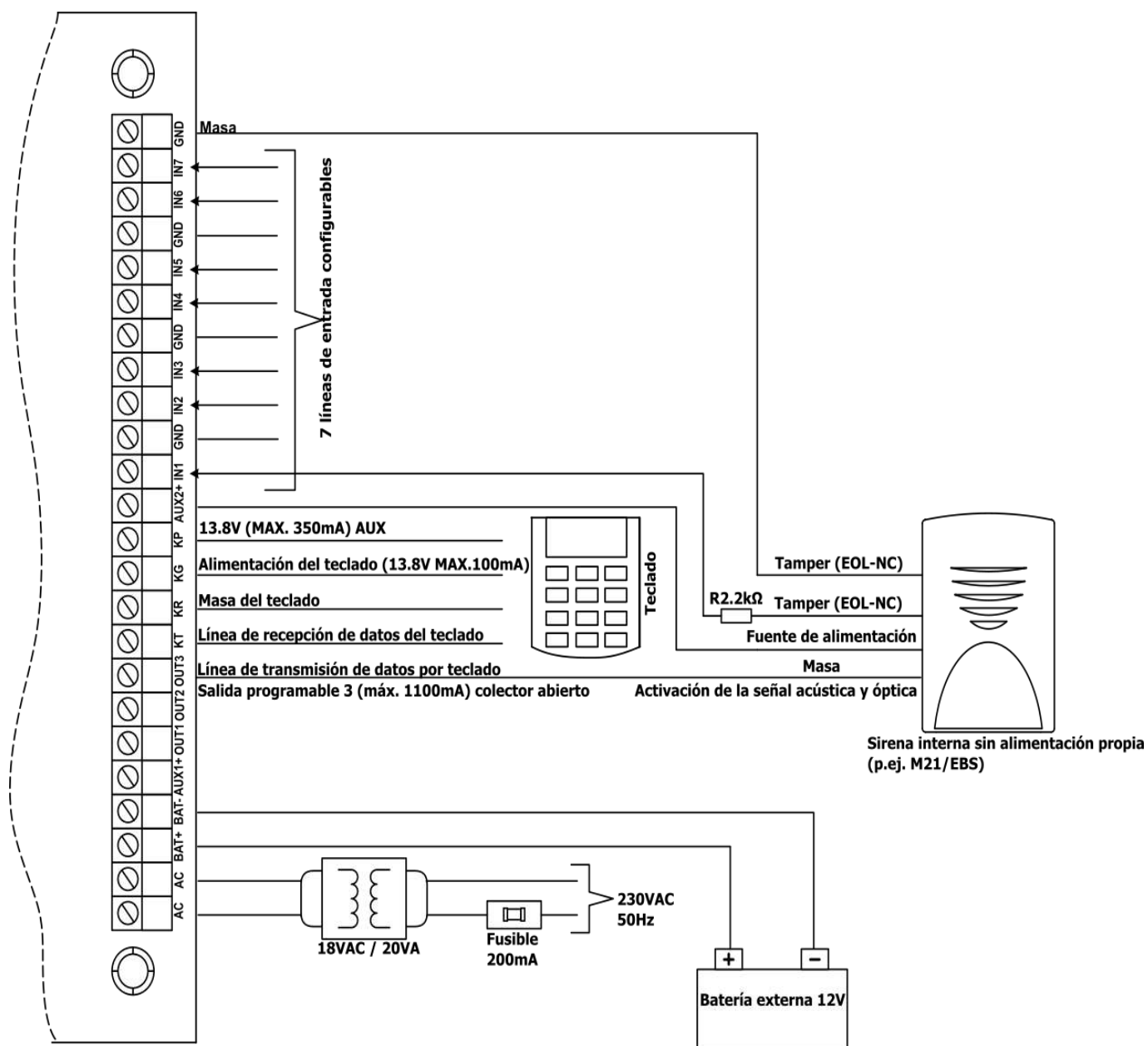


Fig. 4. Conexión ejemplar del avisador interno sin propia alimentación

3.5.2. Avisador externo con propia alimentación

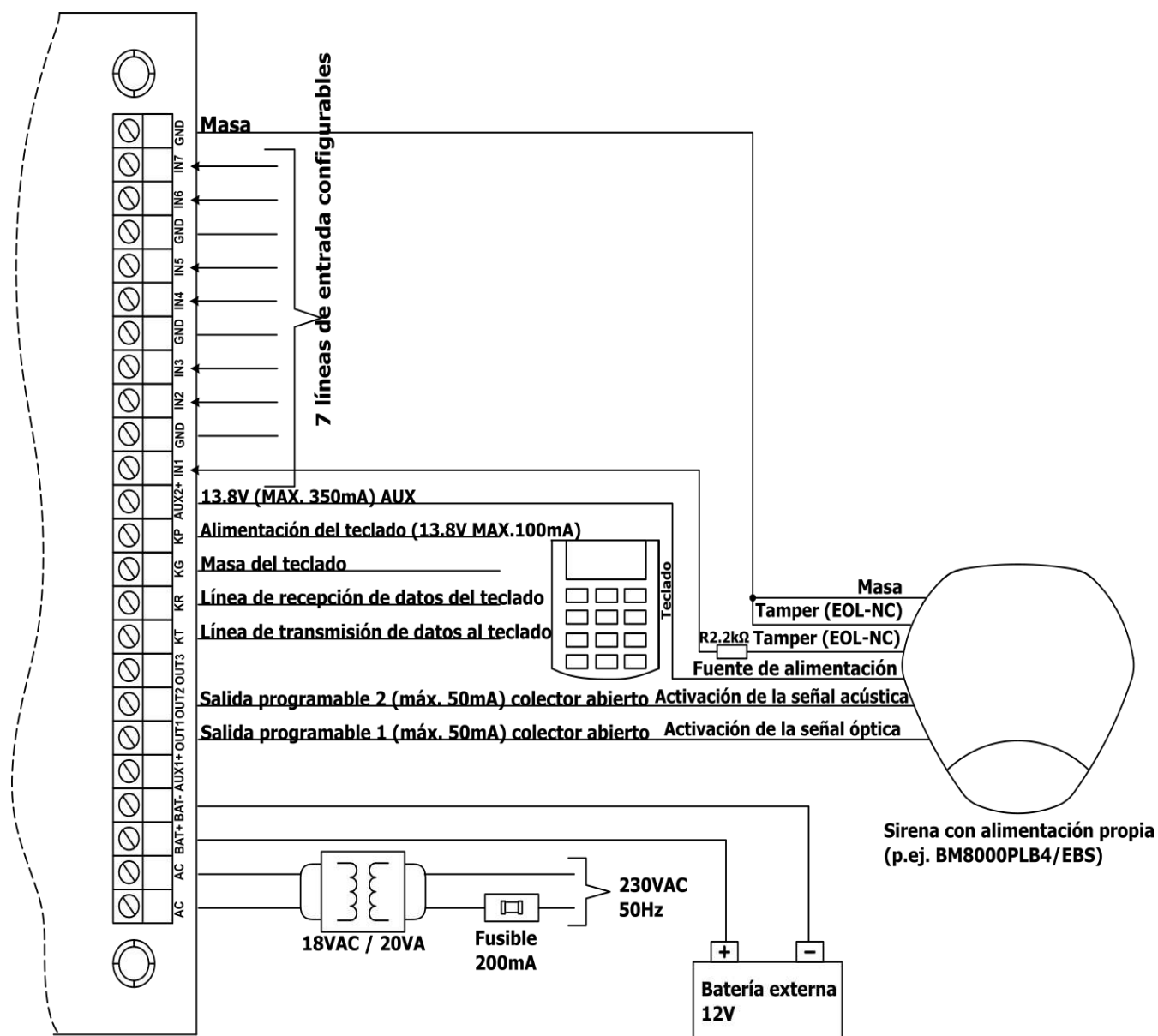


Fig. 5. Conexión ejemplar del avisador externo con propia alimentación

3.6. TECLADO ALÁMBRICO KP32

3.6.1. Descripción de los elementos de teclado

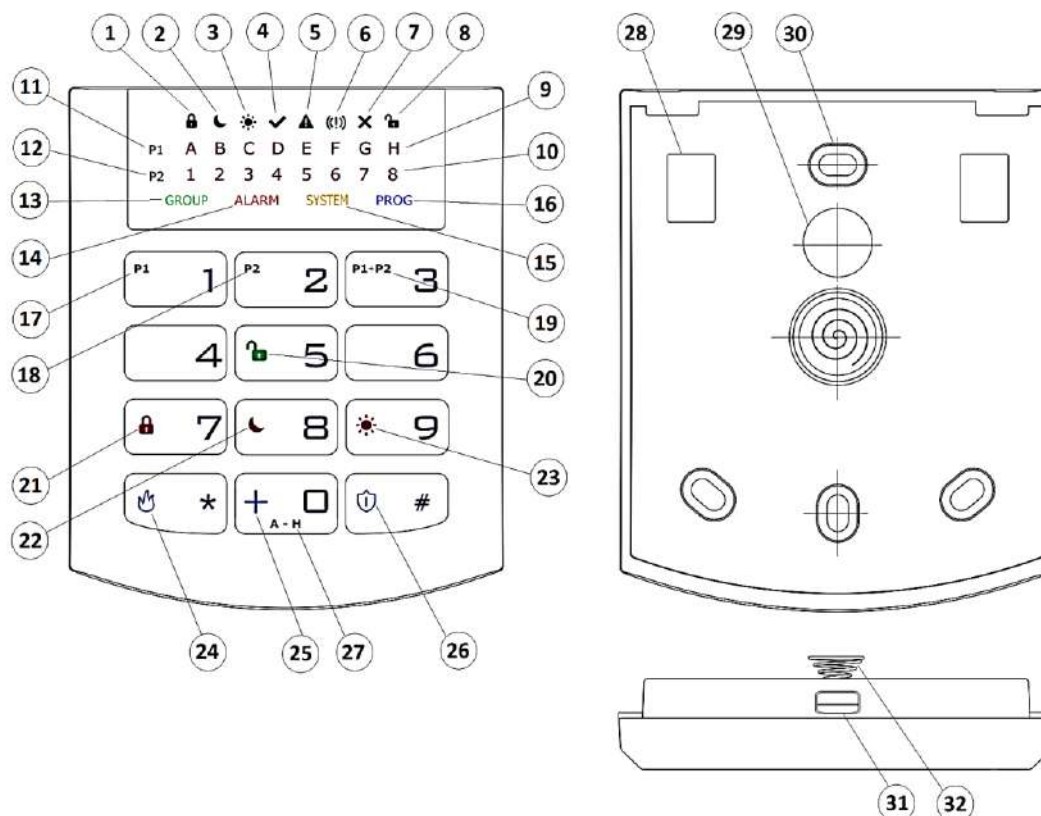


Fig. 6. Teclado KP32

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  y  o  o  hasta que se ilumine el diodo correspondiente (A para la dirección nº 1, B para nº 2 y C para nº 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 EBS Security 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 EBS Config 2.0.

3.7.2. Descripción de los elementos de teclado

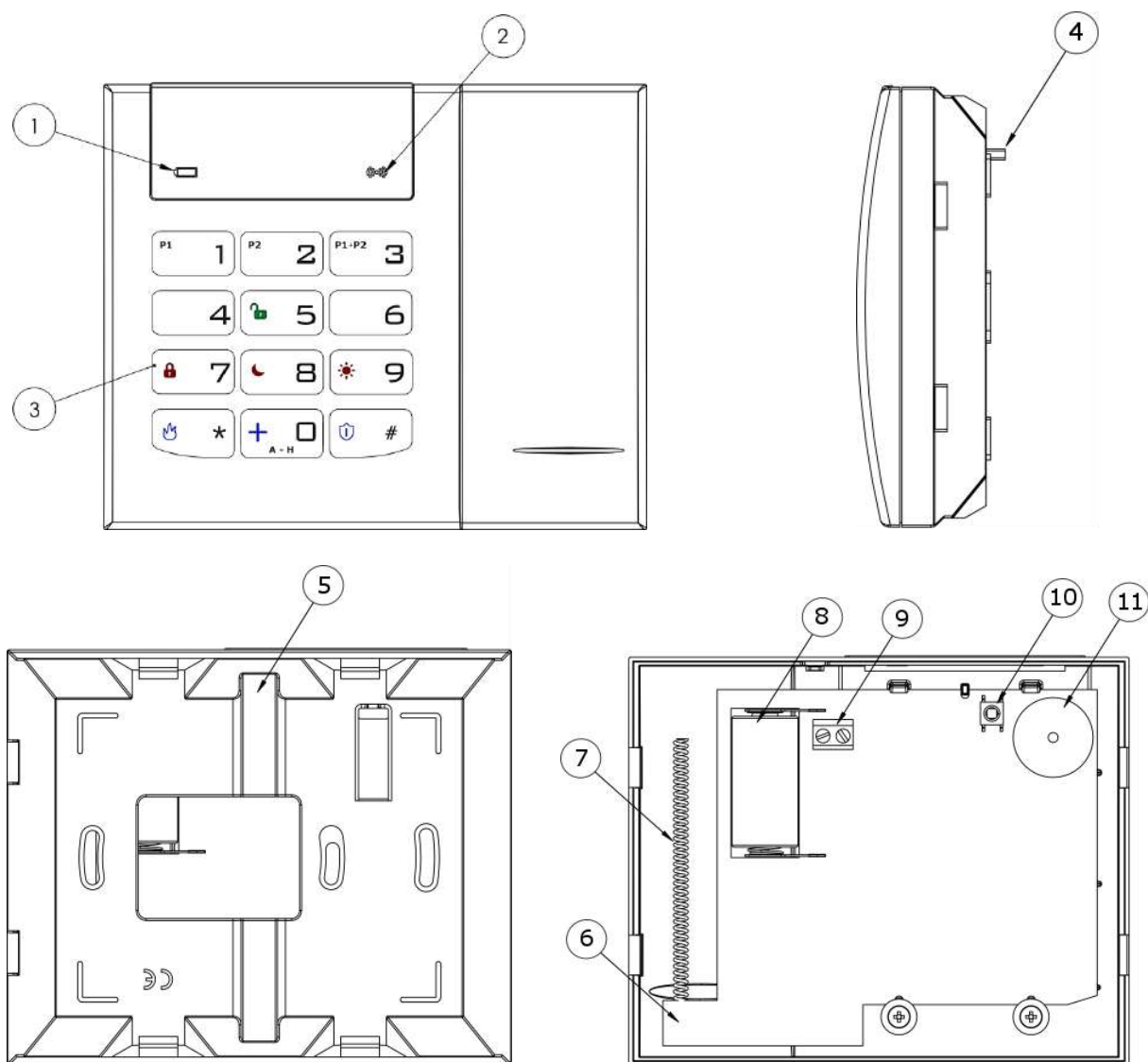


Fig. 7. Vista general y disposición de los elementos del teclado KP2W

1. Diodo de carga baja de la batería (rojo)

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

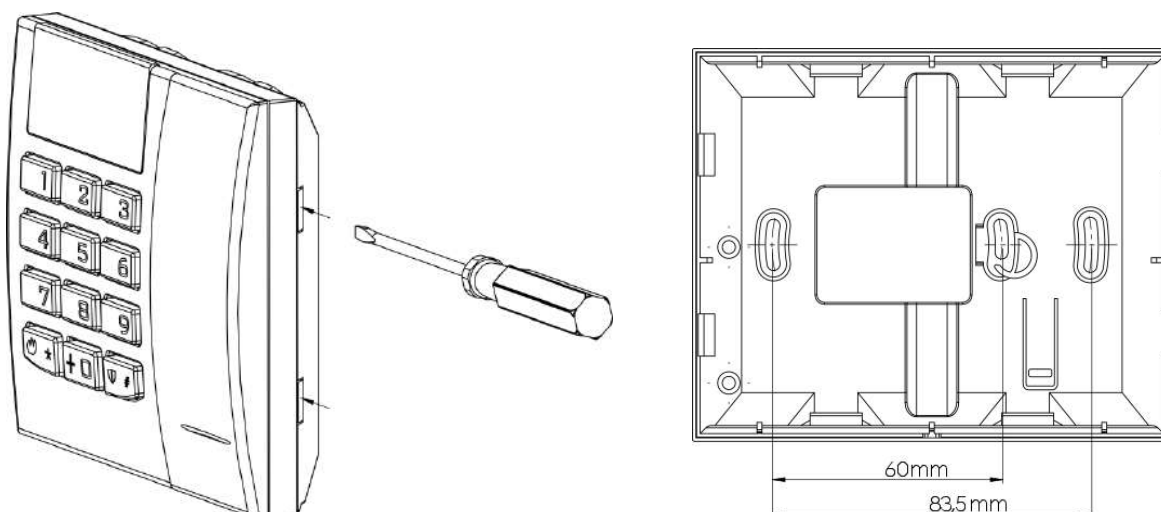


Fig. 8. Cierres de la carcasa y orificios de montaje

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 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 (nº 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.

Panel de control - posición horizontal

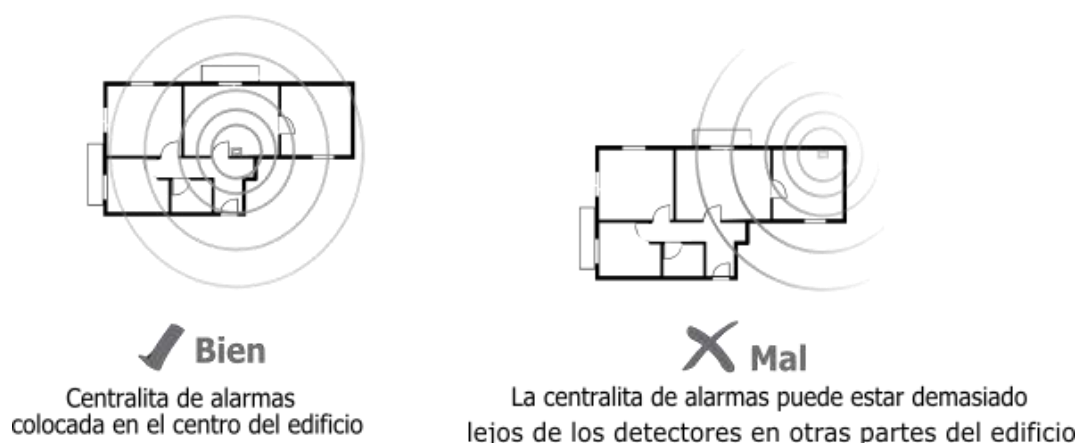


Fig. 9. Situación horizontal de la centralita de alarmas

Centralita de alarmas - posición vertical

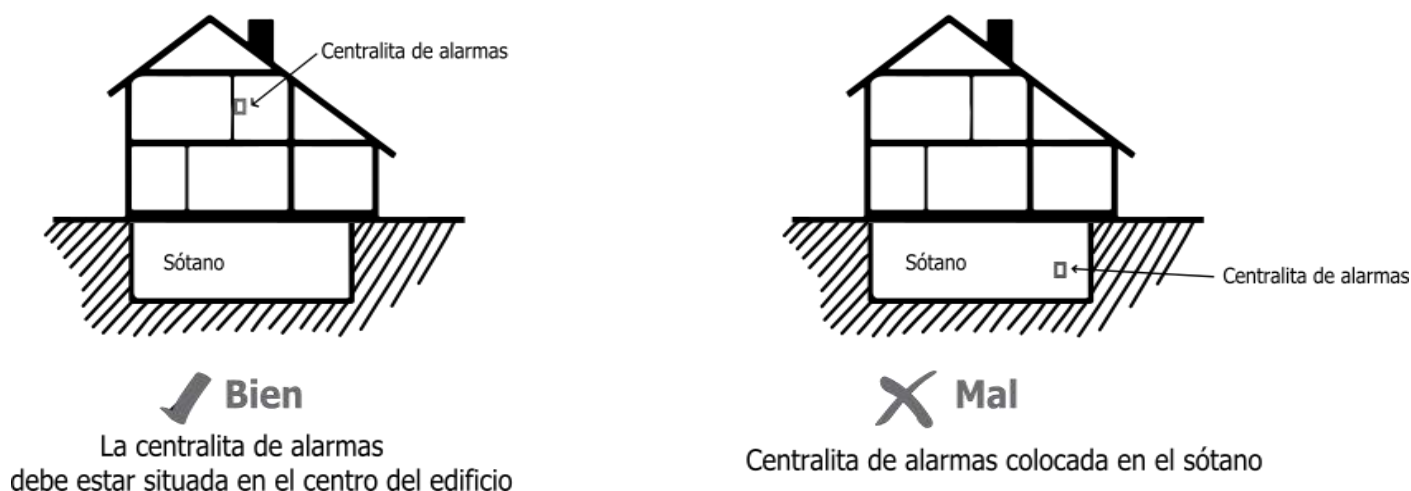


Figura 10. Situación vertical de la centralita de alarmas

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).

