
2CSM600730D0901_REVG | 01.02.2021

Busch-/ABB-secure@home

Manual del sistema

Tipología de Central

Con GSM

SAS-W1.1E	SAS-W1.11E
SAS-W1.1F	SAS-W1.11F
SAS-W3.1E	

Basic

SAS-W2.1E	SAS-W2.11E
SAS-W2.1F	SAS-W2.11F

Contenido

1	Introducción	5
1.1	Dónde encontrar la información	5
1.2	Conformidad.....	5
1.3	Exención de responsabilidad.....	5
1.4	Marcas y copyrights	6
	Uso del sistema	7
2	Interfaz de mando.....	7
2.1	Pantalla.....	7
2.1.1	Significado de los iconos	8
2.1.2	Autenticación	9
2.1.3	Menú principal del usuario.....	9
2.1.4	Estado de cada zona	10
2.2	LED	10
2.3	Interfaz de mando	11
2.3.1	Uso del teclado	11
2.4	Autenticación	12
2.4.1	Identificador del usuario	12
2.4.2	Contraseña	12
2.5	Niveles de autorización	12
3	Activar y desactivar el sistema	14
3.1	Conexión y desconexión con teclado	14
3.1.1	Activación y desactivación rápidas.....	14
3.1.2	Activación total.....	16
3.1.3	Desactivación total.....	17
3.1.4	Activación parcial.....	17
3.1.5	Desactivación parcial	17
3.2	Activación y desactivación con mando a distancia	17
3.3	Activación con forzado de bloqueo	18
3.4	Reiniciar	19
4	Pánico y robo	20
4.1	Activar la alarma pánico	20
4.1.1	Activación con el teclado.....	20
4.1.2	Activación con el mando a distancia	20
4.2	Activar la alarma robo.....	20
4.2.1	Activación con el mando a distancia	20
5	Alarmas y memorias de eventos	21
5.1	Prioridad de las alarmas	21
5.2	Cómo bloquear una alarma	21
5.3	Memorias de los eventos	22
5.3.1	Ver los eventos.....	22
5.3.2	Eventos SMS.....	22
5.3.3	Cómo interpretar un evento memorizado.....	23
6	Mandos a distancia.....	25
6.1	Mando vía mensaje de texto	25
7	Estado de la instalación	26
8	Ajustes de la central	27
8.1	Ajustar pantalla	27
8.2	Ajustar audio.....	28

8.2.1	Volumen beep	28
8.2.2	Feedback sonoro.....	28
8.2.3	Alarmas.....	29
8.3	Regulación de la fecha y hora.....	30
8.4	Cambiar PIN	31
8.5	Modalidad operativa y cambio de idioma.....	32
8.6	Personalice la inserción rápida.....	33
Instalar y configurar el sistema		34
9	Características principales.....	34
9.1	Funciones principales de la central	34
9.2	Capacidad del sistema	34
10	Diseñar una instalación	35
10.1	Información sobre las ondas de radio	35
10.2	Utilizar las zonas	36
10.2.1	Tipos de zonas.....	36
10.2.2	Subdivisión en zonas.....	36
11	Instalación de la central	37
11.1	Ambientes de trabajo.....	37
11.2	Programación	37
11.2.1	Lectura de las secuencias operativas.....	37
11.2.2	37	
11.2.3	Primer encendido.....	38
11.3	Estado del sistema	42
11.3.1	Armar/desarmar el sistema.....	43
11.3.2	Visualizar las zonas de alarma	44
11.4	Autenticación	45
11.5	Señalizaciones generales y de alarma.....	46
12	Programación.....	48
12.1	Creación de la instalación.....	48
12.2	Programación zonas y activadores.....	48
12.2.1	Para programar una nueva zona:.....	48
12.2.2	Para modificar o eliminar una zona:	49
12.2.3	Para programar un sensor:	49
12.3	Programación de dispositivos de sistema	51
12.3.1	Programación de mandos a distancia	51
12.4	Programación de las sirenas externas	55
12.4.1	Parámetros posibles	55
12.4.2	Filtros zonas.....	55
12.4.3	Alarmas.....	56
12.4.4	Eventos.....	56
12.5	Programación de repetidor	57
12.5.1	Parámetros posibles	57
12.6	Programación de los contactos telefónicos.....	58
12.6.1	Mensaje personalizado.....	60
12.6.2	Secuencia de envío de los mensajes telefónicos.....	60
12.6.3	Recepción de llamadas por parte de la central	61
12.7	Home automationfree@home	61
12.7.1	Versión.....	61
12.7.2	Clave.....	61
12.7.3	Reset GTW	61
12.8	Test sistema.....	62

12.9	Gestión de usuarios	64
12.9.1	Modificación de un usuario	65
12.9.2	Cancelación de un usuario	65
13	Mantenimiento	66
13.1	Gestión de la alimentación	66
13.1.1	Batería	66
13.1.2	Red eléctrica.....	66
13.2	Puesta en estado de mantenimiento	66
13.2.1	Sustitución de la batería de la central	66
13.2.2	Sustitución de la tarjeta SIM	67
13.2.3	Sustitución de la batería de los detectores	67
13.2.4	Sustitución de la pila del mando a distancia	67
13.2.5	Sustitución de la batería de la sirena	67
13.2.6	Reset de la central.....	67
13.2.7	Eliminación del historial de eventos	68
13.2.8	Conexión	68
13.2.9	Agregado de dispositivos	68
13.2.10	Cancelación de dispositivos	68
13.2.11	Sustitución de dispositivos	68
13.2.12	Actualización del firmware de la central	69
14	Resolución de problemas	71
15	Características técnicas de la central	73
16	cyber security disclaimer	74
16.1	Network Manager	74

1 INTRODUCCIÓN

Gracias por haber comprado la central BUSCH-/ABB-secure@home. Este manual contiene todas las informaciones útiles para el usuario para el uso cotidiano de la central y del sistema de alarma de intrusión, incluidos los procedimientos de configuración y mantenimiento.

1.1 Dónde encontrar la información

Este manual de instalación contiene todas las informaciones para utilizar, configurar y mantener el sistema y la central de alarmas.

Además, se brindan sugerencias para el diseño de un sistema de alarma de intrusión, se enumeran las características técnicas de la central y se indican los procedimientos para aislar y resolver posibles anomalías de la instalación. La sección de configuración está dirigida exclusivamente al técnico que realiza el montaje de la instalación.

1.2 Conformidad

La central ha sido diseñada y fabricada según los estándares de calidad y seguridad previstos por la normativa y la legislación vigentes. Los requisitos cualitativos están certificados con la colocación de la marca CE de acuerdo con la normativa 1999/05/CE.



¡Advertencia! Debe ser instalada solo por un electricista cualificado.

En la instalación se debe seguir la normativa vigente eléctrica nacional relativa al medio ambiente de instalación. Se recuerda que las conformidades arriba certificadas y las prestaciones del producto pueden estar comprometidas por:

- errónea alimentación eléctrica;
- instalación incorrecta o uso erróneo o inapropiado o disconforme con las instrucciones citadas en los manuales de instalación y uso o en las instrucciones proporcionadas junto con los dispositivos;
- sustituciones de componentes o accesorios originales con otros de tipo no aprobado por el fabricante, o realizadas por personal no autorizado.

En caso de elección de configuraciones no conformes, el etiquetado del producto que certifica la conformidad deberá ser modificada o eliminada.

1.3 Exención de responsabilidad

Las informaciones contenidas en este documento han sido recogidas y controladas con cuidado, sin embargo, ABB y BUSCH-JAEGER no pueden ser considerados responsables por posibles errores tipográficos o inexactitudes técnicas. ABB y BUSCH-JAEGER se reservan el derecho de aportar, en cualquier momento y sin previo aviso, mejoras o modificaciones a los productos descritos en el manual. Además, es posible que este manual contenga referencias o informaciones de productos o servicios no comercializados aún. Dichas referencias o informaciones no significan, en ningún modo que, ABB y BUSCH-JAEGER quiere comercializar dichos productos o servicios.



1.4 Marcas y copyrights

Todas las marcas citadas en el documento pertenecen a los respectivos propietarios.

© Copyright ABB S.p.A. 2018 - Todos los derechos reservados.

© Copyright BUSCH-JAEGER GmbH. 2018 - Todos los derechos reservados.



Código	Marca	Número de aprobación VdS
SAS-W1.1E		
SAS-W2.1E		
SAS-W1.1F		
SAS-W2.1F		
SAS-W1.11E		
SAS-W1.11F		H121004
SAS-W2.11E		
SAS-W2.11F		

¡CUIDADO!

El uso del sistema secure@home de acuerdo con las directrices VdS requiere:



- instalar el keylock para armar/desarmar el sistema desde el exterior de la vivienda. Los detalles sobre la instalación, la configuración y el uso están indicados en el manual 2CSM600756D0901;
- no se deben utilizar mandos a distancia, App y GSM para armar/desarmar el sistema a distancia.

USO DEL SISTEMA

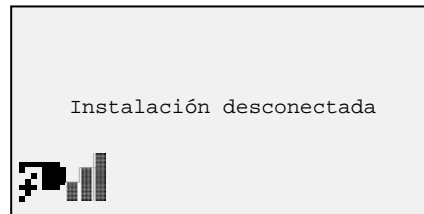
Esta sección contiene todas las informaciones útiles para el usuario para el uso cotidiano de la central y del sistema de alarma de intrusión, además de algunos procedimientos de configuración.

2 INTERFAZ DE MANDO

2.1 Pantalla

La pantalla de cristales líquidos muestra las informaciones relativas a la configuración de la central y al funcionamiento del sistema. Puede contener hasta 8 líneas de texto de 20 caracteres cada una o una serie de iconos o una combinación de textos e iconos.

La pantalla está generalmente apagada y se ilumina cuando se presiona la tecla.



En reposo, la pantalla muestra los siguientes datos:

- Estado de la instalación (activada/desactivada/parcialmente activada (Nota1))
- 2 iconos para indicar, de izquierda a derecha, el estado de alimentación de la central y la conexión GSM.

Pulsando una vez la tecla ▼ se pueden tener informaciones detalladas sobre el estado de cada zona y presionando una segunda vez:

- Número de la versión fw de la central
- dirección física (8 dígitos) de la central
- Fecha y Hora
- conexión a ABB-free@home
- número de la versión fw gateway free@home
- nivel Fw teclado táctil
- nivel de la batería

Nota 1:

Activado *Todas las zonas están activadas con la misma modalidad*

Desactivado *Todas las zonas están desactivadas*

parcialmente *No todas las zonas están activadas o*

activado *Todas las zonas han estado activadas, pero con modalidades no uniformes*

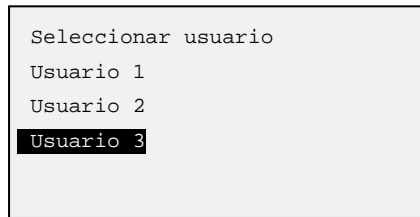
2.1.1 Significado de los iconos

Estado de	Icono	Significado
Teléfono		La conexión a la red telefónica GSM funciona. La intensidad de campo medida se visualiza mediante muescas (de 1 a 3).
		Red telefónica GSM no identificada, tarjeta SIM no instalada, no identificada, vencida o no activada.
		(intermitente) SIM Card con PIN no desactivado
		Módem GSM en modo bajo consumo
		Diagnóstico GSM en curso.
		Supervisión GSM en curso
Sistema de alarma de intrusión		Instalación de alarma de intrusión desconectada.
		Alarma activada en modalidad "Prealarma"
		Alarma activada en modalidad "Interna"
		Alarma activada en modalidad "Externa"
		Retraso en la salida activado al menos en un sensor
		Zona activa las 24 horas
Alimentación de la central		Indica la presencia de alimentación de red de la batería
		Alimentación solo con batería. El porcentaje de color negro del icono indica el estado de carga de la batería. (en el ejemplo, completamente cargada).
		(intermitente) Falta batería

2.1.2 Autenticación

Para autenticarse, desde la ventana en reposo:

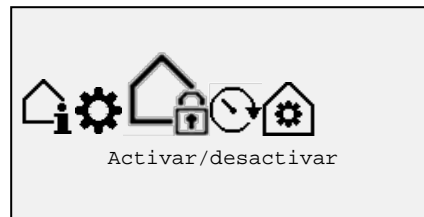
1. Presionar la tecla ok del teclado. Aparece la ventana con los usuarios de nivel 2 definidos en la instalación



2. Seleccionar el usuario de la lista e ingresar el PIN. Las cifras ingresadas aparecen escondidas
3. Presionar la tecla **ok** para confirmar. Si el PIN introducido no es de 5 cifras, no se acepta la tecla **ok**. Si el usuario ingresa un PIN erróneo por décima vez se genera una alarma de sabotaje.
4. Si la autenticación se realizó con éxito, aparece el menú principal de usuario.

2.1.3 Menú principal del usuario

Se presenta como en la pantalla de abajo. Accediendo a esta pantalla, la central se predispone automáticamente sobre el icono "Activar/desactivar"



La tecla **←** permite salir de la pantalla y volver a la ventana de reposo. Las flechas **▶◀** permiten de desplazarse para seleccionar el icono y, por lo tanto, la función deseada.

Icono	Significado
	Activaciones. Permite acceder al menú de conexión y desconexión de todo el sistema de alarma o de zonas individuales.
	Estado y lista de eventos. Permite acceder al menú de visualización de los eventos almacenados por la central y del estado del sistema.
	Pánico. Permite activar la alarma pánico.
	Preferencias. Permite acceder al menú de ajuste de pantalla, audio, fecha y hora y modifica su PIN.
	Acceso Instalador. Permite acceder a la pantalla de los servicios habilitados para un usuario de nivel 3.
	Test del sistema. Permite acceder al menú de test del sistema.
	Salir. Sale del menú principal y reconduce la central al estado de reposo.

2.1.4 Estado de cada zona

El estado de las zonas se obtiene pulsando la tecla ▼ en la ventana de reposo: una zona puede adoptar uno de los estados y, por lo tanto, uno de los iconos descritos en “Sistema de alarma de intrusión” de la tabla Significado de los iconos - pár. 2.1.1

2.2 LED

Junto a la pantalla, a la derecha, están ubicados 4 LED.



Señala que la batería de la central está agotada.



Señala que existen las notificaciones obligatorias memorizadas que no han sido aún visualizadas. Visible con la instalación desactivada.



Señala una alarma (intrusión, manipulación).
No señala las alarmas Robo. Visible sólo a los usuarios autenticados.



Señala la interferencia (jamming) de la instalación.

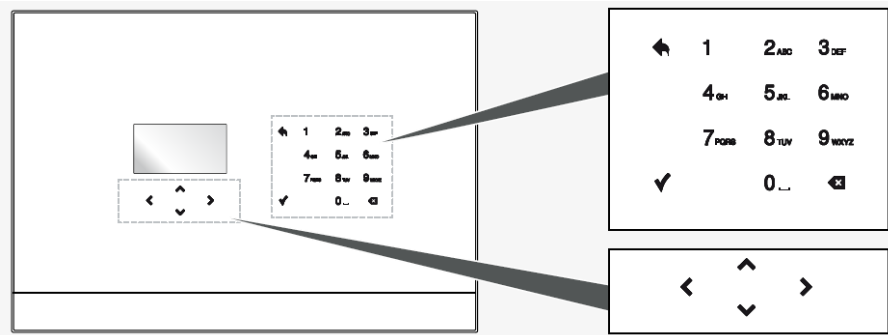
En caso de avería o de alarma, el relativo LED se enciende fijo, con excepción que no funcione la alimentación de red y que solo esté presente la alimentación por batería. En este último caso, para ahorrar corriente, los LED parpadean lentamente (2 segundos encendidas, 6 segundos apagadas). El LED de notificación se apaga automáticamente cuando todas las anomalías pendientes han sido visualizados desplazando las pantallas siguientes con la tecla ‘>’ y volviendo a la pantalla principal.

En caso de alarmas (manipulación o intrusión), tras la operación de reinicio se apaga.

2.3 Interfaz de mando

2.3.1 Uso del teclado

La central se configura con la ayuda del teclado, que permite navegar por el menú e introducir cifras y letras.



El teclado táctil (*) se compone de 17 teclas.

	Permiten navegar por el menú y los iconos.
	Confirma el valor introducido o seleccionado. Si se pulsa en cualquier punto del menú visualizado, guarda los datos y pasa al nivel de menú superior.
	Teclas alfanuméricas que permiten introducir cifras o letras.
	Sale de la sesión de trabajo actual sin guardar.
	Eliminación de un ajuste o de un carácter en función del contexto.

el teclado tradicional (**) se compone de 20 teclas

	Permiten navegar por los menús y los iconos
	Confirma el valor introducido o seleccionado. Si se pulsa en cualquier punto del menú visualizado, guarda los datos y pasa al nivel de menú superior
	Teclas alfanuméricas que permiten introducir cifras o letras
	Sale de la sesión de trabajo actual sin guardar.
	Eliminación de un ajuste o de un carácter en función del contexto.
	Permiten realizar activaciones y desactivaciones rápidas del sistema.

