SPC4xxx/5xxx/6xxx 3.8.5

Manual de instalación y configuración

ID del documento: A6V10276959-c

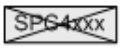
Fecha de edición: 31.08.2017

Datos y diseño sujetos a cambios sin previo aviso. / Oferta sujeta a disponibilidad.

Contenido

1 Significado de los símbolos

Este documento incluye diversos símbolos:

Símbolo	Descripción
	No disponible para SPC42xx, SPC43xx.
	Solo disponible para el controlador SPC con interfaz IP (SPC43xx/SPC53xx/SPC63xx).
	No disponible para instalación de tipo doméstico.
	Sólo disponible en modo libre.
	Encuentre más información sobre el grado de seguridad, la región o el modo en el texto.
	Consulte el Apéndice para obtener más información.

2 Seguridad

Este capítulo abarca:

2.1 Grupo objetivo

Las instrucciones de este documento están destinadas al siguiente grupo objetivo:

A quién va destinado este documento	Formación	Actividad	Condición del equipo
Personal de instalación	Formación técnica para instalaciones eléctricas o en edificios.	Montaje e instalación de todos los componentes de hardware in situ.	Componentes individuales que deben ser montados e instalados.
Personal de puesta en funcionamiento	Con formación técnica apropiada en relación con las tareas, productos, dispositivos o sistemas que se deben poner en servicio.	Poner en servicio el dispositivo o sistema ya completamente montado e instalado en su sitio.	Dispositivo nuevo, completamente montado e instalado, o modificado.

2.2 Instrucciones generales de seguridad

ADVERTENCIA: Antes de instalar y usar este dispositivo, lea las Instrucciones de seguridad. Este dispositivo únicamente se conectará a fuentes de alimentación que cumplan la norma EN60950-1, capítulo 2.5 («Fuente de alimentación limitada»).

2.2.1 Información general

- Conserve este documento para posteriores consultas.
- Este documento siempre debe acompañar al producto.
- Tenga en cuenta también todas las normas o regulaciones de seguridad específicas de su país en materia de planificación de proyectos, funcionamiento y descarte del producto.

Declaración de responsabilidad

- No conecte el dispositivo a la red de alimentación de 230 V si está dañado o le faltan piezas.
- No realice cambios ni modificaciones en el dispositivo a no ser que se mencionen expresamente en este manual y hayan sido aprobados por el fabricante.
- Utilice únicamente piezas de recambio y accesorios autorizados por el fabricante.

2.2.2 Transporte

Daños a la unidad durante el transporte

- Guarde el material de embalaje para futuros transportes.
- No exponga el dispositivo a vibraciones mecánicas o golpes.

2.2.3 Configuración

Interferencias de radio con otros dispositivos en el entorno/EMS

- Al manipular módulos susceptibles a las descargas electrostáticas, observe las directivas sobre descarga electrostática (ESD).

Daños producidos por una ubicación de montaje inadecuada

- Se deben respetar las condiciones ambientales recomendadas por el fabricante. Consulte *Datos técnicos* en la página 35.
- No utilice el dispositivo cerca de fuentes de radiación electromagnética potentes.

Peligro de descarga eléctrica por una conexión incorrecta

- Conecte el dispositivo sólo a fuentes de alimentación con el voltaje especificado. En la etiqueta de características del dispositivo pueden leerse los requisitos sobre el suministro de voltaje.
- Asegúrese de que el dispositivo tenga una conexión fija al suministro eléctrico y que haya un dispositivo de desconexión accesible.
- Asegúrese de que el circuito al cual está conectado el dispositivo esté protegido por un fusible de 16 A (máx.). No conecte a este fusible ningún dispositivo ajeno a la instalación.
- Este dispositivo está diseñado para trabajar con sistemas de alimentación TN. No conecte el dispositivo a otros sistemas de alimentación.
- Ponga a tierra el dispositivo según las normas y prescripciones locales vigentes.
- Tienda las líneas de alimentación primaria y secundaria en la carcasa de manera que no queden paralelas o cruzadas y tampoco en contacto.
- Conduzca la línea telefónica separada de otras líneas al dispositivo.

Riesgo de daños en los cables por tensión mecánica

- Asegúrese de contar con un alivio de tracción suficiente en todas las líneas y cables que salgan del dispositivo.

2.2.4 Funcionamiento

Situación de peligro debida a una falsa alarma

- Asegúrese de comunicar a todos los responsables que proporcionan asistencia antes de probar el sistema.
- Para evitar situaciones de pánico, informe siempre a todos los presentes antes de probar los dispositivos de alarma.

2.2.5 Servicio técnico y mantenimiento

Peligro de descarga eléctrica durante el mantenimiento

- El trabajo de mantenimiento debe ser realizado únicamente por personal especializado.
- Antes de proceder a realizar trabajos de mantenimiento, desenchufe el cable de alimentación, así como cualquier otro cable, de la red eléctrica.

Peligro de descarga eléctrica al limpiar el dispositivo

- No utilice limpiadores líquidos ni aerosoles que contengan alcohol ni amoniaco.

2.3 Significado de los avisos escritos

Aviso escrito	Tipo de riesgo
PELIGRO	Peligro de muerte o de graves daños personales.
ADVERTENCIA	Posible peligro de muerte o de graves daños personales.
Precaución	Peligro de daños personales menores o de daños materiales.
IMPORTANTE	Peligro de fallos en el funcionamiento

2.4 Significado de los símbolos de peligro

ADVERTENCIA: Advertencia de área de peligro

ADVERTENCIA: Advertencia de voltaje eléctrico peligroso

3 Directivas y normas

Este capítulo abarca:

3.1 Directivas de la UE

Este producto cumple los requisitos de las directivas europeas 2004/108/CE «Directiva de compatibilidad electromagnética», 2006/95/CE «Directiva de baja tensión» y 1999/5/CE sobre Equipos terminales de telecomunicaciones y equipos radioeléctricos (R&TTE). La declaración de conformidad de la UE está disponible para las agencias responsables en: http://pcd.vanderbiltindustries.com/doc/SPC

Directiva europea 2004/108/CE «Compatibilidad electromagnética»

La conformidad con la directiva europea 2004/108/CE ha sido probada según los estándares siguientes:

emisión electromagnética	EN 55022 Clase B
inmunidad electromagnética	EN 50130-4

Directiva europea 2006/95/CE «De baja tensión»

La conformidad con la directiva europea 2006/95/CE ha sido probada según los siguientes estándares:

Seguridad	EN 60950-1

3.2 Información general sobre la conformidad con la norma EN50131

Esta sección le proporciona una visión general del cumplimiento de la norma EN50131 por parte del sistema SPC.

Dirección del organismo certificador
VdS (homologación VdS A / C / EN / SES) AG Köln HRB 28788 Sitz der Gesellschaft: Amsterdamer Str. 174, 50735 Köln Geschäftsführer: Robert Reinermann JörgWilms-Vahrenhorst (repres.)

Los productos SPC que se listan han sido probados de conformidad con la norma EN50131-3:2009 y todas las especificaciones RTC pertinentes.

Tipo de producto	Estándar
• SPC6350.320 • SPC6330.320 • SPC5350.320 • SPC5330.320 • SPCP355.300 • SPCP333.300 • SPCE652.100 • SPCK420.100 • SPCK421.100 • SPCE452.100 • SPCE110.100 • SPCE120.100 • SPCA210.100 • SPCK620.100 • SPCK623.100 • SPCN110.000 • SPCN320.000	EN50131 Grado 3
• SPC5320.320 • SPC4320.320 • SPCP332.300 • SPCW110.000 • SPCW112.000 • SPCW114.000 • SPCW130.100	EN50131 Grado 2

En las siguientes secciones de este documento encontrará información específica relacionada con los requisitos de la norma EN50131.

Requisito EN50131 (y sección pertinente)	Documentación de Vanderbilt pertinente
Temperatura de funcionamiento y rango de humedad	Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41
Pesos y dimensiones	Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41
Detalles de fijación	*Montaje de equipamiento del sistema* en la página 47

Requisito EN50131 (y sección pertinente)	Documentación de Vanderbilt pertinente
Instrucciones de instalación, puesta en marcha, mantenimiento, incluyendo las identificaciones de terminales	*Montaje de equipamiento del sistema* en la página 47 *Hardware del controlador* en la página 73
Tipo de interconexiones (consulte 8.8)	Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41 *Cableado de la interfaz X-BUS* en la página 81
Detalles de los métodos de armado y desarmado posibles (consulte 11.7.1 a 11.7.3 y las tablas 23 a 26)	Programación de usuario a través del teclado: • *Armado/Desarmado* en la página 281 • *Configurar un módulo de expansión de conmutador llave* en la página 239 • *Configuración de dispositivos de mando vía radio* en la página 121 • *Disparadores* en la página 295
Piezas reparables	Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41
Requisito de fuente de alimentación en caso de no contar con fuente de alimentación integrada	Consulte las instrucciones de instalación para las fuentes de alimentación de los módulos de expansión SPCP33x y SPCP43x.
Cuando se cuenta con una fuente de alimentación integrada, la información requerida se encuentra en la norma EN50131-6:2008, cláusula 6	Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41
Cantidad máxima de cada tipo de dispositivo ACE y de expansión.	*Cableado de la interfaz X-BUS* en la página 81 Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41
Consumo actual del CIE y cada tipo de dispositivo ACE y de expansión, con y sin condición de alarma.	Consulte las instrucciones de instalación pertinentes.
Clasificación de corriente máxima para cada salida eléctrica	Datos técnicos: • *SPC4000* en la página 35 • *SPC5000* en la página 37 • *SPC6000* en la página 41

Requisito EN50131 (y sección pertinente)	Documentación de Vanderbilt pertinente
Se brindan funciones programables	*Programación de técnico a través del teclado* en la página 125 *Programación de técnico a través del navegador* en la página 183
Cómo se hace que las indicaciones no sean accesibles a los usuario de Nivel 1 cuando los usuarios de Nivel 2, 3 o 4 ya no acceden a la información (consulte 8.5.1)	*Interfaz de usuario del teclado* en la página 101 *Configuración del teclado LCD* en la página 139 *Configuración del teclado Comfort* en la página 140 *Configuración de un módulo de expansión de indicador* en la página 237
Enmascaramiento/Reducción de mensajes/señales de rango procesadas como incidencias de «fallo» o «enmascaramiento» (consulte 8.4.1, 8.5.1 y la tabla 11)	*Opciones del sistema* en la página 254 *Cableado de entradas de zona* en la página 91 *Códigos SIA* en la página 382 El enmascaramiento PIR siempre se informa como una incidencia de enmascaramiento de zona (SIA - ZM). Además, el antienmascaramiento puede provocar una alarma, tamper, problema o ninguna acción adicional según la configuración. Valores por defecto actuales del efecto PIR: **Irlanda** Desarmado - Ninguno Armado - Alarma **Reino Unido, Europa, Suecia, Suiza, Bélgica** Desarmado - Tamper Armado - Alarma
Priorización del procesamiento de señal y mensaje e indicaciones (consulte 8.4.1.2, 8.5.3)	*Uso de la interfaz del teclado LCD* en la página 104 Uso de la interfaz del teclado Comfort - consulte *Acerca del teclado Comfort* en la página 108
Cantidad mínima de variaciones de códigos PIN, claves lógicas, claves biométricas y/o claves mecánicas para cada usuario (consulte 8.3)	*Combinaciones de código PIN de usuario* en la página 390
Método para limitar el tiempo de WD interno para el acceso de Nivel 3 sin autorización de Nivel 2 (consulte 8.3.1)	No admitido - El técnico no puede acceder al sistema sin permiso.
Cantidad y detalles de códigos PIN deshabilitados (consulte 8.3.2.2.1)	*Inhibiciones automáticas* en la página 390
Detalles de los métodos de autorización biométricos utilizados (consulte 8.3.2.2.3)	No aplicable

Requisito EN50131 (y sección pertinente)	Documentación de Vanderbilt pertinente
Método utilizado para determinar la cantidad de combinaciones de códigos PIN, claves lógicas, claves biométricas y/o claves mecánicas (consulte 11.6)	*Combinaciones de código PIN de usuario* en la página 390
Cantidad de entradas de códigos no válidos antes de que se deshabilite la interfaz de usuario (consulte 8.3.2.4)	*Códigos PIN de acceso* en la página 391
Detalles de los medios de autorización temporal para el acceso de usuarios (consulte 8.3.2)	Menús de usuario – Permitir acceso
Si se brinda el armado automático en horarios predeterminados, detalles de la indicación de prearmado y cualquier anulación automática de prevención de armado (consulte 8.3.3, 8.3.3.1)	*Armado/Desarmado* en la página 281
Detalles de las condiciones provistas para el estado de armado (consulte 8.3.3.4)	*Armado/Desarmado* en la página 281 *Configuración del teclado LCD* en la página 139 *Configuración del teclado Comfort* en la página 140 *Editar una salida* en la página 226 *Tipos de zona* en la página 393
Notificación de las señales o mensajes de salida provistos (consulte 8.6)	*Editar una salida* en la página 226 *Armado/Desarmado* en la página 281 *Derechos de usuario* en la página 213
Otras configuraciones de salida a la interfaz con componentes del sistema de intrusión y atraco (consulte 8.2)	*Editar una salida* en la página 226 *Tipos de zona* en la página 393 *Test* en la página 167 *Interfaz de usuario del teclado* en la página 101
Criterios para la eliminación automática del atributo «prueba» (consulte 8.3.9)	*Temporizaciones* en la página 266
Cantidad de incidencias que resultan en inhibición automática	*Inhibiciones automáticas* en la página 390
Si ACE es Tipo A o Tipo B (consulte 8.7) o si es portátil o móvil (consulte 11.14)	Todos los dispositivos están cableados y alimentados por las fuentes de alimentación del sistema. Consulte los datos técnicos pertinentes de las fuentes de alimentación (documentos por separado).
Datos de los componentes de la memoria no volátil (consulte la Tabla 30, paso 6)	Consulte la documentación de los teclados SPCK420/421 y SPCK620/623.
Vida útil de la batería de respaldo de la memoria (consulta 8.10.1)	N/D. Almacenado en memoria no volátil.