Pérdidas de señal después de atravesar diferentes materiales estructurales

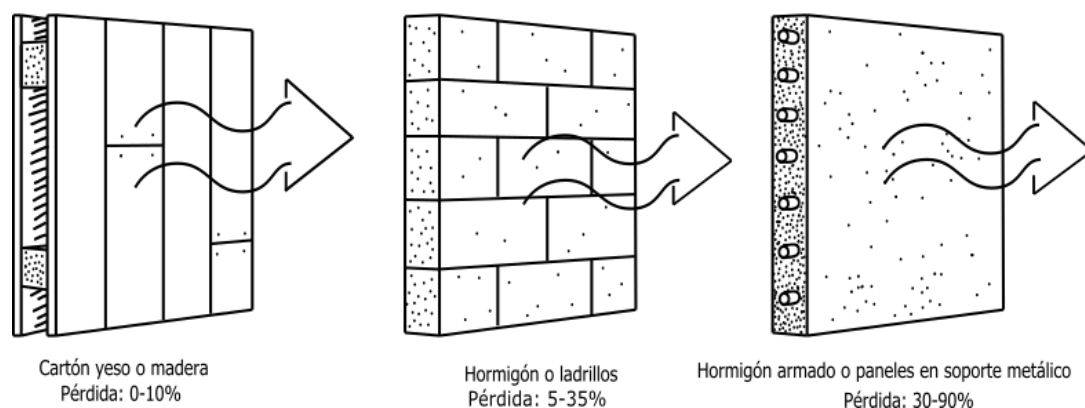


Figura 11. Pérdidas de señal después de atravesar diferentes materiales estructurales

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.

Montaje del detector

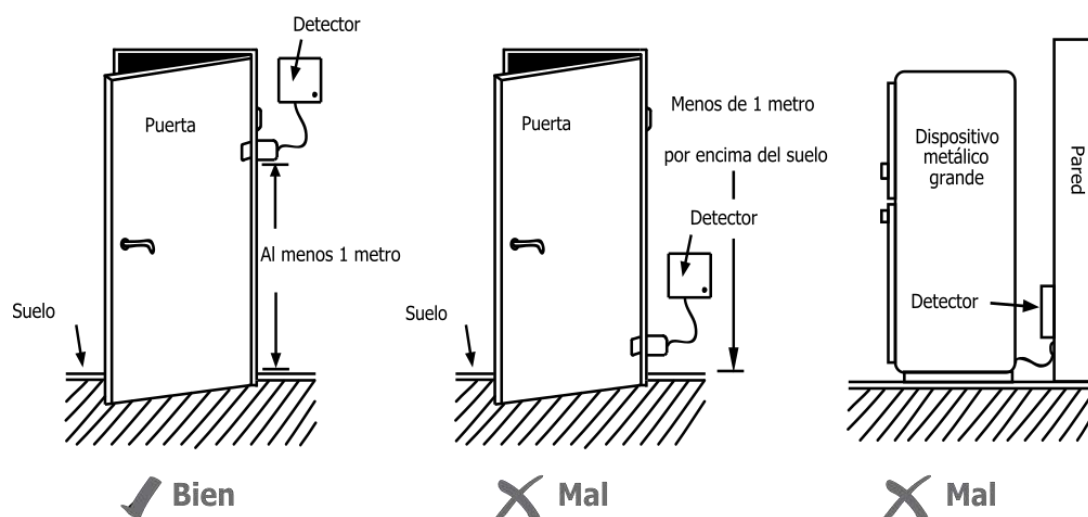


Fig. 12. Montaje del detector

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>  <Argumento> 

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  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  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.



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.

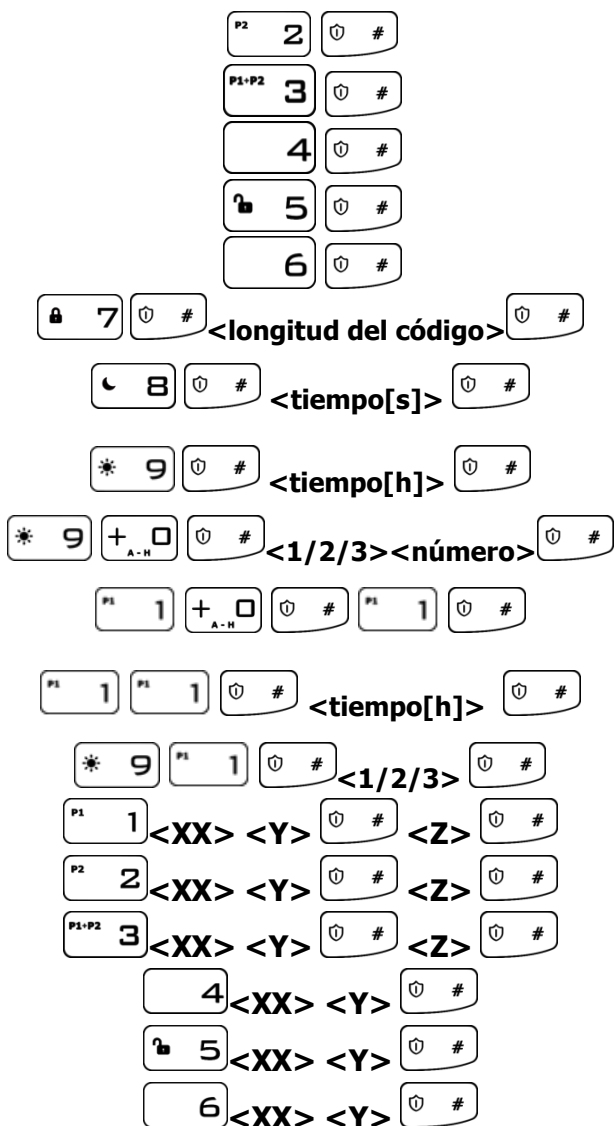
Pasados los 5 minutos de inactividad (sin apretar las teclas) saldremos automáticamente del modo de servicio y reiniciaremos la centralita.

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:



Cambio del código del instalador



- Tiempo de informe de fallo de alimentación CA
- Restablecimiento de la configuración de fábrica
- Configuración de las opciones del sistema
- Administración remota de usuarios
- Opciones avanzadas del sistema
- Cambio de la longitud del código
- Retraso en la desactivación de la señalización de alarmas históricas
- Tiempo de detección del desvanecimiento de los detectores inalámbricos
- Introducción y cambio de números ACN
- Desactivación del informe cíclico de desvanecimiento de los detectores inalámbricos
- Opción del informe cíclico de desvanecimiento de los detectores inalámbricos
- Supresión de números ACN y configuración
- Configuración de entradas (líneas de detección)
- Configuración de salidas
- Configuración de particiones
- Menú de detectores inalámbricos
- Configuración de mandos a distancia
- Botones de alarma

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.



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:

  **<Tiempo (s)>** 

Siendo:

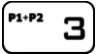
Tiempo: tiempo en segundos

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).

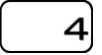
Para protegerse contra la eliminación accidental de configuración, la función deberá ser confirmada, además, con el código de instalador. La función introducida correctamente será confirmada con un tono triple. El uso de esta función ocasionará el reinicio de la centralita con el uso de la configuración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

  **<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.

  **<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 transcurrido 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 será 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 transcurrido 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

  <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. Cuando 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 transcurrido 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.

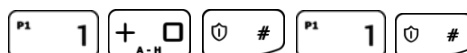
 9  # <tiempo [h]>  #

Este tiempo se expresa 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.



Este tiempo se expresa 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:



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. Cuando 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:



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:



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

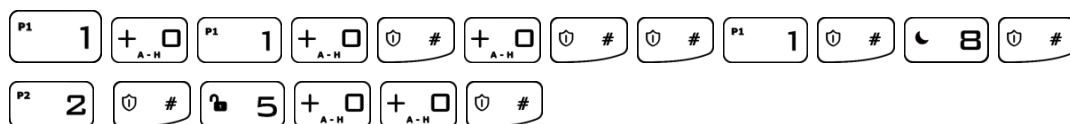
El número **00** permite cambiar los parámetros de todas las líneas del sistema al mismo tiempo,

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:



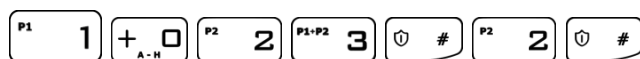
Nota: En caso de una función compuesta (programación de varios parámetros al mismo tiempo), después de introducir el parámetro y confirmarlo con el botón el parámetro se guarda en la memoria de configuración y se espera a que se introduzca el siguiente parámetro y así hasta introducir todos los parámetros 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 para salidas cableadas y de 04 a 06 para salidas inalámbricas como la sirena BM8000PLx-C3W**; 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 + □ P1 1 + □ ⏏ # P1 1 ⏏ # P1 1 P2 2 + □ ⏏ #

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 (no se aplica a las salidas 04, 05 y 06 reservadas para la sirena inalámbrica BM8000PLx-C3W)
 - 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 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:

P2 2 + □ A-H P2 2 P2 2 ⏏ # + □ A-H ⏏ #

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:

P2 2 + □ A-H + □ A-H P1+P2 3 ⏏ # 6 + □ A-H + □ A-H ⏏ #

- **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:

P2 2 + □ A-H + □ A-H 4 ⏏ # 5 + □ A-H + □ A-H ⏏ #



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:

P1+P2 3 <XX> <Y> ⏏ # <Z> ⏏ #

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 + □ A-H 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.

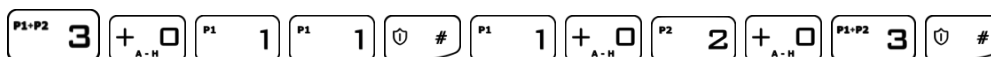
Al activar la función compuesta 3008 (tiempo de desarmado para todas las particiones) se copiará el indicador de activación/desactivación del cronograma de desarmado de la primera a la segunda partición.

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.

Ejemplos:

- 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:

P1+P2 3 + □ P2 2 P1 1 ⬆ # P1 1 + □ 🔒 5 + □ + □ ☾ 8 ⬆ #

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

P1+P2 3 + □ + □ P1+P2 3 ⬆ # 6 + □ ⬆ #

- 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:

P1+P2 3 + □ P2 2 + □ ⬆ # P2 2 + □ 4 + □ 🔒 5 ⬆ # P1 1
⬆ # 4 🔒 5 ⬆ # P1 1 P2 2 + □ ⬆ # P1 1 P2 2 ⬆ #



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:

4 <XX> <Y> ⬆ #

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):

     #  #

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):

     # (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:

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.

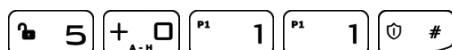
La función «Asistencia médica» funciona de la misma manera que el botón «AYUDA» en el teclado, es decir, genera una alarma médica.

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:



b) añadir el mando n° 1:

5 + 1 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 + + 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:

<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
 - 5: salida 4 (sirena inalámbrica 1)
 - 6: salida 5 (sirena inalámbrica 2)
 - 7: salida 6 (sirena inalámbrica 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:

+ 1 # 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):



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 <i>Ejemplo: 1234 SETTELNUM=3,600987654</i>
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 <i>Ejemplo: 1234 GETTELNUM=2</i>
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 <i>Ejemplo: 1234 SETMESSAGE=4,efraccion</i>
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 <i>Ejemplo: 1234 GETMESSAGE=30</i>
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 <i>Ejemplo:</i> 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. <i>Ejemplo: 1234 GETARMED</i>
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	<pre>XXXX SETNAME=ELEMENT,[NR],VALUE_sin_espacios XXXX SETNAME="ELEMENT,[NR],VALUE_c on_espacios"</pre>

Descripción de comando	Configuración del nombre (posición VALUE) del elemento (valores posibles a continuación) nº. XXXX – código de servicio (ATS) o código de administrador o instalador si tiene permiso de servicio Valores posibles de la posición ELEMENT: <u>PARTITION</u> – nombre de la partición; números 1 y 2 <u>ZONE</u> – nombre de la línea de entrada correspondiente al número determinado; números de 1 a 32 <u>OUTPUT</u> – nombre de la salida correspondiente al número determinado; números de 1 a 3 <u>USER</u>– nombre del usuario con el número determinado; números de 1 a 32 <u>SYSTEM</u> – nombre del edificio en el que funciona la centralita y el sistema de alarma. Nota: para este elemento no se especifica el campo nº. <i>Ejemplo 1:</i> <i>1234 SETNAME=PARTITION,1,Sótano</i> <i>Ejemplo 2:</i> <i>1234 SETNAME="PARTITION,2,Cuarto de niños"</i>
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: <u>PARTITION</u> – recupera la descripción de la partición; números 1 y 2 <u>ZONE</u> – recupera la descripción de la línea de entrada correspondiente al número determinado; números de 1 a 32 <u>OUTPUT</u> – recupera la descripción de la salida correspondiente al número determinado; números de 1 a 3 <u>USER</u>– recupera la descripción del usuario con el número determinado; números de 1 a 32 <u>SYSTEM</u> – 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 nº. <i>Ejemplo 1:</i> 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 **EBS Config 2.0** se puede descargar desde la página www.ebssmart.com. 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. SMARTPHONE – REQUISITOS

La aplicación móvil EBS Config 2.0 solo está disponible para smartphones Android.

Para la instalación y el funcionamiento correctos de la aplicación móvil EBS Config 2.0, se requiere una versión de Android de al menos 5.1 o posterior.

5.4. INSTALACIÓN

Si la tarjeta SIM con el PIN preprogramado tiene un código PIN diferente al 1111, el dispositivo debe configurarse usando EBS Config 2.0 introduciendo el código PIN de la tarjeta SIM preprogramado, en cuyo caso la colocación de la tarjeta SIM solo se puede realizar después de introducir el código PIN correcto. De lo contrario, la tarjeta puede bloquearse (problema de compatibilidad con PIN).

Si la tarjeta SIM tiene el código PIN desactivado o el código PIN es 1111, se puede colocar la tarjeta SIM sin una configuración previa.

5.4.1. PC

Descargue **EBS Config 2.0** para PC desde www.ebssmart.com. Abra el archivo descargado para iniciar el proceso de instalación. Durante la instalación, seleccione el idioma, introduzca los datos, defina la posición de los componentes del programa (ruta de destino: C:\Program Files\EBS\), cree un acceso directo al programa en el escritorio o en la barra de acceso rápido.

5.4.2. Smartphone

Se puede descargar **EBS Config 2.0** para el teléfono desde la tienda 'Google Play'. Una vez finalizado el proceso de instalación, abra la aplicación e inicie la configuración del dispositivo. La interfaz de la aplicación móvil EBS Config 2.0 es la misma que la interfaz de PC.

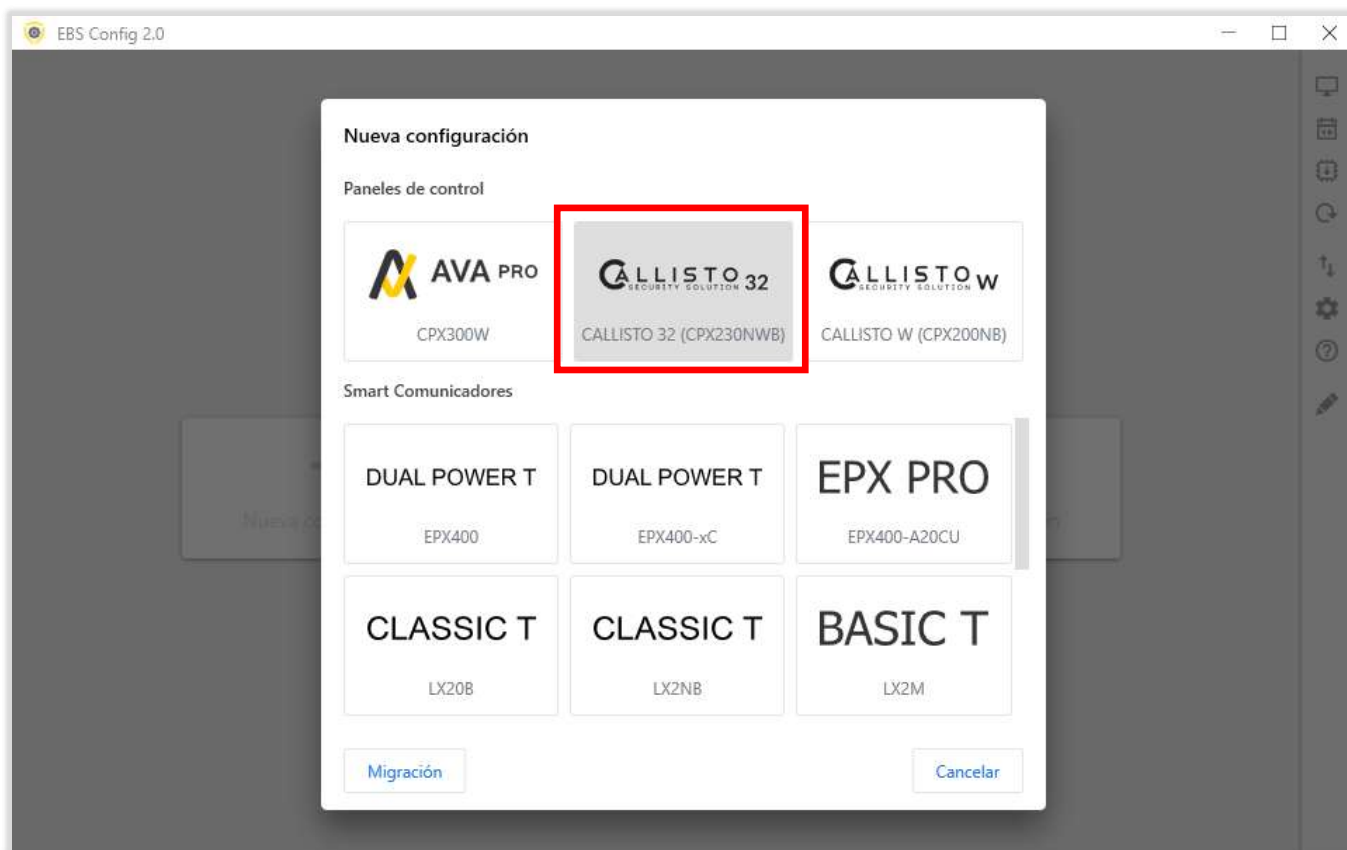
5.5. MENÚ PRINCIPAL DEL PROGRAMA

Tras la instalación y el inicio del programa, se mostrará una vista principal en la pantalla. El menú general está en la parte derecha de la pantalla del programa.



5.5.1. Nueva configuración

Después de instalar y activar **EBS Config 2.0**, haga clic en  Nueva configuración y, a continuación, seleccione CALLISTO 32 (CPX230NWB). Aparece una vista de la nueva configuración del centralita en la pantalla y el **Menú principal** aparece en el lado derecho de la ventana.



5.5.2. Abrir

En caso del fichero con la configuración guardada los datos podrán usarse para programar el dispositivo siguiente. Primero, se debe indicar el catálogo donde se guardó el fichero y, luego, indicar el nombre de fichero. La colección de datos conseguida puede ser modificada por el usuario. Para que los cambios puestos tengan efecto deben ser enviados al dispositivo. Utilice el programador configurándolo en modo de programación.

5.5.3. Guardar

Si programa varios dispositivos en configuraciones diferentes, no tiene que recordar cada una de ellas. Se pueden guardar en el disco duro o disco externo todas las configuraciones del dispositivo con el nombre determinado y cargarse posteriormente. Esta función guarda en el disco toda la información de las ventanas del configurador. Después de seleccionar la función aparecerá la ventana de diálogo con la solicitud de introducir el nombre de fichero. Por defecto, los datos se guardan con la extensión **.cmi** (Configuration Memory Image).