(*) para todos los modelos excepto SAS-W3.1E

(**) solo para el modelo SAS-W3.1E

2.4 Autenticación

Para poder acceder a los menús y operar en la central, hay que autenticarse mediante un identificador y una contraseña que son ambas numéricas. Identificador y contraseña se memorizan en modo cifrado. A cada usuario se le asignan, además, privilegios específicos que definen lo que puede hacer. No existen usuarios predefinidos de fábrica. La duración de la sesión de trabajo es de 3 minutos para los usuarios de nivel 2 y 1 hora para los usuarios de nivel 3.

2.4.1 Identificador del usuario

El identificador del usuario (ID) es un código numérico de 1 cifra variable de 0 a 9 y está asignado de modo progresivo por el sistema.

El ID 0 está reservado a un usuario de nivel 3 (instalador), el ID 1 y siguientes es para un usuario de nivel 2 (usuario) o 4 (encargado del mantenimiento).

Cada sistema debe prever por lo menos un usuario de nivel 3 y un usuario de nivel 2.

2.4.2 Contraseña

La contraseña (PIN) está formada por 5 cifras y es escogida libremente por el usuario. El PIN puede ser modificado solo por su propietario, con el procedimiento dedicado.

2.5 Niveles de autorización

El nivel de autorización determina lo que cada usuario puede y no puede hacer después de haberse autenticado. Existen tres niveles de autorización:

- Nivel 2 reagrupa a los usuarios, es decir, los usuarios que usan cotidianamente el sistema de alarma de intrusión.
- Nivel 3, Instalador: puede crear o modificar la configuración del sistema. Puede haber solo un instalador por sistema. Para poder operar, un usuario de nivel 3 debe ser previamente autorizado por un usuario de nivel 2.
- Nivel 4*. Identifica los usuarios que pueden actualizar o cambiar el firmware de la central, siendo ésta una operación crítica para el buen funcionamiento del sistema sirve para autenticar nuevamente y en modo específico el usuario que ya se había autenticado con otras credenciales de acceso.

El asterisco (*) identifica al mantenedor, ¡preste atención antes de eliminar este usuario!

El usuario de nivel 3 Instalador y el usuario de nivel 2 super usuario corresponden a los niveles homónimos de autorización establecidos por la norma EN 50131-1.

La tabla que sigue muestra los permisos asociados a cada nivel de autorización.

Función	Nivel de acceso		
	2	3	4
	Usuario	Instalador	Encargado del mantenimiento
Activación total	■	■	
Solo conexiones permitidas	■		
Desactivación total	■	■	
Solo desconexiones permitidas	■		
Reinicio I&HAS	■	■	
Verificación funciones I&HAS	■	■	
Integración registro eventos	■	■	
Inhibición / aislamiento / forzado (en función del grado)	■	■	
Adición /variación de los códigos de autorización individuales (permitida solo la variación del propio código)	■	■	
Añadido / eliminación de usuarios y códigos de nivel 2		■	
Añadido / variación datos específicos del sitio		■	
Variación / sustitución firmware			■

3 ACTIVAR Y DESACTIVAR EL SISTEMA

ATENCIÓN:

Para cumplir con el certificado Vds, el keylock debe ser el único dispositivo habilitado para la activación exterior del sistema. Todos los dispositivos configurados o las funciones disponibles en la instalación (mandos a distancia/ teclado de la central/ teléfono móvil/ f@h), deben configurarse para la activación del sistema desde el interior de la vivienda. El keylock permite a los usuarios armar y desarmar el sistema de alarmas secure@home.

El keylock, instalado con la electrocerradura correspondiente, permite que solo se pueda entrar en las áreas protegidas si el sistema de alarmas está desactivado y que este último solo se pueda activar desde el exterior y con la puerta cerrada.

El keylock consta de un teclado de 12 teclas. Las teclas numéricas de 0 a 9 tienen la misma función que el teclado de la central y permiten al usuario introducir un PIN. El botón ON permite activar el sistema, mientras que la tecla OFF efectúa la desactivación total. Para más detalles sobre la instalación, configuración y uso del keylock, consulte el manual 2CSM600756D0901.

Este capítulo ilustra los procedimientos para conectar y desconectar el sistema de alarma de intrusión con teclado y mando a distancia.

Se explican también los procedimientos a activar cuando la central rechaza la operación de conexión a causa de anomalías que encuentra en el sistema o en los componentes.

Para la conexión y desconexión a distancia, véase el capítulo *Mandos a distancia*.

3.1 Conexión y desconexión con teclado

3.1.1 Activación y desactivación rápidas

Se puede realizar la activación o desactivación total de la instalación o una personalización parcial pulsando desde la pantalla principal el botón ▲.

Si hay varios usuarios de nivel 2, seleccionar un usuario de la lista e introducir el PIN; en cambio, si hay solo un usuario, introducir directamente el PIN solicitado.

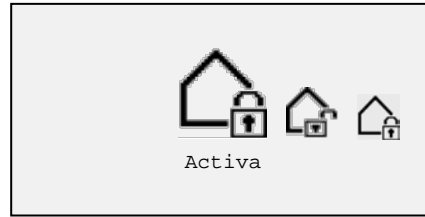
Aparece una pantalla donde se presenta un icono que puede seleccionarse directamente según este criterio:

- Instalación con una o varias zonas activadas: icono de desactivación (como se ilustra en la figura siguiente).



Pulsar OK. La central emite 3 bip y el sistema de alarma de intrusión se desactiva.

- Todas las zonas desactivadas: icono presenta la activación total





Pulsar OK, la central emite 1 bip y se activa el sistema de alarma de intrusión.

- En ambos casos: además de la otra opción, otros 2 iconos de inserciones personalizadas (Favorito 1 y Favorito 2)

Si desea la otra elección, desplazarse con las flechas y confirmar con el botón OK.

Se puede personalizar el mando de activación rápida: en este caso la central ejecuta esta configuración en lugar de aquella predefinida (activación externa total).

Para el modelo SAS-W3.1E, estas funciones también se pueden efectuar mediante las siguientes teclas:

	Activación total
	Desactivación total
	Favorito 1

Si hay varios usuarios, seleccionar un usuario de la lista e introducir el PIN; en cambio, si hay solo un usuario, introducir directamente el PIN solicitado. Si el PIN es correcto, la central efectúa la función asociada.

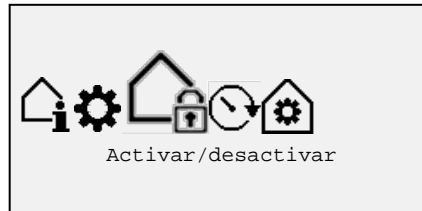
Nota: las activaciones/desactivaciones totales afectan a las zonas para las que el usuario autenticado ha sido autorizado.

3.1.2 Activación total

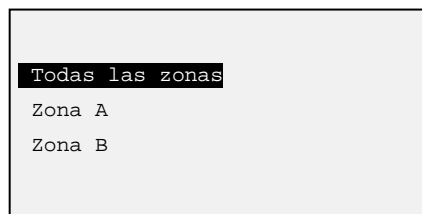
La conexión total del sistema de alarma de intrusión está permitida solo a los usuarios (pines de nivel 2) y al instalador (PIN de nivel 3-si está habilitado por un usuario de nivel 2) que tienen permiso en todas las áreas del sistema.

Para activar todo el sistema de alarma intrusión mediante el teclado:

1. Autenticarse como usuario de nivel 2



2. La central se predispone automáticamente sobre el icono "Activar/Desactivar" Pulsar ok. Seleccionar todas las zonas



3. Y posteriormente pulsar OK.



4. Seleccionar, con las teclas de flecha:

- **Exterior** para activar el sistema en modalidad externa,
- **Interior** para activar el sistema en modalidad interna,
- **Prealarma** para activar el sistema en modalidad prealarma,y confirmar la elección con la tecla **ok**.

La central emite 3 bip y se activan las zonas de alarma de intrusión.

Si en la memoria están presentes señalizaciones de eventos, no se activan las zonas. En cambio, se muestra el primero de los eventos en la memoria aún no examinado. Seleccionar Sistema o Dispositivos para ver todos los eventos, o la leyenda Forzar bloqueo para activar el sistema de alarma (para más información ver el apartado **Activación con forzado de bloqueo**Errore. L'origine riferimento non è stata trovata.)

3.1.3 Desactivación total

La desactivación total del sistema de alarma de intrusión está permitida solo a los usuarios (pines de nivel 2) y al instalador (PIN de nivel 3-si está habilitado por un usuario de nivel 2) que tienen permiso en todas las áreas del sistema.

Para desactivar todo el sistema de alarma de intrusión mediante el teclado:

1. Repetir los puntos de 1 a 2 del párrafo anterior
2. Seleccionar "Desactivada".

La central emite 1 bip y se desactiva el sistema de alarma de intrusión.

3.1.4 Activación parcial

La activación parcial del sistema de alarma anti-intrusión está permitida solo a los usuarios (nivel-lo 2 pines) y al instalador (PIN de nivel 3-si está habilitado por un usuario de nivel 2) en las zonas para las que fueron autorizados.

Para activar parcialmente todo el sistema de alarma de intrusión mediante el teclado:

1. Repetir los puntos de 1 a 2 del párrafo anterior
2. Solo aparecerán las áreas habilitadas. Seleccionar la zona que se quiere activar. Si en fase de programación se le ha dado un nombre significativo a la zona, éste aparecerá en lugar del nombre genérico denominación Zona A, Zona B etc.
3. Seleccionar, con las teclas de flecha:
 - **Exterior** para activar el sistema en modalidad externa,
 - **Interior** para activar el sistema en modalidad interna,
 - **Prealarma** para activar el sistema en modalidad prealarma, y confirmar la elección con la tecla **ok**.

La central emite 3 bip y se activan las zonas de alarma de intrusión.

Si se tienen que activar otras zonas, repetir todo el procedimiento para cada zona a activar.

3.1.5 Desactivación parcial

La desactivación parcial del sistema de alarma de intrusión está permitida solo a los usuarios (pines de nivel 2) y al instalador (PIN de nivel 3-si está habilitado por un usuario de nivel 2) en las zonas para las que fueron autorizados.

Para desactivar parcialmente todo el sistema de alarma de intrusión mediante el teclado:

1. Repetir los puntos de 1 a 2 del párrafo anterior
2. Seleccionar la zona que se quiere desactivar. Si en fase de programación se le ha dado un nombre significativo a la zona, éste aparecerá en lugar del nombre genérico denominación Zona A, Zona B, etc.
3. Seleccionar "desactivada".

La central emite 1 bip y se desactivan las zonas seleccionadas.

3.2 Activación y desactivación con mando a distancia

El mando a distancia puede ser de dos tipos:

- Mando a distancia programable, puede personalizarse, por lo tanto, no hay una tecla predefinida que active o desactive todo el sistema.
- Mando a distancia preprogramado, cuyas teclas están asignadas a funciones específicas.

Remitirse al manual de cada mando a distancia para las modalidades de activación y desactivación de la instalación.

3.3 Activación con forzado de bloqueo

El sistema de alarma anti-intrusión no se activa ante la presencia de las siguientes anomalías:

- Detector en condición activa o averiado.
- Dispositivo antirrobo en condición activa.
- Detector de movimiento interferido o con capacidad reducida.
- Manipulación.
- Avería en la alimentación (red o batería).
- Sirena en avería.
- Problemas de comunicación con los dispositivos.
- Batería baja del mando a distancia
- Problemas del sistema de transmisión de alarmas (GSM).
- Activación realizada mediante el mando a distancia con batería baja
- Otras averías.

Un detector está en condición de activa cuando está señalando una condición de alarma. Por ejemplo, el contacto magnético de una puerta o ventana abierta. Un dispositivo antirrobo está en condición de activa cuando está señalando un intento de robo. Por ejemplo, un mando a distancia cuando se mantiene presionado un pulsador programado por robo.

Un usuario de nivel 2 puede forzar el bloqueo para las zonas de su competencia y activar el sistema de alarma de intrusión. Con el forzado del bloqueo la central ignora las posibles causas que impiden la activación normal del sistema y lo activa.

¡ATENCIÓN!



El forzado del bloqueo es una operación de emergencia para permitir el funcionamiento parcial del sistema de alarma anti-intrusión. Hay que ser conscientes de que a causa de las anomalías presentes la protección ofrecida por el sistema se reduce de modo más o menos grave. Las anomalías que han causado el bloqueo deben ser resueltas lo antes posible para restablecer la plena funcionalidad del sistema.

3.4 Reiniciar

Si el sistema de alarma de intrusión no puede activarse a causa de posibles inhibiciones debidas a alarmas técnicas, averías o alarmas de sabotaje en los detectores, como por ejemplo oscurecimiento-supervisión, es necesario reiniciar el estado de la central o de cada zona. La función permite hacer cesar la señalización persistente de anomalía causada por la falta de transmisión de fin alarma (por ejemplo una alarma técnica impulsiva como alarma por humo, inundación, batería central, etc.).

Para restablecer las anomalías (Memoria de alarmas y Supervisión) de los sensores, se deberán restablecer las diferentes zonas.

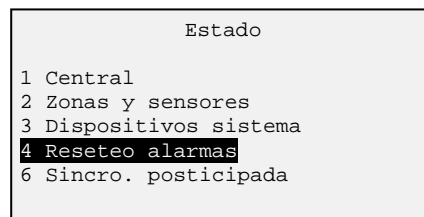
La acción de reinicio se registra en el historial de eventos.

Para reiniciar el sistema o una zona, realizar lo siguiente:

1. Autenticarse como usuario de nivel 2



2. Seleccionar Estado y Eventos y pulsar OK



3. Seleccionar Estado y pulsar OK
4. Seleccionar Reiniciar alarma: seleccionar Sistema para reiniciar todo el sistema o cada zona a reiniciar. Ejecutando el reinicio de sistema se ponen en cero todos los contadores relativos a las alarmas múltiples

4 PÁNICO Y ROBO

Este capítulo ilustra los procedimientos para activar las alarmas de pánico y robo. La alarma pánico la genera voluntariamente el usuario cuando piensa que exista un peligro potencial. Por ejemplo, podría ser la presencia amenazadora de un desconocido. La alarma pánico hace sonar las sirenas, para disuadir, pero no activa el envío de mensajes telefónicos.

La alarma robo es generada voluntariamente por el usuario cuando es víctima de un robo. Este tipo de alarma no hace sonar las sirenas, para evitar reacciones del ladrón, desactiva la instalación si está activada y desencadena el envío de señalizaciones de alarmas telefónicas.

4.1 Activar la alarma pánico

4.1.1 Activación con el teclado

Para activar el evento Pánico, realizar lo siguiente:

1. Autenticarse como usuario de nivel 2
2. Desplazarse con las teclas de flecha al icono Pánico y presionar la tecla ok. Para interrumpir el sonido de las sirenas antes del tiempo programado, desactivar la instalación.



4.1.2 Activación con el mando a distancia

Presionar la tecla del mando a distancia programada para activar el evento Pánico. Para terminar la alarma, interrumpiendo el sonido de las sirenas programadas, presionar la tecla programada del mando a distancia para desactivar el sistema. Remitirse al manual del mando a distancia para mayores detalles.

El certificado VDS no permite armar/desarmar el sistema mediante:

- Mando a distancia
- Controles remotos (App/GSM)

El dispositivo no se debe utilizar para armar/desarmar el sistema desde el exterior.

4.2 Activar la alarma robo

Cuando se activa la alarma robo se bloquean todas las otras alarmas exclusivamente en curso, se desactiva la instalación si está activada y se activan las llamadas telefónicas de voz de alarma por robo.

4.2.1 Activación con el mando a distancia

Presionar la tecla del mando a distancia programada para activar el evento Robo.

Para terminar la alarma, presionar la tecla programada del mando a distancia para desactivar la alarma.

5 ALARMAS Y MEMORIAS DE EVENTOS

5.1 Prioridad de las alarmas

En caso de varias alarmas contemporáneas, de distinto tipo, se señala solo la alarma de prioridad superior. En el caso de que las alarmas tengan la misma prioridad, se señala la primera disparada. La tabla siguiente muestra la prioridad de los diferentes tipos de alarma, donde 1 representa la prioridad máxima.

Tipo de alarma	Prioridad
Intrusión	1
Sabotaje	2
Supervisión	3
Batería baja	4
Sistema	5
Pánico	6
Técnica	7

5.2 Cómo bloquear una alarma

Una alarma se bloquea desactivando el sistema de alarma con el teclado, el mando a distancia o desde remoto. Cuando se bloquea una alarma cesan las señalizaciones sonoras (sirenas) y las telefónicas (mensajes vocales y de texto).

La desactivación total bloquea cualquier tipo de alarma, las desactivaciones parciales pueden bloquear o no bloquear la alarma, como se muestra en la tabla que sigue:

Tipo de alarma	Desactivación		
	Total	Zona en alarma	Zona No en alarma
Intrusión	Bloquea alarma	Bloquea alarma	Alarma continúa
Sabotaje	Bloquea alarma	Bloquea alarma	Alarma continúa
Sistema (1)	Bloquea alarma	Bloquea alarma	Bloquea alarma
Pánico (1)	Bloquea alarma	Bloquea alarma	Bloquea alarma
Técnico (1)	Bloquea alarma	Bloquea alarma	Bloquea alarma

(1) Se aplica también cuando se opera en una zona ya desconectada.