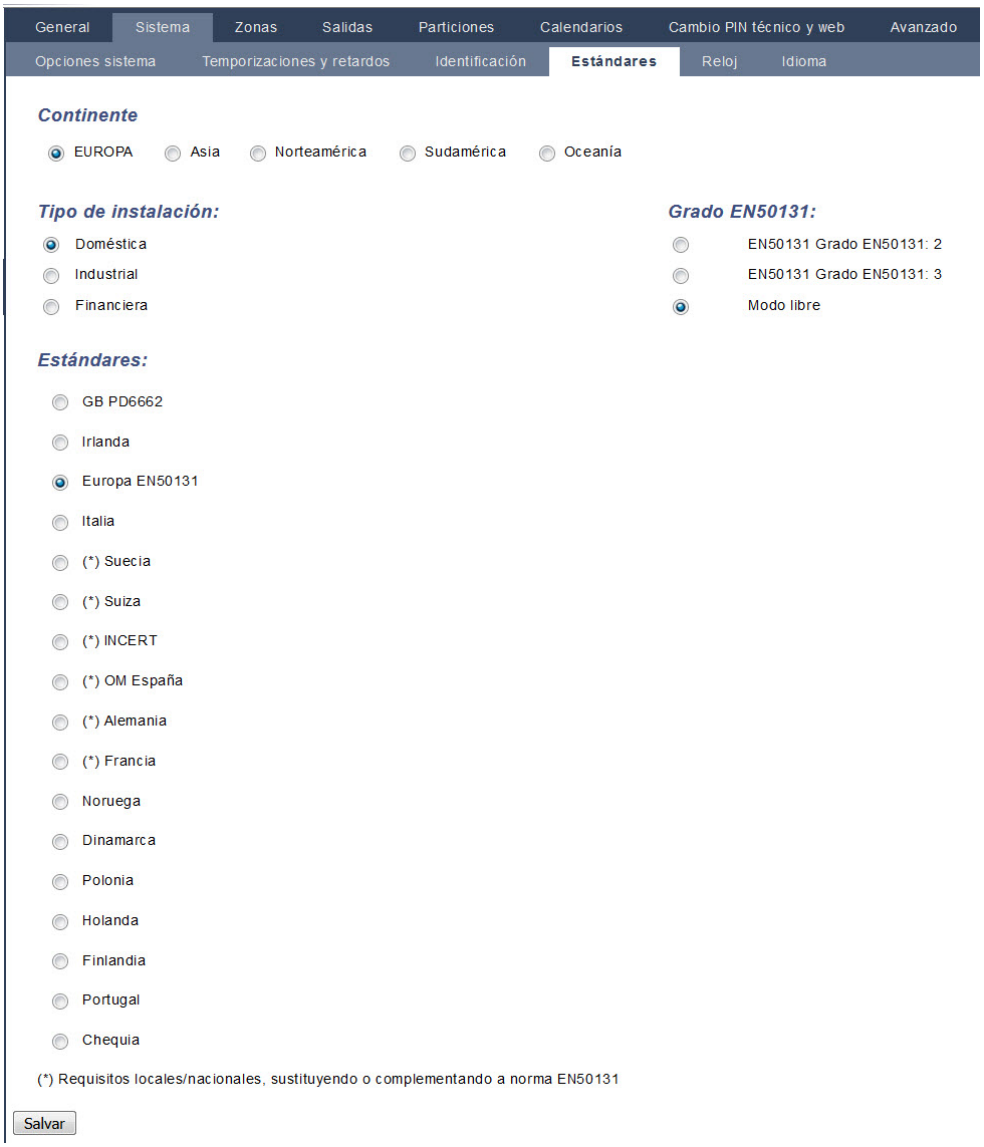
Requisito EN50131 (y sección pertinente)	Documentación de Vanderbilt pertinente
Funciones opcionales provistas (consulte 4.1)	*Programación de técnico a través del teclado* en la página 125 *Programación de técnico a través del navegador* en la página 183
Funciones adicionales provistas (consulte 4.2, 8.1.8)	*Grado libre* en la página 273 *Opciones* en la página 254
Niveles de acceso requeridos para acceder a las funciones adicionales provistas	*Editar* en la página 173 Configuración de usuario (navegador) - consulte *Añadir/Editar un usuario* en la página 209
Detalles de cualquier instalación programable que haría que el sistema de intrusión y atraco no cumpliera con EN 50131-1:2006, 8.3.13 o cumpliera a un nivel de grado de seguridad inferior, con instrucciones respecto de la eliminación consecuente del etiquetado de cumplimiento (consulte 4.2 y 8.3.10).	*Grado libre* en la página 273 *Opciones* en la página 254 *Conformidad con las certificaciones EN50131* en la página opuesta

Los productos SPC que se listan han sido probados de conformidad con la norma EN50131-6 y todas las especificaciones RTC pertinentes.

Tipo de producto	Estándar
• SPC6350.320 • SPC6330.320 • SPC5350.320 • SPC5330.320 • SPCP355.300 • SPCP333.300 • SPCP355.300 • SPCE652.100 • SPCK420.100 • SPCK421.100 • SPCE452.100 • SPCE110.100 • SPCE120.100 • SPCA210.100 • SPCK620.100 • SPCK623.100 • SPCN110.000 • SPCN310.000	EN50131-6
• SPC5320.320 • SPC4320.320 • SPCP332.300	EN50131-6

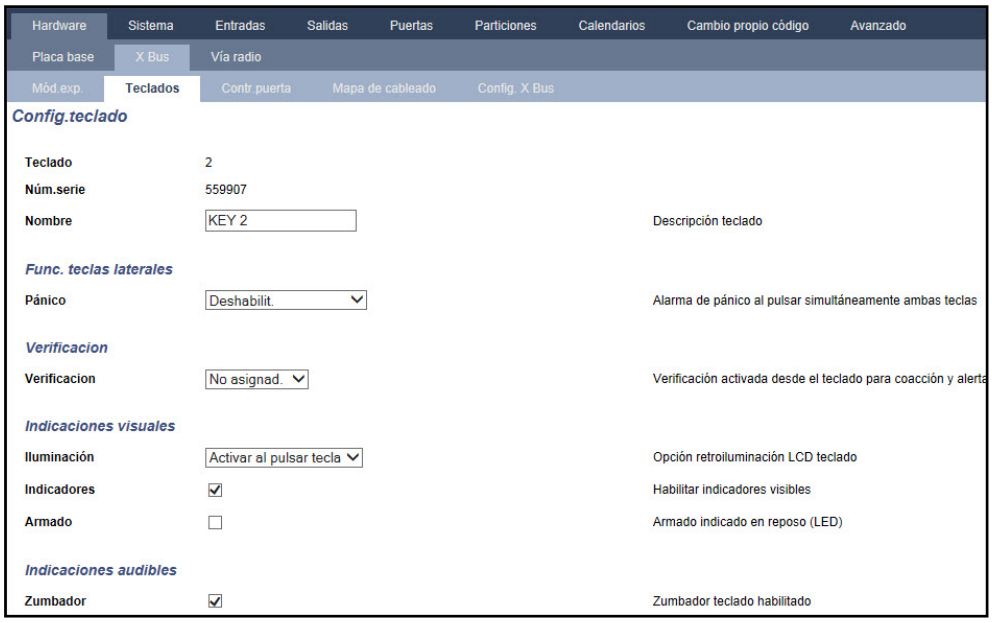
3.2.1 Conformidad con las certificaciones EN50131

Requisitos de software



- En la página de configuración de **Estándares**, seleccione **Europa** en **Región** para implementar los requisitos de la norma EN50131.
- Seleccione **Grado 2** o **Grado 3** para implementar el grado de cumplimiento de la norma EN 50131.
- El ajuste de **Vía radio Tiempo de impedimento de armado** debe ser un valor superior a 0 e inferior a 20.
- El ajuste de **Vía radio Tiempo de pérdida de dispositivo** debe ser un valor inferior a 120.
- **Config. X-BUS, Reintentos** debe tener un valor de 10.
- **Config. X-BUS, Temp. comunicación** debe tener un valor de 5.
- Seleccione **Sincronización hora con red de CA** debajo de **Reloj** para utilizar la configuración como maestro del reloj.

- NO seleccione el atributo **Estado armado** en los ajustes de configuración de **Teclado** para **Indicaciones visuales**.



Requisitos de hardware

- Se debe instalar el kit de tamper trasero (SPCY130) para que las centrales y las fuentes de alimentación cumplan con la norma EN 50131 Grado 3.
- Se deben instalar componentes EN 50131 Grado 3 para los sistemas que cumplen con EN 50131 Grado 3.
- Se deben instalar componentes EN 50131 Grado 2 o Grado 3 para los sistemas que cumplen con EN 50131 Grado 2.
- No es posible dar de alta un dispositivo vía radio con una intensidad de señal inferior a 3.
- La relación recomendada de receptores vía radio respecto a transmisores es de no más de 20 transmisores por cada receptor.
- La función de rotura de cristal se debe utilizar con una interfaz de rotura de cristal conforme a la norma EN.
- Para cumplir con la norma EN50131-3:2009, no arme ni desarme el sistema mediante el SPCE120 (módulo de expansión de indicador) ni con el SPCE110 (módulo de expansión de conmutador de llave).

Se realizan tests del módulo RTB SPCN110 y el módulo GSM/GPRS SPCN320 con centrales EN 50131 Grado 2 y Grado 3 aprobadas y pueden utilizarse con estas centrales aprobadas.

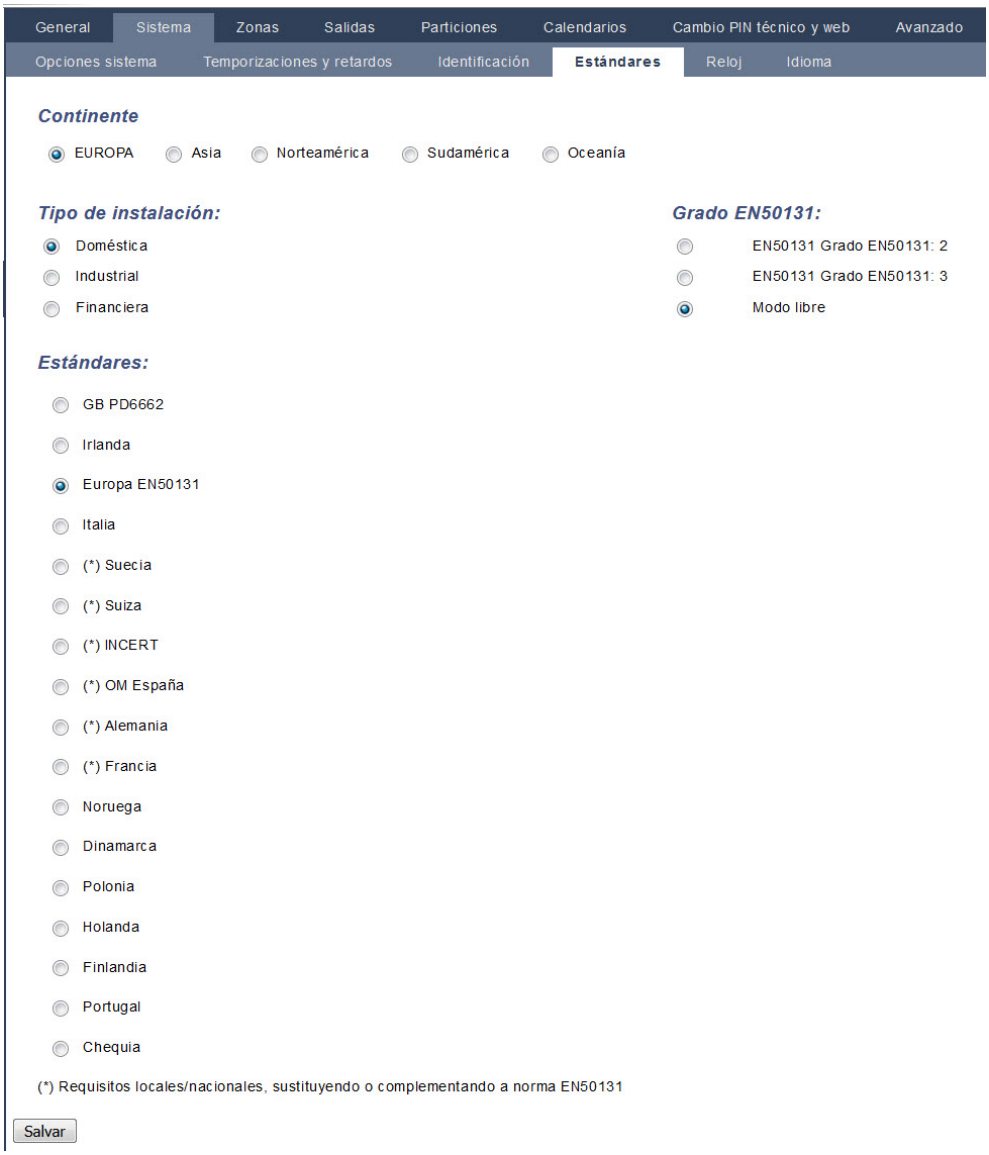
3.2.2 Conformidad con las normas EN 50136-1:2012 y EN 50136-2:2014

Los productos SPC que se listan han sido probados de conformidad con las normas EN 50136-1:2012 y EN 50136-2:2014.

3.2.3 Conformidad con las homologaciones INCERT

Requisitos de software

Al seleccionar Bélgica (*) debajo de **Región**, implementa los requisitos locales/nacionales que sustituyen los requisitos de la norma EN 50131.



Al seleccionar **Grado 2** o **Grado 3**, se selecciona el cumplimiento de la norma EN 50131 más los requisitos INCERT adicionales:

- Solo un técnico puede reiniciar un tamper. Para INCERT, esto es aplicable en todos los grados. Esto generalmente es un requisito para EN 50131 Grado 3.
- Un tamper en una zona inhibida/aislada debe enviarse a la CRA y mostrarse al usuario. Para INCERT, los tampers se procesan para zonas aisladas. En todas las otras variaciones estándar, los tampers se ignoran en las zonas aisladas.
- Los códigos PIN de usuario se deben definir con más de 4 dígitos.

Requisitos de hardware

- La capacidad mínima de la batería para SPC42xx/43xx/52xx/53xx/63xx es 10 Ah/12 V. Si se utiliza una batería de 10 Ah, entonces esta tiende hacia el lado izquierdo de la carcasa y se debe doblar la pestaña de la parte inferior hacia la batería.
- Se debe colocar el puente (J12) en el selector de la batería para usar una batería de 17/10 Ah y retirar la batería de 7 Ah.
- La cantidad de corriente de la salida auxiliar utilizando una batería de 10 Ah para SPC42xx/SPC52xx es:

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	568	543	438	413
24 h	214	189	84	59
30 h	143	118	13	N/A
60 h	2	N/A	N/A	N/A

- La cantidad de corriente de la salida auxiliar utilizando una batería de 10 Ah para SPC43xx/SPC53xx/ SPC63xx es:

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	538	513	408	383
24 h	184	159	54	29
30 h	113	88	N/A	N/A
60 h	N/A	N/A	N/A	N/A

3.2.4 Directrices de conformidad con PD 6662:2010

Este documento contiene todos los criterios para la instalación y puesta en marcha del sistema SPC de modo que cumpla con la norma PD 6662:2010.

3.2.4.1 Productos

Este documento pretende abarcar los siguientes componentes del sistema SPC:

Controlador de grado 2 SPC4320.320-L1	
Controlador de grado 2 SPC5320.320-L1	Módulo de expansión SPCE652.100, 8 entradas/2 salidas
Controlador de grado 3 SPC5330.320-L1	Fuente de alimentación inteligente SPCP332.300 con módulo de expansión de E/S
Controlador de grado 3 SPC5350.320-L1	Fuente de alimentación inteligente SPCP355.300 con módulo de expansión de 8 entradas/2 salidas
Controlador de grado 3 SPC6330.320-L1	Fuente de alimentación inteligente SPCP333.300 con módulo de expansión de E/S
Controlador de grado 3 SPC6350.320-L1	Módulo RTB SPCN110.000
Teclado LCD SPCK420/421.100	Módulo GSM SPCN320.000
Módulo de expansión SPCE452.100, 8 salidas de relé	

3.2.4.2 Resumen de normas

Se proporcionan directrices para la implantación de la conformidad con la norma PD 6662:2010 para un sistema SPC con las siguientes normas relevantes:

PD 6662:2010	BS EN 50136-1-5:2008
BS 4737-3.1:1977	BS EN 50136-2-1:1998 +A1:1998
BS 8243:2010	BS EN 50136-2-2:1998
BS 8473:2006+A1:2008	BS EN 50136-2-3:1998
BS EN 50131-1:2006+A1:2009	BS EN 50131-3:2009
BS EN 50136-1-1:1998+A2:2008	BS EN 50131-6:2008
BS EN 50136-1-2:1998	DD 263:2010
BS EN 50136-1-3:1998	DD CLC/TS 50131-7:2008

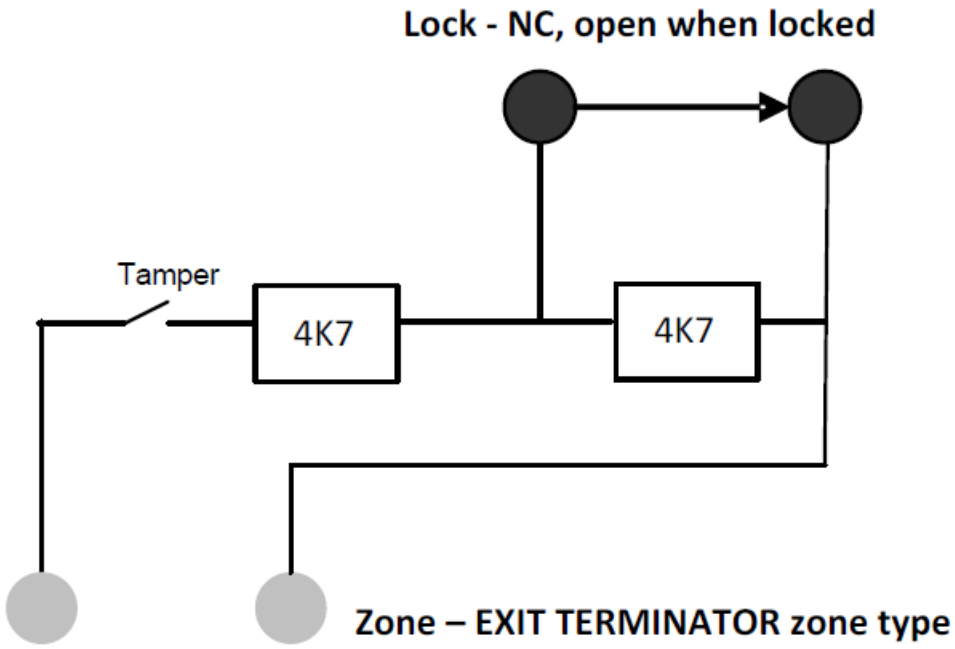
3.2.4.3 Métodos para completar el armado y desarmado

Métodos para completar el armado (BS 8243:2010 - punto 6.3)

La culminación del procedimiento de armado total se consigue con cualquiera de los siguientes métodos:

a) Bloqueo de anulación instalado en la puerta de salida final

El instalador debe instalar un bloqueo de anulación ligada como se indica a continuación:



Se debe configurar una zona de tipo TERMINADOR DE SALIDA para SPC.