5.5.4. Estado del dispositivo



Estado del panel de control - EBS Config 2.0

Detener Inicio

Buscar

15/07/2019

12:27:05.04	Realizar prueba de GPRS
12:27:09.94	Enviando OK
12:28:09.30	Realizar prueba de GPRS
12:28:10.20	Enviando OK
12:29:09.55	Realizar prueba de GPRS
12:29:10.29	Enviando OK
12:30:09.80	Realizar prueba de GPRS
12:30:10.57	Enviando OK
12:31:10.05	Realizar prueba de GPRS
12:31:10.82	Enviando OK
12:32:10.31	Realizar prueba de GPRS
12:32:11.09	Enviando OK
12:33:10.56	Realizar prueba de GPRS
12:33:11.36	Enviando OK
12:34:10.81	Realizar prueba de GPRS
12:34:11.63	Enviando OK
12:35:11.07	Realizar prueba de GPRS
12:35:11.76	Enviando OK
12:36:11.32	Realizar prueba de GPRS
12:36:12.08	Enviando OK
12:37:06.67	Radio stat Recv=16726 RecvEvt=430 SentResp=430
12:37:11.57	Realizar prueba de GPRS
12:37:12.33	Enviando OK
12:38:11.02	Realizar prueba de GPRS

Particiones

1

Salidas cableadas

OUT

1

Dispositivos con zonas

9 10 11 13

93% 93% 93%

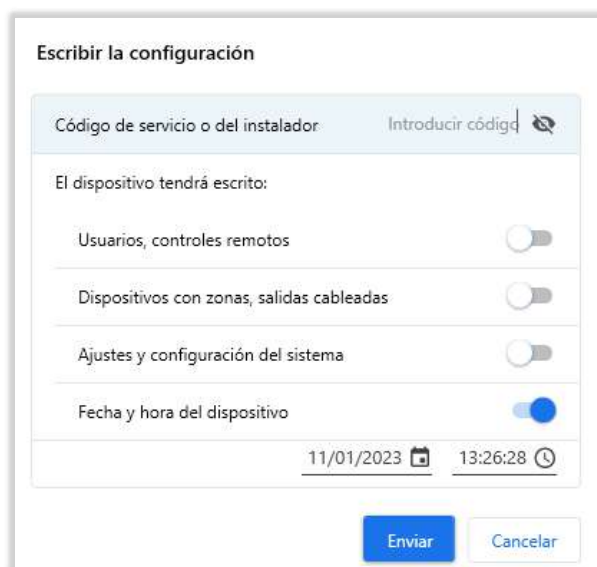
En la ventana "Estado de la central" viene presentada la información relativa al dispositivo: su número de serie, versión del equipo, firmware, fecha y hora configuradas. Además, aquí podrá controlar en tiempo real los siguientes parámetros:

- Estado de conexión con el servidor,
- Estado de alimentación de la red,
- Estado de la batería
- Nivel de señal de red GSM
- Estado de los dispositivos con líneas y de las salidas de cables - porcentaje del nivel de señal; al posicionar allí el cursor, aparecerá información adicional, tal como:
 - Tipo de línea (alámbrica/inalámbrica)
 - Tipo de dispositivo
 - Número de serie
 - Tipo de respuesta, por ejemplo inmediata, sabotaje 24h
 - Przypisanie do partycji
 - Estado: no violado, alarma, sabotaje o no utilizado (detector do asignado a ninguna partición)
- Estado de salidas
- Estado de armado

5.5.5. Leer configuración

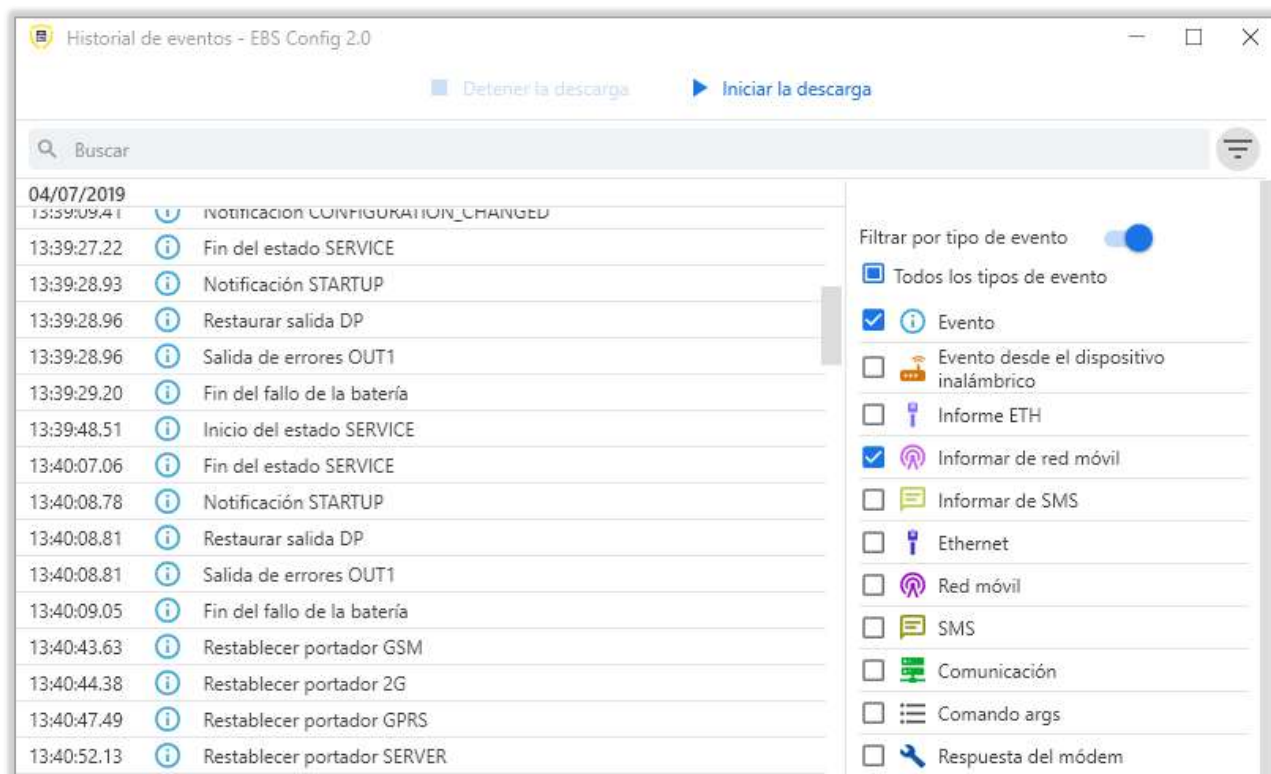
La función lee la información almacenada en la memoria del dispositivo. Dependiendo del tipo de conexión definido (véase el capítulo sobre Configuración de conexión), es posible leer de forma remota el historial de eventos a través de GPRS/LTE o localmente utilizando Bluetooth (SP-PROG-BT, MINI-PROG-BT) y el conector RS232 (SP-PROG, GD-PROG) después de poner el centralita en el modo de programación «Programming mode». Al hacer clic en el botón «Leer configuración», se descargará la configuración almacenada en la memoria del centralita y aparecerá una barra con información sobre una lectura exitosa/fallida en la parte inferior de la aplicación. Los datos descargados del dispositivo podrán guardarse, después se podrán usar para otros dispositivos.

5.5.6. Enviar configuración



Esta función es análoga a la de arriba y permite enviar los datos seleccionados a la memoria del dispositivo. Dependiendo de los cambios realizados, se puede seleccionar el conjunto de información apropiado para enviar. También es posible configurar la fecha y el reloj interno del dispositivo (campo «Hora y fecha del dispositivo»). Al hacer clic en el botón «Enviar», se enviarán los datos definidos y aparecerá la barra de mensajes del envío exitoso/fallido en la parte inferior de la aplicación.

5.5.7. Historial de eventos



Esta función permite leer unos 5.000 últimos eventos técnicos guardados en la memoria del dispositivo. Dependiendo del tipo de conexión definido (véase el capítulo 5.5.10

Configuración de la conexión ) , es posible leer el historial de forma remota utilizando GPRS y localmente utilizando Bluetooth (SP-PROG-BT, MINI-PROG-BT) y conector RS232 (SP-PROG, SP-PROG-BT, GD-PROG). Después de leer el historial correctamente, se pueden buscar los eventos relevantes escribiendo los nombres en el campo con la lupa. También está disponible una función para filtrar datos por tipo de evento y por fecha, lo que permite una navegación rápida de eventos individuales.

5.5.8. Actualización de firmware



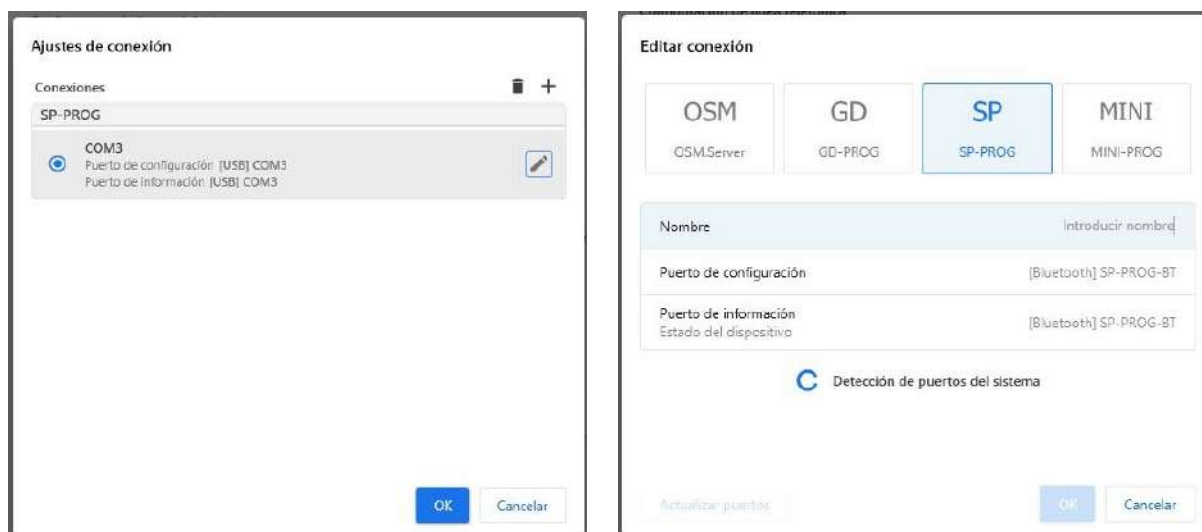
El dispositivo tiene incorporado un bootloader, gracias al que podemos modificar el software del módulo con uno más nuevo. En la ventana que aparece, indique dónde está el archivo correcto y pulse «Actualizar».

5.5.9. Restablecimiento de la configuración de fábrica



Utilice esta opción para recuperar la versión de fábrica de la configuración del sistema. Todos los datos de usuario introducidos anteriormente se eliminarán y reemplazarán por la configuración de fábrica. Los usuarios y dispositivos asignados a los centralites **no se eliminarán**, solo se borrarán las configuraciones eliminadas.

5.5.10. Configuración de la conexión



Después de hacer clic en el signo «+», aparecerá una ventana con los métodos de conexión disponibles:

- **OSM.Server:** conexión remota al servidor OSM.Server a través de LTE, es posible definir los parámetros de la configuración del receptor OSM.Server:
 - Dirección IP del analizador (p. ej., www.ebssmart.com);
 - Puerto en el que el analizador escuchará los comandos (p.ej., 9000)
 - Nombre de analizador (p. ej., primary)

La conexión se guardará después de hacer clic en el botón «OK». A partir de ahora, el programa permitirá conectar el dispositivo de forma remota y leer y almacenar parámetros en la memoria del dispositivo.

- **GD-PROG:** es un tipo de conexión local que funciona con un programador del mismo nombre con un solo puerto asignado.
- **SP-PROG:** bajo este tipo de conexión existen dos programadores:
 - SP-PROG, que dispone de un conector micro USB y RS232, al que se le asignan dos puertos COM. Una configuración utilizada durante la programación, la otra de información utilizada en la supervisión del estado del dispositivo,
 - SP-PROG-BT con un conector micro USB, RS232 y el módulo Bluetooth incorporado. Con la conexión alámbrica la situación es igual que en el caso de SP-PROG. Utilizando la tecnología Bluetooth, tanto en la posición de *Puerto de configuración* como de *Puerto de información*, deberá configurar el mismo puerto dedicado a la comunicación.
- **MINI-PROG-BT:** es un tipo de conexión local que funciona con un programador con el mismo nombre, al que se asigna un puerto COM.

Si los nuevos puertos no aparecen automáticamente cuando se conecta el programador, pulse «Actualizar puertos».

Cuando utilice una conexión Bluetooth, el primer paso debe ser emparejar el programador (SP-PROG-BT, MINI-PROG-BT) con su ordenador/teléfono. En la lista de dispositivos buscados listos para la conexión, seleccione el que esté enchufado al centralita.

Solo después de emparejar el programador con un ordenador, en EBS Config aparece el puerto abierto asignado para la comunicación programador-ordenador.

5.5.11. Configuraciones de la aplicación



En esta ventana es posible elegir uno de los idiomas disponibles de la aplicación y elegir el motivo de color de la interfaz de la aplicación.

5.5.12. EBS Config 2.0 - Información



Seleccione este icono para mostrar la ventana con información adicional:

- Versión de la aplicación (se recomienda utilizar la última versión publicada oficialmente);
- Número de teléfono del Servicio de Asistencia Técnica de EBS;
- Enlace para enviar comentarios, opiniones, observaciones y feedback.

5.6. MENÚ DE CONFIGURACIÓN – HARDWARE

Este capítulo contiene descripciones detalladas y completas de todos los parámetros programables que determinan el funcionamiento del dispositivo.

5.7. RESUMEN

En esta pestaña se presenta tal información como:

- Modelo de dispositivo, número de serie,
- número de particiones creadas en el sistema y de salidas de cables conectadas,
- número de usuarios guardados,
- número de líneas agregadas a la central - sensores, teclados, señalizadores inalámbricos y entradas de cable - y su total.

CALLISTO 32 (CPX230NWB) - Nuevo - EBS Config 2.0

Resumen

HARDWARE

- Resumen
- Ajustes del panel de control
- Particiones
- Dispositivos
- Usuarios
- Configuración de SMS

CENTRO DE MONITORIZACIÓN

- Monitorización de TCP/IP
- Monitorización de SMS
- Modificadores de eventos

CANALES DE CONEXIÓN

Panel de control

Modelo: CALLISTO 32 (CPX230NWB)

Particiones: 0

Salidas cableadas: 0

Sirenas inalámbricas: 0

Usuarios

Usuarios: 1

Controles remotos: 0

Zonas

TOTAL: 0

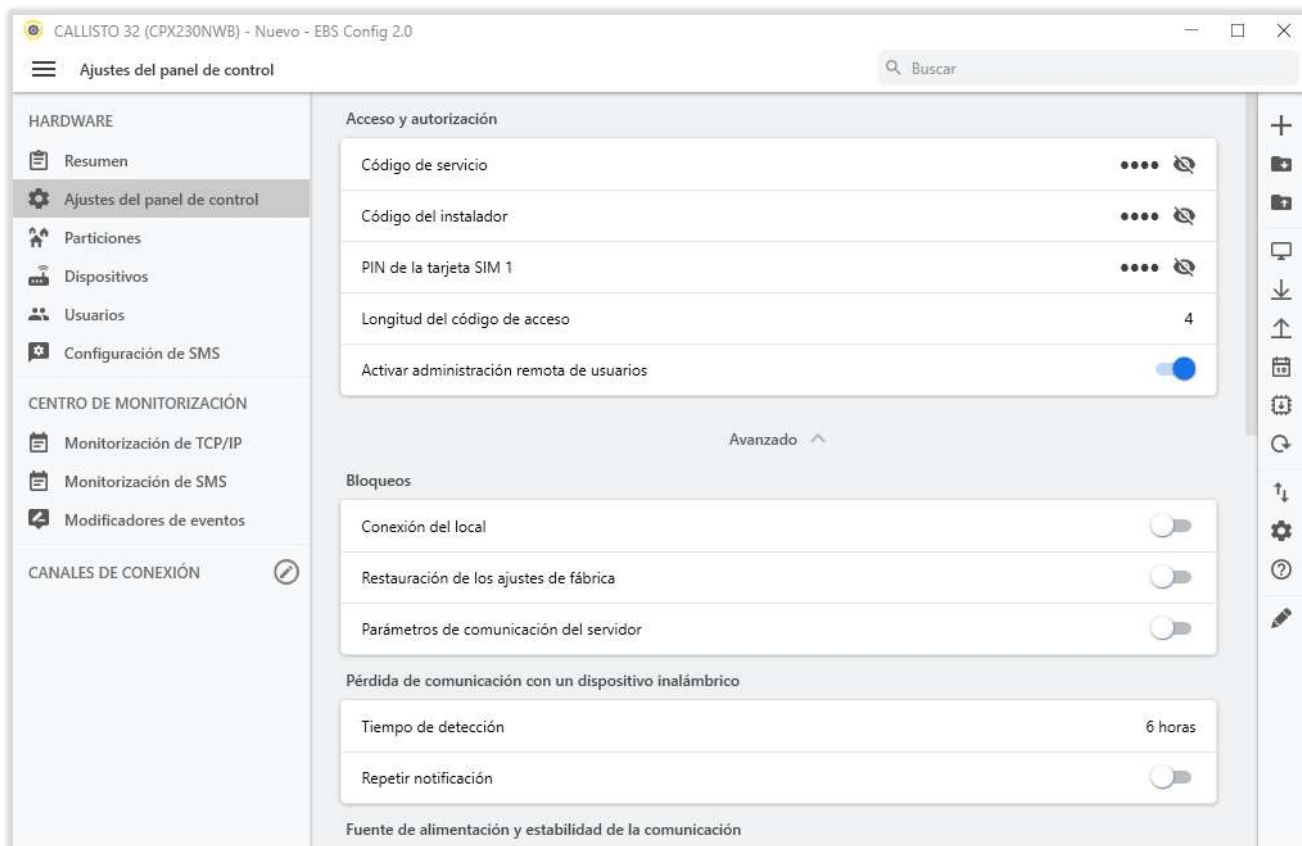
Detectores: 0

Teclados: 0

Entradas por cable: 0

5.8. CONFIGURACIONES DE LA CENTRAL

5.8.1. Acceso y autorización



5.8.1.1. Código de servicio

Este código es el nivel más alto de acceso al sistema. Se usa tanto en el proceso de programación local del dispositivo como en su control a distancia. El código de servicio es, por defecto, 0000. Debe cambiarse durante la primera activación (programación) del dispositivo. Puede contener de cuatro a siete dígitos.

5.8.1.2. Código de instalador

Este código se usa en el proceso de programación local del dispositivo. El instalador que se autoriza mediante este código durante la lectura de los datos del dispositivo **no tiene acceso** a:

- las configuraciones de las secciones: Acceso y autorización, Pérdida de la comunicación de la central con el dispositivo inalámbrico, Alimentación y estabilidad de comunicación - que se encuentran en la pestaña "Configuraciones de la central";
- la pestaña "Canales de comunicación";
- la opción de Permitir gestionar los usuarios a distancia - que se encuentra en la pestaña de "Usuarios";
- a las configuraciones de las secciones: Periodo de validez de los SMS que salen, Restricciones, Transmisión de SMS - que se encuentran en la pestaña "Configuraciones de los SMS",

El código del instalador es, por defecto, 2222. Debe cambiarse durante la primera activación (programación) del dispositivo. Puede tener entre cuatro y siete símbolos. 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.

La lectura del código del instalador desde el nivel de la consola OSM.Server se realizará enviando el comando que diga:

GETPARAM=3,1 -> la respuesta con el código aparecerá en la parte inferior de la ventana de la consola.

La modificación del código del instalador desde el nivel de la consola OSM.Server se realizará enviando el comando que diga:

SETPARAM=3,1,nuevo_código -> donde como nuevo_código hay que introducir una secuencia de entre 4 y 7 cifras

5.8.1.3. PIN de la tarjeta SIM

En este campo introduzca el código PIN de la tarjeta SIM insertada en el dispositivo. Es necesario para activar el sistema automáticamente. Si el número PIN se introduce incorrectamente, una vez insertada la tarjeta y activada la alimentación de la central, el sistema no se activará. La tarjeta bloqueada podrá usarse solamente después de introducir el número PUK (utilizando cualquier teléfono móvil).

Si la tarjeta no tiene PIN, el campo deberá permanecer vacío.

5.8.1.4. Longitud del código de acceso

Esta función permite ajustar la longitud de los códigos de administrador y de usuario (el cambio se aplica a todos los usuarios). El intervalo de longitud es de 4 a 7 dígitos, ambos inclusive. La configuración por defecto es 4.



Sólo se permite reducir la longitud del código si los códigos de usuario acortados no interfieren entre sí.

Al acortar la longitud del código, se recomienda borrar y volver a cargar los usuarios para evitar conflictos.

Por ejemplo:

Existen códigos de 5 dígitos en la base de datos CPX - 44440, 44444, 44449. No será posible acortar la longitud del código a 4 dígitos debido a un conflicto de códigos idénticos. El cambio no se aceptará y aparecerá una ventana de mensaje.

En este caso, una solución es eliminar al usuario o usuarios que tengan códigos similares.

1. Si el código de usuario en la base de datos CPX es más corto que el valor definido, se añade un "0" al código en la base de datos al final del código.

Por ejemplo: Si existe un código 1234 en la base de datos, al cambiar la longitud del código a 6 dígitos, este código se convierte en 123400.

2. Si el código de usuario en la base de datos CPX es más largo que el valor definido, el código de acceso son los 'n' primeros dígitos según el valor establecido.

Por ejemplo: Si existe un código 1234567 en la base de datos, al cambiar la longitud del código a 5 dígitos, este código toma la forma 12345.

3. En el caso de un código bajo coacción:

- Si el código 12345 existe en la base de datos, después de cambiar la longitud del código a 7 dígitos este código toma la forma 1234500, por lo que el código coercitivo es 1234501.