Todas las alarmas se memorizan en la memoria de los eventos mandatarios, analizando la cual se pueden conocer los detalles relativos a la alerta (cuando se ha producido, que tipo de alarma era, cuál dispositivo ha engendrado la señalización de alarma, etc.).

5.3 Memorias de los eventos

Los eventos se registran en la central en dos bloques de memoria:

- Críticos, que puede contener hasta 250 eventos diferentes.
- Secundarios, que puede contener hasta 128 eventos diferentes.

Cuando se alcanza la capacidad máxima del bloqueo, el nuevo evento sobrescribe el evento más antiguo presente en la memoria.

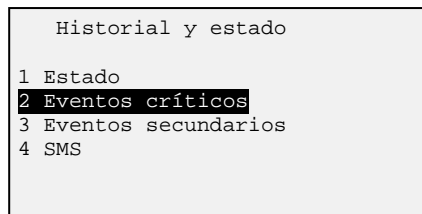
5.3.1 Ver los eventos

Para visualizar los eventos hacer lo siguiente:

1. Autenticarse como usuario de nivel 2



2. Seleccionar Estado y eventos y pulsar OK



3. Seleccionar 2 Eventos críticos para examinar los eventos principales, 3 para aquellos secundarios.
4. Se abre la ventana de detalle de los eventos. Los eventos se visualizan desde el más reciente al más antiguo.
Para desplazarse entre los eventos, usar las teclas ► y ◀.
Para leer las informaciones relativas al evento, ver el párrafo *Cómo interpretar un evento memorizado*.

5.3.2 Eventos SMS

Al pulsar 4 SMS se abre una ventana que muestra el último SMS recibido.

En la pantalla se muestra:

- El número de teléfono del remitente
- el texto del mensaje
- fecha y hora.

En esta ventana, pulsando la tecla ►, se muestra de la misma forma el último SMS enviado desde la central.

Esta información se conserva hasta que se apaga la central.

5.3.3 Cómo interpretar un evento memorizado

Los datos relativos al evento se incluyen en una o varias pantallas. La primera pantalla se aparece a la siguiente:

```

Evento      [n/t]
Fecha Hora
Tipo de evento
Info 4
Info 5
Info 6
Info 7
<Recientes Pasados>

```

donde:

- **[n/t]** indica el número progresivo del evento (n) y el total (t) de los eventos en la memoria.
- **Fecha** es la fecha en la cual se produjo el evento.
- **Hora** es la hora en la cual se produjo el evento.
- **Info 4 ... Info 7** son informaciones adicionales que cambian según el tipo de evento y que están especificadas en las tablas siguientes.
- **>** y **<** permiten navegar hacia adelante y hacia atrás entre los eventos

Eventos principales (obligatorios)					
Tipo de evento	Info 4	Info 5	Info 6	Info 7	Segunda pantalla (Inf)
Activación	Sistema /zona activada	Nombre o ID del usuario que ha activado	Dispositivo usado para la operación		Estado zonas anteriores Estado zonas después de la activación
Desactivación	Sistema /zona desactivada	Nombre o ID del usuario que ha desactivado	Dispositivo usado para la operación		Estado zonas anteriores Estado zonas después de la desactivación
Alarma por robo		Nombre o ID del usuario que ha realizado la operación	Dispositivo usado para la operación		
Alarma intrusión	Tipo de sensor	Posición del sensor			
Alarma manipulación	Tipo de sensor	Posición del sensor			
Supervisión	Tipo de sensor	Posición del sensor			
Alarma interferencia radio	Central				
Sabotaje	Central				
Exclusión del detector	Tipo de sensor	Posición	ID Usuario		
Forzado bloqueo	Activación	Nombre o ID del usuario	Dispositivo usado		
Avería - tipo de avería	Tipo de sensor	Posición			

Eventos principales (obligatorios)					
Tipo de evento	Info 4	Info 5	Info 6	Info 7	Segunda pantalla (Inf)
Batería baja	Tipo de sensor	Posición			
Añadido usuario nivel 2 por usuario nivel 3	Nuevo usuario L. 2-3		PIN Niv3 Índice	PIN Niv2 Índice	
Cambio fecha y hora	ID Usuario				
Variación num. de teléfonos	ID Usuario				
Actualización del SW central	ID usuario				
Encendido central					
Verificación periódica GSM	ID teléf. (1)				
Falta de tensión de red	Nivel de la batería				
Retorno de la tensión de red	Nivel de la batería	Ausencia 230V	Tiempo de red OFF en minutos		
Llamada vocal	Tipo de Alarma	ID teléfonos llamados (1)			
Envío mensaje de texto	Tipo de Alarma	ID teléfonos destinatarios			

(1) En negrita si la llamada ha tenido éxito positivo, es decir, con la respuesta del destinatario, en normal si la llamada no ha tenido éxito.

Eventos secundarios (opcionales)					
Tipo de evento	Info 4	Info 5	Info 6	Info 7	Segunda pantalla
Prealarma de intrusión	Tipo de sensor	Posición Sensor			
Iniciar sesión	ID Usuario				
Cerrar sesión	ID Usuario				

6 MANDOS A DISTANCIA

Si está habilitada, se puede interactuar con la central con GSM a distancia mediante línea telefónica o mensajes SMS. La central debe estar equipada con una SIM Card activa sin PIN. Atención: si se utiliza una SIM prepago, controlar que no haya caducado y que contenga suficiente crédito. Si no se utiliza la red GSM durante mucho tiempo, es posible que el operador haya desactivado la posibilidad de realizar llamadas vocales y/o de enviar SMS. Se recomienda efectuar el test GSM y comprobar el crédito al menos cada tres meses. Consultar la tabla de «resolución de fallos» para más detalles sobre las posibles anomalías.

6.1 Mando vía mensaje de texto

Para aceptar mandos vía mensaje de texto, el número que llama debe estar entre aquellos memorizados en la central y, obviamente, no oscurecido. Si el número no está presente en la lista, o está oscurecido, la central ignora el pedido.

Los privilegios para operar en el sistema están garantizados por el par identificador-password usado para autenticarse mediante el teclado de la central. Todos los mandos requieren autenticación, con excepción de la solicitud de estado y la escena.

Pueden mandar mandos de mensaje de texto los usuarios de nivel 2.

Los mandos se envían mediante un mensaje de texto codificado, al cual la central replica con un mensaje SMS de respuesta o confirmación en claro, salvo que se especifique que no hay que mandar una respuesta.

Para cada mando hay que enviar un SMS distinto.

La estructura general del mando es:

[Mando] [Qué] [Modo] [Usuario + PIN]

Mando	Qué	Modo	Usuario + PIN
Armar	Sistema Zona	Interior Exterior Prealarma	código numérico de 6 dígitos
Desarmar	Sistema Zona		código numérico de 6 dígitos
Escena # (1-10)			
Estado			

El SMS de respuesta/confirmación es del tipo:

Zona A (*) Exterior

Zona B Exterior

Zona C Interior

Zona D Interior

- El asterisco (*) indica una anomalía de zona: el detalle de la anomalía se explicaba en el panel de control o conectando a free@home;
- Hasta 4 zonas, la central envía 1 SMS;
- Más allá de las 4 zonas, la central envía 2 SMS;
- La zona tecnológica (24h) no se enumerará ya que está siempre activa.

Cuando se envía un SMS desconocido o incorrecto, la central responde con un SMS de ejemplo de la sintaxis correcta, de la siguiente manera:

Ejemplo:

Armar ZonaA Interior 111111

Desarmar ZonaA 111111

Escena 1

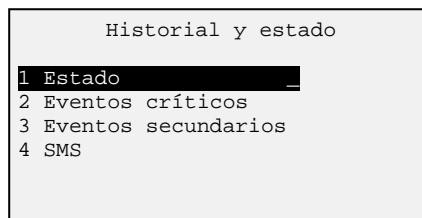
7 ESTADO DE LA INSTALACIÓN

Para verificar el estado de la central y los enlaces de radio:

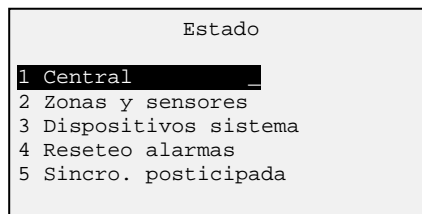
1. Autenticarse como usuario de nivel 2



2. Seleccionar Estado e historial de eventos y pulsar OK



3. Seleccionar Estado



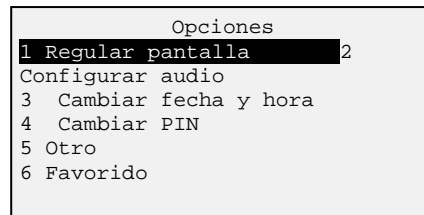
4. Seleccionar Central
se muestran las siguientes informaciones:
 - **Tamper** (manipulación): OK = tamper cerrado / Abierto = manipulación,
 - **Módem** (GSM): - / No disponible
 - **Batería**: NO = ausencia de batería /tensión y temperatura de la batería
 - **Red**: Sí / NO
 - **Dirección**: dirección: dirección hexadecimal de la central.
5. Presionando la tecla > se abre una nueva ventana donde se muestran la calidad actual de las comunicaciones radiales y la ocupación del canal de radio (Duty Cycle, no debe superar 1% del tiempo) en los últimos 15 minutos, en la última hora y en las últimas 24 horas. Si no existen datos aparece el mensaje "no disponible". Al pulsar de nuevo la tecla > se abre otra ventana en la que se muestra información relativa al GSM: el tipo de Módem y la velocidad de uso, el nivel de señal en dBm, el estado de registro en la red y el código de identificación del operador (los códigos de los operadores están indicados en la normativa ITU E.212)
6. Seleccionar zonas y sensores: Se muestran las diferentes zonas y dentro de cada zona se muestra información sobre el estado de los sensores programados.
7. Reset Alarma: permite eliminar todas las anomalías visualizadas en el estado tanto del sistema como de los sensores si se han resuelto: por ejemplo, la operación borra la notificación de "Alarm Mem" pero no elimina una anomalía del tipo "ma-nomination" si permanece en el dispositivo.
8. Sincronización pospuesta: Muestra la lista de sensores, si los hay, en los que se ha realizado un cambio de uno o más parámetros de radio mientras se espera a que este cambio se implemente realmente en el sensor. Si la lista no está vacía, aparece un símbolo de tipo 📶 en la parte superior derecha de la pantalla en el resto de la ventana.

8 AJUSTES DE LA CENTRAL

Este capítulo ilustra los procedimientos para regular la fecha y hora de la central, la iluminación de la pantalla, los feedback sonoros y el sonido de la sirena interna (zumbador).

8.1 Ajustar pantalla

1. Autenticarse como usuario de nivel 2.
2. Desplazarse con las teclas de flecha al icono Opciones y presionar la tecla **ok**



3. Marcar 1 Regular pantalla

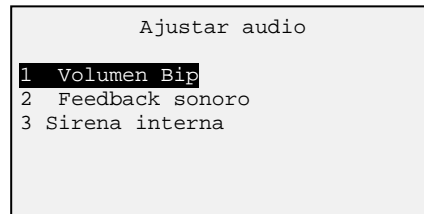


4. Desplazarse con las teclas flechas y seleccionar Sí o No con las teclas flechas para activar o no el apagado automático. Con el autoapagado activado la iluminación de la pantalla se apaga después de 60 segundos desde el último botón presionado.

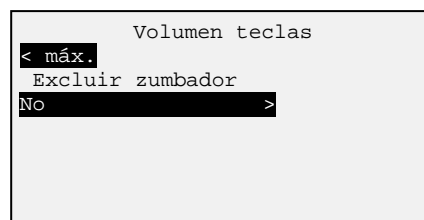
8.2 Ajustar audio

8.2.1 Volumen beep

Para regular los feedback sonoros de las teclas y del zumbador interno, realizar los puntos 1 y 2 del apartado anterior y pulsar Ajustar audio:



Marcar **1** Volumen bip



configurar el volumen del feedback de las teclas o elegir NO para excluirlo.
Configurar Excluir Zumbador en Sí si se quiere excluir totalmente el sonido de la sirena interna.

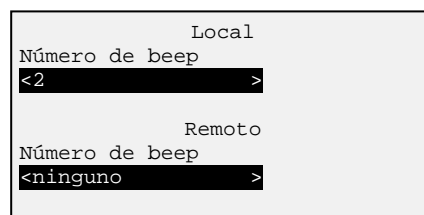
8.2.2 Feedback sonoro

Para regular los feedback sonoros, realizar los puntos 1 y 2 del apartado anterior y pulsar Ajustar audio:

Marcar 2 Feedback sonoro y después ingresar el número que caracteriza el mando del cual se quieren configurar los feedback sonoros. Las opciones posibles son:

- **1 Activación** parcial o total de la instalación
- **2 Desactivación** (total o parcial) de la instalación anti-intrusión.

Aparece una nueva pantalla



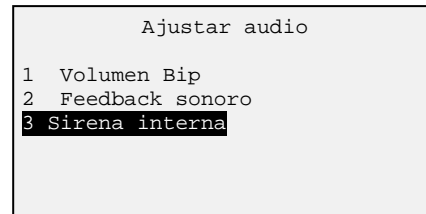
Ahora se puede definir el mando y cuántos bips activar:

- **Local** Comprende el Teclado de la central, el mando a distancia y el activador.
- **Remoto** el feedback sonoro emitido cuando el evento ha sido causado por f@h, GSM.

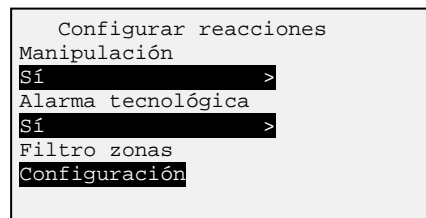
Para cada tipo de feedback es posible elegir el número de bip que se emitirán (desde ninguno a 3).

8.2.3 Alarmas

Para regular el zumbador de la central en caso de alarmas, realizar los puntos 1 y 2 del apartado anterior y pulsar Ajustar audio.



Introducir **3** Sirena Interna.



- **Manipulación**; configurar Sí si se desea que frente a una manipulación la central suene, No si no se desea, Habilitado si se desea que el avisador acústico de la central suene solo con la instalación activada
- **Tecnológico**, es decir, cualquiera de las alarmas tecnológicas eventualmente configuradas (inundación, fuga gas etc.), incluso con el sistema antiintrusión desactivado.



¡CUIDADO!

La configuración Manipulación no es conforme con la norma EN 50131-1

Filtro Zonas, permite seleccionar las zonas a considerar en caso de alarma (solo para alarmas de intrusión y alarmas de manipulaciones de los sensores). Como configuración de fábrica están todas las zonas. Si la alarma se dispara en una zona excluida la sirena interna no será esforzada.

8.3 Regulación de la fecha y hora

La regulación de la fecha y hora es fundamental para la correcta memorización temporal de los eventos en el historial.

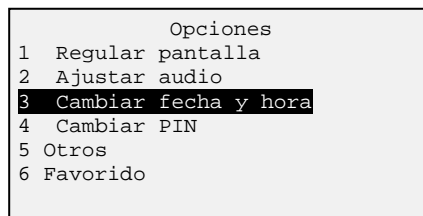
La central gestiona automáticamente el cambio de hora solar - legal y viceversa.

Para modificar la fecha y hora.

1. Autenticarse como usuario de nivel 2



2. Desplazarse con las teclas de flecha al icono Opciones y presionar la tecla **ok**



3. Marcar **3** Cambiar fecha y hora



4. Ingresar la fecha y la hora con las teclas numéricas, usando las teclas de flecha para desplazarse. Confirmar la fecha y la hora ingresadas con la tecla **ok**.

8.4 Cambiar PIN

Para modificar el propio PIN:

1. Autenticarse como usuario de nivel 2.

```
Opciones
1 Regular pantalla
2 Ajustar audio
3 Cambiar fecha y hora
4 Cambiar PIN
5 Otros
6 Favorido
```

2. Desplazarse con las teclas de flecha al icono Opciones y presionar la tecla **ok**
3. Marcar 4 Cambiar PIN

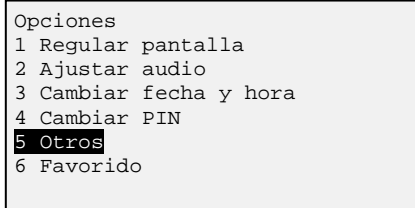
```
Cambiar PIN:
Usuario 1
PIN
*****
Nuevos PIN
*****
Repetir PIN
*****
```

4. Configurar el PIN actual, el nuevo PIN (2 veces) y pulsar OK para guardar todo.

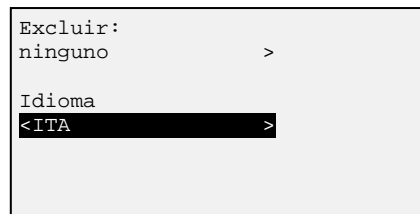
8.5 Modalidad operativa y cambio de idioma

Para modificar la modalidad operativa:

1. Autenticarse como usuario de nivel 2.
2. Desplazarse con las teclas de flecha al icono Opciones y presionar la tecla **ok**



3. Marcar 5 Modalidades operativas



- **Excluir**
 - i. Seleccionar "Forzar bloqueo" para excluir a la prestación: con Forzar Bloqueo Excluido la central realiza la función de activación de la instalación sin pedir una confirmación adicional en caso de presencia de una o más anomalías del sistema.
 - ii. Seleccionar Aviso Led para excluir el triángulo amarillo de "Presencia notificaciones" y la consiguiente necesidad de reinicio. El led, si está deshabilitado, no se encenderá nunca incluso en el caso existan notificaciones memorizadas y aún no visualizadas por el usuario.
 - iii. Seleccionar Todas para excluir tanto el forzador de bloqueo como el led.
 - iv. Seleccionar Ninguna para mantener las configuraciones predeterminadas.