Consulte *Tipos de zona* en la página 393.

b) Pulse el botón interruptor montado fuera de las instalaciones supervisadas

Conecte el botón dentro de una entrada de zona de SPC tal como se indica a continuación:

Se debe configurar una zona de tipo TERMINADOR DE SALIDA para SPC.

Consulte *Tipos de zona* en la página 393.

c) Interruptor de protección (es decir, contacto de puerta) instalado en la partición o puerta de salida final de las instalaciones con alarma

Conecte el interruptor al sistema SPC tal como se indica a continuación:

El contacto está montado en la puerta de salida final y conectado a una zona de Entrada/Salida con un atributo de 'Fin de salida'.

Consulte *Tipos de zona* en la página 393 y *Atributos de zona* en la página 399.

Es posible emitir una señal de fallo de funcionamiento mediante la función de abortar alarma. Esta opción está habilitada por defecto.

Consulte *Opciones* en la página 126 (Teclado) y *Opciones* en la página 254 (Navegador).

d) Llave digital

No es compatible con el SPC.

e) En combinación con una CRA

Este método de armado se lleva a cabo con SPC COM XT o algún otro software de CRA de terceros mediante comandos EDP.

Métodos para completar el desarmado (BS 8243:2010 - punto 6.4)

Los métodos de desarmado se llevan a cabo de la siguiente manera:

6.4.1 En todos los métodos de desarmado del sistema SPC, el usuario recibe una indicación acústica de que el sistema se ha desarmado correctamente. Esta indicación consiste en una secuencia de pitidos procedente del CIE.

6.4.2 Prevención de entrada a las instalaciones supervisadas antes de que se desarme el sistema de alarma contra intrusos (IAS):

a) si se desbloquea la puerta de entrada inicial, el IAS se desarma;

Conformidad por parte del SPC si el tipo de zona Llave armado se utiliza únicamente con el atributo Desarmado. Este tipo de zona no se debe utilizar para el armado.

b) el desarmado del IAS por parte del usuario antes de entrar en las instalaciones supervisadas provoca o permite que la puerta de entrada inicial se desbloquee.

Conformidad por parte del SPC realizando el desarmado mediante un lector de tarjetas de acceso con la opción Desarmado, o una entrada de un sistema de acceso de terceros a una zona Llave armado con un atributo de Desarmado.

6.4.3 Prevención de entrada a las instalaciones supervisadas antes de que se hayan deshabilitado todos los medios de confirmación de alarma de intrusión:

a) El desbloqueo de la puerta de entrada inicial hace que se deshabiliten todos los medios de confirmación.

Operación no permitida por el SPC.

b) La deshabilitación de todos los medios de confirmación por parte del usuario antes de entrar en las instalaciones supervisadas provoca o permite que la puerta de entrada inicial se desbloquee.

Operación no permitida por el SPC.

6.4.4 Apertura de la puerta de entrada inicial deshabilita todos los medios de confirmación de alarma de intrusión

Operación no permitida por el SPC.

6.4.5 Desarmado mediante una llave digital

a) Uso de una llave digital antes de entrar en las instalaciones supervisadas (por ejemplo vía radio).

El SPC satisface este punto cuando el instalador coloca un lector PACE (p. ej., SPCK421) fuera de las instalaciones.

b) Uso de una llave digital después de entrar en las instalaciones supervisadas desde un lugar lo más cercano posible a una puerta de entrada inicial.

Esta funcionalidad está disponible utilizando un lector PACE (p. ej., SPCK421) cerca de la puerta de entrada a unas instalaciones.

Consulte *Tipos de zona* en la página 393 y *Atributos de zona* en la página 399.

ADVERTENCIA: Tenga en cuenta que, al permitirse este método de desarmado, si un intruso consigue forzar la puerta de entrada inicial, no se avisará a la policía, independientemente del progreso del intruso por las instalaciones.

Este método de desarmado del sistema de alarma contra intrusos podría ser inaceptable para su compañía aseguradora.

6.4.6 Desarmado en combinación con una central de recepción de alarmas (CRA)

Conformidad por parte del SPC utilizando un software de CRA de terceros. Debe haber una indicación por fuera del edificio mediante un zumbador o un flash temporizado que funcione en un sistema desarmado durante un período temporizado de, por ejemplo, 30 segundos.

Consulte *Temporizaciones* en la página 130.

3.2.4.4 Requisitos de configuración para el cumplimento de la norma PD 6662:2010.

Recomendaciones para la grabación de condiciones de alarma notificadas remotamente (BS 8243:2010 - Anexos G.1 y G.2)

Las condiciones de alarma se pueden categorizar para su análisis de acuerdo con el Anexo G si el sistema SPC está configurado de tal forma que el temporizador de entrada esté ajustado en menos de 30 segundos y el retardo del marcador esté ajustado en 30 segundos.

Consulte las siguientes secciones:

- *Particiones* en la página 134
- *Añadir/Editar una partición* en la página 275
- *Temporizaciones* en la página 130

Requisitos para sistemas que utilizan rutas de alarma específicas (BS EN 50136-1-2, 1998)

El sistema SPC se debe configurar para que realice una llamada de prueba automática a la CRA.

El sistema SPC se debe configurar con una salida de «Comunicación».

Consulte la siguiente sección:

- *Añadir/Editar una CRA mediante el uso de SIA o CID* en la página 333

Requisitos para equipos utilizados en sistemas con comunicaciones digitales mediante RTB (BS EN 50136-2-2, 1998)

Fallo Salida

El sistema SPC se debe configurar con una salida de «Comunicación».

Consulte las siguientes secciones:

- *Salida* en la página 157 (Teclado)
- *Configurar entradas y salidas de controlador* en la página 224 (Navegador)
- *Añadir/Editar una CRA mediante el uso de SIA o CID* en la página 333

Intentos de retransmisión

Los intentos de retransmisión (Intentos marcación) están configurados en este manual:

- *Añadir/Editar una CRA mediante el uso de SIA o CID* en la página 333
- *Editar la configuración de EDP* en la página 344

Se permite un mínimo de 1 y un máximo de 12 retransmisiones.

Intrusión y atraco - Diseño del sistema (DD CLC TS 50131-7, 2008)

Armado y desarmado

El sistema SPC se puede configurar de manera que el armado se complete mediante «Fin de salida».

Es posible configurar el SPC de manera que se active momentáneamente un dispositivo de aviso al realizarse el armado.

Consulte las siguientes secciones:

- *Temporizaciones* en la página 130
- *Atributos de zona* en la página 399
- *Salida* en la página 157 (Teclado)
- *Editar una salida* en la página 226 (Navegador)

Alarma de intrusión y de atraco confirmada (BS8243:2010 Designación de señales alarma de atraco (HUA) para confirmación secuencial)

El sistema SPC se puede configurar de tal manera que los siguientes escenarios, disparados con más de dos minutos de diferencia de cualquier zona de atraco o dispositivo de atraco (HD), informarán de un evento de alarma de atraco confirmada (HV para SIA y 129 para CID) a la CIE:

- dos activaciones de zona de atraco
- una activación de zona de atraco y de zona de pánico

Si en este período de dos minutos se produce una activación de zona de atraco y de zona de tamper o de zona de pánico, también se enviará una incidencia de alarma de atraco confirmada.

Un atraco confirmado no requerirá la restauración de técnico aunque esta esté habilitada. Una incidencia de atraco confirmado queda registrada en el registro del sistema.

3.2.4.5 Requisitos de puesta en funcionamiento adicionales para el cumplimento de la norma PD 6662:2010.

Información que se debe incluir en la propuesta de diseño del sistema y en el documento final (BS 8243:2010 - Anexo F)

- Durante la instalación, configuración y puesta en funcionamiento de un sistema SPC, el instalador debe seguir las siguientes directrices tal como se especifica en el anexo anteriormente indicado:
- Se recomienda utilizar rutas dobles para la señalización, compatibles con el sistema SPC utilizando las opciones de GSM, RTB y Ethernet.
- El sistema SPC se debe instalar y configurar de manera que proporcione una facilidad de confirmación efectiva. Cualquier excepción a este punto se debe indicar en el documento final.
- Las combinaciones y secuencias que contribuyan a confirmar una alarma deben ser notificadas claramente al usuario final.
- El tiempo de confirmación de intrusión se debe notificar claramente al usuario final.
- Los métodos de armado y desarmado se deben describir claramente al usuario final tal como se detalla en este documento.
- Asegúrese de que el usuario recibe instrucciones escritas para el caso de fallo de bloqueo.

Se recomienda adjuntar la etiqueta de PD 6662:2010 en un lugar adecuado dentro de la carcasa del SPC, junto a la etiqueta de características del producto.

3.2.4.6 Información adicional

Requisitos de red de transmisión – Niveles de rendimiento, disponibilidad y seguridad (BS EN 50136-1-2, 1998 y BS EN 50136-1-5, 2008)

Se ha comprobado y aprobado el cumplimiento por parte del sistema SPC de la norma EN50136-1-1.

Los niveles del SPC se clasifican de la siguiente manera:

Tiempo de transmisión	D2 como máx.
Tiempo de transmisión, valores máx.	M0 – M4
Tiempo de transmisión	T3 como máx.
Disponibilidad	Consulte *Niveles y especificaciones de atenuación del ATS* en la página 404.
Nivel de seguridad de señalización	Comprobado según norma EN50136-1-1 y clasificado como «S0».

3.2.5 Conformidad con las homologaciones VdS

Este documento de instalación abarca la información de instalación requerida para que el producto cumpla con las homologaciones VdS.

Vanderbilt

SPC42xx/43xx/53xx/63xx: Homologación VdS n.° G112104, G112124, y G112128. Certificados VdS EN EN-ST000142, EN-ST000143, EN-ST000055, EN-ST000056, EN-ST000057, EN-ST000058, EN-ST000061, EN-ST000062.

Siemens

SPC42xx/43xx/53xx/: Homologación VdS n.° G116035. Certificados VdS EN EN-ST000225, EN-ST000226, EN-ST000227, EN-ST000228, EN-ST000229, EN-ST000230, EN-ST000231, EN-ST000232.

En esta sección se describe el cumplimiento de las homologaciones VdS por parte de este sistema.

Configurar el software para el cumplimiento de las homologaciones VdS

Para que el sistema cumpla las homologaciones VdS, se debe realizar lo siguiente:

1. Inicie sesión en la central con el navegador.
2. Haga clic en **Modo técnico completo**.
3. Haga clic en **Configuración > Sistema > Normas**.
4. Seleccione **Europa** en la sección **Continente** de la página.
5. Seleccione **Alemania** en la sección **Estándares** de la página.
6. Seleccione el grado VdS requerido por su tipo de instalación.

Transmisión de fallos de hardware — en **Configuración > Sistema > Opciones del sistema**, se debe seleccionar la opción **Habilitada + transmisión (10 s)** de la lista desplegable del **Modo salida watchdog**.

Los fallos de hardware no se transmiten si el Técnico ha accedido al sistema.

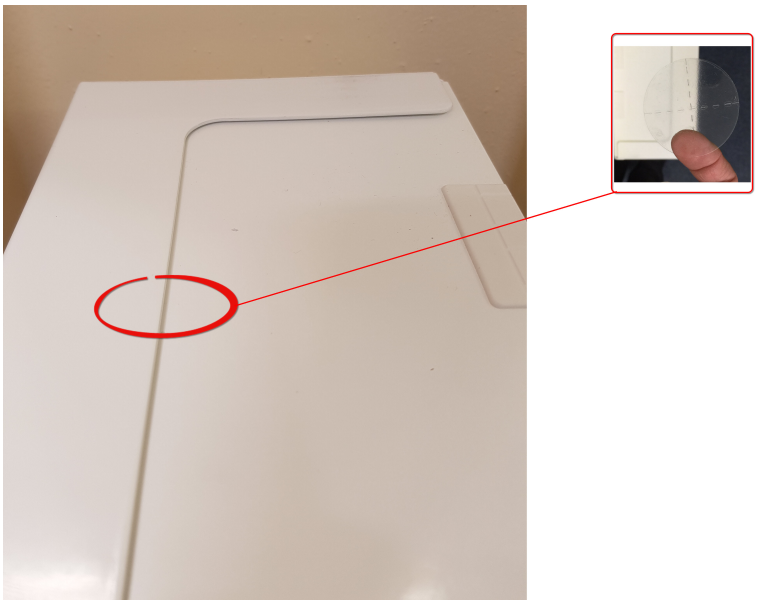
Hardware

El cumplimiento de las homologaciones VdS requiere lo siguiente:

- Una carcasa G5 con tamper frontal implantado, como requisito mínimo.
- Los teclados no muestran información de estado si el sistema está armado.
- El número de zonas admitidas es el siguiente:
  – 512 zonas en configuración de anillo
  – 128 zonas por X-Bus en configuración multipunto (punta)
- Las siguientes combinaciones de RFL no cumplen las normas VdS:
  – 1 k, 470 ohmios
  – 1 k, 1 k, 6k6 ohmios

3.2.6 Conformidad con las homologaciones NF y A2P

Dirección del organismo certificador	
Certificación CNPP	
Pôle Européen de Sécurité - Vernon	**Certificación AFNOR**
Route de la Chapelle Réanville	11 rue François de Pressensé
CD 64 - CS 22265	93571 Saint Denis La Plaine Cedex
F-27950 SAINT MARCEL	www.marque-nf.com
www.cnpp.com	



Para cumplir con las regulaciones de instalación NF y A2P, esta carcasa debe estar sellada con la etiqueta de tamper adjunta luego de la instalación.

Los productos SPC que se listan han sido probados de conformidad con la norma NF324 - H58, con referencia a RTC50131-6 y RTC50131-3, y las certificaciones EN vigentes. Consulte *Conformidad con las certificaciones EN50131* en la página 23.