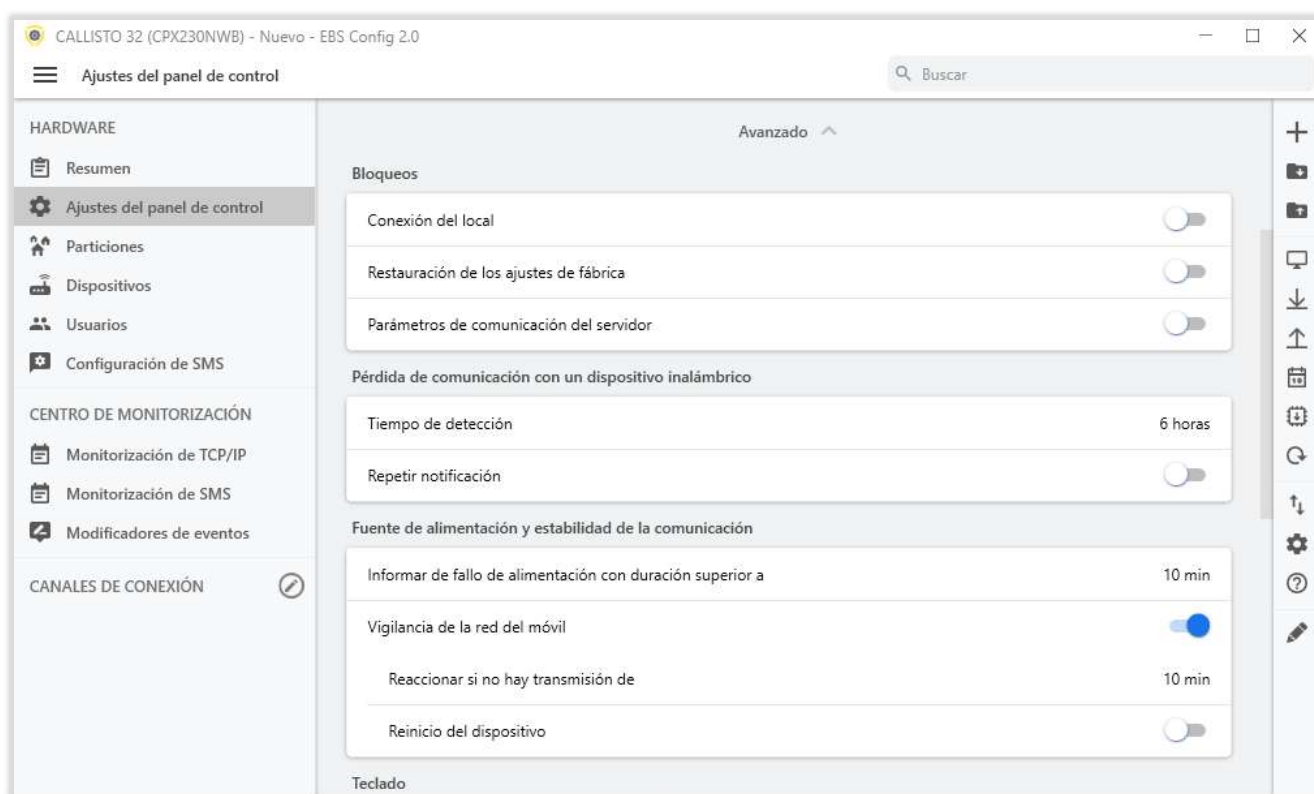
- Si el código 12345 existe en la base de datos, después de cambiar la longitud del código a 4 dígitos este código se convierte en 1234, por lo tanto el código coercitivo se convierte en 1235.

5.8.1.5. Permitir la administración remota de usuarios

Esta opción permite gestionar a distancia las cuentas de los usuarios del sistema de alarmas. Una vez marcada, aparecerá la ventana "Acceso a los datos de los usuarios" que solicitará la introducción del código del administrador.

¡Atención! ¡Si el administrador / usuario quiere utilizar la aplicación móvil EBS Security, esta opción tiene que estar activada!

5.8.2. Bloqueos



5.8.2.1. Bloqueo de la instalación

Tras la activación de esta función el usuario no podrá armar el edificio mediante ninguna vía (como SMS/GPRS, mando, entrada de armado, teclado). Solamente será posible desarmar el sistema.

Todo intento de armado será rechazado por la centralita. La información sobre el rechazo del armado aparecerá en el visualizador del teclado, en el diario de incidencias EBS Config 2.0 y en OSM.Server.

5.8.2.2. Bloqueo del restablecimiento del estado de fábrica

Esta función le permite desactivar la posibilidad de restaurar el código de instalador predeterminado de fábrica. Sin embargo, al restaurar la configuración por defecto, tras seleccionar la opción "Restaurar configuración por defecto", aparecerá una ventana solicitando el código de instalador o el código de servicio (ATS).

Cuando se activa esta función, el fabricante recomienda cambiar el código de acceso del instalador y el código de servicio (ATS) por el nuevo.

NOTA: Si se pierden los códigos recién configurados, será necesario enviar los dispositivos bloqueados al servicio EBS.

5.8.2.3. 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»,

será 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.

5.8.3. Pérdida de comunicación con el dispositivo inalámbrico

Esta función permite reportar la pérdida de la transmisión desde los sensores inalámbricos a la estación de monitoreo.

5.8.3.1. Tiempo de detección

Aquí tendrá que definir en qué tiempo desde la detección de la pérdida de comunicación con el dispositivo inalámbrico (como mín. al cabo de 2 horas, como máx. al cabo de 24 horas) la central enviará la información correspondiente a la estación de monitoreo. El valor configurado por defecto es de 6 horas.

5.8.3.2. Envío cíclico de notificaciones

Esta opción activa el envío de los informes cíclicos sobre la pérdida de los sensores inalámbricos a la estación de monitoreo en periodos definidos (si se produce una pérdida de comunicación continua). En el campo "Repetir cada [h]", moviendo el deslizador, podrá configurar entre 2 y 24 horas.

5.8.4. Alimentación y estabilidad de comunicación

5.8.4.1. Informe sobre la falta de alimentación AC superior a

Aquí tendrá que definir el tiempo después del cual se reportará la avería de alimentación.

5.8.4.2. Control de conexión con la red móvil

Esta opción permite que la central reaccione automáticamente cuando pierda la comunicación con la red móvil GSM o cuando la transmisión GPRS no sea posible.

Después de activarla, aparecerán dos campos adicionales.

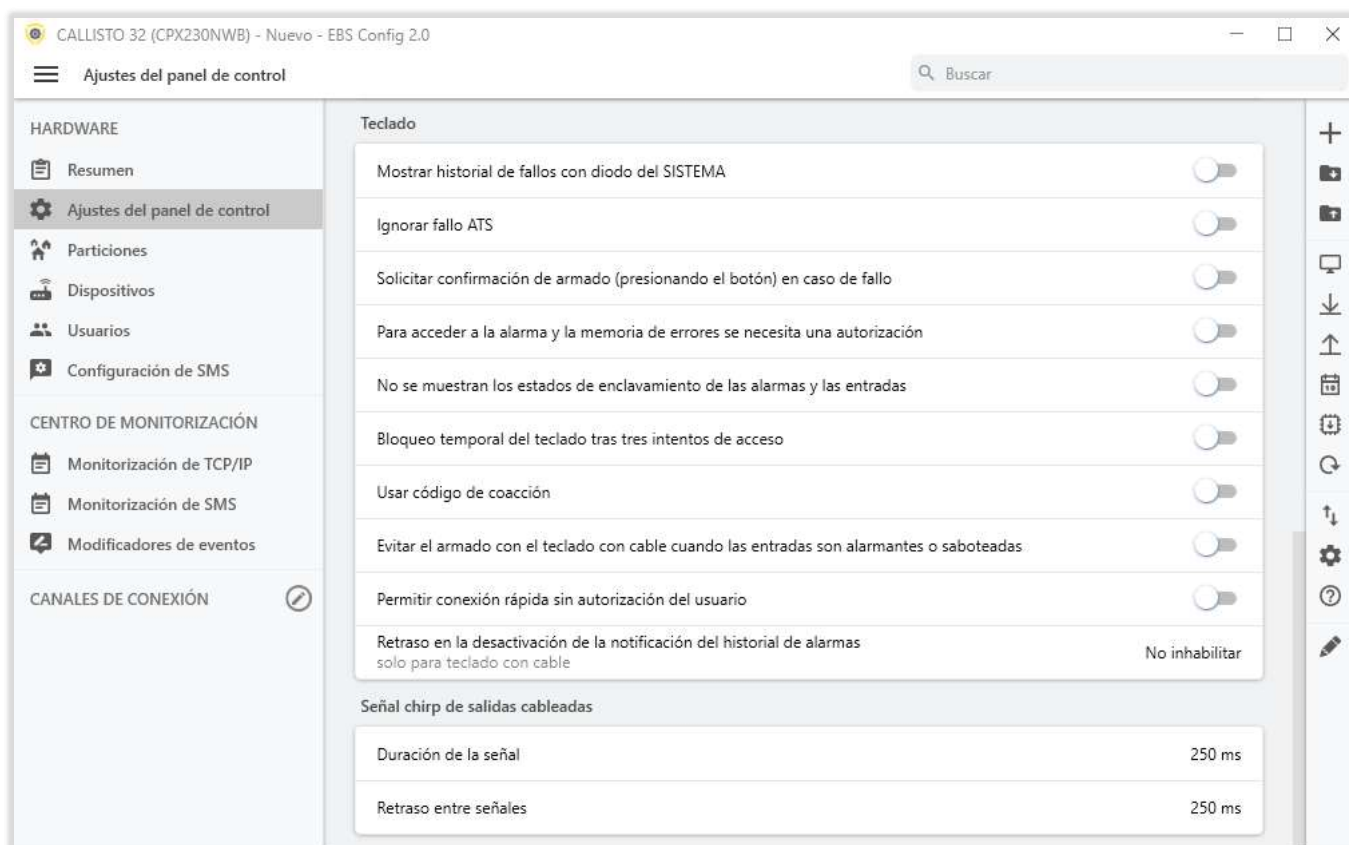
5.8.4.2.1. Reaccionar si no hay transmisión durante

Aquí tendrá que definir tiempo desde la detección de la pérdida de comunicación con la red (falta de transmisión) después del cual el dispositivo iniciará el reseteo del módem.

5.8.4.2.2. Reinicio del dispositivo

Aquí tendrá que definir el tiempo desde la detección de la pérdida de comunicación con la red (falta de transmisión) después del cual el dispositivo iniciará el reseteo de sí mismo (y no solo del módem).

5.8.5. Teclado y mando



5.8.5.1. Señalización de la memoria de averías mediante el parpadeo del diodo SISTEMA

La selección de esta opción señalará la aparición y finalización de fallos en el sistema mediante el parpadeo del LED SYSTEM en el teclado KP32/KP2W hasta que se borre la memoria de fallos.

5.8.5.2. Ignorar fallo ATS

Al seleccionar esta opción se desactiva la indicación de pérdida de comunicación con el servidor en el teclado KP32/KP2W.

5.8.5.3. Exigir confirmación de armado (pulsando #) 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.*

5.8.5.4. El acceso al historial requiere autorización

La selección de esta opción limita la visualización del historial de alarmas y del historial de fallos. El acceso al historial se realiza tras introducir el código de usuario. Esta opción debe estar activada para cumplir con el Grado 2.

5.8.5.5. No visualización del estado de alarma y bloqueo

Al seleccionar esta opción, las violaciones de línea y los bloqueos de línea actuales no se mostrarán en el teclado. Esta opción debe estar activada para el cumplimiento del Grado 2.

5.8.5.6. Bloqueo temporal del teclado después de tres intentos fallidos de acceso

Al seleccionar esta opción se activa el bloqueo del teclado. Cuando se introducen 3 códigos incorrectos consecutivamente, el teclado se bloquea durante un periodo de 90 segundos. Durante este tiempo, no se puede acceder a ninguna función del panel de control desde el teclado. Una vez transcurrido el tiempo de bloqueo, se producirá el siguiente bloqueo del teclado después de introducir 3 códigos erróneos consecutivamente. La introducción de un código correcto (por ejemplo, después de 2 códigos incorrectos) pone a cero el contador de códigos incorrectos. Esta opción debe estar activada para mantener la conformidad con el Grado 2.

5.8.5.7. Utilizar código de coacción

Un código de coacción (código de coacción) permite generar un evento adicional durante el armado/desarmado para informar a la central receptora de una amenaza sin alarma acústica.

5.8.5.8. Deshabilitar armado de teclado cableado durante violación de zona o manipulación.

Seleccionando esta opción se deshabilitará el armado con KP32 cuando las zonas sean violadas o manipuladas. La violación/manipulación de cualquier zona asignada al sistema se señala mediante el apagado del diodo READY - D para la zona perteneciente a la partición 1, 4 para la zona perteneciente a la partición 2. Cuando el sistema está dividido en dos particiones, basta con que un detector de una de ellas sea violado/manipulado para que la central se desarme. Al intentar armar, el teclado cableado emitirá un pitido alto de un segundo con el encendido simultáneo de los LEDs GRUPO, ALARMA, SISTEMA y PROG durante aproximadamente 4 segundos. Los fallos del sistema no afectan a esta opción.

NOTA: Opción disponible a partir de la versión de firmware 2.8.8.

5.8.5.9. Permitir el armado rápido sin autorización del usuario.

Si se selecciona esta opción, el armado rápido del sistema mediante el teclado estará disponible sin necesidad de introducir un código de autorización de usuario.

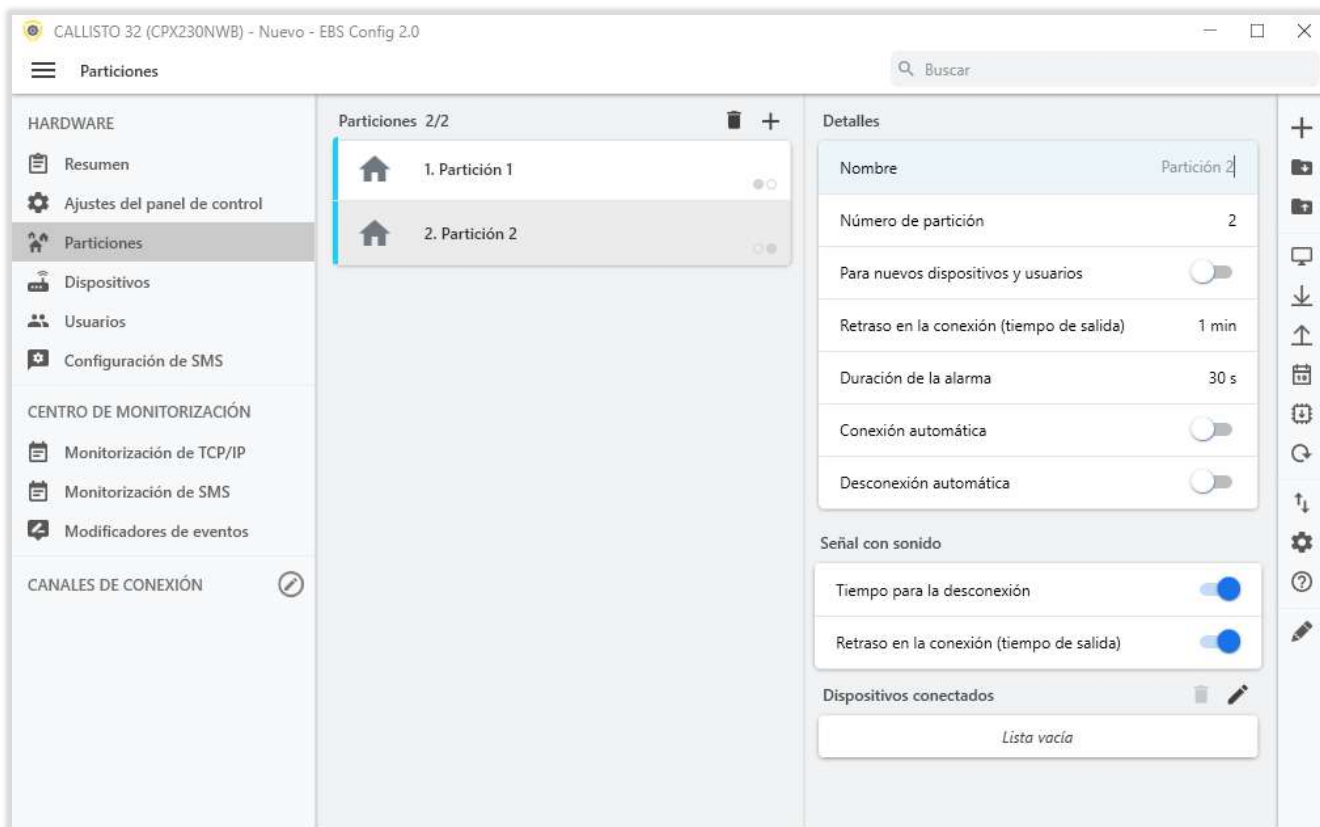
5.8.5.10. Retraso en la desconexión de la señalización de alarmas históricas

Esta función sólo está disponible cuando está activada la opción "Desactivar la señalización de alarma histórica tras el desarmado". Establece el retardo en segundos tras el cual las alarmas históricas dejarán de presentarse en el teclado. Es decir, cuando el sistema está armado y hay violaciones de las zonas de entrada señaladas por el parpadeo de los LEDs F y 6, los LEDs se apagarán una vez desarmado y transcurrido el tiempo definido. La visualización del estado de las alarmas seguirá disponible después de introducir la función 3# hasta que el usuario las borre.

5.8.6. Pitido de las salidas cableadas

Cuando se activa cualquier salida, se genera una señal acústica. En el campo "Duración de la señal" puedes fijar la duración del sonido (haciendo clic en el campo se amplía la lista), mientras que en el campo "Intervalo entre señales" defines el intervalo entre sonidos sucesivos.

5.9. PARTICIONES



La pestaña presenta el número de las particiones creadas y permite configurarlas. Para agregar una partición nueva, pulse **+** en la sección de *Particiones*, para eliminar **✖**.

5.9.1. Detalles

5.9.1.1. Nombre y número de la partición

En el campo de "Nombre" podrá agregar cualquier nombre de 15 caracteres. En el campo de "Número de partición" podrá adscribirle cualquier número entre 1 y 2.

5.9.1.2. Para dispositivos y usuarios nuevos

Tras activar esta opción, todas las salidas de cables, dispositivos tales como sensores, teclados y sirenas inalámbricas, así como usuarios, que se agreguen a partir de entonces, serán adscritos a la partición/es dada/s.

5.9.1.3. Retraso en el armado (tiempo para salir)

Aquí tendrá que definir el tiempo necesario para salir del área de la partición en curso de armar. Una vez transcurrido el tiempo definido, la partición se armará.

5.9.1.4. Duración del alarma

Aquí se determina el tiempo de señalización del alarma por el teclado que pertenezca a la partición dada.

5.9.1.5. Armado / desarmado automático

En esta sección, puede configurar los parámetros para el armado y desarmado automático de cada partición.

Al hacer clic en el control deslizante  de una opción determinada, la activamos. Después de la activación, aparece un campo adicional donde puede configurar el tiempo de armado / desarmado automático.



A la hora de armado establecida, comienza la cuenta atrás del retardo de salida –el usuario puede anular 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.

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 transcurrido este tiempo, se generará un evento de bloqueo. La entrada permanecerá bloqueada hasta que se desarme la partición.