¡ATENCIÓN!



La exclusión de la función Forzar bloqueo y la exclusión del led no son conformes a la norma EN 50131-1.

- **Idioma:** seleccionar el idioma deseado

¡ATENCIÓN!



La selección del idioma tiene efecto inmediato o tiempo de carga breve. La única excepción es el cambio del/al italiano, para el cual se reinicia automáticamente el sistema.

8.6 Personalice la inserción rápida

Para configurar un mando de activación rápida personalizado:

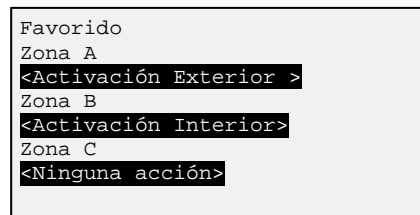
1. Autenticarse como usuario de nivel 2.
2. Desplazarse con las teclas de flecha al icono Opciones y presionar la tecla **ok**.



3. Ingresar 6 Favorido: se abre una ventana



4. Seleccione el favorito que desea editar (1/2) y presione OK



5. Para cada zona de la instalación definir el tipo de activación deseado entre los siguientes:
 - Externo
 - Interior
 - Prealarma
 - Deshabilitado
 - Ninguna acción

Esta configuración personalizada, una vez guardada, se ejecutará todas las veces que se ejecuta un mando de "activación rápida" en lugar de la Predeterminada (Activación total).

INSTALAR Y CONFIGURAR EL SISTEMA

Esta sección del manual contiene todas las informaciones para configurar y mantener la central de alarmas. Además, se brindan sugerencias para el diseño de un sistema de alarma de intrusión, se enumeran las características técnicas de la central y se indican los procedimientos para aislar y resolver posibles anomalías de la instalación.

Esta sección está dirigida al técnico que realiza el montaje de la instalación.

9 CARACTERÍSTICAS PRINCIPALES

9.1 Funciones principales de la central

La central se comunica con los otros dispositivos de la instalación en radiofrecuencia y pone a disposición del usuario las siguientes funcionalidades:

- gestión de los dispositivos anti-intrusión y para la seguridad doméstica;
- gestión de señalizaciones antipánico;
- mandos de accionamiento para dispositivos externos;
- notificación de las alarmas, mediante mensajes vocales o mensajes de texto, a los números telefónicos programados;
- control remoto del sistema mediante mensaje de TEXTO;
- integración de la instalación de Home Automation Busch-/ABB-free@home

9.2 Capacidad del sistema

La central gestiona hasta 8 zonas programables, cada una de las cuales puede contener hasta un máximo de 64 detectores, por un total de 64 presentes en el sistema. El número de zonas efectivas se determina durante la configuración de la central.

Las zonas pueden programarse individualmente como:

- alarma de intrusión - hasta un máximo de 7 zonas
- alarmas tecnológicos (humo, inundación, gas) - 1 zona activa las 24 horas;

La central gestiona hasta:

- 4 sirenas externas
- 4 repetidores de señal; (1)
- 16 dispositivos mandos a distancia para la activación o desactivación de la instalación de alarma de intrusión; (1)
- 12 números de teléfono programables a los cuales enviar las señalizaciones de alarma y de los eventos.

(1) los repetidores de señal son dispositivos no certificados IMQ-Sistemas de seguridad

10 DISEÑAR UNA INSTALACIÓN

Diseñar una instalación de alarma de intrusión y seguridad con dispositivos radio alimentados con batería es simple, sólo hay que respetar algunas medidas simples. Un buen proyecto garantiza una instalación fácil y un funcionamiento correcto de la instalación. En este capítulo se suministran todas las informaciones necesarias para lograr estos objetivos.

10.1 Información sobre las ondas de radio

Los sistemas que utilizan las ondas de radio para la conexión de los dispositivos ofrecen la gran ventaja de poder instalar y conectar los diferentes aparatos sin tener que realizar obras complejas de cableado. Como desventaja requieren una mayor atención en el posicionamiento de los dispositivos, para poder obtener la mejor conexión radio.

La calidad de una conexión de radio es directamente proporcional a la potencia de la señal que alcanza el dispositivo. Esta potencia está influida por la distancia entre los dispositivos (la potencia de la señal de radio decrece con el cuadrado de la distancia) y por posibles fenómenos de absorción de la señal causados por obstáculos a lo largo del recorrido de las ondas de radio.

Potencia restante después del cruce	Material atravesado
90-100%	Mobiliario de madera o plástico, materiales sintéticos (por ej., pléxiglas), vidrio, ladrillos perforados, pladur
65-85%	Ladrillos macizos, mármol, acuarios
10-60%	Hormigón armado, estructuras metálicas (electrodomésticos, tuberías, cercas)
0-10%	Planchas metálicas, espejos

10.2 Utilizar las zonas

Las zonas sirven para agrupar funcionalmente los detectores, para un mejor uso de la instalación. En fase de configuración es posible determinar tanto el número de zonas como su tipología.

10.2.1 Tipos de zonas

Las zonas pueden programarse como:

- alarma de intrusión: sirve para reagrupar los detectores que señalan los intentos de intrusión y que deben estar habilitados solo cuando sirve, es decir, cuando el ambiente a proteger está sin vigilancia;
- activa las 24 horas del día: sirve para reagrupar los detectores que deben estar siempre activos para realizar señalizaciones relativas a la seguridad, por ejemplo, los detectores por inundación, los detectores de humo, los detectores de gas y, en general, los detectores tecnológicos;

La zona de alarma de intrusión puede estar configurada en modalidad prealarma, alarma interna, alarma externa.

En las modalidades prealarma y alarma interna se presupone que los ambientes no estén totalmente deshabitados y, por lo tanto, no se activan algunos tipos de señalización (sirenas externas y mensajes telefónicos).

En la modalidad Alarma externa, en caso de alarma, se activarán todas las señalizaciones previstas por el sistema. Todas estas acciones son configurables.

¡ATENCIÓN!



La zona técnica (24 horas) y las modalidades de prealarma y alarma interna no son conformes con la norma EN 50131-1. Las funciones relativas a la seguridad doméstica como, por ejemplo, los detectores por inundación, los detectores de humo, los detectores de gas y, en general, los detectores tecnológicos y las funciones de Home Automation no están cubiertos por las normas EN 501311 y EN 501313.

10.2.2 Subdivisión en zonas

La subdivisión de la instalación de la alarma de intrusión en zonas permite una mayor flexibilidad en su gestión y satisface mejor las exigencias del usuario.

Por ejemplo, se pueden asociar los detectores perimetrales (por ejemplo, apertura puertas y ventanas) a una zona y aquellos de infrarrojos pasivos a otra. Así, el usuario podrá activar solo la primera zona de noche, cuando duerme, y ambas cuando deja la vivienda sin vigilancia. Con esta configuración se señalarán los intentos de intrusión mientras se duerme, permitiendo igualmente el libre desplazamiento de las personas dentro de la vivienda cuando fuese necesario. La posibilidad de activar y desactivar zonas diferentes es muy útil también cuando se posee un garaje, una tienda, un taller o un laboratorio que están contiguos a la vivienda. En este caso la posibilidad de asociar los diferentes ambientes a zonas diferentes permite defenderlos selectivamente, con una instalación sola, introduciendo la protección anti-intrusión cuando no hay nadie.

11 INSTALACIÓN DE LA CENTRAL

Para la instalación y fijación de la central, remitirse a la guía rápida - "Hoja de instalación".

11.1 Ambientes de trabajo

La central gestiona 2 ambientes de trabajo distintos: el entorno usuario final y el entorno instalador. Para acceder a estos dos entornos se requieren dos autentificaciones específicas: una de nivel 2 y una de nivel 3.

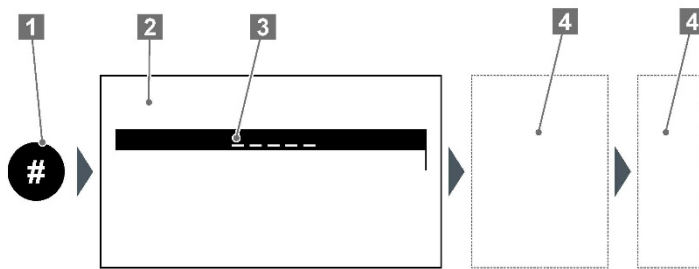
Cuando está en funcionamiento, el primer acceso es siempre de nivel 2, al que puede seguir una autentificación de nivel 3 si se accede al menú del instalador.

Accediendo como usuario de nivel 2 la central presenta lo descrito en el párrafo *2.1.3 Menú principal usuario*.

Accediendo a la sección instalador  se presenta la pantalla del medio ambiente específico:

11.2 Programación

11.2.1 Lectura de las secuencias operativas



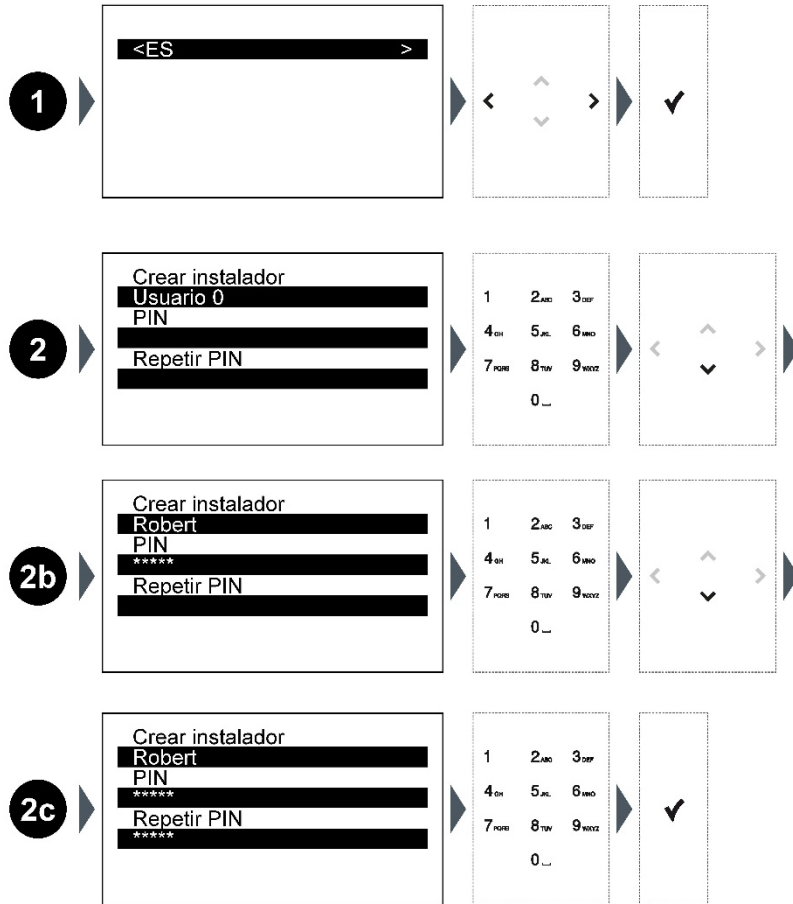
1	Número de la secuencia
2	Pantalla
3	Línea seleccionada/destacada
4	Medio de intervención sobre la central (teclas alfanuméricas, flechas, etc.).

11.2.2

11.2.3 Primer encendido

Con ocasión del primer encendido de la central o tras un "reset", es necesario proceder a la configuración (ajuste del idioma, creación de los usuarios, adquisición de los dispositivos de seguridad, creación de zonas, etc.).

Siga el proceso siguiente para la programación de la central:



¡CUIDADO!

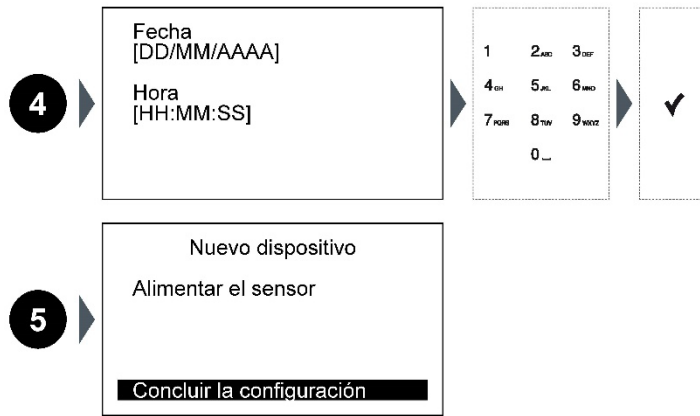


¡ES MUY IMPORTANTE GUARDAR CON CUIDADO EL PIN!

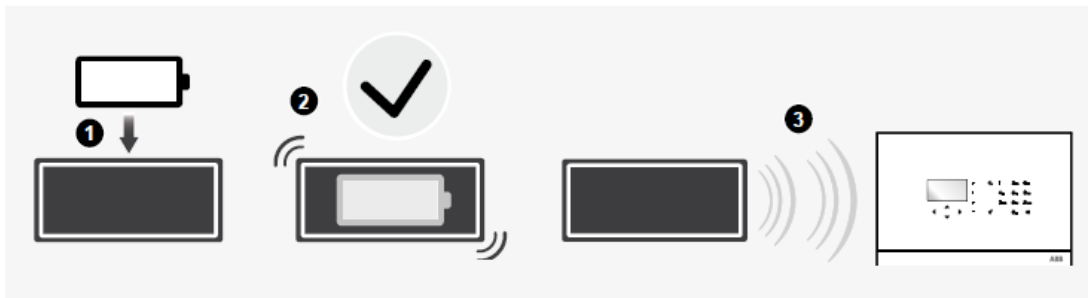
Por motivos de seguridad, la pérdida de este PIN requiere la utilización de un software específico de mantenimiento.



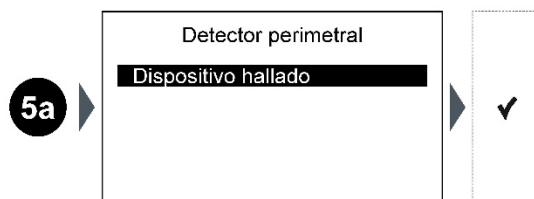
INFO: La secuencia 3 solo se visualiza cuando la central secure@home está conectada por cable BUS a un System Access Point free@home.



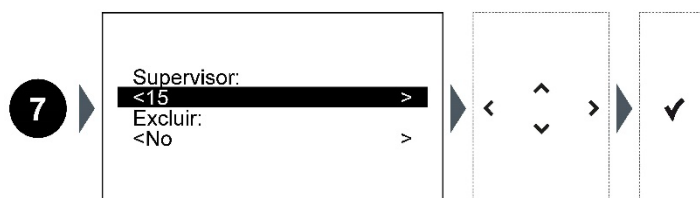
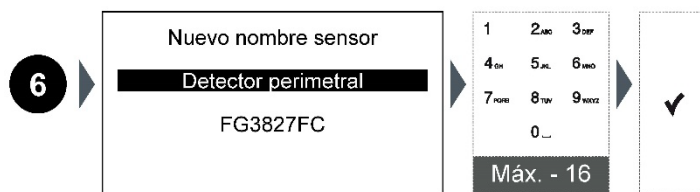
INFO: Para efectuar las operaciones de introducción de la batería del dispositivo que se debe configurar, consulte la hoja de instrucciones correspondiente.



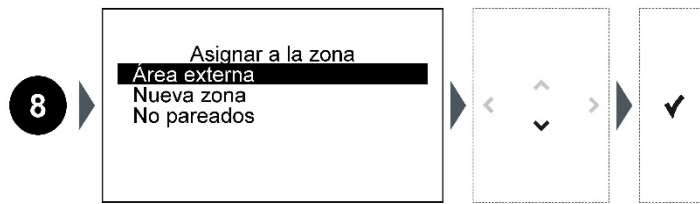
INFO: La imagen representa un dispositivo genérico. La configuración puede efectuarse sobre todos los dispositivos secure@home.



INFO: En caso de conexión con free@home, se saltarán los puntos 6, 7 y 8.



INFO: El menú de configuración varía en función de las características del dispositivo de seguridad instalado.

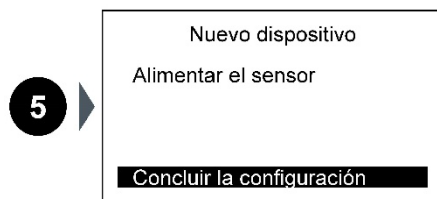


INFO: La secuencia 8 solo es válida para los sensores antiintrusión. Los sensores de seguridad doméstica (humo, inundación) se asignarán automáticamente a una zona activa H24.