Tipo de producto	Configuración	Estándar	Marca
SPC6350.320 + SPCP355.300 (Cert. 1233700001A0)	60 h, sin supervisión	NF Grado 3, Clase 1	
SPC5350.320 + SPCP355.300 (Cert. 1233700001B0)	60 h, sin supervisión		
SPC6350.320 (Cert. 1233700001A0)	60 h, sin supervisión		
SPC5350.320 (Cert. 1233700001B0)	60 h, sin supervisión		
SPC6330.320 + SPCP333.300 (Cert. 1232200003)	60 h, sin supervisión	NF Grado 3, Clase 1	
SPC5330.320 + SPCP333.300 (Cert. 1232200003)	60 h, sin supervisión		
SPC6330.320 (Cert. 1232200003)	30 h, supervisado		
SPC5330.320 (Cert. 1232200003)	30 h, supervisado		

Tipo de producto	Configuración	Estándar	Marca
SPC5320.320 (Cert. 1222200003)	36 h, sin supervisión	NF Grado 2, Clase 1	
SPC4320.320 (Cert. 1222200003)	36 h, sin supervisión		
SPCN110.000 SPCN320.000 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF Grado 2 y 3, Clase 1	

4 Datos técnicos

Este capítulo abarca:

4.1 SPC4000

Particiones programables	4
Máx. número de códigos PIN de usuario	100
Controles remotos	Hasta 32
Dispositivos PACE	32
Alarma de pánico vía radio	Hasta 128
Memoria de eventos	1.000 incidencias de intrusión, 1.000 incidencias de acceso
Número de zonas incorporadas	8
Máx. número de zonas cableadas	32
Máx. número de zonas vía radio	32 (restar zonas cableadas)
Máx. número de detectores vía radio de Intrunet por receptor vía radio (recomendado)	20
Resistencia RFL	Doble 4k7 (predeterminado), se pueden configurar otras combinaciones de resistencias
Número de relés incorporados	1 flash (30 V CC/1 A corriente de conmutación resistiva)
Número de col. abiertos incorporados	2 sirena interior/exterior, 3 libremente programables (cada uno con una corriente de conmutación resistiva máxima de 400 mA, suministrada a través de salida auxiliar)
Versión	V3.x
Capacidad de puertas	Máx. 4 puertas de entrada o 2 puertas de entrada/salida
Número de lectores de tarjetas	Máx. 4

Módulo de radio	• SPC4221: receptor RF SiWay integrado (868MHz) • SPC4320.220: Opcional (SPCW111) • SPC4320.320: Opcional (SPCW110)
Verificación	4 zonas de verificación con un máx. de 4 cámaras IP y 4 dispositivos de audio.
Vídeo	Hasta 16 imágenes previas a la incidencia/16 posteriores a la incidencia (resolución JPEG 320 x 240, máx. 1 imagen/segundo)
Audio	Hasta 60 seg. previo/60 seg. posterior de grabación de audio
Bus de campo 1)	X-BUS sobre RS-485 (307 kb/s)
Número de dispositivos de campo 2)	Máx. 11 (4 teclados, 2 módulos de expansión de puerta, 5 módulos de expansión de entrada/salida)
Dispositivos de campo conectables	• Teclados: SPCK42x, SPCK62x • Módulos de expansión de puerta: SPCA210, SPCP43x • Módulos de expansión con E/S: SPCE65x, SPCE45x, SPCP33x, SPCE110, SPCE120, SPCV32x
Interfaces	• 1 X-BUS (1 punta) • 1 RS232 • USB (conexión a PC) • SPC43xx: Adicionalmente 1 Ethernet (RJ45)
Contacto de tamper	Tamper con muelle frontal, 2 entradas auxiliares de contacto de tamper
Tensión de alimentación	Tipo A (por EN50131-1)
Voltaje de red	230V CA, + 10%/ -15% / 50Hz
Fusible de red	250mA T (pieza reemplazable en bloque de terminales de red)
Consumo de energía	SPC42xx: Máx. 160mA a 230V CA SPC43xx: Máx. 200mA a 230V CA
Corriente de funcionamiento	Controlador SPC42xx: Máx. 160mA a 12V CC Controlador SPC43xx: Máx. 200mA a 12V CC
Corriente de reposo	Controlador SPC42xx: Máx. 140 mA a 12 V CC (165 mA con RTB, 270 mA con GSM, 295 mA con RTB y GSM) Controlador SPC43xx: Máx. 170 mA a 12 V CC (195 mA con RTB, 300 mA con GSM, 325 mA con RTB y GSM)
Voltaje de salida	13-14 V CC en condiciones normales (con alimentación de red CA y batería completamente cargada), mín. 10,5 V CC con alimentación de un dispositivo secundario (antes de cerrarse el sistema como protección contra descarga mínima de batería)
Activador de bajo voltaje	7,5 V CC
Protección contra sobretensión	15,7 V CC

Ondulación de pico a pico	Máx. 5% del voltaje de salida
Alim. auxiliar (nominal)	Máx. 750mA a 12V CC
Tipo de batería	SPC422x/4320: YUASA NP7-12FR (7 Ah), batería no suministrada
Cargador de batería	SPC422x/4320: Máx. 72 h para el 80 % de capacidad de la batería
Protección de la batería	Corriente limitada a 1A (protegida por fusible), protección contra descarga mínima a 10,5V CC ±3%
Actualización de software	Actualización local y remota para controlador, periféricos y módems GSM/RTB.
Calibración	No se requieren comprobaciones de calibración (calibrada en fabricación)
Piezas reparables	No hay piezas reparables
Temperatura de servicio	de -10 a +50 °C
Humedad relativa	Máx. 90% (sin condensación)
Color	RAL 9003 (blanco señal)
Peso	SPC422x/4320: 4,500 kg
Dimensiones (An. x Al. x Pr.)	SPC422x/4320: 264 x 357 x 81 mm
Carcasa	SPC4320.320: Pequeña carcasa de metal (acero dulce de 1,2 mm) SPC422x.220: Pequeña carcasa con base metálica (acero dulce de 1,2 mm) y tapa de plástico
La carcasa puede contener hasta	SPC422x/4320: 1 módulo de expansión adicional (tamaño 150 x 82 mm)
Coeficiente IP	30
ATS	3
ATP	8
Perfiles de incidencias	5
Excepciones de incidencia	10
Perfiles de comandos	5

1) Máx. 400 m entre dispositivos/tipos de cable IYSTY 2 x 2 x Ø 0,6 mm (mín.), UTP cat 5 (núcleo sólido) o Belden 9829.

2) Se pueden direccionar más módulos de expansión de E/S en lugar de un teclado o un módulo de expansión de puerta, pero el número de entradas/salidas programables no puede exceder los límites especificados para el sistema.

4.2 SPC5000

Particiones programables	16
Máx. número de códigos PIN de usuario	500

Controles remotos	Hasta 100
Dispositivos PACE	250
Alarma de pánico vía radio	Hasta 128
Memoria de eventos	10.000 incidencias de intrusión, 10.000 incidencias de acceso
Número de zonas incorporadas	• SPC5320/5330 — 8 • SPC5350 — 16
Máx. número de zonas cableadas	128
Máx. número de zonas vía radio	120 (restar zonas cableadas)
Máx. número de detectores vía radio de Intrunet por receptor vía radio (recomendado)	20
Resistencia RFL	Doble 4k7 (predeterminado), se pueden configurar otras combinaciones de resistencias
Salidas de relé	• SPC5320/5330 — 1 flash (30 V CC/1 A corriente de conmutación resistiva) • SPC5350 — 4 (conmutación de polo único, 30 V CC/máx. 1 A corriente de conmutación resistiva)
Salidas electrónicas	• SPC5320/5330 — 5 salidas: – 2 sirenas interiores/exteriores – 3 programables. Máximo 400mA corriente de conmutación resistiva por salida, suministrada por salida auxiliar. • SPC5350 — 8 salidas. Máximo 400 mA corriente de conmutación resistiva por salida – 5 salidas de alimentación estándar – 3 salidas supervisadas
Versión	V3.x
Capacidad de puertas	Máx. 16 puertas de entrada o 8 puertas de entrada/salida
Número de lectores de tarjetas	Máx. 16
Módulo de radio	Opcional (SPCW110)
Verificación	16 zonas de verificación con un máx. de 4 cámaras IP y 16 dispositivos de audio.
Vídeo	Hasta 16 imágenes previas a la incidencia/16 posteriores a la incidencia (resolución JPEG 320 x 240, máx. 1 imagen/segundo)
Audio	Hasta 60 seg. previo/60 seg. posterior de grabación de audio
Bus de campo 1)	X-BUS sobre RS-485 (307 kb/s)

Número de dispositivos de campo 2)	Máx. 48 (16 teclados, 8 módulos de expansión de puerta, 16 módulos de expansión de entrada/salida)
Dispositivos de campo conectables	• Teclados: SPCK42x, SPCK62x • Módulos de expansión de puerta: SPCA210, SPCP43x • Módulos de expansión con E/S: SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	• 2 X-BUS (2 en punta 1 lazo) • 2 RS232 • 1 USB (conexión a PC) • SPC53xx: Adicionalmente 1 Ethernet (RJ45)
Contacto de tamper	• SPC5320/5330: Tamper con muelle frontal, 2 entradas auxiliares de contacto de tamper • SPC5350: Interruptor de tamper frontal/trasero
Tensión de alimentación	Tipo A (por EN50131-1)
Voltaje de red	230 V CA, + 10%/-15%, 50 Hz
Fusible de red	• SPC5320/5330: 250 mA T (pieza reemplazable en bloque de terminales de red) • SPC5350: 800 mA T (pieza reemplazable en bloque de terminales de red)
Consumo de energía	• SPC5320/5330: Máx. 200mA a 230V CA • SPC5350: Máx. 500 mA a 230V CA
Corriente de funcionamiento	• Controlador SPC5320/5330: Máx. 200mA a 12V CC • SPC5350: Máx. 210mA a 12V CC
Corriente de reposo	Controlador SPC53xx: Máx. 170 mA a 12 V CC (195 mA con RTB, 300 mA con GSM, 325 mA con RTB y GSM)
Voltaje de salida	13-14 V CC en condiciones normales (con alimentación de red CA y batería completamente cargada), mín. 10,5 V CC con alimentación de un dispositivo secundario (antes de cerrarse el sistema como protección contra descarga mínima de batería)
Activador de bajo voltaje	11 V CC
Protección contra sobretensión	• SPC5320/5330: 15,7 V CC • SPC5350: 15 V CC nominal
Ondulación de pico a pico	Máx. 5% del voltaje de salida
Alim. auxiliar (nominal)	• SPC5320/5330: Máx. 750mA a 12V CC • SPC5350: Máx. 2.200 mA a 12 V CC (8 salidas con fusibles por separado, 300 mA por salida)

Tipo de batería	• SPC5320: YUASA NP7-12FR (7 Ah), • SPC5330: YUASA NP17-12FR (17 Ah) • SPC5350: YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) • SPC5350: FIAMM FGV22703 (12 V 27 Ah) Pila no incluida
Cargador de batería	• SPC5320: Máx. 72 h, • SPC5330/5350: Máx. 24 h para el 80 % de capacidad de la batería
Protección de la batería	• SPC5320/5330: Corriente limitada a 1 A (protegida por fusible), protección contra descarga mínima a 10,5 V CC ±3% • SPC5350: Corriente limitada a 2 A (protegida por fusible restablecible PTC), protección contra descarga mínima a 10,5 V CC
Actualización de software	Actualización local y remota para controlador, periféricos y módems GSM/RTB.
Calibración	No se requieren comprobaciones de calibración (calibrada en fabricación)
Piezas reparables	• SPC5320/5330: No hay piezas reparables • SPC5350: 8 fusibles de cristal (400 mA AT) para salidas de 12 V CC
Temperatura de servicio	de -10 a +50 °C
Humedad relativa	Máx. 90% (sin condensación)
Color	RAL 9003 (blanco señal)
Peso	• SPC5320: 4,500 kg • SPC5330: 6,400 kg • SPC5350: 18,600 kg
Dimensiones (An. x Al. x Pr.)	• SPC5320: 264 x 357 x 81 mm • SPC5330: 326 x 415 x 114 mm • SPC5350: 498 x 664 x 157 mm
Carcasa	• SPC5320: Pequeña carcasa de metal (acero dulce de 1,2 mm) • SPC5330: Carcasa de metal con bisagras (acero dulce de 1,2 mm) • SPC5350: Carcasa de metal (acero dulce de 1,5 mm)
La carcasa puede contener hasta	• SPC5320: 1 módulo de expansión adicional • SPC5330: 4 módulos de expansión adicionales (tamaño 150 x 82 mm) • SPC5350: 4 módulos de expansión adicionales (150 x 82 mm)
Clasificación IP/IK	30/06
ATS	5
ATP	15
Perfiles de incidencias	10
Excepciones de incidencia	50
Perfiles de comandos	8

1) Máx. 400 m entre dispositivos/tipos de cable IYSTY 2 x 2 x Ø 0,6 mm (mín.), UTP cat 5 (núcleo sólido) o Belden 9829.

2) Se pueden direccionar más módulos de expansión de E/S en lugar de un teclado o un módulo de expansión de puerta, pero el número de entradas/salidas programables no puede exceder los límites especificados para el sistema.

4.3 SPC6000

Particiones programables	60
Máx. número de códigos PIN de usuario	2500
Controles remotos	Hasta 100
Dispositivos PACE	250
Alarma de pánico vía radio	Hasta 128
Memoria de eventos	10.000 incidencias de intrusión, 10.000 incidencias de acceso
Número de zonas incorporadas	• SPC6320/6330 — 8 • SPC6350 — 16
Máx. número de zonas cableadas	512
Máx. número de zonas vía radio	120 (restar zonas cableadas)
Máx. número de detectores vía radio de Intrunet por receptor vía radio (recomendado)	20
Resistencia RFL	Doble 4k7 (predeterminado), se pueden configurar otras combinaciones de resistencias
Salidas de relé	• SPC6320/6330 — 1 flash (30 V CC/1 A corriente de conmutación resistiva) • SPC6350 — 4 (conmutación de polo único, 30 V CC/máx. 1 A corriente de conmutación resistiva)
Salidas electrónicas	• SP6320/6330 — 5 salidas: – 2 sirenas interiores/exteriores – 3 programables. Máximo 400mA corriente de conmutación resistiva por salida, suministrada por salida auxiliar. • SPC6350 — 8 salidas. Máximo 400 mA corriente de conmutación resistiva por salida – 5 salidas de alimentación estándar – 3 salidas supervisadas
Versión	V3.x
Capacidad de puertas	Máx. 64 puertas de entrada o 32 puertas de entrada/salida

Número de lectores de tarjetas	Máx. 64
Módulo de radio	Opcional (SPCW110)
Verificación	32 zonas de verificación con un máx. de 4 cámaras IP y 32 dispositivos de audio.
Vídeo	Hasta 16 imágenes previas a la incidencia/16 posteriores a la incidencia (resolución JPEG 320 x 240, máx. 1 imagen/segundo)
Audio	Hasta 60 seg. previo/60 seg. posterior de grabación de audio
Bus de campo 1)	X-BUS sobre RS-485 (307 kb/s)
Número de dispositivos de campo 2)	Máx. 128 (32 teclados, 32 módulos de expansión de puerta, 64 módulos de expansión de entrada/salida)
Dispositivos de campo conectables	• Teclados: SPCK42x, SPCK62x • Módulos de expansión de puerta: SPCA210, SPCP43x • Módulos de expansión con E/S: SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	• 2 X-BUS (2 en punta 1 lazo) • 2 RS232 • 1 USB (conexión a PC) • SPC63xx: Adicionalmente 1 Ethernet (RJ45)
Contacto de tamper	• SPC6330: Tamper con muelle frontal, 2 entradas auxiliares de contacto de tamper • SPC6350: Interruptor de tamper frontal/trasero
Tensión de alimentación	Tipo A (por EN50131-1)
Voltaje de red	230 V CA, +10%/-15%, 50Hz
Fusible de red	• SPC6330: 250 mA T (pieza reemplazable en bloque de terminales de red) • SPC6350: 800 mA T (pieza reemplazable en bloque de terminales de red)
Consumo de energía	• SPC6330: Máx. 200mA a 230V CA • SPC6350: Máx. 500 mA a 230V CA
Corriente de funcionamiento	• SPC6330: Máx. 200mA a 12V CC • SPC6350: Máx. 210mA a 12V CC
Corriente de reposo	Controlador SPC63xx: Máx. 170 mA a 12 V CC (195 mA con RTB, 300 mA con GSM, 325 mA con RTB y GSM)
Voltaje de salida	• SPC6330: 13-14 V CC en condiciones normales (con alimentación de red CA y batería completamente cargada), mín. 10,5 V CC con alimentación de un dispositivo secundario (antes de cerrarse el sistema como protección contra descarga mínima de batería) • SPC6350: 13-14 V CC en condiciones normales (con alimentación de red CA y batería completamente cargada), mín. 10,5 V CC con alimentación de un dispositivo secundario (antes de cerrarse el sistema como protección contra descarga mínima de batería)

Activador de bajo voltaje	11 V CC
Protección contra sobretensión	• SPC6330: 15,7 V CC • SPC6350: 15 V CC nominal
Ondulación de pico a pico	Máx. 5% del voltaje de salida
Alim. auxiliar (nominal)	• SPC6330: Máx. 750mA a 12V CC • SPC6350: Máx. 2.200 mA a 12 V CC (8 salidas con fusibles por separado, 300 mA por salida)
Tipo de batería	• SPC6330: YUASA NP17-12FR (17 Ah) • SPC6350: YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) • SPC6350: FIAMM FGV22703 (12 V 27 Ah) Pila no incluida
Cargador de batería	SPC63xx: Máx. 24 h para el 80 % de capacidad de la batería
Protección de la batería	• SPC6330: Corriente limitada a 1 A (protegida por fusible), protección contra descarga mínima a 10,5 V CC ±3% • SPC6350: Corriente limitada a 2 A (protegida por fusible restablecible PTC), protección contra descarga mínima a 10,5 V CC, indicador de bajo voltaje a 11 V CC
Actualización de software	Actualización local y remota para controlador, periféricos y módems GSM/RTB.
Calibración	No se requieren comprobaciones de calibración (calibrada en fabricación)
Piezas reparables	• SPC6330: No hay piezas reparables • SPC6350: 8 fusibles de cristal (400 mA AT) para salidas de 12 V CC
Temperatura de servicio	de -10 a +50 °C
Humedad relativa	Máx. 90% (sin condensación)
Color	RAL 9003 (blanco señal)
Peso	• SPC6330: 6,400 kg • SPC6350: 18,600 kg
Dimensiones (An. x Al. x Pr.)	• SPC6330: 326 x 415 x 114 mm • SPC6350: 498 x 664 x 157 mm
Carcasa	• SPC6330: Carcasa de metal con bisagras (acero dulce de 1,2 mm) • SPC6350: Carcasa de metal (acero dulce de 1,5 mm)
La carcasa puede contener hasta	• SPC6330: 4 módulos de expansión adicionales (tamaño 150 x 82 mm) • SPC6350: 6 módulos de expansión adicionales (150 mm x 82 mm) o 1 controlador adicional + 4 módulos de expansión
Clasificación IP/IK	30/06
ATS	10
ATP	30

Perfiles de incidencias	20
Excepciones de incidencia	100
Perfiles de comandos	10

1) Máx. 400 m entre dispositivos/tipos de cable IYSTY 2 x 2 x Ø 0,6 mm (mín.), UTP cat 5 (núcleo sólido) o Belden 9829.