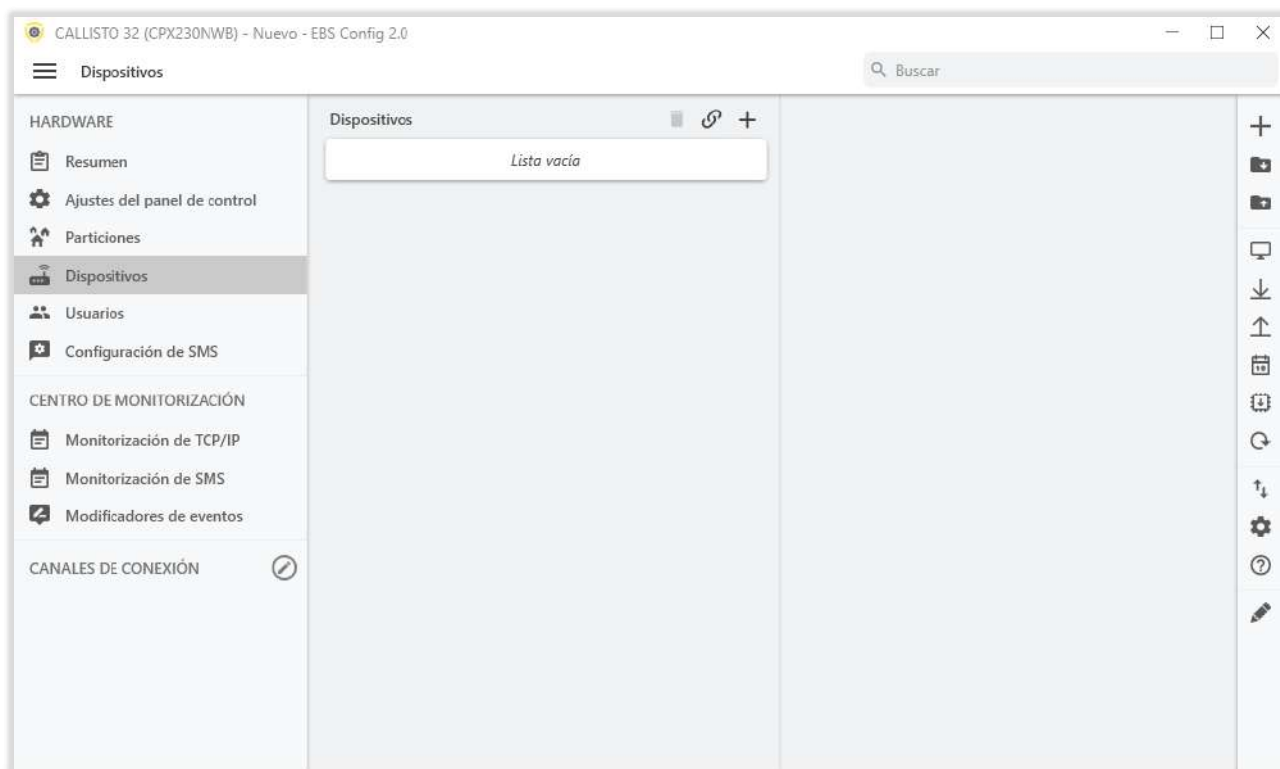
Si la hora del sistema se adelanta (por ejemplo, al cambiar la hora de invierno a verano), se omitirán los eventos de armado/desarmado programados durante este tiempo. Por ejemplo: si el armado automático está programado para las 02:30, al cambiar la hora de invierno a verano (de 2:00 a 3:00), no se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

5.9.2. Dispositivos asignados

Aquí puede ver los dispositivos asignados a la partición, así como añadir nuevos dispositivos pulsando el lápiz. Aparecerá una lista de dispositivos, donde podrá decidir qué dispositivos se asignarán a la partición haciendo clic en el control deslizante situado junto al dispositivo correspondiente.

5.10. DISPOSITIVOS

El panel de control dispone de 32 líneas de monitorización (entradas) totalmente configurables y 3 salidas controladas por software. Estas líneas pueden dividirse de cualquier manera entre dos particiones. Cada línea y cada salida tienen una serie de parámetros programables que se describen a continuación. Para añadir un dispositivo, zona y/o salida cableada, pulse **+**. En la ventana que aparece, seleccione el elemento adecuado, asígnele un nombre, seleccione el número de línea (para la entrada) y/o el número de salida y, a continuación, guarde los datos introducidos pulsando el botón Añadir.



5.10.1. Agregación de dispositivos inalámbricos

La unidad permite añadir hasta 32 detectores inalámbricos etiquetados de A1 a A8, de B1 a B8, de C1 a C8 y de D1 a D8, correspondientes a los símbolos del teclado KP32.

Los dispositivos inalámbricos (detectores, teclados, mandos a distancia, sirenas inalámbricas) pueden añadirse de dos maneras. La primera - pulsando el símbolo Añadir , seleccionando Dispositivo Inalámbrico en "Tipo de Línea/Dispositivo", introduciendo el número de serie que se encuentra en el dispositivo.

Añadir zona o dispositivo

Dispositivo inalámbrico

IN

Entrada cableada

OUT

Salida cableada

Parámetros necesarios

Número de serie

Introducir número de serie

El tipo de dispositivo es desconocido

Añadir

Cancelar

¡ATENCIÓN! ¡Para agregar los dispositivos de esta manera será necesario enviar la configuración a la central!

La segunda manera utiliza la comunicación por la radio. Para agregar un dispositivo nuevo, deberá asegurarse de que no está emparejado con otro sistema (véase las instrucciones para los distintos dispositivos). De ser así, primero deberá desemparejarlo; de lo contrario, podrá proceder al emparejamiento.

Para ello, pulse el símbolo  *Detectar dispositivo*. La central entrará en el modo de agregación e iniciará la detección de dispositivos. Inserte la batería en el dispositivo (si no estaba insertada) o estimule / presione el switch de sabotaje (si las baterías ya estaban insertadas), para que el dispositivo envíe el comunicado de emparejamiento. Aparecerá una ventana con el nombre y el número de serie del dispositivo detectado y agregado.

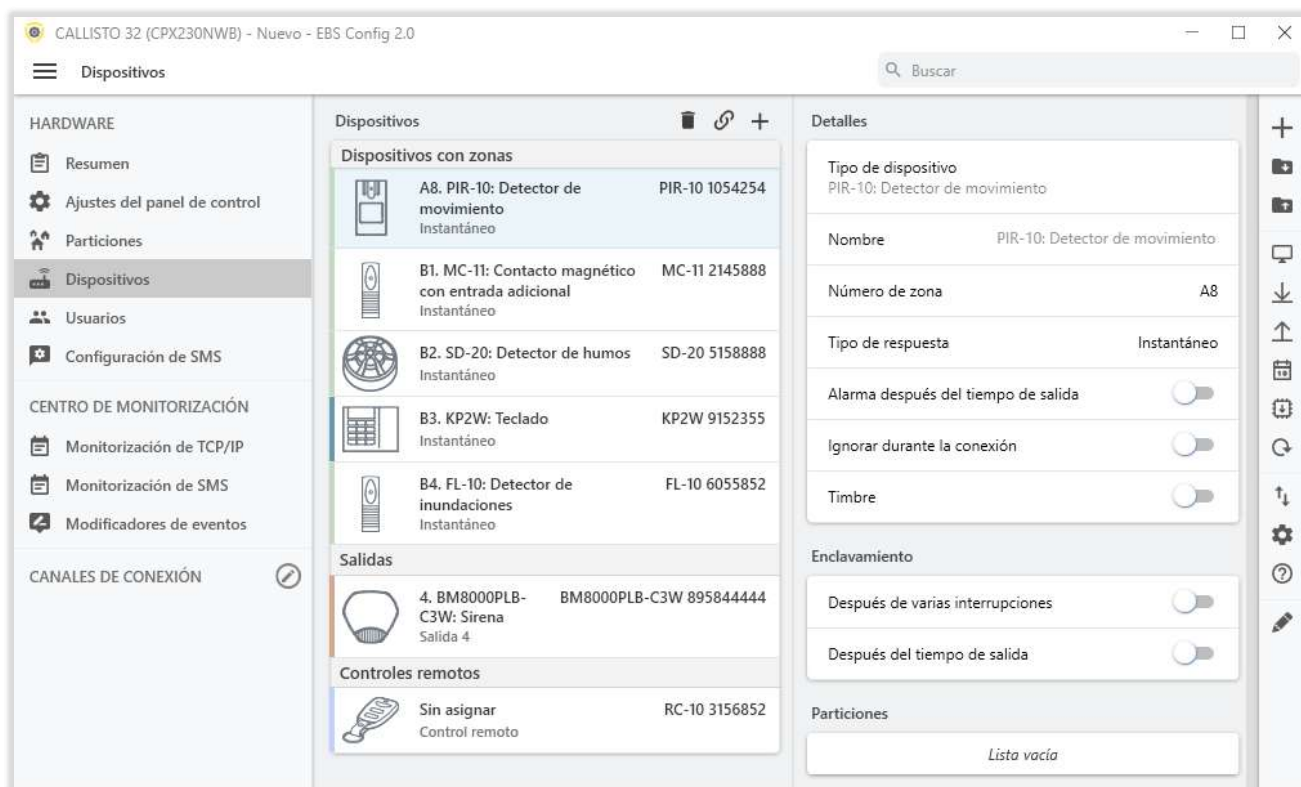
¡ATENCIÓN! Este método no se aplica al dispositivo de alarma BM8000PLx-C3W.

El grupo de dispositivos con líneas incluye: detectores magnéticos MC-10, MC-11, detectores de movimiento PIR-10, PIR-11, detectores de humo SD-20, detectores de rotura de cristales GB-10, detectores de desplazamiento MD-10, teclados KP2W, detectores de inundación FL-10 y dispositivos de señalización inalámbricos.

5.10.2. Dispositivos con líneas

El grupo de dispositivos con líneas incluye: detectores magnéticos MC-10, MC-11, detectores de movimiento PIR-10, PIR-11, detectores de humo, SD-20, detectores de rotura de cristales GB-10, detectores de desplazamiento MD-10, detectores de inundación FL-10, detectores de gas GS-21 y GS-22, teclados KP2W y dispositivos de señalización inalámbricos .

5.10.3. Detectores inalámbricos (familia MC, PIR, GB, SD, MD, FL y GS)



En la sección Detalles, puede dar un nombre al detector seleccionado, cambiar el número de línea en relación con el dado al añadirlo, establecer el tipo de respuesta, activar la opción "Alarma tras tiempo de salida". En la sección Bloqueo, puede especificar después de qué número de violaciones bloquear el detector. En la sección Particiones, puede asignar un detector a una partición.

5.10.3.1. Tipo de reacción

- **Bloqueada** - Esta línea significa el bloqueo permanente. No enviará ninguna información acerca del cambio de su estado.
- **Instantáneo** - La violación de esta línea disparará un alarma inmediata si el sistema está armado.
- **Retrasada** - Este tipo de línea se utiliza normalmente para manejar los sensores de entradas a edificios. 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 tiempo para la entrada para la partición seleccionada. Para evitar que el sistema dispare una alarma, debe desarmarse antes de que haya transcurrido el tiempo programado.
- **24hrs contra asalto** - Esta línea dispara el alarma inmediata independientemente de que el sistema esté armado o no.
- **De armado/desarmado por infracción** - Esta línea podrá utilizarse para armar 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.

Atención: Para las líneas alámbricas es recomendable configurar la salida como NC o NO para este tipo de respuesta.

- **De 24hrs de sabotaje** - Esta línea podrá utilizarse para conectar los circuitos de sabotaje de los sensores. 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.
- **Retrasada condicionalmente** - La línea podrá usarse si el teclado del sistema no se encuentra en la primera área violada al acceso 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 el tiempo para la entrada es descontado, la línea se portará como retrasada, en caso contrario se portará como inmediata.
- **De 24hrs contra asaltos silenciosa** - La violación de esta línea provocará el envío de la información sobre el evento, independientemente de que el sistema esté armado o no. La violación de la línea no ocasiona la activación de la salida y aviso de teclado.
- **De 24hrs contra incendio** - Funciona de manera similar a la línea de 24hrs contra asaltos.
- **Perimetral** - Línea que se arma 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 mediante el código, sin que se seleccione el modo de armado, la violación de esta línea durante la cuenta atrás del tiempo para salir provocará el armado del sistema en el 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. Esta línea tiene asignado un retraso y se comporta como una línea temporizada normal cuando el sistema está armado.

- **De 24hrs contra gas** - Funciona de manera similar a la línea de 24hrs contra asaltos.
- **De 24hrs contra inundaciones** - Funciona de manera similar a la línea de 24hrs contra asaltos.
- **Nocturna (desactivada durante la noche)** - Este tipo de línea se utiliza para los sensores situados en lugares por donde pueda moverse la gente durante la 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 retrasada** - Cuando el sistema esté armado en el modo nocturno, la violación de esta línea provocará la cuenta atrás del tiempo para entrar. 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.
- **De armado/desarmado por el cambio de estado** - La violación de esta línea armará la partición a la que esté adscrita. 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.

Atención: Para las líneas alámbricas es recomendable configurar la salida como NC o NO para este tipo de respuesta.

5.10.3.1.1. Retraso

El parámetro de "Retraso" aparecerá cuando se seleccione para el dispositivo el tipo de reacción siguiente: retrasada, retrasada condicionalmente, perimetral de salida, nocturna retrasada. En este campo se determina el tiempo de retraso después del cual se generará el alarma, contando desde el momento de la detección de la violación de la línea. Cuando despliegue la lista, aparecerán los valores más frecuentes desde 1 s hasta 15 min. Para seleccionar un retraso no estándar, podrá introducir otro valor conveniente.

5.10.3.2. Alarma después del retardo de salida

Tras la activación de esta opción, una vez transcurrido el tiempo para salir de la partición armada, la línea que ésta tenga adscrita y que quede violada (p.ej. apertura del sensor MC-30) generará el alarma del sistema.

Si esta opción está desactivada, el primer alarma de la línea se generará una vez se restablezca su estado normal (p.ej. cierre del imán con el sensor MC-30) y se produzca una violación nueva.

5.10.3.3. Ignorar a la hora de rearmar

Tras la activación de esta opción, durante el armado de la partición el sistema no averiguará si la línea está violada o no - y podrá armarse incluso con la línea violada. Cuando esta opción esté desactivada y se produzca una violación, la partición no se armará (a no ser que el usuario esquivé el bloqueo del armado - véase el capítulo 4.2.3.1. En el caso de avería, requiera armado doble desde el teclado).

5.10.3.4. Timbre

La función Timbre se utiliza para informar a las personas que se encuentran en el recinto de una violación de las líneas de entrada (por ejemplo, cuando se abre la puerta de entrada). Durante una violación, se activa una señal acústica mediante el teclado (cuando el sistema está desarmado), sin enviar un informe de alarma a la central receptora.

Cuando el sistema consta de más de un teclado, todos emitirán un pitido cuando se viole una zona (sólo se aplica a los teclados cableados).

5.10.3.5. Bloqueo

Esta opción permite bloquear cualquier línea, de ahí que los cambios de su estado queden ignorados por el sistema y no sean reportados al estación de monitoreo. Las líneas bloqueadas automáticamente (Alcanzado el número de violaciones y Transcurrido el tiempo para salir) serán desbloqueadas automáticamente una vez desarmada la partición a la que pertenezcan.

Alcanzado el número de violaciones

Tras marcar esta opción aparecerá una partida adicional de *Violaciones*, en la cual, mediante el deslizador, podrá configurar el bloqueo de la línea cuando se alcance el número configurado de violaciones (entre 1 y 100).

Transcurrido el tiempo para salir

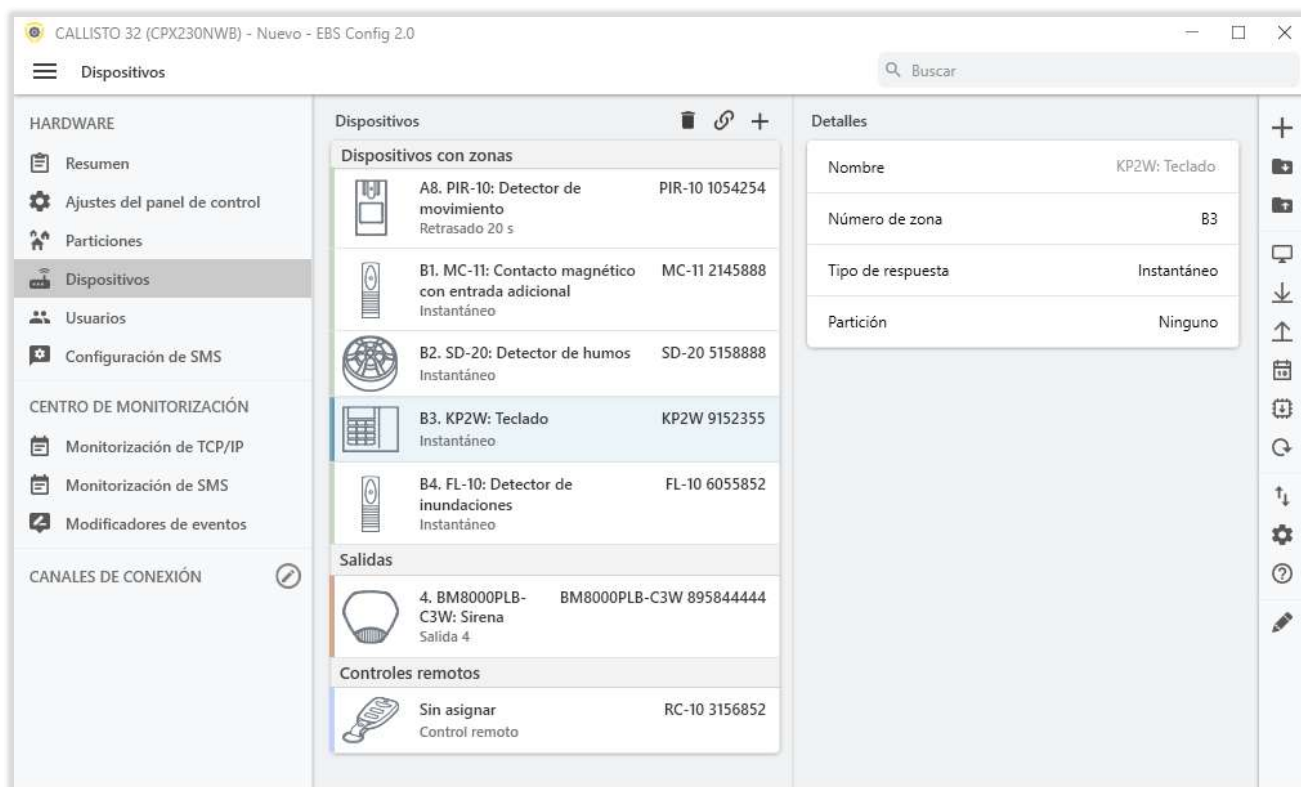
Tras marcar esta opción, la línea se bloqueará (se activará la función bypass) si se encuentra violada o en el estado de sabotaje en el momento de armado. También se generará un evento de bloqueo, lo que permite informar la estación de monitoreo sobre el fallo. Si para la misma línea se marca también la opción de "alarma una vez transcurrido el tiempo para salir", entonces el "bloqueo una vez transcurrido el tiempo para salir" tendrá la prioridad - la línea quedará bloqueada y no generará alarma.

5.10.3.6. Particiones

En esta sección podrá adscribir el sensor a la partición dada.

5.10.4. KP2W teclado

En la sección Detalles, es posible dar un nombre a la selección, cambiar el número de línea en relación con el dado al añadirla, establecer el tipo de respuesta o asignar un teclado a una partición.



Atención: El teclado inalámbrico KP2W sólo puede asignarse a una partición.

5.10.4.1. Tipo de reacción

- **Bloqueada** - Esta línea significa el bloqueo permanente. No enviará ninguna información acerca del cambio de su estado.
- **Instantáneo** – La violación de esta línea disparará un alarma inmediata si el sistema está armado.

5.10.5. Sirena exterior BM8000PLx-C3W (compatible a partir de la versión FW 2.11.4)

Para que la sirena de exterior BM8000PLx funcione, es necesario conectar a la placa un módulo transceptor llamado controlador.

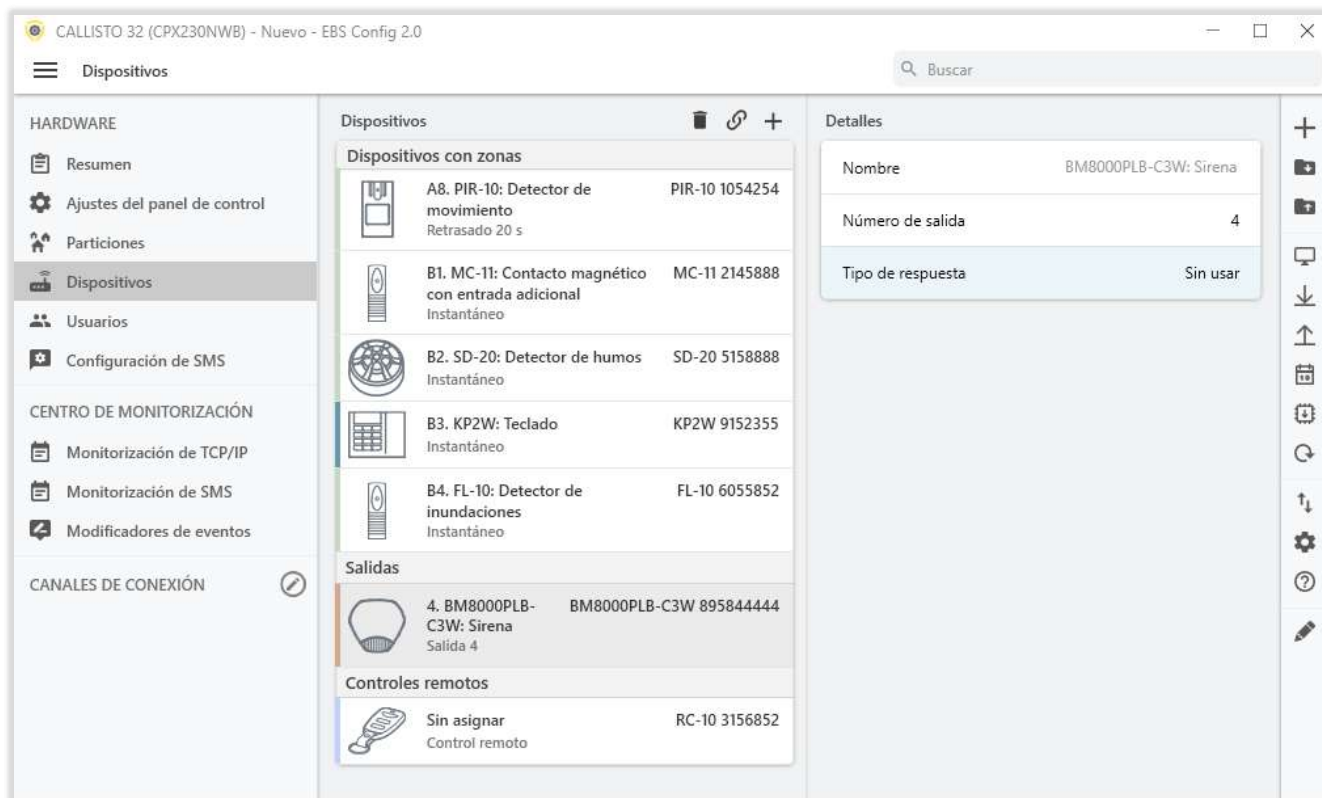
Atención: Consulte el manual del controlador WLM C3W para conocer el método de instalación con el panel de control.