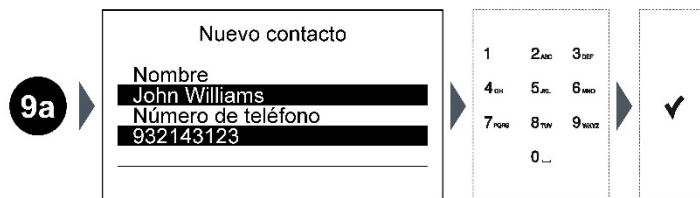
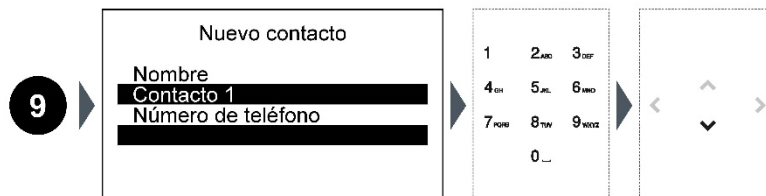
Los dispositivos del sistema (mandos a distancia, sirenas, repetidores, etc.) no están asignados a ninguna zona específica.

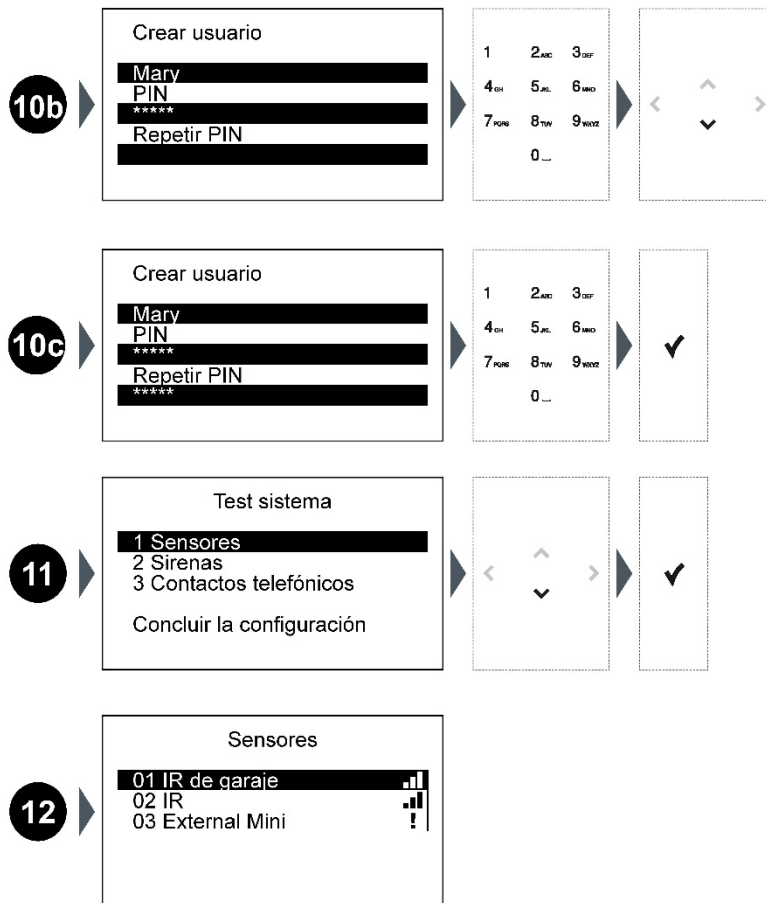


Una vez que se crea la zona y se le asigna el sensor, la central regresa a la pantalla número 5.



INFO: Se puede proceder a la adquisición de un nuevo dispositivo siguiendo el procedimiento indicado en las pantallas 5 a 8; de lo contrario, para completar la instalación seleccione "Concluir Setup":



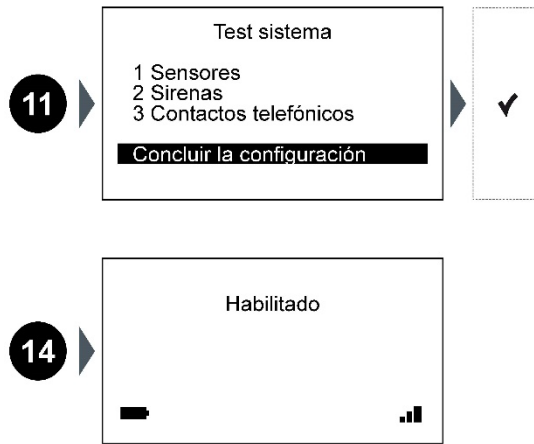


	Señal de radio óptima.
	Señal de radio buena.
	Señal de radio insuficiente: traslade el sensor para mejorar la comunicación o añada repetidor de señal.
	Anomalía (manipulación, enmascaramiento, fallo, etc.): verifique el sensor.

Para conocer los detalles del dispositivo instalado es necesario seleccionar la opción correspondiente (ej.: "01 IR de garaje") y confirmar con la tecla .

Detalles sensor:
 F8B4C0B2 - 20 dbm
 Tipo de sensor INFO
 IR interno
 Último rx
 Fecha hora

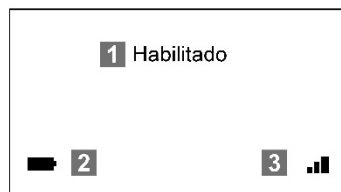
Para regresar a la pantalla 14 y proceder a la finalización de la programación, vuelva a la pantalla anterior con la tecla .



Nota: En caso de pérdida del PIN del instalador y/o del usuario, por motivos de seguridad, no será posible modificarlos desde la central; será necesario resetear el sistema mediante un software específico de mantenimiento y repetir las operaciones 1-2-4-9.

11.3 Estado del sistema

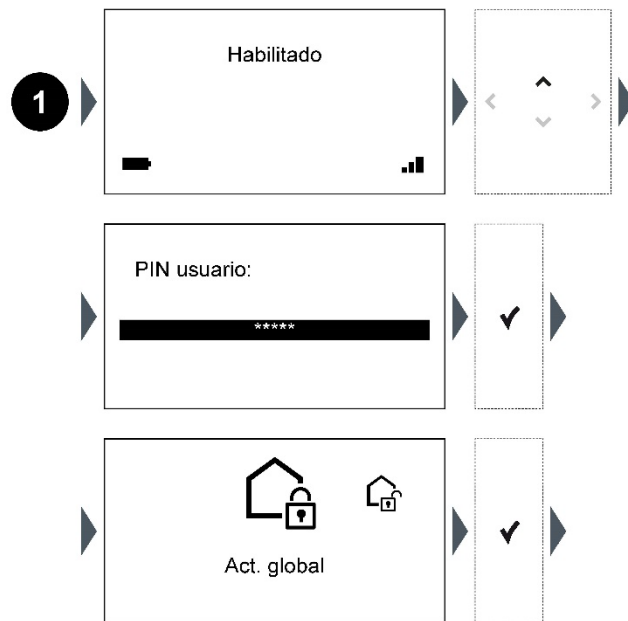
Una vez terminada la programación es posible visualizar la Pantalla Inactiva:



Estado de	Icono	Significado
1		En la pantalla inactiva se podrá visualizar uno de los siguientes mensajes: Habilitado: todas las zonas están habilitadas de la misma manera. Deshabilitado: todas las áreas están deshabilitadas. Parcial: las zonas están habilitadas de manera diferente o alguna está deshabilitada.
2		El icono de la batería visualizada puede indicar uno de los siguientes estados:
		Batería conectada y en fase de carga: la central está conectada a la red de 220 V.
		Batería conectada: no obstante, la central está conectada a la red de 220 V.
		Red ausente: la central se alimenta a través de la batería (con indicación del nivel de carga).
3		El icono GSM indica, a través del número de rayas, el nivel o la falta de señal.
		Señal GSM óptima.
		Señal GSM buena.
		Señal GSM baja.
		Señal GSM ausente.


11.3.1 Armar/desarmar el sistema

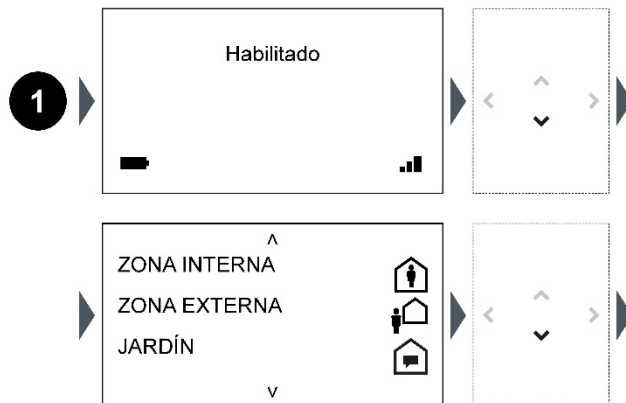
Desde la Pantalla inactiva se puede armar/desarmar rápidamente el sistema pulsando la tecla



INFO: La activación global por defecto habilitará todo el sistema en modo Habilitación externa, mientras no se defina una modalidad/combinación de activación de las zonas preferidas, para asociarlas a esta instrucción.

11.3.2 Visualizar las zonas de alarma

Desde la Pantalla inactiva se puede visualizar el estado de las zonas de alarma configuradas presionando la tecla :



Prealarma: las eventuales alarmas de intrusión se notifican de modo silencioso (por ejemplo, mediante notificaciones "push" o SMS), excluyendo el uso de las sirenas.




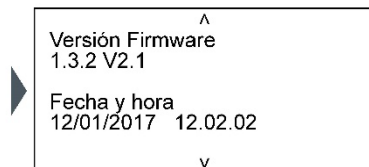
Activación interior: las eventuales alarmas de intrusión se señalan únicamente a través de sirena interna, integrada en la central, y de notificaciones (por ejemplo, "push" o SMS), excluyendo el uso de sirenas externas.



Activación exterior: en caso de alarma, activa todos los tipos de señalización previstos por el sistema, incluyendo las sirenas externas.

Desplazándose más hacia abajo con la tecla  se llega a la página que muestra el estado del sistema.

INFO: Si es necesario desplazarse a través de varias páginas, mantenga pulsada la tecla  para moverse velozmente hacia abajo y llegar directamente a la última pantalla.



INFO: Verifique en la página web la versión del Firmware: <https://new.abb.com/low-voltage/products/building-automation/product-range/intrusion-alarm-systems/system/abb-secureathome>
Si es necesario, instale la versión actualizada.

11.4 Autenticación

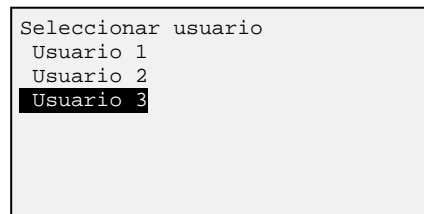
Para información general sobre la autenticación, remitirse al capítulo 2.4.




¡ATENCIÓN!

En el modo de trabajo, ningún usuario de nivel 3 podrá acceder al sistema a menos que esté autorizado por un usuario de nivel 2.







1. Presionar la tecla ok del teclado. Aparece la ventana con los usuarios de nivel 2 definidos en la instalación:







2. Seleccionar el usuario de la lista e ingresar el PIN. Las cifras introducidas aparecen como asteriscos (*).
3. Presionar la tecla **ok** para confirmar. Si el PIN introducido no es de 5 cifras, no se acepta la tecla **ok**. Si el usuario ingresa un PIN erróneo por décima vez se genera una alarma de sabotaje.
4. Si la autenticación se realizó con éxito, aparece el menú principal de usuario (descrita en el capítulo 2.3).
5. Seleccionando el icono  se entra, previo ingreso de un PIN válido, en la pantalla Instalador.



Acceso instalador (nivel 3)

Icono	Significado
	Zonas y sensores. Permite acceder al menú de programación de las zonas y de los sensores.
	Test del sistema. Permite acceder al menú de test del sistema.
	Dispositivos de sistema permite acceder al menú de programación de los dispositivos de sistema (mandos a distancia, teclados, sirenas, repetidores)
	Mantenimiento. Permite acceder al menú de mantenimiento del sistema (acceso permitido sólo a un usuario de nivel 4).
	Gestión de usuarios: permite gestionar los usuarios del sistema definiendo sus PIN, derechos y vínculos de acceso.
	Contactos: permite programar los números de teléfono y definir los eventos asociados a ellos.

	Acceso remoto: define los parámetros de conexión con la Home Automationf@h
	Activaciones. Permite acceder al menú de conexión y desconexión de todo el sistema de alarma o de zonas individuales.
	Estado y lista de eventos. Permite acceder al menú de visualización de los eventos memorizados por la central y del estado del sistema.
	Salir. Sale del menú principal y reconduce la central al estado de reposo.

11.5 Señalizaciones generales y de alarma

La central gestiona las situaciones de alarma o anomalía con las señalizaciones siguientes:

causa	LED o zumbador del dispositivo LED	Central			Sirena			Mensaje vocal (1)	SMS (1)
		Pantalla	Sonido	Sonido	Flash				
Prealarma	■		■				■	■	
Alarma de intrusión interna	■		■				■	■	
Alarma de intrusión externa	■		■	■	■		■	■	
Alarma sabotaje sistema con instalación activada externa			■	■	■		■	■	
Alarma sabotaje sistema con instalación desactivada			□				■	■	
Alarma de sabotaje sensor con instalación activada externa			■	■	■		□	□	
Alarma sabotaje sensor con instalación desactivada o activada interna/prealarma			■				□	□	
Alarma oscurecimiento		■	■	■			□	□	
Alarma pánico			■	■	□				
Alarma por robo							□	□	
Alarma socorro							□	□	
Alarma de incendio			□	□	□		□	□	
Alarma por fuga de gas			□	□	□		□	□	
Alarma por inundación			□	□	□		□	□	
Alarma tecnológico			□	□	□		□	□	
Ausencia GSM		■							
Ausencia de red 230 V		■					□	□	
Retorno de red 230 V		■					□	□	
Batería baja en los dispositivos							□	□	
Avería en el dispositivo							□	□	

causa	LED o zumbador del dispositivo LED	Central		Sirena			Mensaje vocal (1)	SMS (1)
		Pantalla	Sonido	Sonido	Flash			
Batería baja en la central	■	■					<input type="checkbox"/>	<input type="checkbox"/>
Asistencia técnica							<input type="checkbox"/>	<input type="checkbox"/>
Avería radio		■					<input type="checkbox"/>	<input type="checkbox"/>
Activación antirrobo interna		■	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activación antirrobo externa		■	■	■	■		<input type="checkbox"/>	<input type="checkbox"/>
Activación antirrobo prealarma		■	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Desactivación antirrobo		■	■	■	■		<input type="checkbox"/>	<input type="checkbox"/>

■ señalización habilitada de fábrica conforme con la norma EN 50131-1.

señalización opcional programable

(1) si está previsto en el dispositivo

12 PROGRAMACIÓN

En el primer encendido la secuencia guiada de pasos (Wizard), detallada en el manual Quick Guide de la Central, permite realizar la primera programación de la instalación.

Se puede ampliar o modificar esta primera configuración desde la pantalla del instalador:



Los iconos se describen en el párrafo *11.2.1 Autenticación*.

12.1 Creación de la instalación

La creación de la instalación consiste en la adquisición y programación de los diferentes dispositivos (detectores, repetidores, mandos a distancia y sirenas) y servicios (teléfonos) necesarios, en la creación y configuración de los usuarios y en la prueba final del sistema. Durante la sesión de trabajo se puede navegar hacia atrás entre los menús presionando la tecla **←**, sin tener que autenticarse para cada operación.



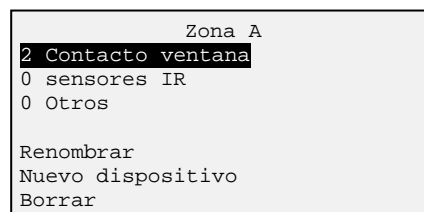
¡ATENCIÓN!

Si se sale inadvertidamente del menú principal, y se vuelve a la pantalla del sistema en reposo, habrá que autenticarse nuevamente.

12.2 Programación zonas y activadores

12.2.1 Para programar una nueva zona:

1. Entrar en la pantalla Instalador, autenticándose como usuario de nivel 3.
2. Seleccionar el icono de Zonas y sensores
3. Aparece la lista de las zonas ya creadas en la instalación y la zona tecnológica (siempre presente).
4. Seleccionar Nueva zona
5. Modificar la etiqueta predeterminada (opcional)



12.2.2 Para modificar o eliminar una zona:

Seleccionar la zona deseada.

Aparece la pantalla donde se pueden visualizar los sensores programados en la zona.

Seleccionar:

- Renombrar para modificar la etiqueta de la zona.
- Cancelar para eliminar la zona

12.2.3 Para programar un sensor:

- Repetir los puntos de 1 a -3 del párrafo 6.3.1
- Seleccionar Nuevo Dispositivo: la central permanece en espera, hacer aprender a la central el detector siguiendo las instrucciones que se adjuntan al dispositivo: el detector permanece en espera de los parámetros durante 5 minutos antes de entrar en modo "bajo consumo".

```
Nuevo dispositivo
Espera dispositivo...

Concluir setup
```

- Realizada la adquisición, aparece la pantalla siguiente:

```
Etiqueta:
[           ]
Dirección:
F831CB41
Tipo:
IR para exteriores
Señal:
-36 dbm
```

La lista de los parámetros se desarrolla en varias páginas. Para desplazarse entre las páginas, usar las teclas de flecha.

Los parámetros visualizados con carácter normal, no en negrita, son de sola lectura.