2) Se pueden direccionar más módulos de expansión de E/S en lugar de un teclado o un módulo de expansión de puerta, pero el número de entradas/salidas programables no puede exceder los límites especificados para el sistema.

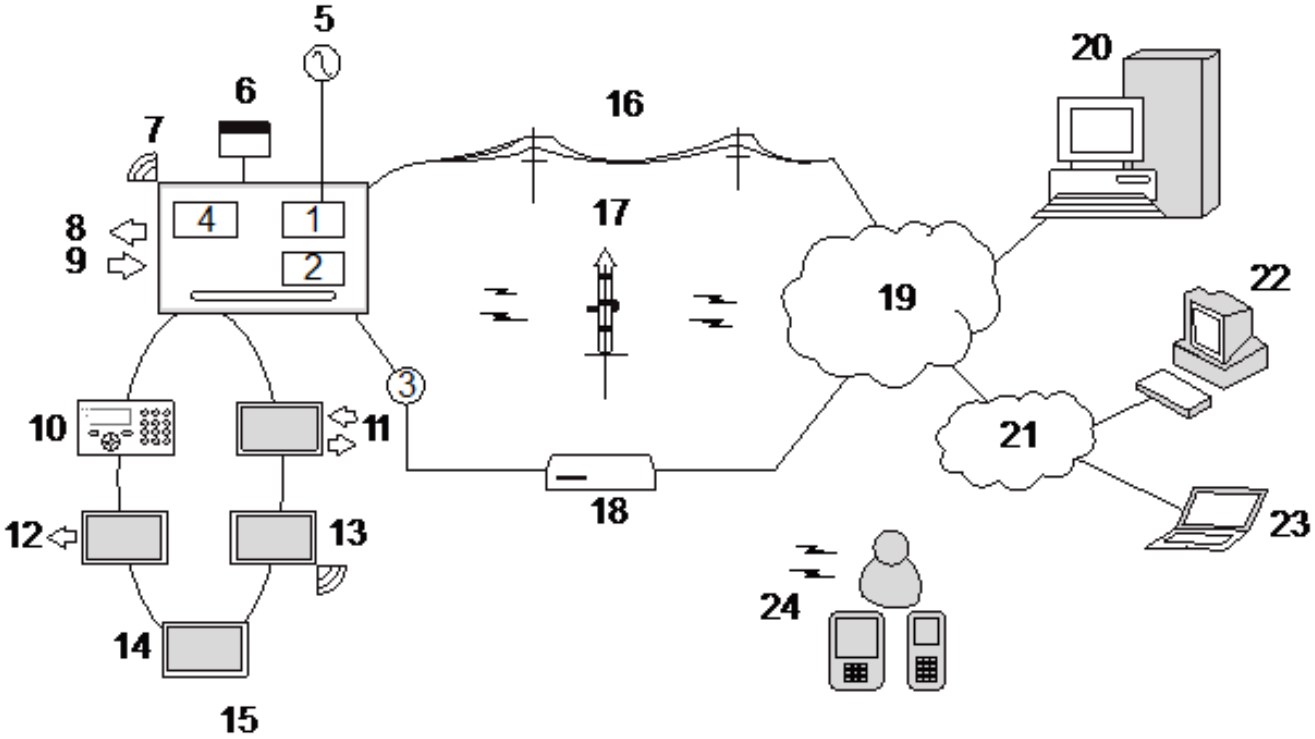
4.4 SPCP355.300

Número de zonas incorporadas	8
Resistencia RFL	Doble 4k7 (predeterminado), se pueden configurar otras combinaciones de resistencias
Salidas de relé	3 (conmutación de polo único, 30 V CC / máx. 1 A corriente de conmutación resistiva)
Salidas electrónicas	3 supervisadas (cada una de ellas máx. 400 mA corriente de conmutación resistiva),
Interfaces	X-BUS (entrada, salida, ramal)
Voltaje de red	230V CA, de +10 a -15%, 50Hz
Corriente de funcionamiento	Máx. 245 mA a 12 V CC (todos los relés activados)
Corriente de reposo	Máx. 195mA a 12V CC
Voltaje de salida	13-14 V CC en condiciones normales (con alimentación de red CA y batería completamente cargada),
Alim. auxiliar (nominal)	Máx. 2.360 mA a 12 V CC (8 salidas con fusibles por separado, máx. 300 mA por salida)
Tipo de batería	• YUASA NP24-12 (12 V 24 Ah) • Alarmcom AB1227-0 (12 V 27 Ah) • FIAMM FGV22703 (12 V 27 Ah) Pila no incluida
Contacto de tamper	Interruptor de tamper frontal/trasero
Temperatura de servicio	de 0 a +40°C
Carcasa	Carcasa de metal (acero dulce de 1,5mm)
Color	RAL 9003 (blanco señal)
Dimensiones	498 x 664 x 157 mm
Peso (sin baterías)	18,400 kg (carcasa con cubierta), 11,300 kg (carcasa sin cubierta)
Clasificación IP/IK	30/06

5 Introducción

El controlador de la serie SPC es un auténtico controlador híbrido con ocho zonas cableadas incorporadas que se comunican con dispositivos intrusos.

El diseño flexible del controlador permite combinar y sincronizar los componentes funcionales (RTB/GSM/RF) para mejorar la capacidad del sistema. Al utilizar este enfoque, el instalador puede garantizar una instalación eficiente con un cableado mínimo.



Visión general

Número	Descripción	Número	Descripción
1	RTB	13	Módulo de expansión vía radio
2	GSM	14	F.alimentación
3	Ethernet	15	Configuración en lazo
4	Receptor vía radio	16	Red RTB
5	Toma de CA general	17	Red GSM
6	Batería de 12V	18	Router de banda ancha
7	RF	19	Red
8	Salidas cableadas (6)	20	Central
9	Entradas cableadas (8)	21	LAN/WLAN
10	Teclados	22	Escritorio de servicio
11	Módulo de expansión IO	23	Usuario remoto
12	Módulo de expansión de salida	24	Interfaces móviles

6 Montaje de equipamiento del sistema

Este capítulo abarca:

6.1 Montaje de una carcasa G2

La carcasa G2 del SPC se suministra con una cubierta metálica o de plástico. La cubierta está unida a la base de la carcasa por dos tornillos de fijación ubicados en la parte superior y en la inferior de la cubierta delantera.

Para abrir la carcasa, retire ambos tornillos con el destornillador adecuado y levante la cubierta directamente desde la base.

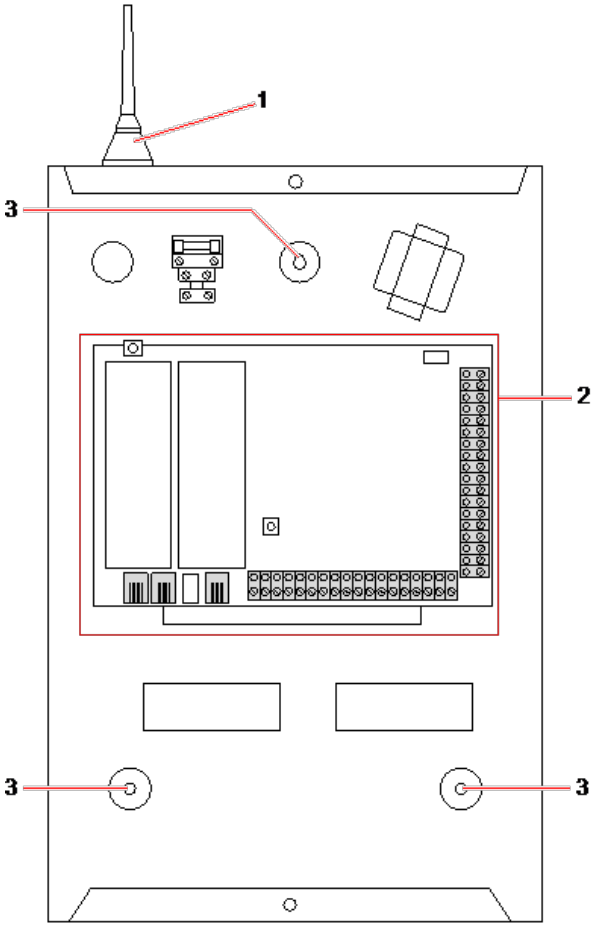
La carcasa G2 incluye la placa de circuito impreso (PCB) del controlador, montada sobre cuatro soportes. Se puede montar un módulo de entrada/salida opcional directamente debajo de la PCI del controlador. Se puede colocar una batería con capacidad máxima de 7 Ah debajo del controlador.

Debe instalarse una antena exterior opcional en carcasas con tapa metálica si se requiere la funcionalidad vía radio. Si se coloca una antena en la unidad, debe habilitarse en el firmware.

La carcasa G2 del SPC cuenta con tres orificios roscados para el montaje en pared de la unidad.

Para montar la carcasa en la pared, retire la cubierta y coloque el orificio para el tornillo de fijación inicial en la parte superior de la carcasa. Marque, en la ubicación deseada de la pared, la posición del orificio de este tornillo y taladre el orificio. Atornille la unidad a la pared y marque la posición de los dos orificios de los tornillos inferiores con la unidad alineada verticalmente.

Se recomienda el uso de tornillos con un vástago de 4 a 5 mm, un diámetro de cabeza mínimo de 8 mm y un largo mínimo de 40 mm para el montaje de la carcasa. Es posible que se requieran más puntos de fijación según la construcción de la pared.



Carcasa estándar

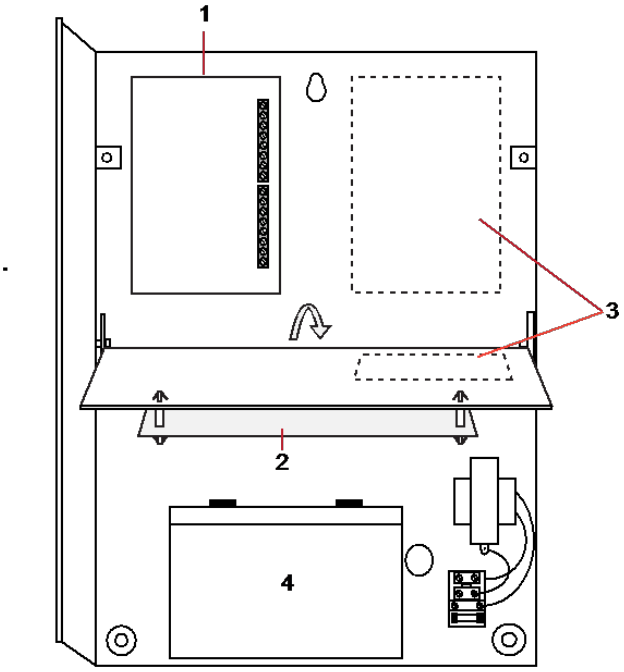
Número	Descripción
1	Antena vía radio
2	Controlador SPC
3	Orificios de los tornillos para el montaje mural

6.2 Montaje de una carcasa G3

La carcasa G3 del SPC se suministra con una cubierta frontal metálica. La cubierta está unida a la base de la carcasa mediante bisagras y asegurada con un tornillo en la parte derecha de la cubierta delantera.

Para abrir la carcasa, retire los tornillos con el destornillador adecuado y abra la cubierta delantera.

La carcasa G3 contiene la PCI (Placa de Circuito Impreso) del controlador montada sobre un soporte de montaje con bisagras. Los módulos de expansión y las fuentes de alimentación se pueden montar en la parte inferior del soporte de montaje con bisagras y también en la pared trasera de la carcasa, debajo del soporte de montaje.

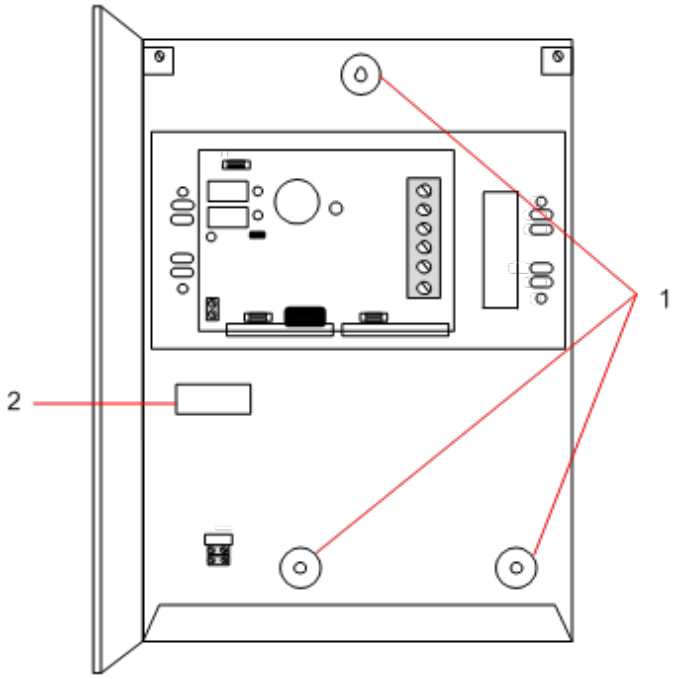


Número	Descripción
1	Módulos de expansión / fuente de alimentación
2	Controlador
3	Módulos de expansión / fuente de alimentación
4	Batería

Debe instalarse una antena exterior opcional en carcasas con tapa metálica si se requiere la funcionalidad vía radio. Si se coloca una antena en la unidad, debe habilitarse en el firmware.

La carcasa G3 del SPC cuenta con tres orificios roscados para el montaje en pared de la unidad (vea el punto 1 a continuación).

Se recomienda el uso de tornillos con un vástago de 4 a 5 mm, un diámetro de cabeza mínimo de 8 mm y un largo mínimo de 40 mm para el montaje de la carcasa. Es posible que se requieran más puntos de fijación según la construcción de la pared.



Para montar la carcasa en la pared:

1. Abra la cubierta y coloque el orificio para el tornillo de fijación inicial en la parte superior de la carcasa.
2. Marque, en la ubicación deseada de la pared, la posición del orificio de este tornillo y taladre el orificio.
3. Atornille la unidad a la pared y marque la posición de los dos orificios de los tornillos inferiores con la unidad alineada verticalmente.

Requisitos de tamper trasero

Es posible que las normas locales exijan contar con un interruptor de tamper trasero.

El interruptor de tamper trasero se suministra junto con los paneles SPC en carcasas G3, y también está disponible como extra opcional con un kit de montaje (SPCY130). Los paneles G3 según la norma EN50131 (SPCxx3x.x20) se suministran, por defecto, con un kit de tamper trasero.