El controlador permite la comunicación inalámbrica entre el panel de control y la sirena inalámbrica.

Añadir un dispositivo de alarma al sistema mediante EBS Config 2.0 sólo es posible introduciendo el número de serie haciendo clic en  la sección Dispositivo.

En la ventana que aparece, introduzca el número de serie S/N que se encuentra en la etiqueta del dispositivo de señalización (el tipo de dispositivo aparecerá automáticamente después de introducir los dos primeros dígitos), y en la posición Número de salida seleccione la salida 4, 5 ó 6 reservada para los dispositivos de señalización inalámbricos.

Una vez completados los datos, pulse OK. El dispositivo será visible en la lista de dispositivos guardados.

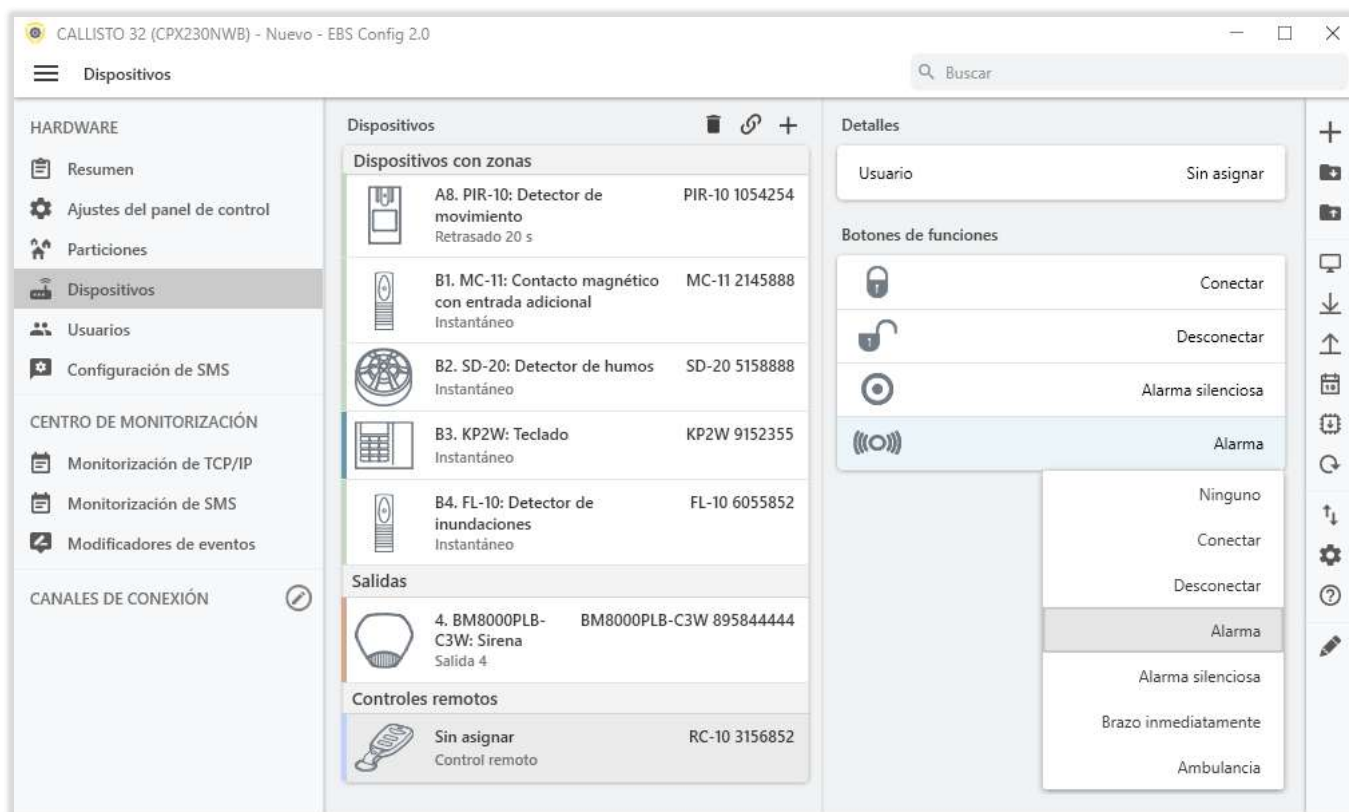


5.10.5.1. Tipos de salida

- No usadas – La salida es inactiva.
- Alarma – La salida se activa en el momento de detectar una alarma.
- 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.

El último paso importante es enviar los dispositivos guardados a la memoria de la centralita pulsando Enviar  en la barra de acceso rápido. Esto es necesario para que el dispositivo de alarma se comunique con el panel de control (a través del controlador).

5.10.6. Mando a distancia RC-10



El configurador permite añadir y configurar mandos a distancia para el control inalámbrico del panel de control. El procedimiento para añadir un mando a distancia es el mismo que para añadir otros dispositivos inalámbricos (consulte la sección 5.10.1).

En la sección Detalles, tras ampliar la lista, se puede asignar el mando a distancia seleccionado a un usuario.

En la sección Funciones de los botones, a cada uno de los 4 botones se le puede asignar una acción que realizará el panel de control al pulsarlo:

- La función "Armar" significa armar el panel en modo completo.
- La función "Desarmar" significa desarmar la central.
- La función "Alarma" significa activar una alarma con señalización acústica.
- La función "Alarma silenciosa" significa una alarma sin señalización acústica.
- La función "Asistencia médica" funciona según el mismo principio que el botón "AYUDA" del teclado, es decir, genera una alarma médica.
- La función "Armar Inmediatamente" le permite armar el sistema inmediatamente, omitiendo el tiempo de salida establecido.,

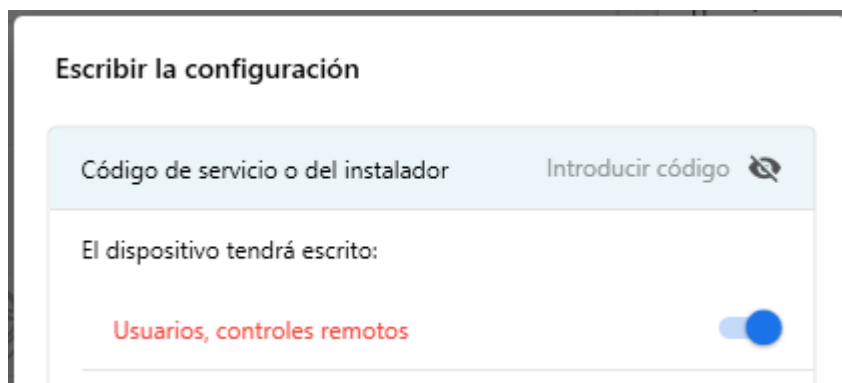


Atención: Asegúrese de que el número de usuario seleccionado está activado por el Administrador (se debe generar un código de acceso para este número).

Las alarmas del mando a distancia funcionan independientemente de si la partición correspondiente está armada o no. Para ambos tipos de alarma, se puede enviar un mensaje al centro de supervisión, dependiendo de la configuración del panel de control.

El fabricante recomienda asignar el botón marcado con ((O)) a una alarma normal y el botón (O) a una alarma silenciosa. Como el panel de control permite asignar las teclas del mando a distancia a distintas funciones, es posible activar la alarma con un botón diferente.

La información de configuración del mando a distancia se enviará automáticamente a la central. No obstante, el fabricante recomienda que, una vez añadido y configurado el mando o mandos a distancia, se envíe esta información pulsando la flecha "Enviar" de la barra de acceso rápido. Aparecerá la ventana de envío de la configuración, en la que deberá seleccionar con el control deslizante la opción "Usuarios, mandos a distancia".



5.10.7. Entradas de cables

En la sección de *Detalles* podrá poner/cambiar el nombre, seleccionar el modo de trabajo de la entrada, configurar el tipo de reacción (véase el capítulo *Tipo de reacción*), configurar la sensibilidad adecuada, activar la opción de "Alarma una vez transcurrido el tiempo para salir" (véase el capítulo *Alarma después del retardo de salida*) e "Ignorar al armar" (véase el capítulo *Ignorar a la hora de rearmar*). En la sección de *Bloqueo* podrá determinar el número de violaciones después del cual se bloqueará el sensor (véase el capítulo *Bloqueo*). En la sección de *Particiones* podrá adscribir el sensor a la partición.

5.10.7.1. Modo

Este parámetro permite determinar el estado estable de la 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 / TEOL.

NO - modo de configuración de la línea de entrada que permite reconocer dos estados: normal (vigilancia) - relé NO abierto, y de alarma (violación) - relé NO cerrado.

NC - modo de configuración de la línea de entrada que permite reconocer dos estados: normal (vigilancia) - relé NC cerrado, y de alarma (violación) - relé NC abierto.

EOL - modo de configuración de la línea de entrada por parámetros, que permite reconocer tres estados de trabajo: normal (vigilancia), alarma (violación) y avería, gracias al uso del resistor de parametrización con el valor de 2,2kΩ.

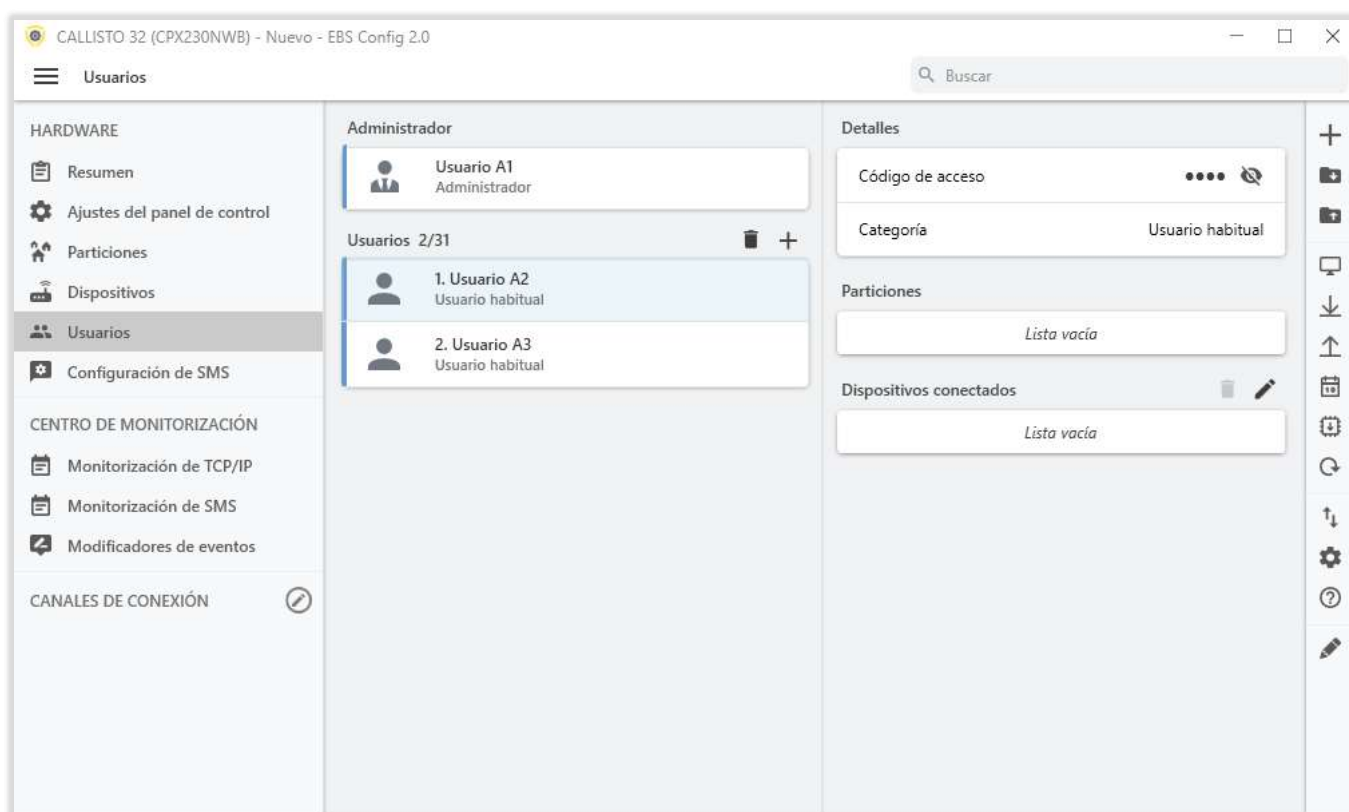
DEOL - modo de configuración de la línea de entrada por dos parámetros, que permite reconocer 4 estados de trabajo: normal (vigilancia), alarma (violación), sabotaje y avería de la línea (p.ej. cortocircuito del cable), gracias al uso de dos resistores de parametrización con el valor de 1,1kΩ.

TEOL - modo de configuración de la línea de entrada que permite doblar la líneas, es decir, conectar dos sensores alámbricos a la misma borna de la central. Esta configuración permite detectar de qué detector proviene la alarma, la información de sabotaje es compartida. Para cada detector son necesarias dos resistencias.

5.10.7.2. 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. Cuando despliegue la lista, aparecerán los valores más comunes, desde 250 ms hasta 2 s. Para seleccionar un retraso no estándar, podrá introducir otro valor conveniente.

5.11. USUARIOS



Para activar la opción de *Edición de gestión de usuarios* será necesario conocer el código del administrador que deberá introducirse en la ventana que aparezca. El código predeterminado de administrador es 1111.

Después de una correcta autorización, en la pestaña aparecerán las opciones y parámetros adicionales para configurar y gestionar los usuarios.

El **Administrador** se agrega al sistema por defecto y tiene el acceso más amplio al sistema de todos los usuarios. Está autorizado a gestionar los usuarios, (p.ej. agregar/eliminarlos, cambiar los códigos, categorías) y acceder a todas las particiones, lo cual no se podrá cambiar. En la sección de *Detalles* podrá cambiar el nombre y el código de acceso del administrador. En la sección *Dispositivos asignados*, se pueden asignar los mandos a distancia correspondientes.

Podrá agregar al **nuevo usuario** pulsando **+** al lado de la sección de *Usuarios*. Además de cambiar el nombre y el código de acceso, podrá cambiar sus autorizaciones en la partida de *Categoría* en la sección de *Detalles*, así como otorgar el acceso a las particiones (todas o solamente las seleccionadas) en la sección de *Particiones*.

Existen 2 categorías de usuarios con diferentes niveles de acceso a las funcionalidades del sistema:

- **Usuario habitual** - esta categoría se asignará por defecto al nuevo usuario. Podrá armar y desarmar, tendrá acceso desde la aplicación móvil EBS Security al historial de alarmas y averías, estado de entradas, así como al bloqueo de las entradas, cambios de su código, ensayos de las entradas y salidas,
- **No autorizado** – un usuario que podrá únicamente armar el sistema.

5.12. CONFIGURACIONES DE SMS

CALLISTO 32 (CPX230NWB) - Nuevo - EBS Config 2.0

Configuración de SMS

Buscar

HARDWARE

- Resumen
- Ajustes del panel de control
- Particiones
- Dispositivos
- Usuarios
- Configuración de SMS**

CENTRO DE MONITORIZACIÓN

- Monitorización de TCP/IP
- Monitorización de SMS
- Modificadores de eventos

CANALES DE CONEXIÓN

Gestión de SMS

- Llamar antes de enviar SMS
- Eliminar los mensajes SMS no enviados al desconectar la partición
- Aceptar comandos SMS: De cualquier persona

Período de validez de los mensajes SMS enviados

- Pruebas enviadas periódicamente al servidor: Máximo
- Eventos enviados al servidor: Máximo
- Eventos enviados al usuario: Máximo
- Respuestas para comandos SMS: Máximo

Límites

- Activo
- Cantidad máxima: 10
- Reinicio del contador: 1 hora
- Pruebas enviadas periódicamente al servidor
- Eventos enviados al servidor
- Eventos enviados al usuario
- Respuestas para comandos SMS

Reenvío de SMS 0/2

Lista vacía

Notificaciones de SMS

5.12.1. Gestión de SMS

5.12.1.1. Llamar antes de enviar un SMS

La opción "Llamar antes de enviar SMS" debe seleccionarse si el usuario desea recibir información adicional sobre un mensaje SMS entrante. Si esta opción está activada, el dispositivo llama al número de teléfono del usuario antes de enviar un SMS para informarle de la recepción de un mensaje SMS.

La llamada puede tardar varias decenas de segundos en intentarse, y el usuario puede rechazarla o contestarla. Una vez que el usuario responde a la llamada, el dispositivo se desconecta. Independientemente de lo que haga el usuario, el intento de llamada va seguido de un mensaje SMS. Una vez que se ha enviado un mensaje al primer usuario (al primer número de teléfono definido), se intenta llamar al siguiente usuario y enviarle un mensaje.

Con más mensajes por enviar, no se realiza un intento de llamada de voz más a menudo que cada 15 minutos.

5.12.1.2. Borrar SMS no enviados al desarmar la partición

Al activar esta opción, los mensajes SMS relacionados con la partición desarmada y todo el sistema (excepto la partición armada si permanece en el sistema) se borrarán al desarmar.

Si el usuario desarma todas las particiones, se borrarán todos los SMS pendientes.

Los mensajes SMS relacionados con nuevos eventos que se produzcan después de que la partición se haya desarmado se almacenarán en la memoria del dispositivo y se enviarán lo antes posible.

Nota: El fabricante no recomienda el uso de esta opción ya que reduce la seguridad del sistema. Sólo para usuarios avanzados.

5.12.1.3. Aceptar comandos SMS

El usuario puede restringir el acceso remoto al dispositivo (por medio de SMS) a números de teléfono específicos. El listado creado de números (hasta 5) significa que solamente de estos números será posible controlar el dispositivo.

Las opciones disponibles son:

- **De todos:** Significa que la comunicación es posible desde cualquier número de teléfono.
- **No aceptar:** Significa falta de la posibilidad de comunicación.
- **De números seleccionados:** Significa que la comunicación sólo es posible con los números de teléfono de la lista. Se permite definir hasta 5 números.

Tras seleccionar «Permitir a los seleccionados» se obtiene el acceso al campo de edición. Introduzca los números siguientes en el campo, a continuación haga clic al botón de «Añadir» para mover el número a la tabla de abajo. Al situar el cursor en la línea dada con el número y al hacer clic en 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 incluyan la secuencia dada, por ejemplo: 600123456 o bien 601234567.

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

5.12.2. Periodos de validez de los mensajes salientes SMS

El usuario podrá limitar el número de SMS que será enviado por el emisor. Dado que la forma básica de transmisión debe ser LTE, esta restricción es importante, principalmente por razones económicas.

Para permitir el acceso a grupos de información que estarán sujetos a restricciones:

- Pruebas periódicas enviadas al servidor;
- Eventos enviados al servidor;
- Mensajes SMS enviados al usuario;
- Respuestas a los comandos SMS.

5.12.3. Restricciones

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 la frecuencia (en minutos / horas / días) de puesta a cero del contador de los mensajes SMS enviados.

Los siguientes tipos de información se pueden conectar a las restricciones (dependiendo de si se seleccionan):

- Pruebas periódicas enviadas al servidor;
- Eventos enviados al servidor;
- Mensajes SMS enviados al usuario;
- Respuestas a los comandos SMS.

5.12.4. Reenvío de SMS

El dispositivo es capaz de transmitir los mensajes recibidos SMS a los determinados números de teléfonos según las reglas configuradas. Esta función podrá resultar indispensable en el caso de las notificaciones por SMS sobre el estado de la cuenta. En esta ventana se puede introducir hasta 5 reglas para la transmisión de mensajes SMS.

Añadir reenvío de SMS

Remitente

introducir número de teléfono

Destinatario

introducir número de teléfono

Añadir

Cancelar

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 principio hasta el final, es decir, el resultado del tratamiento de la regla no influye en el tratamiento de las reglas siguientes. También significa que un determinado mensaje SMS puede ser enviado a varios números de teléfono o que el mismo mensaje puede ser enviado varias veces al mismo número. Este es el caso cuando una condición impuesta al número de teléfono del remitente se cumple para al menos dos reglas que tienen 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.