Éstos son:

- **Dirección:** dirección hexadecimal del detector.
- **Tipo:** denominación genérica del detector.
- **Señal:** nivel de la señal radio del detector, medido en dBm (decibeles mW).
- **Repetidor:** identificador del detector usado, si el detector se comunica con la central no directamente sino mediante un detector. "No configurado" significa que el detector se comunica directamente con la central.

Configurar los parámetros. La tabla del párrafo siguiente enumera todos los

parámetros para los detectores, su significado y los valores que pueden asumir.

Desplazarse con las flechas para seleccionar el valor deseado entre los disponibles.

- Presionar guardar o la tecla ok para guardar la configuración.
- Asociar el sensor a una zona.




¡ATENCIÓN!

Los sensores tecnológicos se asignan automáticamente a través del sistema a la zona tecnológica.

12.2.3.1 Parámetros para detectores


La tabla enumera los posibles parámetros comunes a los diferentes detectores. Los otros parámetros específicos de un tipo de detector se ilustran en el manual del detector.

Parámetro	Significado	Valores admisibles
Etiqueta	Sirve para identificar mejor el detector. Se aconseja usar un nombre descriptivo y unívoco, por ejemplo, COCINA, SALA, BAÑO, PATIO, etc.	Caracteres alfanuméricos, longitud máx 16 caracteres.
Excluir	Excluir el detector (la central ignora sus señalizaciones de alarma), manteniendo la configuración. Corresponde a la función de aislamiento como lo define la norma EN 50131-1.	SÍ, <u>NO</u>
Supervisión	Selecciona la frecuencia con la cual la central constata que el detector funciona.	NO, <u>15</u> , 45 (1)
Retardo (2)	Tiempo de retraso entre la activación del sistema de alarma y la activación de las alarmas cuando se sale de los espacios protegidos o tiempo de retardo entre la revelación de una intrusión y la señalización de alarma cuando se accede a un local protegido. Permite salir de los locales protegidos después de haber activado la alarma con el dispositivo de mando, sin hacer saltar la señalización o entrar en los locales protegidos y desactivar el sistema de alarma colocado en el interior de los mismos. El tiempo de retardo en entrada debería aplicarse solo a los detectores que cubren el recorrido entre el punto de ingreso (puerta, persiana garaje, etc.) y el dispositivo de mando. En caso de valores diferentes configurados en varios sensores, el tiempo de retraso aplicado en la salida es equivalente al mayor de estos valores en el interior de una única zona. En la entrada se aplica el tiempo configurado en el sensor que genera la alarma de intrusión. En presencia de uno o varios sensores retardados, tras la activación de la alarma, se muestra el icono  en la parte superior derecha de la pantalla, durante el tiempo de salida.	<u>NO</u> , 15, 30, 60, 90. Con No la señalización de la alarma es inmediata. (2)

Los valores subrayados son las configuraciones de fábrica.

(1) Frecuencias diferentes de 15 minutos no son conformes con la norma 50131-6 par. 4.5.1.

(2) Las programaciones con tiempo de retardo diferentes de 0 no son conformes con las normas EN 50131-1 y EN 50131-3.

(3) Las modificaciones posteriores aportadas en los parámetros fuera de este intervalo, se memorizan en la central y aplicados en el detector en su primera transmisión útil: esta situación se es notificada a través de un pequeño icono  arriba a la derecha de la pantalla.

12.3 Programación de dispositivos de sistema

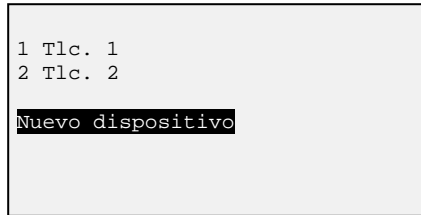
Desde este menú se pueden programar los mandos a distancia, sirenas y repetidores. Entrar en el menú de programación, autenticándose como usuario de nivel 3.

12.3.1 Programación de mandos a distancia

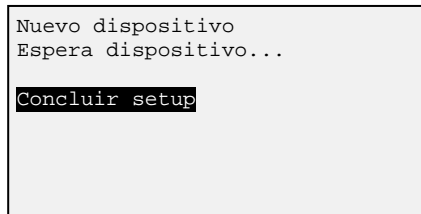


¡ATENCIÓN! La transmisión a la central por parte del control a distancia se produce en modalidad criptada y con un código variable que tiene un número de combinaciones posibles sobre la transmisión de un solo mando de 65536.

Seleccionar el icono "dispositivos de sistema" y, después, "mandos a distancia":



Seleccionar "Nuevo dispositivo" y pulsar OK



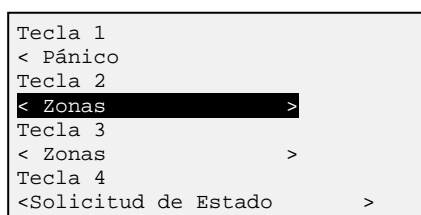
Hacer aprender a la central el mando a distancia siguiendo las instrucciones adjuntas al dispositivo. Ahora se puede programar la configuración del mando a distancia, que es distinta para las 2 tipologías.

12.3.1.1 Configuración de los mandos a distancia numéricos

Para este tipo de mando (códigos SAD-W2.1F y SAD-W2.11F) se puede configurar según se desee todas las 5 teclas.

Icono	Nombre	Configuración de fábrica	Personalizable
1	Tecla 1	Pánico	Tecla Sí / LED No
2	Tecla 2	Activación total externa	Tecla Sí / LED Sí
3	Tecla 3	Activación total interna	Tecla Sí / LED Sí
4	Tecla 4	Solicitud de Estado	Tecla Sí / LED Sí
5	Tecla 5	Desactivación total	Tecla Sí / LED Sí

Seleccionar el mando numérico de la lista y pulsar la tecla ok. Se abre la ventana que permite asociar una función a cada botón.



Posicionarse en la tecla, configurar la función deseada a través de las flechas <>. Las funciones posibles son:

Tipo de asociación	Significado
Zonas	El botón activa/desactiva una o varias zonas
Funcionalidad	Ejecuta una de las funciones enumeradas aquí abajo
N.A.	No configurado

No configurado	Funcionalidad	Acción
Seguridad	Robo	Ejecuta alarma silenciosa
	Pánico	Inicio alarma sonora
	Socorro	Activa el evento socorro
	Solicitud de estado	Activa el funcionamiento

Seleccionando **Zonas** aparece otra pantalla donde se podrá configurar la acción elegida. Usar las teclas flechas y el botón ok para guardar.

Cíclico se aplica a cualquier zona configurada con tipo "activación" en una cualquiera de las tres modalidades previstas. No se aplica cuando se elija como tipología la "desconexión". Para las funciones especiales no está prevista la modalidad cíclica.

Por defecto, los botones de los mandos a distancia solo activan el modo impreso en el propio botón o la función programada.

Con la opción del modo cíclico, el mando a distancia activa y desactiva cíclicamente su respectivo estado cada vez que se pulsa una tecla. El sistema de alarmas se puede activar pulsando un botón y se desactiva volviendo a pulsar el mismo botón.



¡ATENCIÓN!

El bloqueo en activación no está activo en caso de que se pulse el botón cíclico, que resulta, por lo tanto, no conforme con la norma EN 50131-1.

Zonas: Para cada zona se puede seleccionar la modalidad de activación, desactivación o Ninguna (no configurado).



Notación pantalla	Descripción
Externo	Activación Exterior
Interior	Activación Interior
Prealarma	Activación Prealarma
Desactivado	Desactivación
No configurado	Ninguna acción






Configurar los LED. Se pueden configurar los LED 2...5 para que aparezca visualmente el estado de una o varias zonas, mientras no es configurable el LED 1 (de servicio). El LED puede iluminarse de tres colores predefinidos diferentes y no configurables:

Color	Significado del led
Verde	Zona/s desactivada/s
Rojo	Zona/s activada/s
Ámbar	Bloqueo en activación (*)

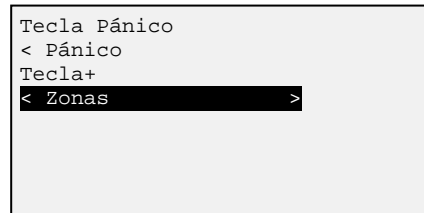
Cuando varias zonas hacen referencia al mismo LED, se aplica la siguiente regla: todas desactivadas de color verde, una o varias activadas de color rojo. Mediante la selección múltiple se pueden definir las zonas asociadas al led.

12.3.1.2 Configuración de los mandos a distancia preconfigurados



En este tipo de mandos a distancia (códigos SAD-W1.1F y SAD-W1.11F) están preconfiguradas todas las funciones. Se pueden personalizar solo las teclas  y .

Icono	Nombre	Configuración de fábrica	Personalizable
	Tecla Pánico	Pánico	Tecla Sí / LED No
	Tecla de Activación Externa	Activación total externa	Tecla No / LED No
	Tecla de Activación Interna	Activación total interna	Tecla No / LED No
	Tecla+	Solicitud Estado en caso de central independiente Tecla free@home en caso de central conectada a free@home	Tecla Sí / LED No
	Tecla Desactivación	Desactivación total	Tecla No / LED No

Para configurar las teclas personalizables, seleccionar el mando a distancia de la lista y pulsar el botón ok. Se abre la ventana que permite asociar una función.

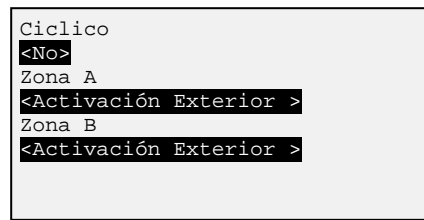


Posicionarse en la tecla a personalizar, configurar la función deseada a través de las flechas <>. Las funciones posibles son:

Tecla	Tipo de asociación	Significado
	Funcionalidad	Pánico / Socorro / Robo
	Zonas	El botón activa/desactiva una o varias zonas
	Solicitud de Estado	Ejecuta la solicitud de estado
	No asociado	

En negrita los valores predeterminados.

Seleccionando **Zonas** aparece otra pantalla donde se podrá configurar la acción elegida. Usar las teclas flechas y el botón ok para guardar.



Cíclico se aplica a cualquier zona configurada con tipo “activación” con cualquiera de las tres modalidades previstas. No se aplica cuando se elija la tipología la “desconexión”.

Zonas: Para cada zona se puede seleccionar la modalidad de activación, desactivación o Ninguna (no configurado).

Notación pantalla	Descripción
Externo	Activación Exterior
Interno	Activación Interior
Prealarma	Activación Prealarma
Desactivado	Desactivación
No configurado	Ninguna acción

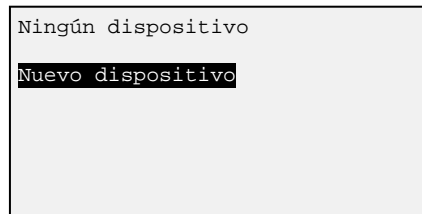
Los Led no son programables y asumen el significado siguiente:

Color	Significado del led
Led 2	Encendido rojo si la instalación activada es externa
Led 3	Encendido rojo si la instalación activada es interna
Led 4	Encendido Rojo si al menos una zona asociada al mismo está activada. Encendido Verde si todas las zonas asociadas al mismo están desactivadas. Apagado si se utiliza como mando free@home.
Led 5	Encendido verde con la instalación desconectada

12.4 Programación de las sirenas externas

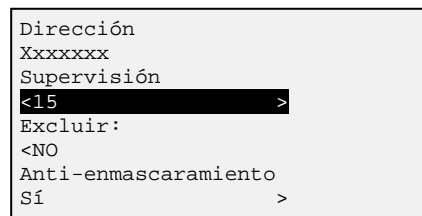
El sistema puede gestionar hasta 4 sirenas. Para programar las sirenas:

1. Entrar en el menú de programación, autenticándose como usuario de nivel 3.
2. Seleccionar el icono "dispositivos de sistema"
3. Ingresar 2 sirenas externas y aparece la siguiente pantalla:



4. Pulse OK. La central sigue en espera del servicio PIN: pulsar el Servicio PIN consultando el manual de la sirena.

12.4.1 Parámetros posibles



- **Supervisión.** Permite seleccionar la frecuencia con la cual la central constata que la sirena funciona. (No/15/45). El parámetro que se configura es el intervalo de tiempo entre un control y el siguiente.
- **Excluir: Sí/No.** Permite excluir la sirena externa
- **Anti-enmascaramiento: Sí/No.** Permite excluir la protección de anti-deslumbramiento (Jamming).
- **Tamper: Sí/No.** Si está configurado en Sí la Sirena suena si existen manipulaciones en la central (tamper o deslumbramiento), de lo contrario, se ignoran.
- **Alarma tecnológica: Sí/No.** Si es NO excluye los timbres en las alarmas tecnológicas también si están configurados los parámetros en el campo de alarmas - tipo Tecnológico.

12.4.2 Filtros zonas

Permite configurar los filtros personalizados por la sirena, es decir, la zona (o las zonas) de asignación de la sirena o definir las condiciones por las cuales suena, en caso de alarma. Las opciones son: Todas las zonas o un subconjunto de zonas.

12.4.3 Alarmas

Permite modificar, si se quiere, los parámetros de funcionamiento como el tipo de sonido, la duración, etc. de la sirena en los eventos de alarma.

```

REACCIONES Sirena
1      Alarmas (*)
2 Tecnológico

```

(*) Las alarmas comprende: **Alarma de intrusión externa, alarma de sabotaje de la zona, Pánico y Alarmas sabotajes de sistema** cuando el parámetro “sabotajes de sistema” esté configurado en Sí.

Se pueden configurar diferentes parámetros para las distintas alarmas. Para configurar los parámetros de un cierto tipo de alarma, desplazarse con las teclas de flecha al correspondiente para seleccionarlo y presionar la tecla OK para guardar.

Los parámetros que se pueden modificar en la ventana que se abre son:

Tipo alarma / evento	Timbre	Frecuencia	Duración	LED
Alarmas tipo 1	Sweep / Bitonal/ Ninguna	Arriba /Abajo	10 s/ 30 s / 3 m / 9 m **	SI / NO
Alarma 2 Tecnológica	Sweep/ Bitonal/ Ninguna	Arriba/Abajo	10 s/ 30 s / 3 m / 9 m **	SI / NO
Activación externa	1 bip largo / 3 bip breves / ninguno			1 parpadeo largo /3 breves / NO
Desactivación	1 bip largo / 3 bip breves / ninguno			1 parpadeo largo / 3 breves / NO

(**) Para garantizar la conformidad con las normas EN 501311 y EN 501313 el tiempo de activación de las sirenas debe ser mayor de 90 segundos y menor de 15 minutos (salvo reglamentaciones locales o nacionales diferentes).

En **negrita** están las configuraciones de fábrica. Para modificar un parámetro desplazarse al mismo con las teclas de flecha y presionar la tecla OK para confirmar la selección.



¡ATENCIÓN!

Los tipos de timbre Sweep baja frecuencia, bitonal alta frecuencia y Bitonal baja frecuencia no se ajustan a la norma EN 50131-1.

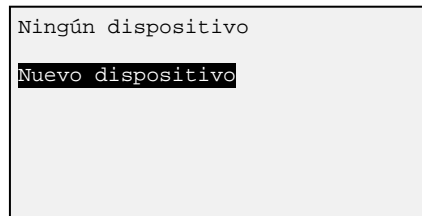
12.4.4 Eventos

Permite modificar, si se quiere, los parámetros de funcionamiento de la sirena para los eventos de activación y desactivación del sistema de alarma, con procedimiento similar a la de la anterior **Alarma**.

12.5 Programación de repetidor

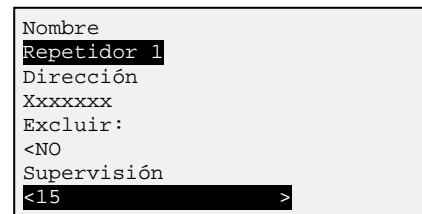
El sistema puede manejar hasta 4 repetidores. Para programar el repetidor:

1. Ingrese al menú de programación, autenticándose como usuario de nivel 3.
2. Seleccionar el icono "dispositivos de sistema"
3. Ingrese 3 para el repetidor, aparece la siguiente pantalla:



4. Pulse OK. La unidad de control está esperando el pasador de servicio: Presione el PIN de servicio y consulte el manual del repetidor.

12.5.1 Parámetros posibles



- **Nombre.** Permite establecer una etiqueta.
- **Excluir: Sí/No.** Permite excluir el repetidor
- **Supervisión.** Permite seleccionar la frecuencia con la que la unidad de control garantiza que las funciones de repetidor (no/15/45). El parámetro que se configura es el intervalo de tiempo entre un control y el siguiente.

12.6 Programación de los contactos telefónicos

Función disponible solamente para las versiones de central con GSM.