6.2.1 Montaje de un kit de tamper trasero

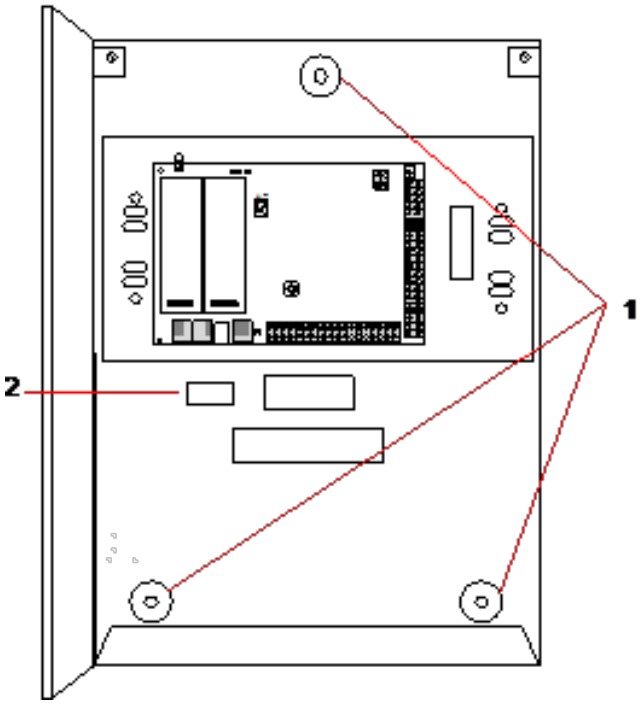
El kit de tamper trasero del SPC incluye centrales de control SPC y fuentes de alimentación con la opción de usar un tamper trasero, además un tamper delantero.

El kit de tamper trasero incluye las siguientes partes:

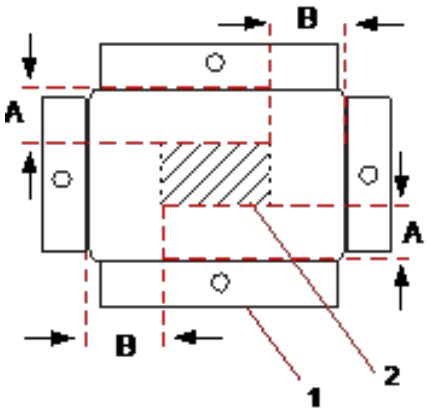
- Interruptor de tamper
- Conectores para enchufar el interruptor de tamper trasero al controlador
- Placa de fijación en pared

Montaje de la placa de fijación en pared

1. Coloque el SPC en la posición adecuada sobre la pared utilizando los tres puntos de fijación (vea el punto 1 a continuación).



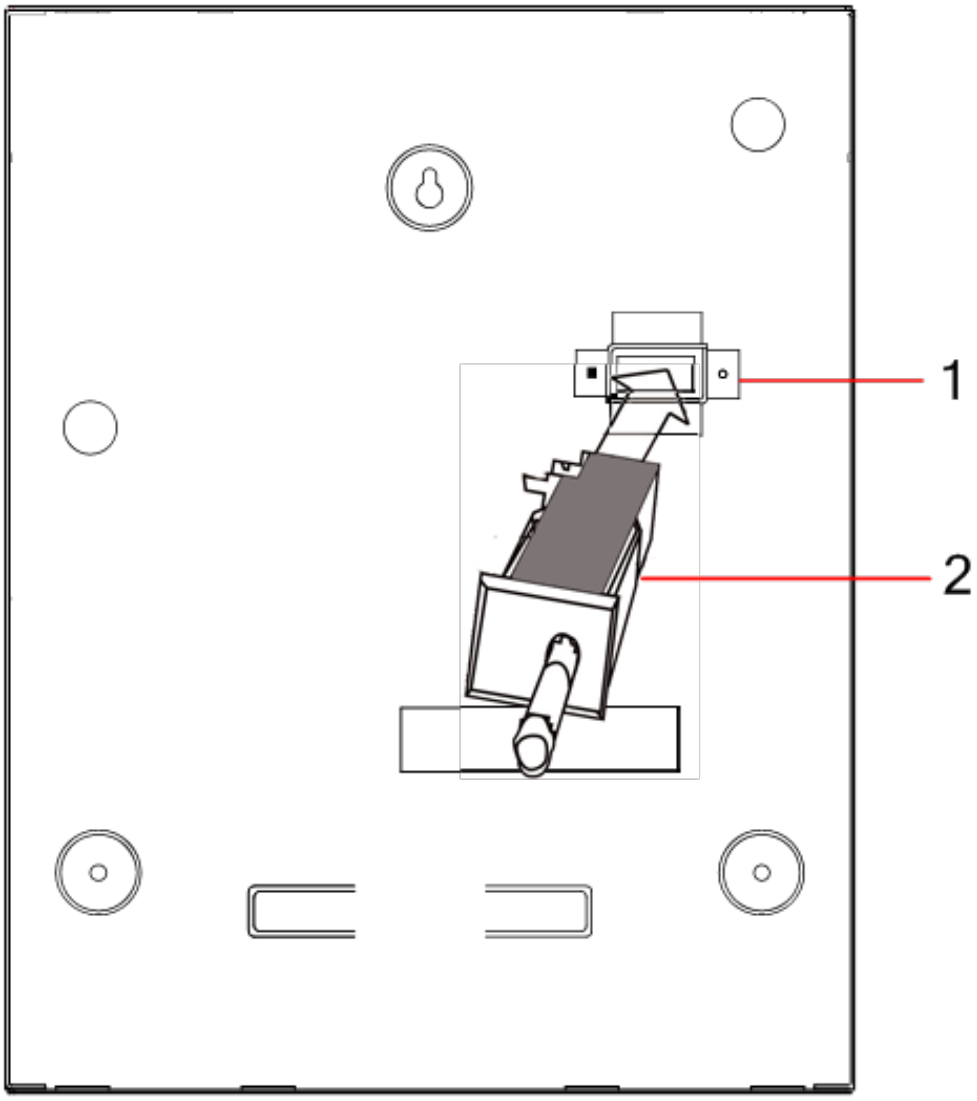
2. Dibuje una línea alrededor del recorte del tamper trasero (vea el punto 2 a continuación) para que sirva como guía para la placa sobre la pared donde se fijará. Retire la carcasa de la pared.
3. Coloque la placa de pared (vea el punto 1 a continuación) sobre la pared, centrándola con precisión alrededor del rectángulo dibujado previamente (vea el punto 2 a continuación).



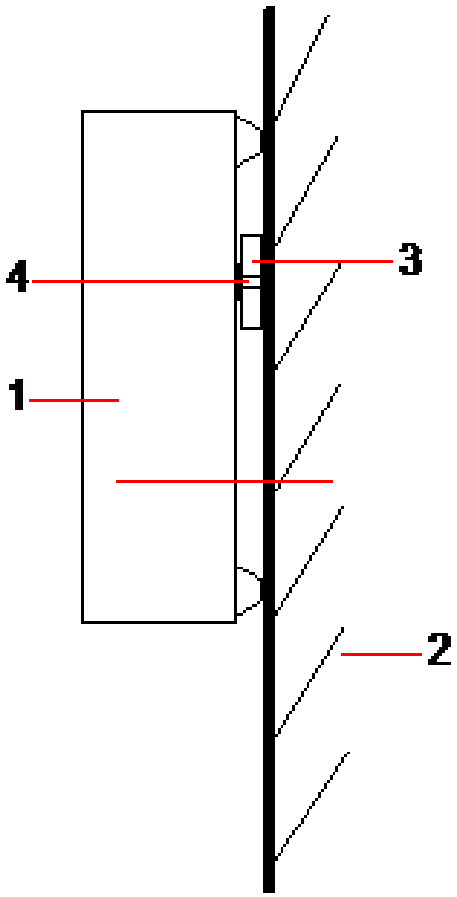
4. Asegúrese de que los cuatro rebordes sobre la placa de pared estén al ras de la pared.
5. Marque los cuatro puntos de fijación en la placa de pared.
6. Perfore y utilice los tornillos adecuados (máx. 4 mm) para el sustrato de la pared.
7. Coloque la placa contra la pared.

Colocación del interruptor de tamper trasero

1. Inserte el interruptor de tamper (vea el punto 2 a continuación) en la parte trasera de la carcasa para que el émbolo esté hacia afuera (vea el punto 1 a continuación).



2. Coloque la carcasa sobre la pared utilizando los tres puntos de fijación que retiró previamente (vea el punto 2 a continuación). Asegúrese visualmente de que la placa esté al ras de la carcasa de metal.



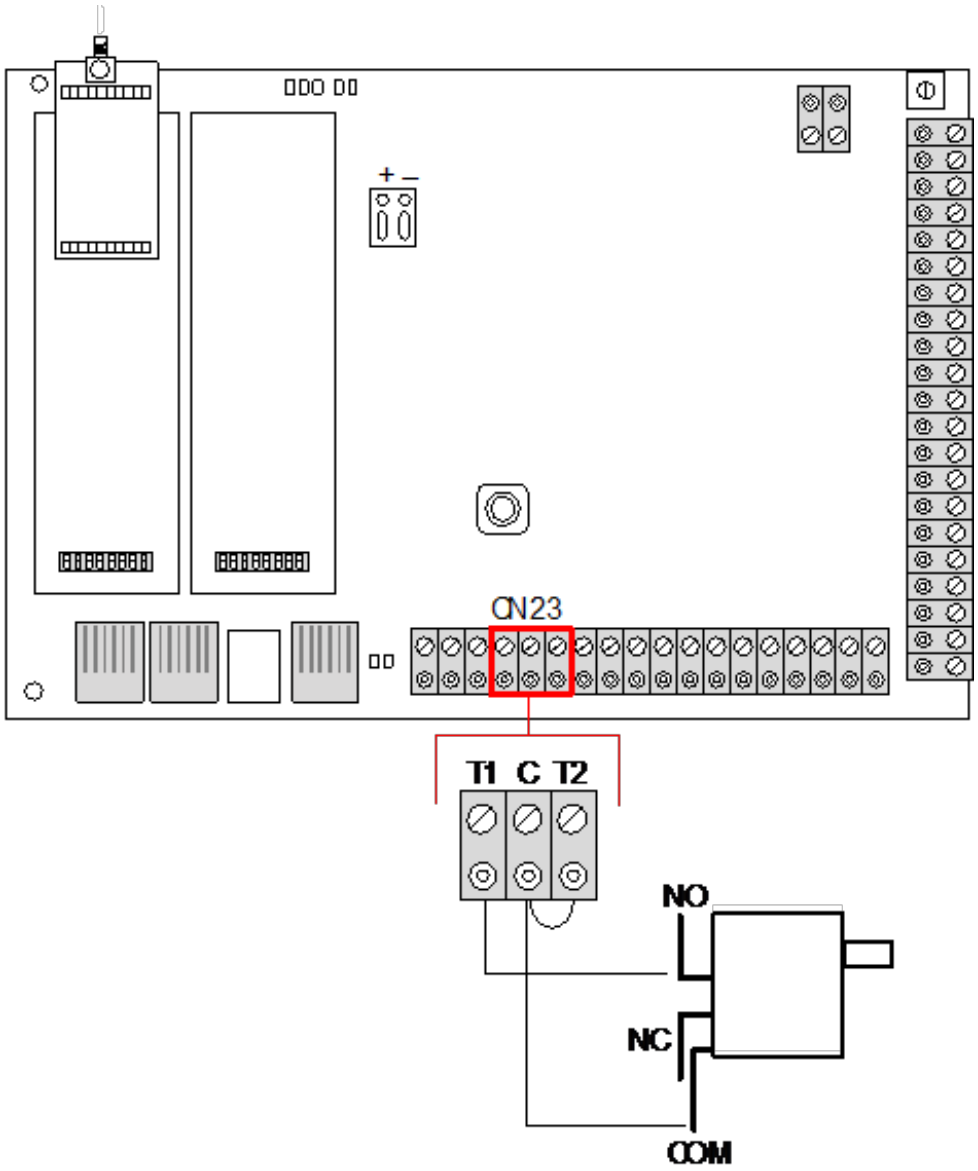
Número	Descripción
1	Carcasa
2	En pared
3	Placa de fijación en pared
4	Interruptor de tamper

ADVERTENCIA: Si la placa de fijación en pared no está alineada con precisión, es posible que la carcasa no se asiente correctamente en los puntos de fijación.

Cableado del interruptor de tamper trasero a la central de control

Todas las centrales de control tienen entradas adicionales configuradas como entradas de tamper diseñadas para cablear el interruptor de tamper y no requieren programación.

El sistema detectará este interruptor de tamper como ‘Tamper aux. 1’.



1. Conecte NA en el interruptor de tamper a T1 en el controlador.
2. Conecte COM en el interruptor de tamper a C en el controlador. Asegúrese de no haber retirado el puente T2.
3. Una vez cableado el interruptor de tamper, se puede poner en marcha el controlador de forma normal.

6.2.2 Instalación de la batería de conformidad con EN50131

Para cumplir con la norma EN50131, se debe retener la batería dentro de la carcasa para detener el movimiento. Esto se logra al doblar las pestañas en la parte trasera de la carcasa con bisagras para mantener la batería en su lugar.

Si se utiliza una batería de 7 Ah, entonces esta tiende hacia el lado izquierdo de la carcasa y se debe doblar la pestaña de la parte inferior hacia la batería.

Si se utiliza una batería de 17 Ah, entonces esta tiende hacia el lado derecho de la carcasa y se debe doblar la pestaña del medio hacia la batería.

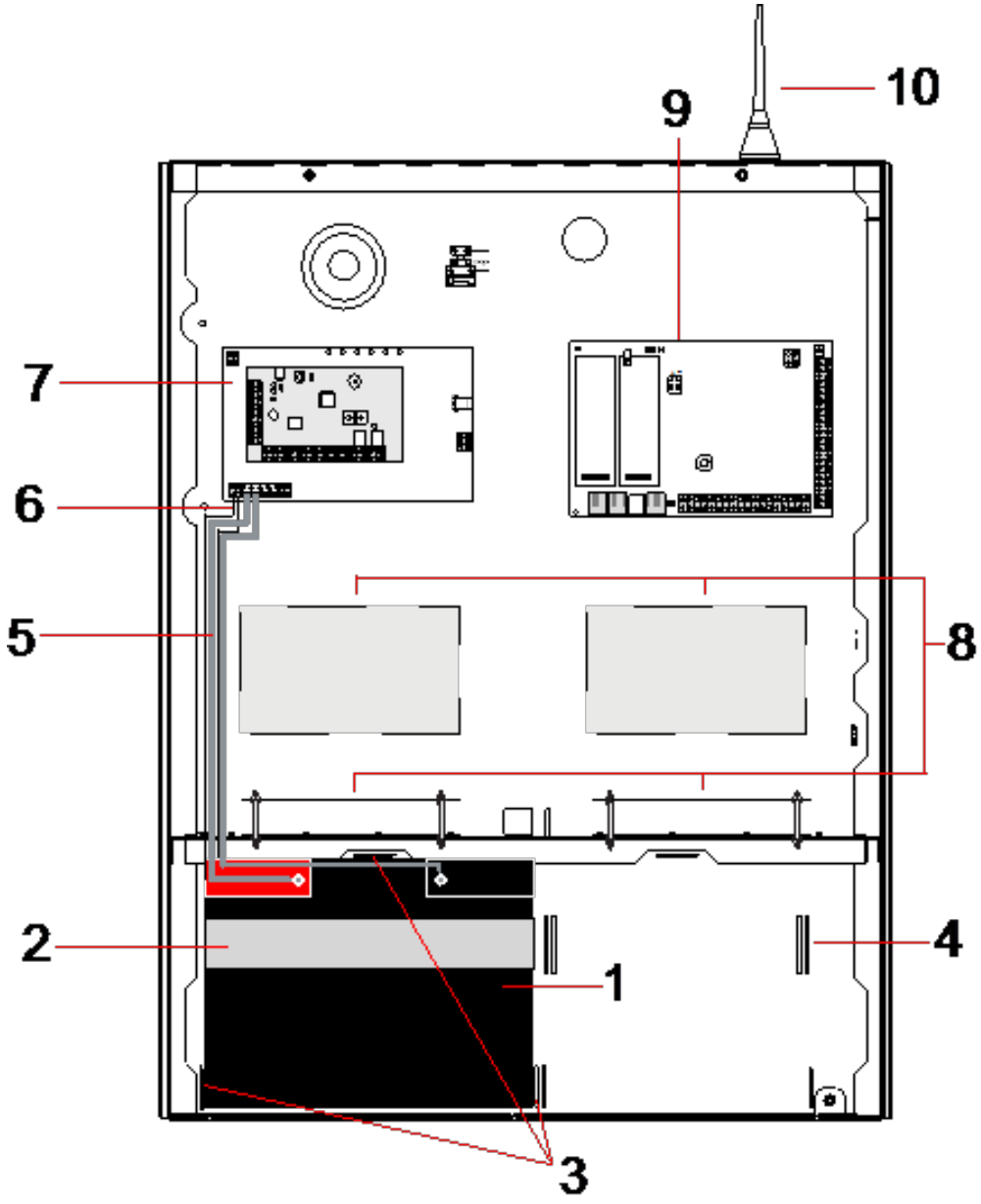
Se debe tener cuidado al doblar las pestañas de la batería para no dañarla. Si se perciben indicios de daño de la batería o hay una fuga de electrolitos, debe descartar la batería de conformidad con lo establecido por las regulaciones actuales y usar una nueva batería.