5.12.5. Notificaciones por SMS

CALLISTO 32 (CPX230NWB) - Nuevo - EBS Config 2.0

Configuración de SMS

HARDWARE

Resumen

Ajustes del panel de control

Particiones

Dispositivos

Usuarios

Configuración de SMS

CENTRO DE MONITORIZACIÓN

Monitorización de TCP/IP

Monitorización de SMS

Modificadores de eventos

CANALES DE CONEXIÓN

Notificaciones de SMS

Mensajes SMS personalizados 0/32

Lista vacía

Mensajes de eventos

Alarma de los detectores
iniciar/terminar

Manipulación de detectores
iniciar/terminar

Salidas cableadas
on/off, fallos

Sirenas inalámbricas y teclados con cable
encendido/apagado, comunicación, manipulación, alimentación

Alimentación del panel de control
Fallos

Estado de los detectores
comunicación, batería, servicio,

Particiones
conectar/desconectar

Eventos de emergencia
pánico, incendio, ayuda, coacción

Comunicación con el centro de monitorización
interferencia

Notificaciones de SMS 0/10

Lista vacía

ES

CENTRALITA DE ALARMAS CPX230NWB – MANUAL DE INSTALADOR

89 / 137

El usuario tiene la posibilidad de definir los comunicados que, en el caso de que ocurra el evento dado (p.ej. cambio del estado de la entrada), se enviarán a los números de teléfono privados. Al mismo tiempo hay que recordar la necesidad de definir las limitaciones en este aspecto.

5.12.6. Contenidos únicos de mensaje

En esta sección puede añadir un nuevo (pulsando **+**) y editar los ya definidos (pulsando **✎**) el texto de los mensajes SMS únicos que se pueden asignar a los eventos de la sección "Estado". La longitud máxima total del mensaje es de 2000 caracteres.

5.12.7. Notificaciones de SMS 0/10

En esta sección puede definir hasta 10 números de usuarios que serán informados de los eventos seleccionados mediante los mensajes SMS definidos que se les han asignado. Para ello, pulse y **+** defina el número de teléfono en la ventana que aparece, seleccione el tipo de eventos a enviar y confirme entonces pulsando **Añadir**:

Añadir notificación de SMS

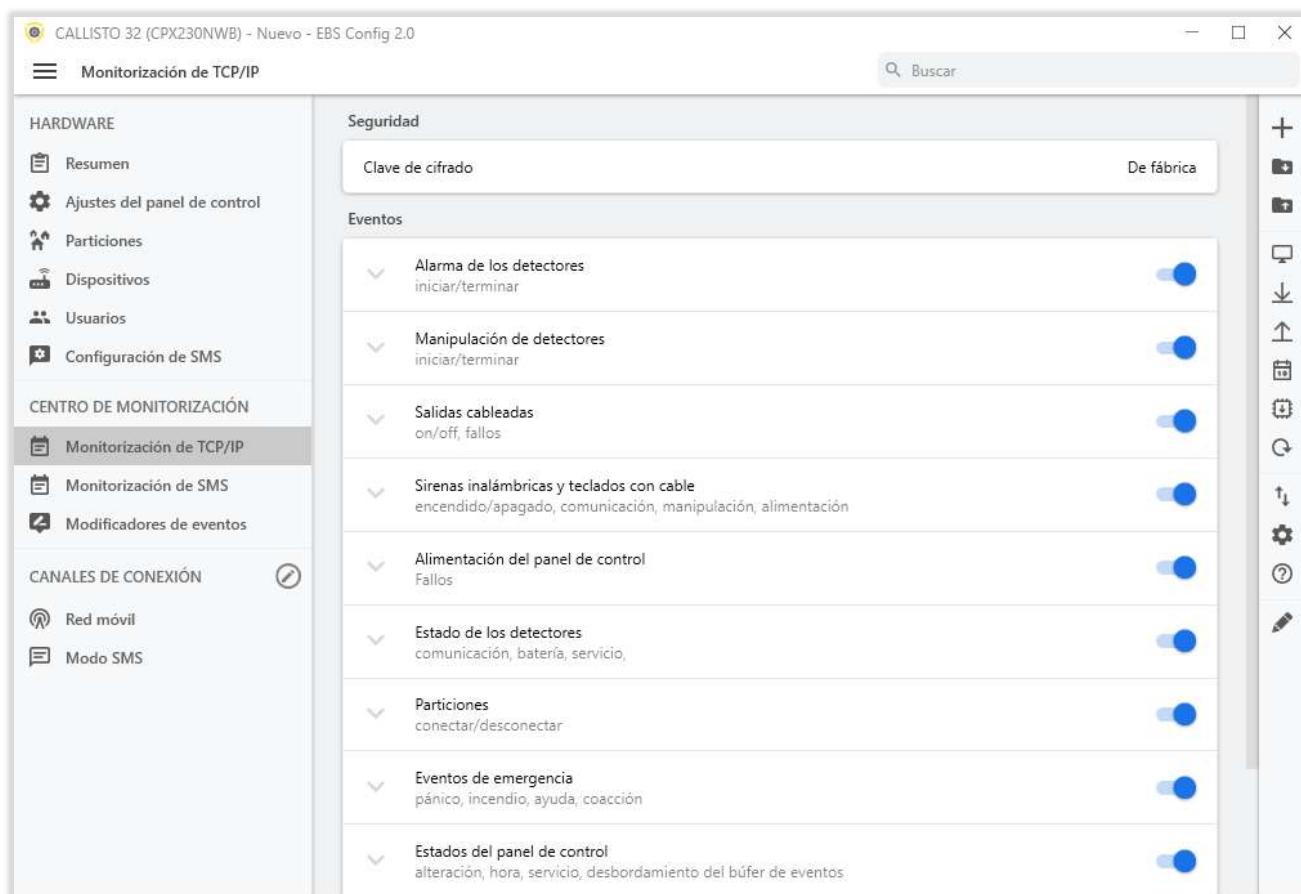
Número de teléfono introducir número de teléfono

Eventos

▼ Alarma de los detectores iniciar/terminar	☐
▼ Manipulación de detectores iniciar/terminar	☐
▼ Salidas cableadas on/off, fallos	☐
▼ Sirenas inalámbricas y teclados con cable encendido/apagado, comunicación, manipulación, alimentación	☐
▼ Alimentación del panel de control Fallos	☐
▼ Estado de los detectores comunicación, batería, servicio,	☐
▼ Particiones conectar/desconectar	☐
▼ Eventos de emergencia pánico, incendio, ayuda, coacción	☐
Comunicación con el centro de monitorización	☐

Añadir **Cancelar**

5.13. MONITOREO TCP/IP, MONITOREO DE SMS



5.13.1. Seguridad - clave de encriptación

Para garantizar la máxima seguridad en la transmisión, los datos se cifran con una clave AES. Esta opción puede utilizarse para transmisiones LTE y SMS.

Al seleccionar "Personalizado", aparece una ventana en la que es posible establecer un código propio (256 bits - caracteres 0-9 y A-F) o utilizar la configuración por defecto.

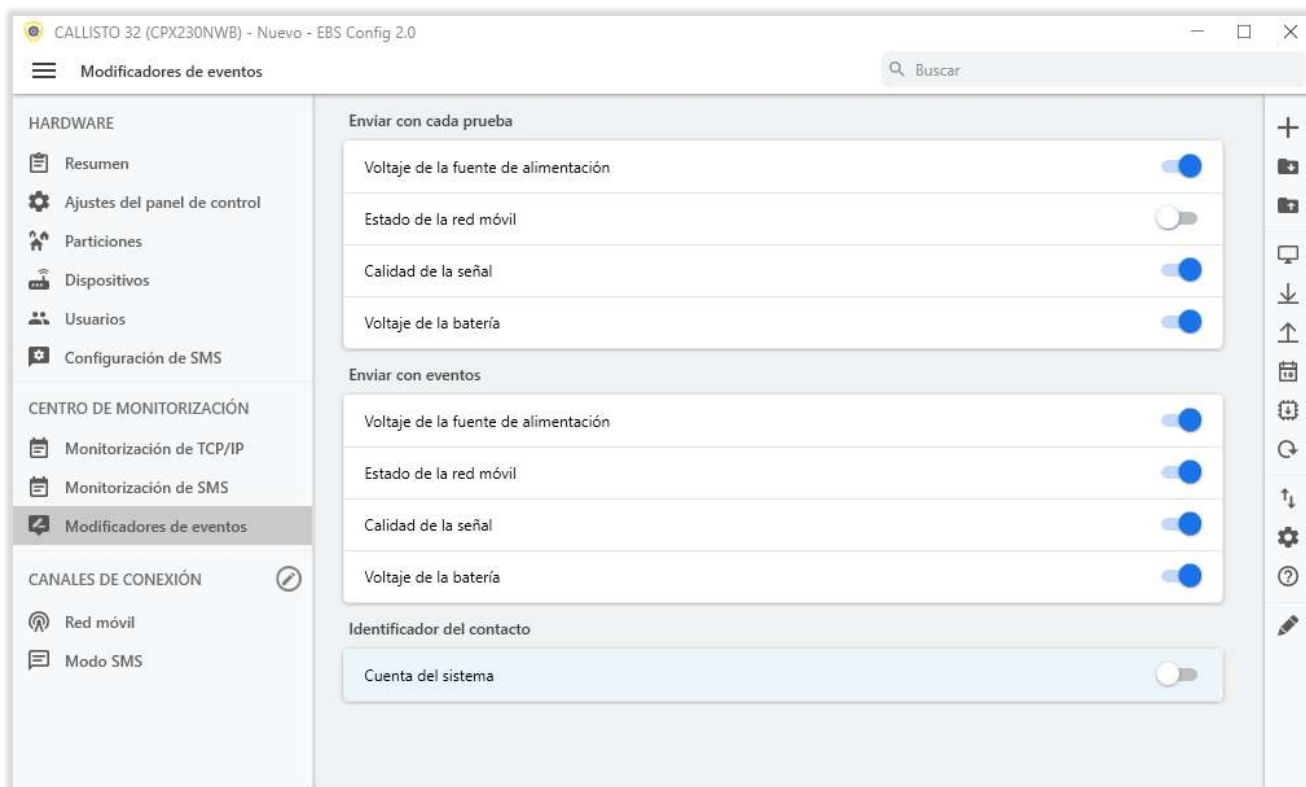
5.13.2. Eventos

En esta sección podrá determinar cuál de las señales disponibles generadas por el dispositivo será transmitida a la estación de monitoreo por cada uno de los dispositivos agregados. Se trata de la siguiente información:

- Alarma desde el sensor - información sobre el principio y fin de las violaciones y bloqueos;
- Sabotaje de sensores - información sobre el sabotaje (apertura del tamper) de los sensores y sobre su fin (cierre del tamper);
- Salidas - información sobre la activación y desactivación de salidas y sobre averías;
- Alimentación y batería - información sobre las averías de la alimentación y la batería, así como sobre sus fines;
- Estado de los dispositivos inalámbricos - información sobre la falta de comunicación y su restablecimiento, bloqueo temporal, batería casi agotada, avería y tiempo para servicio;
- Particiones - información sobre el armado/desarme;
- Situación de alarma - información, entre otras, sobre las alarmas de asalto;

- Estado de la central - información sobre los resets del módem, pérdida del reloj, principio y fin de la falta de comunicación de las tarjetas, etc.
- Comunicación con el centro de monitoreo - información sobre la actualización del tiempo, cambio de configuración, principio y fin de interferencias, etc.
- Informativos - información sobre el arranque de la central, CLIP o sobre la introducción de código erróneo, etc.

5.14. MODIFICADORES DE EVENTOS

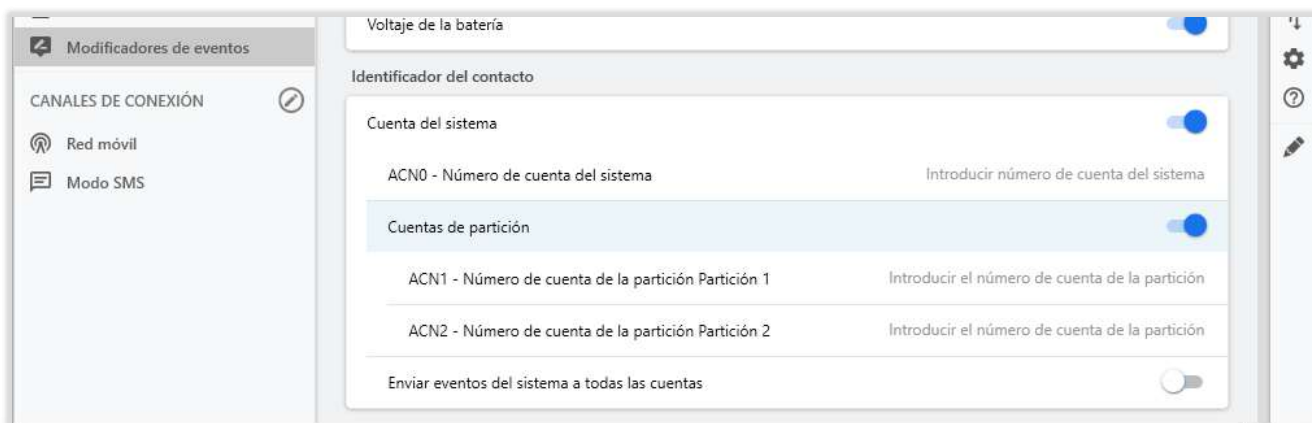


Es posible definir dos conjuntos separados: para la señal de prueba (enviado en forma cíclica según la configuración en la pestaña Acceso) y para los demás eventos. Si marca la casilla, la información de este tipo se transmitirá al software receptor. Si no se selecciona, no se envía ninguna información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

5.14.1. Identificador del contacto (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.

5.14.1.1. 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.

5.14.1.2. 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.



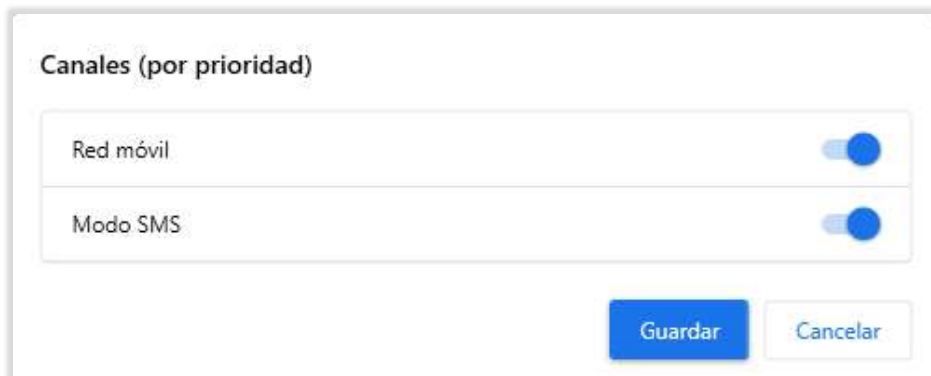
ATENCIÓN: Si introduce un número de cuenta para una sola partición, no será posible enviar la configuración a la centralita. Deben introducirse ambos números (ACN1 y ACN2).

5.14.1.3. Enviar eventos del sistema a todas las cuentas

Si se selecciona esta opción, los eventos del sistema se enviarán a todas las cuentas, es decir, a la cuenta del sistema (ACN0) y a las cuentas de sus subsistemas: partición 1 - ACN1 y partición 2 - ACN2.

5.15. CANALES DE COMUNICACIÓN

En función de qué módulos se hayan montado sobre la placa PCB y si se ha introducido la tarjeta SIM en el dispositivo CPX230NWB, debe seleccionar los canales de conexión adecuados: Red móvil, modo SMS. Para ello, haga clic en  y seleccione las partidas adecuadas.



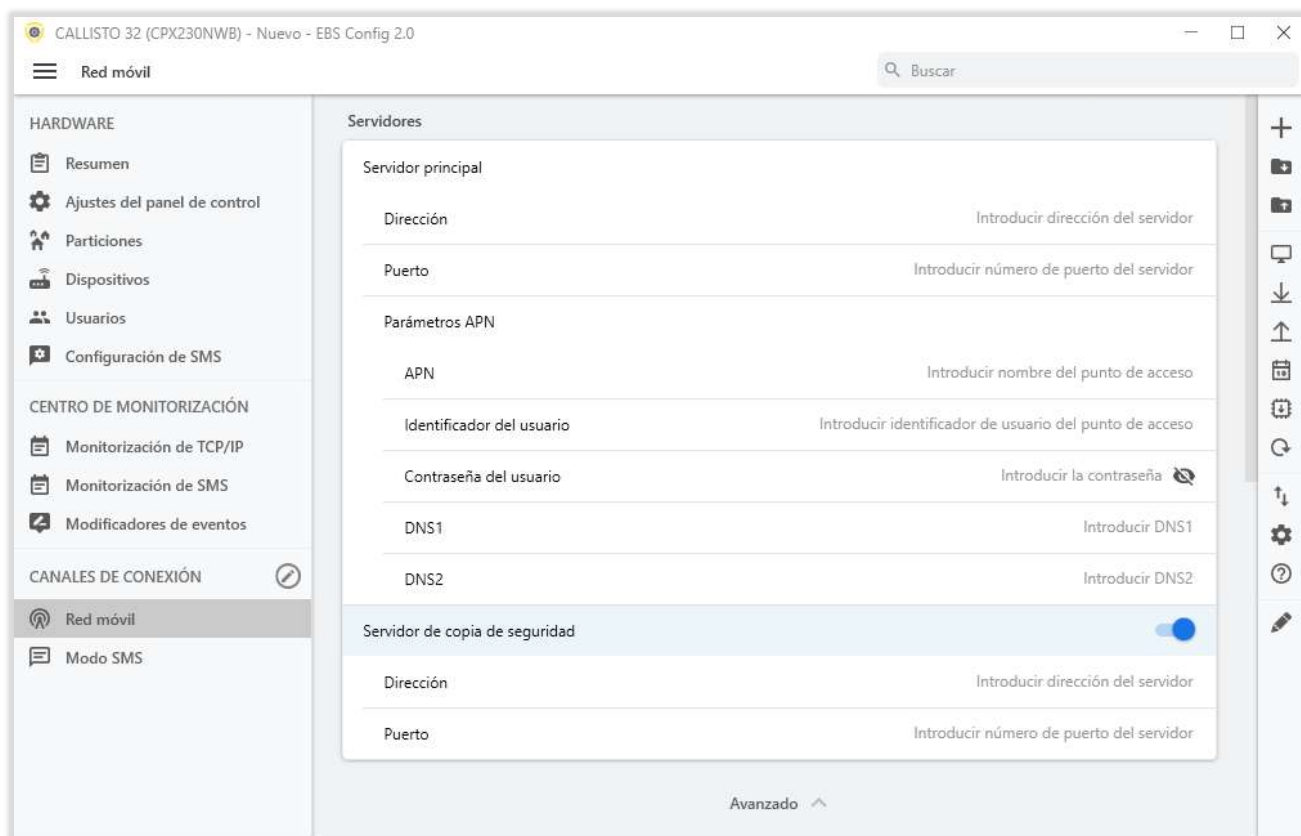
Una vez marcados los canales seleccionados, aparecerán las partidas adicionales: llave de cifrado para TCP/IP en el caso de marcar Ethernet/WiFi o la red móvil y/o llave de cifrado para los SMS si está marcado el modo SMS.

Las llaves de cifrado de fábrica están configuradas por defecto, pero hay posibilidad de cambiar las configuraciones por unas no estándar.

ATENCIÓN: Una vez leídas las configuraciones del dispositivo, se produce la detección automática de los módulos montados y la aparición de las pestañas de configuración correspondientes.

5.16. RED MÓVIL

Si al módulo GSM se ha introducido una sola tarjeta SIM, la pestaña tendrá el siguiente aspecto:



5.16.1. Servidores

En esta sección deberán definirse los parámetros del servidor primario y de emergencia (si se va a usar). Tras marcar la opción de *Servidor de emergencia*, aparecerán los parámetros adicionales y las opciones relativas a las configuraciones del servidor de emergencia y los principios de su colaboración con el servidor primario.

Dirección 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.

Puerto de servidor

Determina el puerto del servidor que en el servidor fue destinado para recibir los datos del aparato.

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.

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

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).

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).

5.16.2. Conexión

5.16.2.1. Periodo de prueba de los eventos

El dispositivo envía, con el intervalo determinado, la señal «Prueba» que informa a la estación de monitoreo que el dispositivo está funcionando. Al hacer clic sobre el campo, se desplegará la lista de valores disponibles - entre 20 segundos y 8 horas. Al seleccionar la partida "No estándar", podrá introducir cualquier valor dentro de este rango temporal.

5.16.2.2. Servidor primario

Intervalo entre los distintos intentos de conectarse

Si el dispositivo no puede conectarse al servidor primario hará otro intento una vez transcurrido el tiempo definido en este campo.