El sistema puede gestionar hasta 12 números telefónicos. Para programar un número de teléfono:

1. Autenticarse como Instalador y seleccionar Contactos.

```

Contactos
1 Contactos 1
2 Contactos 2
Nuevo contacto
Grabar mensaje
  
```

2. Seleccionar Agregar Contacto

```

Contacto
Nombre
<Contacto 3 >
Número
33612345678
  
```

3. Asignar un nombre al número de teléfono, para poderlo identificar más fácilmente. El nombre puede tener hasta una longitud de 16 caracteres alfanuméricos.
 - o Marcar con el teclado el número de teléfono. La longitud máx. es de 16 cifras.
 - o Pulsar la tecla Ok: aparece la siguiente pantalla

```

Interrumpible
<no
Mensaje audio
1 >
Eventos
Eliminar contacto
  
```

- Interrumpible: con configuración Sí significa que, en caso de respuesta a la llamada vocal, el siguiente número ya no es más llamado.
- Mensaje de audio: índice del mensaje personalizado a agregar al mensaje vocal predefinido.
- Eventos:
 - o Seleccionar eventos y para cada evento activar la elección deseada entre
 - Solo SMS
 - Solo llamada vocal
 - Llamada vocal+SMS
 - Ninguna (predeterminado salvo para los primeros 3 eventos)

```

Contacto
Nombre
<Contacto 3 >
Número
33612345678
  
```

Los eventos programables son:

Evento	Tipo envío	Filtro
Intrusión	VOZ / TEXTO	Zona alarma
Sabotaje	VOZ / TEXTO	Zona alarma
Sabotaje central	VOZ / TEXTO	
Robo	VOZ / TEXTO	
Socorro	VOZ / TEXTO	
Incendio	VOZ / TEXTO	Zona tecnológica
Gas	VOZ / TEXTO	Zona tecnológica
Inundación	VOZ / TEXTO	
Asistencia técnica(***)	VOZ / TEXTO	
Ausencia 230V (*)	VOZ / TEXTO	
Retorno de la red 230V	VOZ / TEXTO	
Tecnológico	VOZ / TEXTO	Zona tecnológica
Contacto ON	VOZ / TEXTO	Zona tecnológica
Verificación periódica GSM	VOC (**)	
Batería baja	VOZ / TEXTO	
Batería Central	VOZ / TEXTO	
Activación	VOZ / TEXTO	
Desactivación	VOZ / TEXTO	
Oscurecimiento	VOZ / TEXTO	
Avería hardware	VOZ / TEXTO	
Avería radio	VOZ / TEXTO	

VOZ indica un mensaje vocal, TEXTO un mensaje de texto.

(*) después de 15 min. de ausencia de red continua (retardo máximo previsto por la norma EN50131-1 y EN50131-3 equivalente a 60 min.)

(**) Se efectúa una vez al día (18:00 h). Este evento se debe habilitar en al menos uno de los números de teléfono programados. La falta de esta configuración conlleva la decadencia de la norma EN50136-1.

(***) El evento de Asistencia técnica se genera al producirse una anomalía de falta de supervisión por parte de un sensor/sirena/repetidor presente en la instalación.

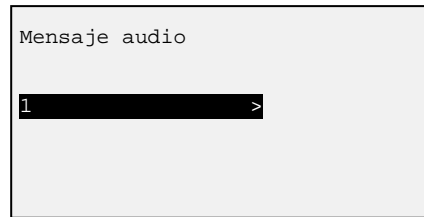


¡ATENCIÓN!

El tiempo de entrega del mensaje SMS está determinado por el funcionamiento de la red del operador telefónico y no existe certeza de su inmediato reenvío.

12.6.1 Mensaje personalizado

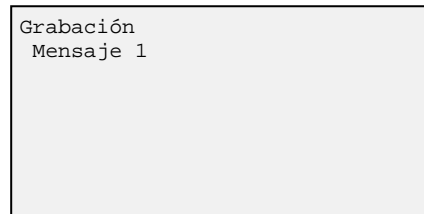
Seleccionar Grabar mensaje. Aparece la lista de mensajes. Se pueden grabar hasta 9 mensajes diferentes, cada uno de 14 segundos de duración.



El mensaje personal, si ha sido programado, es puesto en fila después del mensaje pregrabado específico que la central envía después de un evento.

El mensaje debe contener siempre la indicación de donde se ha verificado el evento señalado. Por ejemplo, un mensaje personalizado genérico podría ser "en la casa de Mario Rossi, via Roma 15, Milán".

Seleccionar el número correspondiente al mensaje que se quiere grabar. Se abre la ventana de grabación.



Presionar la tecla ok para iniciar la grabación. Después de aprox. 2 seg la barra deslizante indica el tiempo de grabación progresivo.

Presionar nuevamente la tecla ok para interrumpir la grabación.

Para verificar la calidad de la grabación provocar el envío del mensaje vocal desde el menú Prueba Sistema > Teléfonos.

12.6.2 Secuencia de envío de los mensajes telefónicos

Los mensajes de texto se reenvían inmediatamente a todos los números configurados.

Las llamadas vocales siguen estas reglas:

- Se llaman en secuencia los números programados como vocales.
- Si el número de teléfono está ocupado o no responde después de 4 timbres, la central corta la llamada y pasa al número de teléfono sucesivo de la secuencia.
- Terminado el primer ciclo de llamadas (todos los números de teléfono activos), la central trata de llamar los números que no han respondido. La central ejecuta 3 ciclos de llamada con los números que no han respondido, antes de interrumpir la secuencia de envío de mensajes.
- El mensaje vocal se repite 3 veces, antes de que la central cuelgue.

El mensaje enviado está compuesto por una parte pregrabada específica al evento que ha causado la llamada vocal y por una parte variable, que sigue la primera, que puede ser un mensaje grabado personalizado o, si falta, la indicación genérica "en instalación antirrobo".

12.6.3 Recepción de llamadas por parte de la central

Cuando uno se conecta telefónicamente a la central, los tonos son siempre aceptados, aún si el número del teléfono que llama no corresponde a uno de los 12 números en la lista.

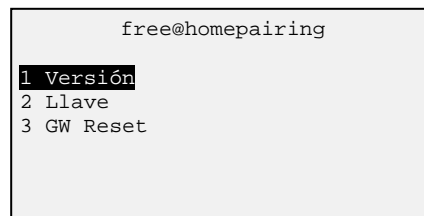
12.7 Home automationfree@home

Esta sección ilustra cómo verificar el estado y los parámetros del gatewayfree@Home. Para la configuración de free@home remitirse al manual específico de este sistema.

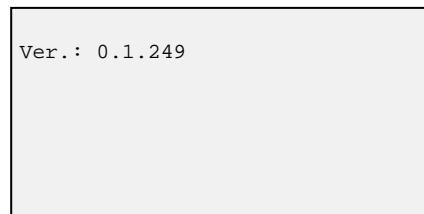
No disponible en el modelo SAS-W3.1E.

12.7.1 Versión

1. Para ver la versión
2. Entrar en el menú de programación, autenticándose como usuario de nivel 3.
3. Seleccionar el icono "free@homepairing"



4. Ingresar **1 Versión**: aparecen las informaciones relativas a la versión FW del soporte free@Home



12.7.2 Clave

Ejecutar los puntos de 1 a 2 del párrafo anterior e ingresar 2 Clave. Se abre una pantalla que visualiza 32 "digitos" que identifican de modo unívoco el gateway presente en la central. Estos códigos se envían, una vez, al sistema free@home, como se indica en el manual de programación free@home: pulsar OK para realizar la operación.

12.7.3 Reset GTW

Permite rearmar el gatewayfree@home. El procedimiento dura 1 minuto aproximadamente.

12.8 Test sistema

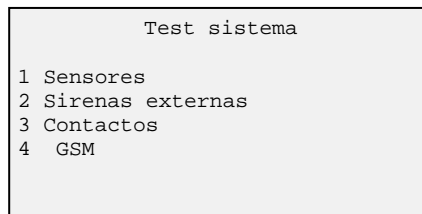
Todo el sistema debe ser probado al final de las operaciones de instalación y sucesivamente con regularidad, por lo menos una vez cada 6 meses, para constatar que todos sus dispositivos y sus funciones operan correctamente. Se puede probar también un solo subsistema, o solo algunos de los mismos, para constatar su funcionamiento. La prueba parcial es útil en caso de modificaciones limitadas del sistema que interesan solo su dispositivo o una de sus funciones.

La inactividad permitida para la función prueba del sistema es de 10 minutos, transcurridos los cuales el sistema vuelve al funcionamiento normal. Toda vez que se realiza una prueba, por ejemplo, se verifica un detector que envía una señal de verificación a la central, la cuenta regresiva reinicia a partir de 10 minutos.

La prueba del sistema se realiza con un nivel de recepción atenuado de 6 dB tal como prescribe la norma EN 50131-5-3.

Para probar el sistema de alarma:

1. Autenticarse y desplazarse en la pantalla de Test Sistema.
2. Pulsar OK

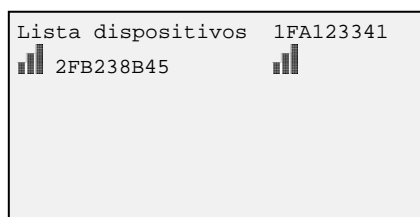


Seleccionar el subsistema que se quiere probar, marcando el número correspondiente. Si el subsistema no contiene dispositivos la elección es ignorada.

3. Según el subsistema escogido, se abrirán nuevas ventanas y podrá ser necesario realizar las acciones para activar los dispositivos interesados.

Detectores

Después de haber escogido 1 Sensores como subsistema, seleccionar la zona y excitar los diferentes detectores de modo oportuno, por ejemplo, pasando por delante de los detectores IR, abriendo y cerrando puertas y ventanas para los contactos magnéticos, vertiendo agua para los detectores de inundación, etc.



Para cada zona se enumeran todos los detectores posibles y una vez realizada la recepción, la capacidad de la señal mediante 1, 2, 3 muescas como se observa en la figura.

Evidenciando con las teclas de flecha la posición del detector y presionando la tecla ok se abre una nueva ventana de detalle que contiene para fines de diagnóstico:

- Dirección hexadecimal del detector.
- Nivel de la señal.
- Tipo de detector.
- Estado del detector. Las abreviaturas visualizadas significan:
 - M.AL memoria de alarma
 - ON contacto abierto del detector
 - OFF contacto cerrado del detector
 - TAM. sabotaje antiapertura
 - DES. sabotaje anti-desmontaje
 - BAT. batería descargada
 - FAL. avería genérica
 - SUPE anomalía de supervisión
 - EXCL detector excluido (corresponde a "detector aislado" como definido por la norma EN 50131)
- Fecha y hora de recepción.

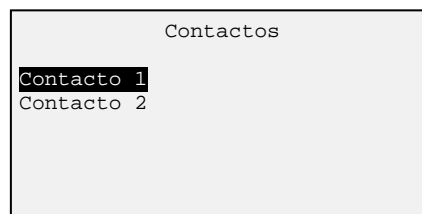
Sirenas exteriores

Después de haber escogido 4 Sirenas como subsistema, seleccionar de la lista el dispositivo que interesa y presionar la tecla ok.

En la nueva ventana en la fila Test: seleccionar el tipo de timbre deseada y pulsar OK: La sirena seleccionada suena en el modo seleccionado, con volumen intermedio, por 10 segundos y sus LED parpadean.

Contactos

Después de haber escogido Contactos aparece la lista de todos los números de teléfono disponibles. Los números configurados están evidenciados con el símbolo ►.



Seleccionar el número de teléfono que interesa y presionar la tecla ok.

Seleccionar el tipo de test deseado (llamada vocal o mensaje de TEXTO) y pulsar OK.

GSM

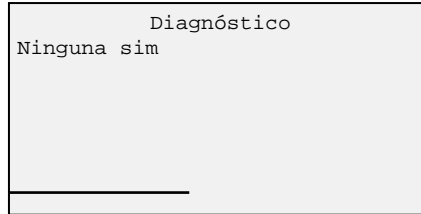
Una vez seleccionado 4 GSM como subsistema, inicia el Diagnóstico y en la parte inferior aparece una barra de desplazamiento para indicar el tiempo de la



verificación, como se muestra en la siguiente figura.

Al finalizar, si no se detecta ningún problema, aparece el mensaje "Ok"; de lo contrario, durante el diagnóstico se mostrarán en la ventana el o los errores identificados.

Ejemplo:

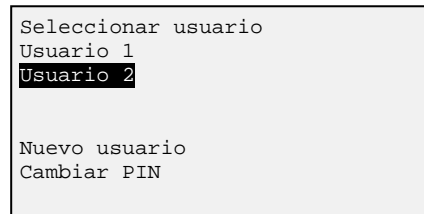


La lista de errores GSM está descrita detalladamente en la tabla “errores GSM”, en la sección 14: “Resolución de problemas”.

12.9 Gestión de usuarios

Esta función puede ser ejecutada por un usuario de nivel 3. Se pueden crear nuevos usuarios, modificar el propio PIN o borrar usuarios existentes. Para mayores informaciones sobre los criterios de autenticación de los usuarios y sus privilegios asociados, véanse los párrafos Primer encendido y Niveles de autorización.

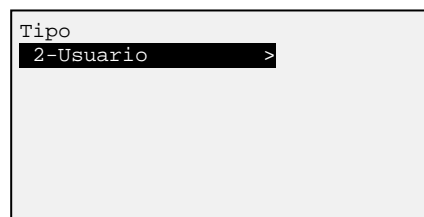
Abriendo el menú aparece la lista de los usuarios creados:



Esta función puede ser ejecutada por un usuario de nivel 3. Se pueden crear nuevos usuarios, modificar el propio PIN o borrar usuarios existentes. Para mayores informaciones sobre los criterios de autenticación de los usuarios y sus privilegios asociados, véanse los párrafos Primer encendido y Niveles de autorización.

Abriendo el menú aparece la lista de los usuarios creados.

Para crear un nuevo usuario seleccionar nuevo usuario, pulsar OK y en la ventana siguiente elegir el nivel (2-usuario / 3-Instalador / 4 - Encargado del mantenimiento) y pulsar OK.



- Etiqueta: Asignar un nombre significativo al usuario (por ejemplo, nombre, apellido o ambos), para poderlo identificar más fácilmente. El nombre puede tener hasta una longitud de 16 caracteres alfanuméricos. Los caracteres se agregarán usando el teclado. Para borrar un carácter erróneo, desplazar el cursor con las flechas sobre el carácter e introducir el carácter correcto o el espacio para cancelarlo.
- PIN: introducir una contraseña a elección de 5 cifras.
- Repetir el PIN marcado para una verificación de consistencia
- Zonas: son las zonas donde puede operar el usuario que se está creando. Como condición predefinida el nuevo usuario puede operar en todas las zonas. Desplazarse con las teclas flechas en las zonas interesadas y agregarlas.

Presionar la tecla ok para guardar el nuevo usuario.

12.9.1 Modificación de un usuario

Para modificar un usuario:

- Autenticarse e Ingresar Gestión de usuarios.
- Seleccionar el usuario y en la ventana siguiente, modificar el perfil, es decir, las zonas asociadas en las que puede funcionar.
- Confirmar con OK.

12.9.2 Cancelación de un usuario

Para cancelar un usuario:

- Autenticarse e Ingresar Gestión de usuarios.
- Seleccionar el usuario y en la ventana siguiente seleccionar Eliminar PIN.
- Confirmar con OK.

Se muestra el identificador del PIN (en las figuras de ejemplo el número 2) y solicita la confirmación de la cancelación. Seleccionar con las teclas de flecha si confirmar la cancelación (SÍ) o si anularla (NO). La opción escogida se refleja en negativo. Presionar la tecla ok para confirmar la elección.

13 MANTENIMIENTO

13.1 Gestión de la alimentación

13.1.1 Batería

La central mide constantemente la tensión de la batería.

Cuando la tensión es menor de:

- 6,9 Vcc. la central realiza la recarga;
- 5,5 Vcc. la central señala el evento de “Batería descargada” y apaga todas las alimentaciones. El calendario RTC sigue actualizándose. Al volver la tensión de red la central reinicia el sistema;
- 1,5 Vcc la central señala el evento de “Batería averiada” y enciende el LED relativo a la batería.

13.1.2 Red eléctrica

En caso de ausencia de alimentación de red (230 Vca):

- Se apaga inmediatamente la retroiluminación de la pantalla de la central (la pantalla se vuelve a encender si se marca en el teclado).
- Se desactiva el gateway Home Automation (parada inteligente después de haber controlado que todos los nodos estén sin alimentación).
- La gestión del módulo GSM sigue la evolución de la carga de la batería.
- Después de 15 minutos continuativos de falta de tensión, la central señala el evento de ausencia de red.
- El terminal USB permanece siempre activo.

Al volver la tensión de red el módulo GSM reanuda su funcionamiento.

Después de 15 minutos continuativos de retorno de la tensión de red, la central señala el evento de retorno de red.

13.2 Puesta en estado de mantenimiento

Para poner en estado de mantenimiento el sistema, activar la función Test sistema. Para salir del estado de mantenimiento, salir del menú.

13.2.1 Sustitución de la batería de la central

Para sustituir la batería de la central:

1. Poner en estado de mantenimiento el sistema.
2. Desenganchar la central del bastidor de soporte y fijarla en posición de mantenimiento.
3. Abrir el compartimento de la batería y sacar la batería usada.
4. Introducir la nueva batería y volver a cerrar el compartimento de la batería.
5. Desenganchar la central de la posición de mantenimiento y fijarla nuevamente al bastidor de soporte.
6. Salir del estado de mantenimiento del sistema.



¡ATENCIÓN! La batería usada debe sustituirse con una idéntica con clase de inflamabilidad UL94HB o mejor.