6.3 Montaje de una carcasa G5

La carcasa G5 del SPC consta de una base metálica y una cubierta frontal. La cubierta está unida a la base de la carcasa por cuatro tornillos de fijación ubicados en la parte superior y en la inferior de la cubierta delantera.

Para abrir la carcasa, retire todos los tornillos con el destornillador adecuado y levante la cubierta directamente desde la base.

La carcasa G5 incluye la placa de circuito impreso (PCB) del controlador y la fuente de alimentación inteligente SPCP355.300, ambas montadas sobre cuatro soportes. Un módulo de expansión de 8 entradas / 2 salidas está montado encima de la fuente de alimentación. Se incluyen cuatro soportes adicionales para ofrecer la opción de montar el módulo de expansión de 8 entradas/2 salidas debajo de la placa de la fuente de alimentación en la carcasa G5. También pueden montarse módulos de expansión adicionales en la carcasa tal como se muestra en la siguiente figura.



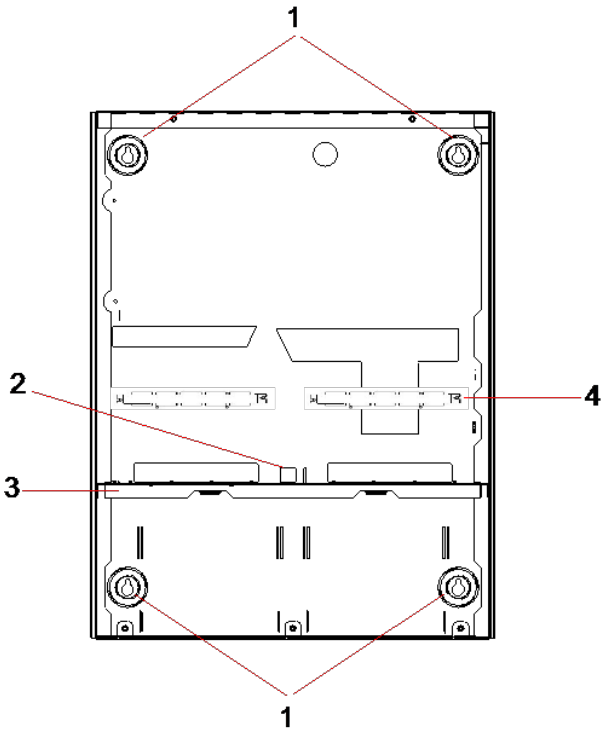
Número	Descripción	Número	Descripción
1	Batería	6	Conductores de temperatura de la batería

Número	Descripción	Número	Descripción
2	Correa para la batería	7	F.alimentación
3	Lengüetas de fijación	8	Posiciones para módulos de expansión opcionales
4	Orificios para la correa	9	Controlador
5	Conductores de la batería	10	Antena

En el compartimento de la batería, en la parte inferior de la carcasa, se pueden alojar dos baterías, con una capacidad máxima de 27 Ah.

Si se necesita la funcionalidad vía radio, se debe instalar una antena externa opcional en la carcasa metálica. Hay orificios troquelados disponibles en tres posiciones, en la parte superior de la carcasa, donde se puede instalar la antena. Si se coloca una antena en la unidad, debe habilitarse en el firmware.

La carcasa G5 del SPC cuenta con cuatro orificios roscados para el montaje mural de la unidad.



Número	Descripción
1	Orificios de fijación en las esquinas
2	Sección de tamper
3	Estante de separación del compartimento de la batería
4	Abertura de la ranura de telecomunicaciones

6.3.1 Protección de tamper

El interruptor de tamper y el soporte de tamper trasero están fijados a la carcasa. El interruptor, si se utiliza solo, sirve únicamente como tamper frontal y, si se utiliza con el soporte de tamper trasero, como protección de tamper frontal y trasero. Dependiendo de las normas locales, se requerirá una protección de tamper trasero o frontal.

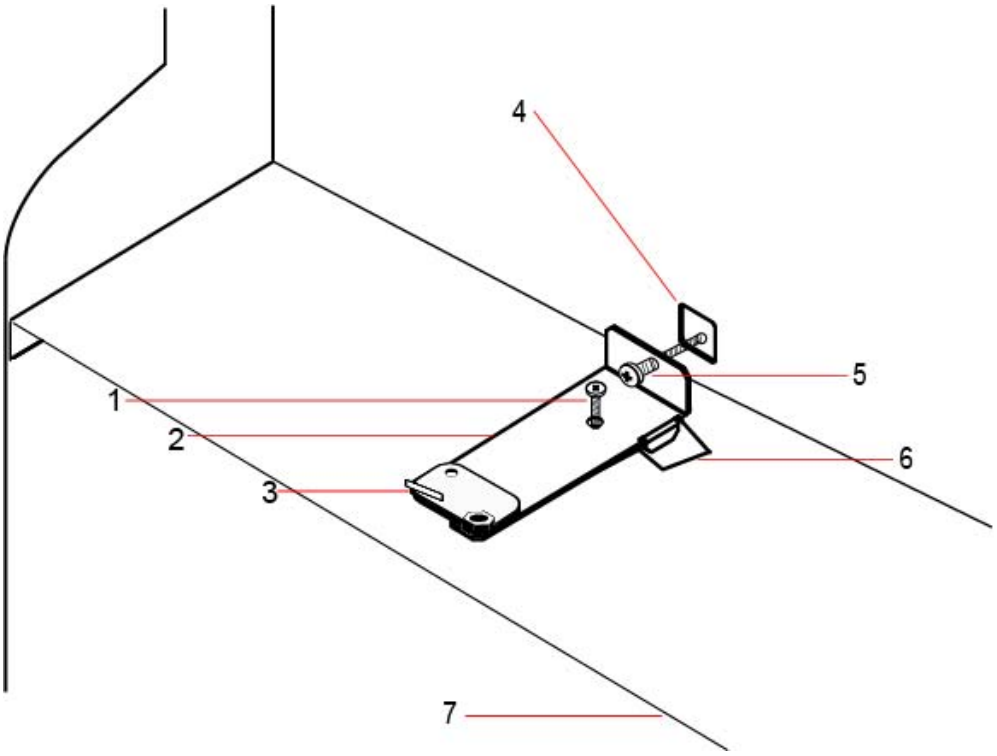
El soporte de tamper queda fijado firmemente a su sitio mediante un tornillo de fijación. Recuerde retirar este tornillo si el sistema se pone en servicio con protección de tamper trasero. No retire este tornillo si se utiliza únicamente el tamper frontal.

6.3.2 Montaje de la carcasa con protección de tamper

Para el montaje de la carcasa:

1. Con la plantilla de montaje incluida en el suministro, marque las cuatro posiciones de taladrado para fijar la carcasa a la pared.
2. Taladre los orificios e introduzca los tornillos adecuados (vea plantilla adjunta) en la pared. Deje que los tornillos sobresalgan 1,5 cm de la pared.
3. La carcasa G5 está preconfigurada para tamper frontal únicamente. Si desea configurar la carcasa para tamper frontal y trasero, retire el tornillo de fijación del tamper frontal (elemento 1).

   El soporte de tamper se desplaza al extremo derecho de la ranura de orientación (elemento 6).
4. Monte la carcasa G5 en la posición adecuada en la pared y apriete los cuatro tornillos de montaje. Asegúrese de que la carcasa quede a ras con la superficie de la pared.
5. Mueva el soporte de tamper hacia el extremo izquierdo de la ranura de orientación y apriete el tornillo de tamper trasero (elemento 5) a la pared. El soporte de tamper debe quedar perpendicular a la pared trasera de la carcasa.



6. Instale la tapa sobre la carcasa para comprobar la conexión del interruptor de tamper. Levante la tapa aproximadamente 1mm para activar el interruptor de tamper.

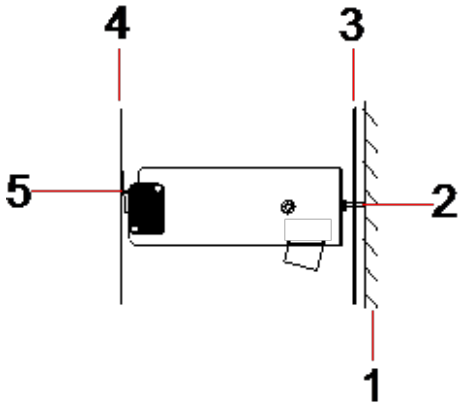
Número	Descripción	Número	Descripción
1	Tornillo de fijación de tamper frontal	5	Tornillo de tamper trasero
2	Soporte de tamper	6	Ranura de orientación
3	Interruptor de tamper	7	Estante de separación del compartimento de la batería

Número	Descripción	Número	Descripción
4	Abertura para el tamper trasero		

ADVERTENCIA: Si el tornillo de tamper trasero no está bien fijado contra la pared, la protección de tamper puede verse afectada. Si se retira o se desplaza la carcasa de la pared, se debe volver a comprobar el correcto funcionamiento del contacto del tamper trasero, y reajustarse si es necesario.

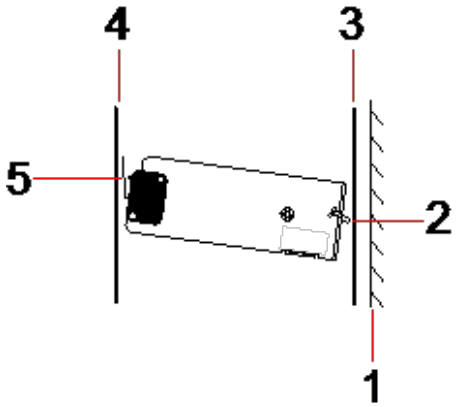
6.3.2.1 Funcionamiento del tamper

Interruptor de tamper - normal



Número	Descripción
1	En pared
2	Tornillo de tamper trasero
3	Pared trasera de la carcasa
4	Tapa de la carcasa
5	Contacto del interruptor de tamper cerrado

Interruptor de tamper - desplazado



Número	Descripción
1	En pared

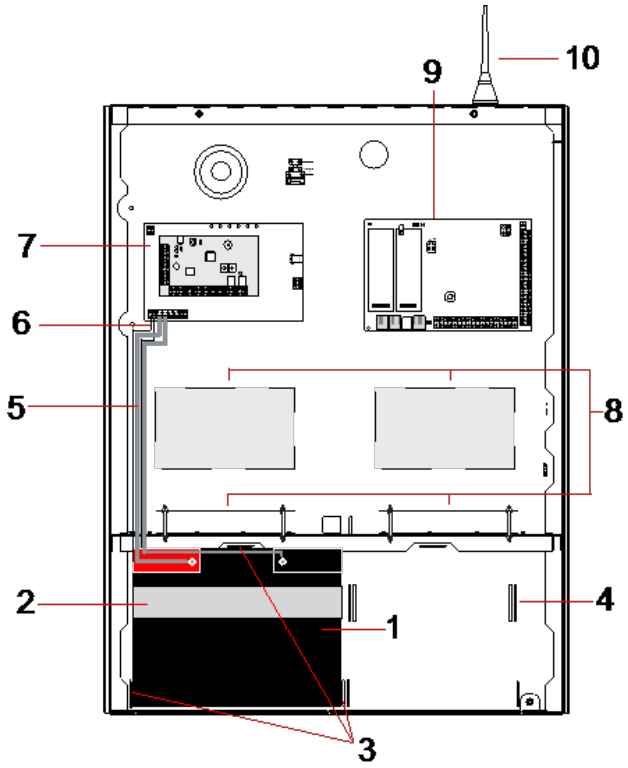
Número	Descripción
2	Tornillo de tamper trasero
3	Pared trasera de la carcasa
4	Tapa de la carcasa
5	Contacto del interruptor de tamper abierto

Si la carcasa se retira de la pared o se desplaza, el tornillo de soporte de tamper ya no queda seguro contra la pared, haciendo pivotar el soporte. Esto hace que el interruptor de tamper se salga de la tapa y abra el contacto del interruptor.

ADVERTENCIA: Si el tornillo del soporte de tamper no está bien fijado contra la pared, la protección de tamper puede verse afectada.

6.3.3 Instalación de las baterías

Si se utilizan dos baterías en la carcasa G5, se recomienda que ambas tengan el mismo amperaje.



Número	Descripción	Número	Descripción
1	Batería	6	Conductor de temperatura de la batería
2	Correa de sujeción	7	F.alimentación
3	Lengüetas de sujeción de la batería	8	Posiciones para módulos de expansión opcionales

Número	Descripción	Número	Descripción
4	Orificios para la correa	9	Controlador
5	Conductores de la batería	10	Antena

Para instalar las baterías:

1. Coloque las baterías en el compartimento para baterías.
2. Presione las lengüetas metálicas de la parte superior y de ambos lados hacia las baterías.
3. Fije las baterías a la carcasa mediante una correa para la batería. Asegúrese de que la correa queda enhebrada a través de los orificios situados en la parte trasera del compartimento de la batería y alrededor de la batería, con los dos extremos de la correa en la parte frontal de la batería.
4. Abroche firmemente los dos extremos de la correa mediante el cierre de Velcro. Compruebe que la correa queda bien apretada alrededor de la batería.
5. Conecte un extremo de los conectores de la batería con los terminales positivo y negativo de la batería, y los otros extremos con las entradas positiva y negativa correspondientes de la fuente de alimentación.

PRECAUCIÓN: Al instalar la batería, conecte siempre primero el conector positivo (+) a la batería antes de conectar el negativo (-). Al retirar la batería, retire siempre primero el conector negativo (-) antes de retirar el positivo (+).

6. Conecte los extremos sueltos de los conectores de supervisión de temperatura adjuntos a las entradas de supervisión de temperatura de la batería en la fuente de alimentación.

6.4 Montaje de un teclado

Consulte las instrucciones de instalación correspondientes.

Encontrará las guías de instalación disponibles en http://www.spcsupportinfo.com/connectspcdata/userdata.

6.5 Montaje de un módulo de expansión

Consulte las instrucciones de instalación correspondientes.

Encontrará las guías de instalación disponibles en http://www.spcsupportinfo.com/connectspcdata/userdata.