Número de pruebas de conectarse al servidor antes de cambiar al servidor de emergencia

En este campo debe definirse el número de intentos que, en los intervalos configurados (parámetro descrito arriba), realizará el dispositivo para conectarse con el servidor primario en el caso de intentos fallidos. Una vez realizado el número de intentos definido (entre 1 y 100), el dispositivo iniciará el procedimiento de conectarse al servidor de emergencia.

Esta opción estará activa solamente en el caso de que el servidor de emergencia esté definido.

Siempre intente conectarse primero al servidor primario.

La activación de esta opción significa que el dispositivo intentará primero conectarse al servidor primario, independientemente de los parámetros definidos para el servidor de emergencia (en particular, el número de intentos de conectarse). Esta opción tiene un parámetro superior que los parámetros para el servidor de emergencia.

5.16.2.3. Servidor de emergencia

Intervalo entre los distintos intentos de conectarse

Si el dispositivo no puede conectarse al servidor de emergencia, hará otro intento una vez transcurrido el tiempo definido en este campo.

Número de intentos de conectarse al servidor antes de cambiar al servidor primario

En este campo debe definir el número de intentos que, en los intervalos configurados (parámetro descrito arriba), realizará el dispositivo para conectarse con el servidor de emergencia en el caso de intentos fallidos. Una vez realizado el número de intentos definido (entre 1 y 100), el dispositivo iniciará el procedimiento de conectarse al servidor primario.

Esta opción estará activa solamente en el caso de que el servidor de emergencia esté definido.

Desconectar al cabo del periodo

Tras marcar este campo, el dispositivo se desconectará del servidor de emergencia al cabo del tiempo definido. Su funcionamiento posterior dependerá del parámetro "Siempre intentar primero conectarse al servidor primario". Si esta opción está activada, el dispositivo hará el intento de conectarse al servidor primario. Si está desactivada, el dispositivo continuará el procedimiento de conectarse al servidor de emergencia hasta terminarlo; si no consigue conectarse, emprenderá los intentos de conectarse al servidor primario.

5.16.3. Estabilidad de conexión

5.16.3.1. Control de transmisión de datos móviles

Esta opción permite que la central reaccione automáticamente en el caso de registrar la falta de transmisión móvil. Después de activarla, aparecerán dos campos adicionales.

Reaccionar si no hay transmisión durante

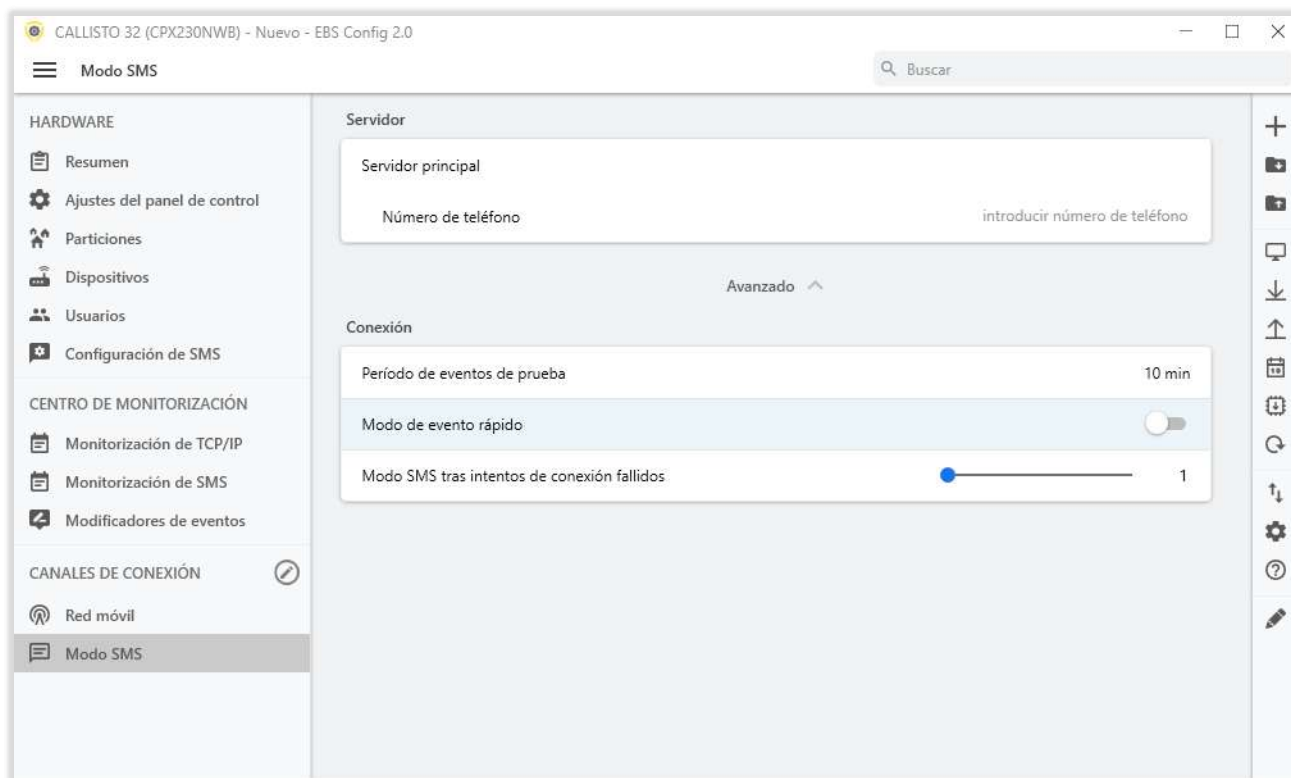
Aquí tendrá que definir tiempo desde la detección de la pérdida de comunicación con la red (falta de transmisión) después del cual el dispositivo iniciará el reseteo del módem.

Reinicio del dispositivo

Aquí tendrá que definir el tiempo desde la detección de la pérdida de comunicación con la red (falta de transmisión) después del cual el dispositivo iniciará el reseteo de sí mismo (y no solo del módem).

5.17. MODO SMS

El modo SMS podrá ser tanto un canal autónomo de transmisión de datos como un canal de reserva para la transmisión móvil GPRS. Si al módulo GSM se ha introducido una sola tarjeta SIM, la pestaña tendrá el siguiente aspecto:



El dispositivo pasará al modo SMS cuando ocurran problemas.

5.17.1. Número de teléfono

Aquí se introducirá el número del módem GSM conectado a la estación de monitoreo OSM.Server. A este número se enviarán los SMS independientemente, tan pronto que esta vía de transmisión de datos se defina y en el momento cuando el dispositivo tenga problemas con la transmisión GPRS.

En el caso de que este campo se quede vacío o se introduzca solamente una cifra (incluido 0), el dispositivo en ningún caso pasará al modo SMS.

5.17.2. Periodo de prueba de los eventos

Aquí tendrá que definir cada cuánto tiempo el dispositivo ha de enviar la señal de "Prueba" para informar a la estación de monitoreo de que el dispositivo está trabajando. Al hacer clic sobre el campo, se desplegará la lista de valores disponibles - entre 1 minuto y 8 horas. Al seleccionar la partida "No estándar", podrá introducir cualquier valor dentro de este rango temporal.

5.17.3. Periodo de incidencias rápidas

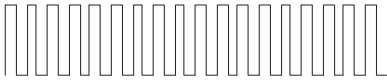
En caso de perder la conexión GPRS, la información sobre los eventos entrantes se enviará por mensaje SMS inmediatamente, incluso cuando el dispositivo no ha pasado aún al modo SMS.

6. SEÑALIZACIÓN CON DIODOS LED

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

6.1. 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		_____	_____

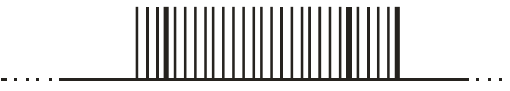
6.2. ALCANCE DE GSM

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		_____	_____

6.3. 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		_____	_____

6.4. 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 de servicio			
Programación en el modo CSD			

6.5. 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			

6.6. 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)	

6.7. 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.

7. AJUSTES GRADE 2

7.1. 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.
- Utilizar códigos de usuarios con una longitud mínima de 5 caracteres.
- Conectar la centralita a una 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 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 Configurador, en la opción Monitoreo, 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.

7.2. 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.

8. ADITIVOS

8.1. 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.

8.1.1. Parámetros de configuración

8.1.1.1. 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.

8.1.1.2. 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

8.1.1.3. PW

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

8.1.1.4. 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

8.1.1.5. 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

8.1.1.6. 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).

8.1.1.7. 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).

8.1.1.8. 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.

8.1.1.9. 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.

8.1.1.10. 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 (000000000000000110) elimina el bloqueo de las entradas: IN1, IN2 RLIMIT=2 ocasiona la eliminación de bloqueo de la entrada IN1
-------------	---

8.1.1.11. 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

8.1.1.12. SETMASK

Formato:	SETMASK=id_tipo,índice,máscara
Restricciones:	<i>id_tipo</i> 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. <u>PARA:</u> SETMASK=2,19,0x100 Activación de la función <i>Bloqueo de la instalación</i> 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 <i>Bloqueo de restauración de los ajustes predeterminados</i> 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). <u>ATENCIÓN:</u> 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 <i>Permitir el armado rápido sin autorización del usuario</i> que permite armar el sistema sin necesidad de introducir el código de acceso.

8.1.1.13. CLEARMASK

Formato:	CLEARMASK=id_tipo,índice,máscara
Restricciones:	<i>id_tipo</i> 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. <u>PARA:</u> CLEARMASK=2,19,0x100 Desactivación de la función <i>Bloqueo de la instalación</i>. Después de desactivar esta función, el usuario podrá armar y desarmar la centralita. CLEARMASK=2,19,0x200 Desactivación de la función <i>Bloqueo de restauración de los ajustes predeterminados</i>. 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 <i>Permitir el armado rápido sin autorización del usuario</i>. Después de desactivar esta función, solo será posible armar el sistema introduciendo el código de acceso.

8.1.2. 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.

8.1.2.1. DISC

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

8.1.2.2. 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

8.1.2.3. 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

8.1.2.4. 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.

8.1.2.5. 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

8.1.2.6. 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». <i>o</i> – número de salida (1–3) <i>s</i> – estado de destino(1 – activo, 0 – inactivo) <i>tiempo</i> – 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
-------------	--

8.1.2.7. 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.

8.1.2.8. 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 (nº_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.

8.1.2.9. 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: <i>líneas</i> – 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) <i>particiones</i> – 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. <i>salidas</i> – 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 <i>tensión_batería</i> – tensión de la batería en mV (12000 = 12V). Cuando la batería no está conectada, las lecturas pueden ser incorrectas y ser unos 9V (9000) <i>tensión_CA</i> – tensión CA en los bornes CA CPX230NWB (detrás del transformador) en mV (18000 = 18V) <i>bloqueo_líneas</i> – 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.

8.1.2.10. 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, <i>delay</i> es el tiempo en segundos CPGETALARMSHOWTIME:OFF – si la función «Desactivar la señalización de alarmas históricas tras el desarmado» no está activa

8.1.2.11. 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 <i>delay</i> es el valor de retardo en segundos (0-99999999) o el texto <i>OFF</i> para deshabilitar la funcionalidad (la señalización no se desactiva). Con el valor cero, la señalización de alarmas se desactiva en el momento de desarmado. El comando devuelve: CPSETALARMSHOWTIME:EOK – ejecución correcta CPSETALARMSHOWTIME:EEFORMAT – formato de comando o rango del parámetro <i>delay</i> 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

8.1.2.12. 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: <i>system</i> – valor ALL (para eventos del sistema enviados a todas las cuentas) o ACN0 (para eventos del sistema enviados a la cuenta ACN0) <i>acn_id</i> – identificador de la cuenta ACN, 0 para ACN0, 1 para ACN1, 2 para ACN2. <i>acn_value</i> – 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

8.1.2.13. 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. <i>system</i> – valor ALL (para eventos del sistema enviados a todas las cuentas) o ACN0 (para eventos del sistema enviados a la cuenta ACN0) <i>acn_id</i> – identificador de la cuenta ACN, 0 para ACN0, 1 para ACN1, 2 para ACN2 <i>acn_value</i> – número de cuenta de dos bytes (de preferencia en formato hexadecimal: 0xFFFF) Son posibles 3 pares (acn_id:acn_value), uno para cada cuenta. <u>ATENCIÓN:</u> • 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: ○ Ningún número de cuenta ○ Solo la cuenta principal (ACN0) ○ 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

8.1.3. Comandos de gestión de usuarios

8.1.3.1. 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 <i>adminPassword</i>
Descripción	Recupera la lista de usuarios definidos en el dispositivo. <i>adminPassword</i> es la contraseña del administrador del sistema. El comando devuelve: CPGETUSERS:id:name:partitions,... Siendo <i>id</i> el número de usuario, <i>name</i> el nombre de usuario (puede estar vacío), <i>partitions</i> 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

8.1.3.2. 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. <i>Password</i> es la contraseña del usuario, <i>id</i> es el número del usuario, <i>partitions</i> 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 existe CPGETUSERID:EPERMISSIONS 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

8.1.3.3. 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 <i>adminPassword</i>
Descripción	Fija los permisos del usuario a la partición. <i>Id</i> es el número del usuario al que modificamos los permisos, <i>partitions</i> 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, <i>adminPassword</i> 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

8.1.3.4. 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 <i>adminPassword</i>
Descripción	Cambia la contraseña del usuario. <i>Id</i> es identificador del usuario cuya contraseña se cambia, <i>password</i> es su nueva contraseña y <i>adminPassword</i> 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:EPERMISSIONS,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

8.1.3.5. 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 <i>adminPassword</i>
Descripción	Añade a un nuevo usuario. <i>Id</i> es número de usuario, <i>partitions</i> son particiones para las que el usuario tendrá permisos – bit 0 corresponde a la partición 1, bit 1 a la partición 2, <i>password</i> es contraseña del nuevo usuario, <i>category</i> – toma valor <i>NODISARM</i> – si se especifica, el usuario no podrá desarmar la partición (disponible a partir de la versión de firmware 2.8.8) , <i>adminPassword</i> – si el comando se envía a través de ATS, debe ingresarse 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:EPERMISSIONS,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

8.1.3.6. 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 <i>adminPassword</i>
Descripción	Elimina al usuario. <i>Id</i> es número de usuario, <i>adminPassword</i> 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:EPERMISSIONS,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

8.1.3.7. 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). <i>newPassword</i> 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: EPERMISSIONS 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.

8.1.3.8. 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 <i>id</i> es el número de usuario. El comando devuelve: CPGETUSERRIGHTS:EOK,id,category[,...] Si el usuario existe. Posibles valores del campo <i>category</i>: <i>USER</i> para un usuario típico, <i>NODISARM</i> para un usuario sin derechos de desarme CPGETUSERRIGHTS:ENOT_EXISTS,id Cuando el usuario no existe CPGETUSERRIGHTS:EPERMISSIONS,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

8.1.4. Comandos para administrar particiones, líneas y salidas

8.1.4.1. 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 <i>password</i>
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: <u>Ready</u> toma el valor de 1 si el sistema está listo para el armado, 0 si no lo está. <u>CurrentPartitionAlarms</u> 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. <u>alarmHistory</u> 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. <u>otherAlarmHistory</u> 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. <u>zoneTampers</u> es un vector de bits que indica los sabotajes de las líneas. El bit 1 (contando desde 0) corresponde a la línea A1. <u>keypadTampers</u> es un vector de bits que indica los sabotajes de los teclados. El bit 0 significa el teclado 1. <u>zones</u> – 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. <u>zonesLock</u> – 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. <u>partitions</u> – 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. <u>outputs</u> – 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:EPERMISSIONS
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

8.1.4.2. 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 <i>password</i>
Descripción	<i>password</i> es la contraseña de administrador del sistema o de usuario El comando devuelve: CPGETFAILURES:outFailures,powerOutFailures,powerInFailures,keypadCommFailures,keypadPowerFailures,otherFailures Siendo: <u>outFailures</u> es un vector de bits que indica los fallos de las salidas. El bit 1 (contando desde 0) significa la salida 1. <u>powerOutFailures</u> 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. <u>powerInFailures</u> 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. <u>keypadCommFailures</u> es un vector de bits que indica los fallos de comunicación con los teclados. El bit 0 significa el teclado 1. <u>keypadPowerFailures</u> es un vector de bits que indica los fallos de alimentación avisados por los teclados. El bit 0 significa el teclado 1. <u>otherFailures</u> 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:EPERMISSIONS 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

8.1.4.3. 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 <i>password</i>
Descripción	Rearma las particiones determinadas. <i>partitions</i> 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 <i>partitions</i> igual a cero no tiene mucho sentido, porque nada cambiará: si <i>partitions</i> es 0, la contraseña de usuario no se comprobará y el estado devuelto por el comando será igual a EOK. El parámetro <i>delay</i> puede tomar el valor <i>NOW</i> (armar inmediatamente la partición definida sin esperar el retardo de salida configurado) o <i>DEFAULT</i> (armar la partición después del retardo de salida). <i>Password</i> 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. Las frases <i>STAY</i> y <i>SLEEP</i> antes del vector con particiones son opcionales. <i>STAY</i> significa que las particiones se armarán en modo perimetral y <i>SLEEP</i> 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 <i>NOW</i> y ejecutado CPSETPARTITIONS=[STAY/SLEEP]partitionsList:EOK,x,y – cuando el comando ha sido enviado con el parámetro <i>DEFAULT</i> 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 (<i>partitionList</i> puede ser diferente del campo <i>partitions</i> 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 (<i>partitions,password</i> son argumentos del comando) CPSETPARTITIONS=[STAY/SLEEP]partitions:EPERMISIONS – cuando el usuario con la contraseña dada no existe

8.1.4.4. 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 <i>password</i>
Descripción	Desarma las particiones determinadas. <i>partitions</i> 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 <i>partitions</i> igual a cero no tiene mucho sentido, porque nada cambiará: si <i>partitions</i> es 0, la contraseña de usuario no se comprobará y el estado devuelto por el comando será igual a EOK. <i>Password</i> 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. <i>partitionList</i> es una lista de particiones que han sido desarmadas mediante comando (<i>partitionList</i> puede ser diferente del campo <i>partitions</i> 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 (<i>partitions,password</i> son argumentos del comando) CPUNSETPARTITIONS=partitions:EPERMISSIONS – cuando el usuario con la contraseña dada no existe

8.1.4.5. 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 <i>password</i>
Descripción	Bloquea permanentemente las líneas dadas. Genera eventos <i>INPUTx_LOCK</i>. <i>zones</i> 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 <i>zones</i> igual a 0 no tiene mucho sentido porque nada cambiará. <i>Password</i> 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:EPERMISSIONS Cuando el usuario no tiene permisos a la respectiva partición CPZONESLOCK:ENOT_EXISTS Cuando el usuario con la contraseña dada no existe

8.1.4.6. 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 <i>password</i>
Descripción	Elimina el bloqueo permanente y temporal de las líneas dadas. Genera eventos <i>INPUTx_UNLOCK</i>. <i>zones</i> 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 <i>zones</i> igual a 0 no tiene mucho sentido porque nada cambiará. <i>Password</i> 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:EPERMISSIONS Cuando el usuario no tiene permisos a la respectiva partición CPZONESUNLOCK:ENOT_EXISTS Cuando el usuario con la contraseña dada no existe

8.1.4.7. 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 <i>password</i>
Descripción	<i>password</i> 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 <i>P1Zones</i>, <i>P2Zones</i> 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:EPERMISSIONS 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

8.1.4.8. 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 <i>password</i>
Descripción	<i>password</i> 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 <i>P1Outputs,P2Outputs</i> 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

8.1.5. Comandos para la gestión de dispositivos inalámbricos

8.1.5.1. 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 <i>id</i> 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 nº 1, id=1 al mando nº 2, etc.), para los detectores inalámbricos es el número de la línea menos 1 (id=0 corresponde al detector nº 1, id=1 al detector nº 2, etc.), <i>SERIALNO</i> 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

8.1.5.2. 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. <i>hours</i> 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=:Epermissions – cuando no hay permisos o el código es incorrecto CPDETECTORLOST=:EID – cuando el rango de datos es incorrecto CPDETECTORLOST=:EFORMAT – cuando el formato del comando es incorrecto

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

8.1.6.1. 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 <i>oldpwd</i> a <i>newpwd</i>. 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.

8.1.6.2. 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 <i>state</i> igual a 1) o deshabilita (si <i>state</i> igual a 0) la opción «Bloqueo de los ajustes de comunicación». Para que el comando funcione, como argumento <i>ats_password</i> 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

8.1.6.3. 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:EPERMISSIONS cuando se ha enviado con permisos distintos de ATS

8.2. 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 (standby): relé NO abierto y alarma (violación): relé NO cerrado.

NC – una configuración de la línea de entrada que permite identificar dos estados: normal (standby): 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

9. 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
2020.08.20 / 1.6 / 2.11.4	Se ha agregado información sobre la sirena inalámbrica BM8000PLx-C3W
2022.06.13 / 1.8 / 2.12.2	Añadir información sobre nuevos modelos de dispositivos
2023.01.12 / 2.0 / 2.12.3	