¡Advertencia! Únicamente puede ser instalado por un electricista cualificado.

13.2.2 Sustitución de la tarjeta SIM

Para sustituir la tarjeta SIM, poner en estado de mantenimiento el sistema y consultar la hoja de instalación presente en la caja de la central.

13.2.3 Sustitución de la batería de los detectores

Para reemplazar la batería de un detector:

1. Poner el sistema en estado de mantenimiento.
2. Abra el detector, sustituya la pila vieja y ciérrela de nuevo según las instrucciones del manual del sensor.
3. Realice una prueba del sistema en el detector para verificar su funcionamiento correcto.

13.2.4 Sustitución de la pila del mando a distancia

Para cambiar la pila de un mando a distancia

1. Abra el mando a distancia, sustituya la pila y ciérrela de nuevo según las instrucciones del manual del aparato.
2. Entre en el menú System Test y pulse cualquier tecla del mando a distancia.
3. Salga por la ventana de descanso y compruebe que el dispositivo funciona correctamente.

13.2.5 Sustitución de la batería de la sirena

1. Entre en el menú System Test (Prueba del sistema) y realice el procedimiento de prueba de la sirena como se describe en la sección dedicada.
2. A partir de ahora, tiene 5 minutos para abrir la sirena sin que suene alterada.
3. Abra la sirena de acuerdo con las instrucciones del manual, sustituya la batería vieja y ciérrela de nuevo.
4. A continuación, vuelva a realizar una prueba de sirena para comprobar que funciona correctamente.

13.2.6 Reset de la central

Para llevar la central a los valores de fábrica, cancelando las programaciones y configuraciones efectuadas:

1. Autenticarse como usuario de nivel 2 y entrar en la pantalla Instalador autenticándose como nivel 3: seleccionar el icono de Mantenimiento.
2. Autenticarse con el nivel 4. Si no está presente, la central solicita la creación de un usuario de nivel 4.
3. En la nueva pantalla marcar 2 Reset valores de fábrica.

Después del restablecimiento de fábrica, la unidad de control genera una nueva clave de cifrado.



¡ATENCIÓN!

La operación de reset de la central no puede anularse y implica una nueva y completa configuración del sistema.

13.2.7 Eliminación del historial de eventos

Para eliminar el historial de eventos:

1. Llevar a cabo los puntos 1 y 2 del apartado anterior
2. En la nueva pantalla, introducir 6 Eventos y, a continuación, confirmar.

La central elimina todos los eventos (críticos y secundarios) de su memoria.



¡CUIDADO!

La eliminación de los eventos no es conforme con la norma EN 50131-1

13.2.8 Conexión

Este menú permite activar una sesión de mantenimiento del sistema a través del SW Secure@Home Manager. Antes de llevar a cabo cualquier procedimiento proporcionado por el paquete SW (Backup, Clona, Reset Pin), active la conexión a través del menú mencionado previamente: en la pantalla aparece un mensaje de tipo «SW conexión habilitada»; a continuación, conecte el cable USB y proceda siguiendo la información incluida en el manual del SW Secure@Home.

13.2.9 Agregado de dispositivos

Para añadir nuevos dispositivos después de la puesta en funcionamiento del sistema, seguir las instrucciones para la programación de los diferentes dispositivos contenidos en el capítulo Programación.

13.2.10 Cancelación de dispositivos

Para cancelar un dispositivo que ya no es necesario:

1. Autenticarse como usuario de nivel 2 y entrar en la pantalla Instalador autenticándose como nivel 3: seleccionar Programación.
2. Seleccionar la zona y el tipo de dispositivo que se quiere quitar y pulsar el botón ok.
3. Se abre la ventana de detalle que permite asegurarse que el dispositivo seleccionado sea el deseado.
4. Si el dispositivo seleccionado es aquel deseado, desplazarse a través de todos los parámetros y al final de la lista seleccionar "Quitar" y pulsar OK para cancelarlo.
5. La central pide confirmar su extracción. Seleccionar Sí para sacar el dispositivo, NO para no eliminarlo, y confirmar la elección con la tecla ok.
6. Presionar la tecla ESC para salir del menú.

13.2.11 Sustitución de dispositivos

Para sustituir un dispositivo primero eliminar del sistema el dispositivo antiguo y después agregarlo nuevamente.



¡ATENCIÓN!

La cancelación del dispositivo implica la pérdida de todos los parámetros de configuración. Antes de cancelar definitivamente el dispositivo anotarse los valores de sus parámetros, enumerados en la ventana de detalle.

Posteriormente, cuando se añade el nuevo dispositivo, usar para la programación de los parámetros los mismos valores anteriormente anotados.

13.2.12 Actualización del firmware de la central

Se recomienda actualizar primero el gateway via free@home y, después, el firmware de la central Secure@Home. Para la actualización mediante free@home, consulte el manual específico de este sistema.

Para actualizar el firmware de la central:

1. Descargue el firmware desde <https://new.abb.com/low-voltage/products/building-automation/product-range/intrusion-alarm-systems/system/abb-secureathome>
2. Haga doble clic en *SAS_Wx_FW_ABB-secure@home_VXXX.cab* para extraer el *FILENAME.uc3*
3. Guarde el *FILENAME.uc3* en una llave USB



¡ATENCIÓN!

El dispositivo USB debe ser formateado FAT 32.

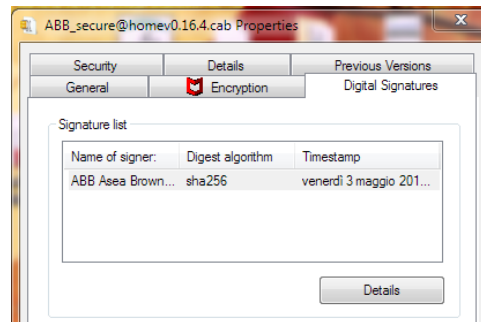
El *FILENAME.uc3* debe ser el único archivo en la llave USB

4. Autenticarse como usuario de nivel 2 y entrar en la pantalla Instalador autenticándose como nivel 3: seleccionar el icono de Mantenimiento.
5. Autenticarse con el nivel 4. Si no está presente, la central solicita la creación de un usuario de nivel 4.
6. En la nueva pantalla marcar 1 Actualizar FW desde USB.
7. Desenganchar la central del bastidor de soporte.
8. Introducir el dispositivo USB con el nuevo firmware en la puerta USB en la parte posterior de la central y presionar la tecla ok.
9. La central carga el nuevo firmware y al final muestra un mensaje que incluye el éxito de la operación.
10. Sacar el dispositivo USB y fijar nuevamente la central al bastidor de soporte.
11. Salir del estado de mantenimiento del sistema.

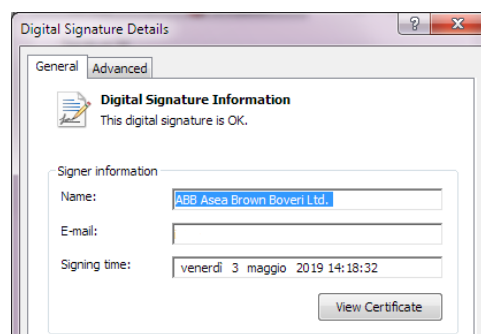
El archivo de actualización proviene de ABB con una firma digital. Las firmas digitales aseguran que el firmware proviene de ABB y protegen el firmware contra alteraciones después de la publicación.

Para verificar que la firma es válida, siga estos pasos:









1. Haga clic con el botón derecho del ratón en el archivo .cab recibido.
2. Seleccione Propiedades y haga clic en la pestaña Firmas digitales.





3. Se abre una nueva ventana, como la siguiente. En la línea superior se puede observar que el certificado es válido.



14 RESOLUCIÓN DE PROBLEMAS

Problema	Causa	Solución
Icono  (1)	Falta la tarjeta SIM.	Introducir una SIM Card activa, sin PIN.
	La tarjeta SIM está colocada pero no hace contacto.	Introducir correctamente la tarjeta SIM, después de haber limpiado sus contactos.
	Se ha agotado el crédito de la tarjeta SIM.	Recargar la tarjeta SIM, si es del tipo a recarga.
	Red GSM no detectada.	Verificar que exista cobertura por parte de la señal de la red telefónica.
	SIM Card caducada o desactivada	Contactar con el operador de telefonía y reactivar la SIM
	SIM no válida	El tipo de SIM no es compatible, por ejemplo USIM
Icono  Intermitente (1)	La SIM introducida tiene activado el PIN	Retirar la SIM de la central, introducirla en un teléfono móvil y desactivar el PIN.
Icono  (1)	Diagnóstico GSM en curso.	Se apaga automáticamente al finalizar el proceso. En caso de que permanezca fija, consultar en la lista del historial secundario el tipo de «GSM Fault» registrado y resolver el problema.
Icono de la batería intermitente	La batería no está conectada.	Conectar la batería o controlar su conexión.
Icono  (2)	Falta alimentación de red	Controlar la alimentación de red.
LED  encendido (3)	La batería está defectuosa o no está conectada.	Sustituir o conectar la batería
LED  encendido	Interferencia en los canales de radio	Verificar si algún dispositivo electrónico o fuente de interferencia electromagnética está impidiendo la radiocomunicación entre central y dispositivos.
LED  encendido (3)	Existen señalizaciones de alarma aún no vistas.	Ver las señalizaciones.
LED  encendido (4)	Existen notificaciones obligatorias aún no vistas.	Visualizar las notificaciones. Si el problema está resuelto, el led se apaga una vez revisado por parte de un usuario autenticado.
No me recuerdo el PIN		En caso de que no se pueda volver a acceder, utilizar el procedimiento «reset PIN» incluido en el «software Secure@Home Manager», que se puede descargar desde la página web de ABB.
Cuando se activa el sistema es necesario ejecutar Forzar bloqueo.	Existen puertas o ventanas abiertas	Controlar el cierre de puertas y ventanas
	La carga de las baterías de los sensores, de las sirenas o del mando a distancia se está agotando.	Sustituir las baterías gastadas.
	Han sido manipuladas.	Controlar si se han producido alteraciones y, si fuese posible, solucionarlas

Problema	Causa	Solución
	Ha habido alarmas de intrusión	Acceder al estado de la instalación y «resetear» la memoria de alarmas en el/los sensor/es afectado/s.
	Hay eventos (led  encendido) que todavía no se han visualizado	Resolver el problema, acceder al estado de la instalación y visualizar la anomalía: el led  se apaga automáticamente
	La red telefónica no funciona correctamente.	Controlar que exista crédito residual en la tarjeta SIM y que haya señal de red telefónica

(1) Para todas las anomalías asociadas al GSM, es posible conocer los detalles del problema consultando la lista de los eventos secundarios. Las anomalías están resumidas en la siguiente tabla

(2) Se enciende tras una interrupción de la red de al menos 10 segundos

(3) Visible solo con la autenticación (usuario de nivel 2) realizada

(4) Visible solo con la instalación desactivada

Como se indica en la nota (1), se pueden conocer en detalle algunas anomalías o situaciones relativas al GSM, consultando el historial de eventos secundarios. Al abrir la lista de eventos secundarios, las anomalías relativas al GSM se representan en una pantalla del siguiente tipo.

Evento	[n/t]
Fecha	Hora
GSM Fault	
Tipo de anomalía	
Estado GSM	
<Recientes	Pasados>

La siguiente tabla resume los posibles tipos de error GSM:

#	Tipo Anomalía	Estado GSM	Descripción	Notas
1	SMS	Spam Clean	La central ha reconocido mensajes entrantes inapropiados y los está eliminando.	La operación puede requerir algunos minutos.
2	No Sim	GSM OFF	SIM Card no introducida o introducida de manera incorrecta	
3	-105		Campo (en dBm) del GSM insuficiente	
4	Power supply fault	GSM OFF	Falta EPS (alimentación principal): el módem pasa al estado de bajo consumo. Se reactiva solo en caso de necesidad (llamadas vocales y/o envío de SMS salientes)	
5	CREG 3	GSM OFF	Registro de la SIM no permitido	La SIM Card podría estar caducada
6	CREG 0	GSM OFF	Registro SIM fallido	A los 10 intentos se registra este estado
7	SIM PIN	GSM OFF	La SIM tiene activado el PIN	
8	MINFO	GSM RST	Error en la detección de la velocidad del módem	

15 CARACTERÍSTICAS TÉCNICAS DE LA CENTRAL

MODELO	Central Busch-/ABB-secure@home	
TIPOS DE PRODUCTO	SAS-W1.1E, SAS-W2.1E, SAS-W1.1F, SAS-W2.1F, SAS-W1.11E, SAS-W2.11E, SAS-W1.11F, SAS-W2.11F, SAS-W3.1E	
CAMPO DE APLICACIÓN	Seguridad, anti-intrusión y Home Automation	
NIVEL DE PRESTACIÓN	Grado de seguridad	2 - Modelos con GSM 1 - Modelos sin GSM
	Clase ambiental	I
	Prescripciones de notificación	Opción B
TECNOLOGÍA DE COMUNICACIÓN	Entre los dispositivos de radio	Transmisión bidireccional en FM 868,3 MHz Alcance 300 m en campo libre
	Red telefónica <i>(solo algunos modelos)</i>	Módulo GSM Dual band (900 MHz / 1800 MHz) Potencia máx. de transmisión 2 W Antena interna
	Con dispositivos de cable	Interfaz RS485, placa de bornes de 3 cables
	Home Automation	ABB-free@home en bus de 2 cables
	Con ordenador	Puerto USB tipo A Puerto USB tipo B
	AlarmTransmissionSystem (ATS)	Categoría SP2 (EN50136-2) ack: pass-through
CARACTERÍSTICAS ELÉCTRICAS	Alimentación	230 Vca ± 10%, frecuencia 50/60 Hz Alimentador tipo A
	Corriente	Stand-by: 45 mA – En condiciones de alarma: 85 mA
	Batería tampón	Recargable NiMh, 6 V, 1600 mAh Garantiza el respeto de la norma EN 50131-1 apar. 9
	Prueba de cables para evitar la propagación vertical de la llama	Conforme con los estándares IEC 60332-1-2 para los cables de sección 0,5 mm ² o superior y IEC 60332-2-2 de sección inferior a 0,5 mm ² .
CARACTERÍSTICAS FÍSICAS	Grado de protección	IP20
	Dimensiones (L x H x P)	272 x 187 x 48 mm
	Peso	0,85 kg
CONDICIONES DE EMPLEO	Clase ambiental	I (interna)
	Temperatura de uso	-5...+45 °C (*)
	Humedad relativa	Media 75% no condensante, pico 90%
	Instalación	De pared
FUNCIONALIDADES ESPECÍFICAS	CPU	Microprocesador con 64 kB RAM y 128 kB memoria flash
	Display gráfico	LCD retroiluminado 128 x 64 pixel
	Teclado	Capacitiva con 17 teclas o teclado de 20 teclas en el modelo SAS-W3.1E
	Indicador acústico	Sirena piezoeléctrica para interior autoalimentada Potencia 85 dB a 1 m
	Protección	Tamperantisabotaje y a prueba de extracciones

(*) Testado en el intervalo +5...+40 °C para los requisitos de la clase ambiental I según la norma 50130

16 CYBER SECURITY DISCLAIMER

Este producto está diseñado para conectarse y comunicar información y datos a través de una red Interfaz. Es responsabilidad exclusiva del cliente proporcionar y asegurar continuamente una conexión segura entre el la red de productos y clientes o cualquier otra red (según sea el caso). El cliente deberá establecer y mantener las medidas apropiadas (tales como, pero no limitándose a la instalación de cortafuegos, aplicación de medidas de autenticación, encriptación de datos, instalación de programas antivirus, etc) para proteger el producto, la red, su sistema y la interfaz contra cualquier tipo de seguridad infracciones, acceso no autorizado, interferencia, intrusión, fuga y/o robo de datos o información. ABB y sus afiliados no son responsables por daños y/o pérdidas relacionadas con tales infracciones de seguridad, cualquier acceso no autorizado, interferencia, intrusión, fuga y/o robo de datos o información.

16.1 Network Manager

Los productos de Network Manager están diseñados para conectarse y comunicar información y datos a través de una interfaz de red, que debe conectarse a una red segura. Es su única responsabilidad proporcionar y asegurar continuamente una conexión segura entre el producto y su red o cualquier otra red (según sea el caso) y establecer y mantener medidas apropiadas (como, por ejemplo, se limita a la instalación de firewalls, la aplicación de medidas de autenticación, el cifrado de datos, instalación de programas antivirus, etc.) para proteger el producto Network Manager, la red, su sistema e interfaces contra todo tipo de infracciones de seguridad, acceso no autorizado, interferencia, intrusión, fugas y/o robo de datos o información. ABB y sus filiales no son responsables de daños y/o pérdidas relacionados con tales infracciones de seguridad, acceso no autorizado, interferencia, intrusión, fugas y/o robo de datos o información. Aunque ABB proporciona pruebas de funcionalidad en los productos y actualizaciones que publicamos, su propio programa de pruebas para cualquier actualización del producto u otras actualizaciones importantes del sistema (para incluir cambios de código, cambios de archivos de configuración, actualizaciones de software de terceros o parches, cambio de hardware, etc.) garantizar que las medidas de seguridad que ha implementado no hayan se ha comprometido y la funcionalidad del sistema en su entorno es como se esperaba.