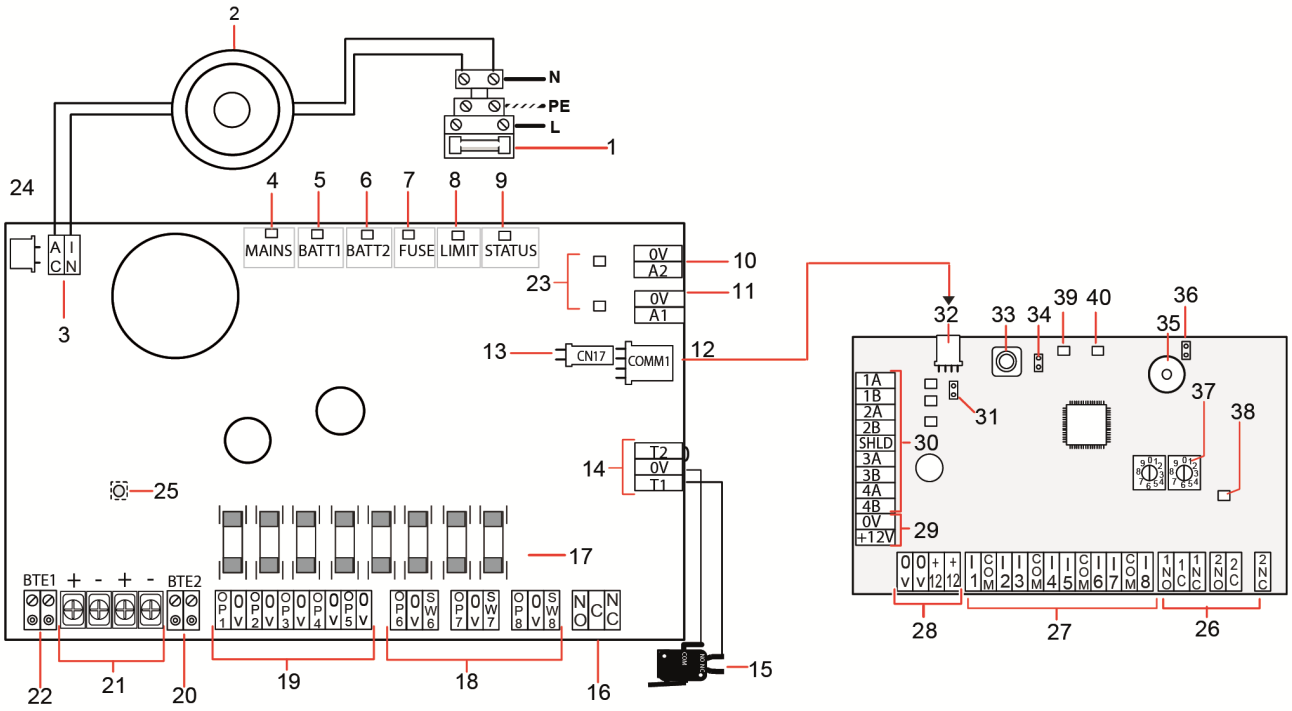
7 Fuente de alimentación inteligente

En esta sección se describen los componentes y el cableado de la fuente de alimentación inteligente.

7.1 Fuente de alimentación inteligente SPCP355.300

La fuente de alimentación inteligente SPCP355.300 es una fuente de alimentación combinada con un módulo de expansión de 8 entradas / 2 salidas dentro de una carcasa G5. La fuente de alimentación cuenta con el respaldo de baterías de 2x24Ah o de 2x27 Ah, y posee ocho salidas de potencia y dos salidas lógicas.

El módulo de expansión supervisa la fuente de alimentación controlando las sobreintensidades, los fallos en los fusibles, la tensión alterna, las comunicaciones y la potencia de salida de la batería. El módulo de expansión es alimentado por la fuente de alimentación y recibe los datos de esta a través de un cable conector. También actúa como interfaz con el controlador SPC a través del X-BUS SPX.



Número	Descripción
Fuente de alimentación inteligente SPCP355.300	
1	Entrada de red C.A. y bloque de fusibles
2	Transformador de entrada
3	AC IN: Entrada de alimentación de CA
4	MAINS: LED de alimentación de red eléctrica
5	BATT1: LED de estado de carga de batería 1
6	BATT2: LED de estado de carga de batería 2

Número	Descripción
7	FUSE: LED de fallo de fusible
8	LIMIT: LED de límite de corriente
9	STATUS: LED de estado
10	A2: Salida de alimentación de 14,5 V. • No respaldado por batería • Protegido con fusible restablecible PTC, 300 mA (elemento 23 en imagen anterior)
11	A1: Se conecta con la entrada de alimentación (+/-) en el SPC5350/6350.
12	COMM1: Interfaz de 4 clavijas del módulo de expansión. Se conecta con el elemento 32, conexión de alimentación y datos, en la imagen anterior con un cable directo.
13	Referencia de reloj: se conecta con la referencia de reloj en el SPC5350/6350.
14	T1, T2: Entradas de interruptor de tamper. Conéctelas al interruptor de tamper frontal/trasero. Consulte *Montaje de la carcasa con protección de tamper* en la página 57.
15	Interruptor de tamper frontal/trasero. Consulte *Montaje de la carcasa con protección de tamper* en la página 57.
16	NA/NC: Salida de relé lógica configurable NA/NC. Consulte *Cableado de las salidas* en la página 68 para obtener más información.
17	Fusibles de cristal: fusibles T de 400mA para salidas 1-8.
18	OP 6–8 y SW 6–8: Salidas de alimentación (OP) y salidas lógicas (SW) combinadas. Salidas de alimentación estándar de 12 V CC combinadas con salidas lógicas configurables de drenaje abierto (4k7 RFL con/sin supervisión).
19	OP 1–5: Salidas de alimentación estándar de 12 V CC. Para más información, consulte la nota de advertencia debajo de esta tabla.
20	BTE2: Entrada de supervisión de temperatura de batería 2.
21	BATT1 y BATT2: Conectores de batería 1 y 2.
22	BTE1: Entrada de supervisión de temperatura de batería 1.
23	Fusibles PTC: Fusibles con amperaje de 300 mA. Para protección de las salidas A1 y A2. Para obtener más información consulte *Recuperación del sistema* en la página 71.
24	Fusible PTC: Fusible con un amperaje de 5 A. Protege la entrada de alimentación de C.A. (elemento 3 en la imagen anterior). Para obtener más información consulte *Recuperación del sistema* en la página 71.
25	Interruptor de arranque de fuente de alimentación: Para más información, consulte *Recuperación del sistema* en la página 71.
Módulo de expansión	

Número	Descripción
26	NA/NC: Salidas de relé lógicas. El módulo de expansión cuenta con dos salidas de relé lógicas configurables NA/NC. Para obtener más información, consulte *Cableado de las entradas* en la página 67.
27	I 1–8: Entradas. El módulo de expansión cuenta con 8 entradas incorporadas que se pueden configurar como zonas de alarma de intrusión en el sistema SPC. Para obtener más información, consulte *Cableado de las entradas* en la página 67.
28	Fuente de alimentación auxiliar de 12 V: No utilizar. El módulo de expansión recibe la alimentación a través de COMM1 en la fuente de alimentación inteligente SPCP355.300.
29	Potencia de entrada de X-BUS: No utilizar. El módulo de expansión recibe la alimentación a través de COMM1 en la fuente de alimentación inteligente SPCP355.300.
30	Interfaz X-BUS: El bus de comunicaciones conecta módulos de expansión en el sistema SPC.
31	Jumper de terminación: Este jumper siempre está colocado por defecto. Para obtener más información, consulte *Cableado de la interfaz X-BUS* en la página 66.
32	Interfaz de 4 clavijas de fuente de alimentación: Se conecta con COMM1 en la fuente de alimentación inteligente SPCP355.300 (elemento 12 en la imagen anterior), conector de alimentación y datos, con un cable directo.
33	Interruptor de tamper frontal: No se utiliza. El tamper frontal/trasero conectado a las tomas T1 y T2 de la fuente de alimentación inteligente SPCP355.300 es el único tamper necesario para esta instalación.
34	JP1: Se debe instalar el bypass de tamper frontal.
35	Zumbador: Activado para localizar el módulo de expansión. Consulte *Localizar* en la página 138 para obtener más información.
36	JP6: Bypass de tamper trasero. Se debe instalar.
37	Interruptores de direccionamiento manual: Activan la configuración manual del ID del módulo de expansión.
38	LED de estado de X-BUS: Indica el estado del X-BUS cuando el sistema está en modo TÉCNICO COMPLETO, como se muestra a continuación: • Parpadeo lento (cada 1,5 segundos): Estado de comunicaciones de X-BUS OK. • Parpadeo rápido (cada 0,2 segundos): Indica una de las siguientes opciones: – Indica el último módulo de expansión en línea para configuraciones en punta. – Indica un problema de comunicación entre dos módulos de expansión. Si hay dos módulos de expansión parpadeando rápidamente, el problema está entre estos dos módulos de expansión.
39	LED: Sin utilizar.
40	LED de estado de F.A.

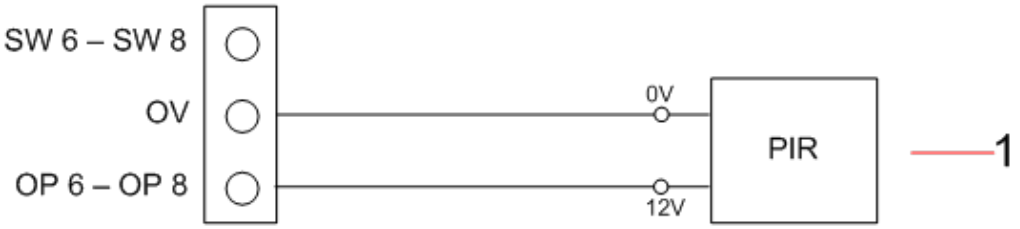
ADVERTENCIA: El consumo máximo de corriente de carga combinado de todas las salidas de 12 V CC (OP 1-8) más COMM1 no debe sobrepasar los 2,4 A. Cada salida individual, y la salida A2, no debe sobrepasar los 300 mA. Si la corriente del dispositivo requiere más de 300 mA, se recomienda disponer las salidas en paralelo.

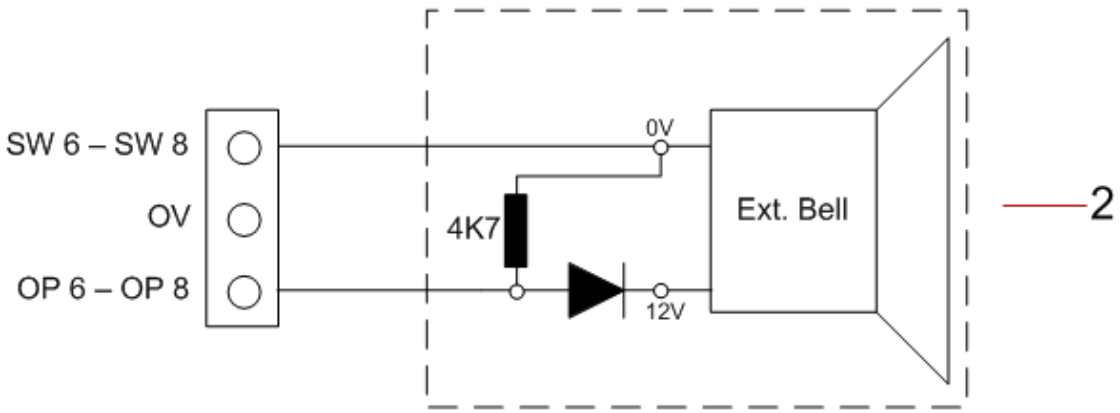
Añadir módulos de expansión adicionales

Si se añaden módulos de expansión adicionales a la carcasa G5, debe asegurarse de que los tampers frontal y trasero estén desactivados instalando los jumpers apropiados. En una carcasa G5, la propia carcasa y la fuente de alimentación inteligente SPCP355.300 gestionan los tampers frontal y trasero.

7.1.1 Salidas supervisadas

La fuente de alimentación inteligente SPCP355.300 admite tres salidas lógicas de drenaje abierto que se pueden supervisar para la detección de tamper. La detección de tamper de salida está habilitada en la configuración. La detección de tamper de salida se habilita conectando una RFL de 4k7 en paralelo con el dispositivo de carga, como una sirena exterior. También se necesita un diodo de potencia (1N4001 por ejemplo, o similar), si no hay uno ya en el dispositivo externo.





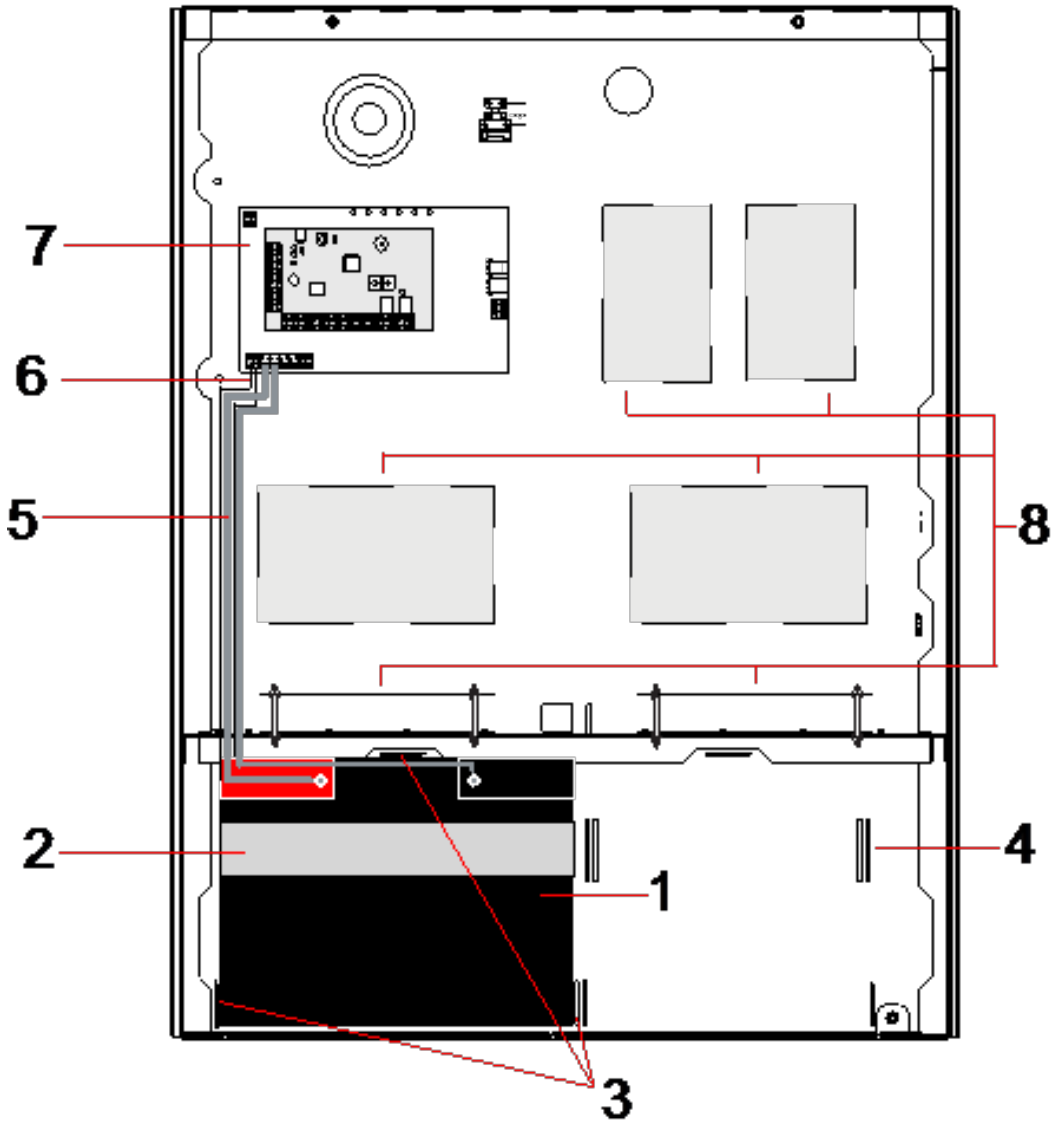
Número	Descripción
1	Salida de alimentación estándar de 12 V
2	Salida lógica conmutada configurable y supervisada de 12 V C.C.

7.1.2 Baterías

Esta sección abarca:

7.1.2.1 Instalación de las baterías

En esta sección se describe la instalación de baterías para la fuente de alimentación inteligente SPCP355.300 y la carcasa G5.



Número	Descripción
1	Batería
2	Correa para la batería
3	Orificios de montaje
4	Orificios para la correa
5	Conductores de la batería
6	Conductores de temperatura de la batería
7	Fuente de alimentación / módulo de expansión
8	Posiciones de montaje para módulos de expansión adicionales.

Se recomienda utilizar dos baterías. Estas baterías deben ser del mismo tipo y la misma capacidad.

1. Instale las baterías en el compartimento para baterías.
2. Asegúrelas con las correas para batería incluidas en el suministro, asegurándose de que la correa queda enhebrada a través de los orificios situados en la parte trasera del compartimento de la batería y alrededor de la propia batería.
3. Asegure los dos extremos de la correa en la parte frontal de la batería, asegurándose de que la correa quede apretada firmemente.
4. Conecte los conectores de la fuente de alimentación inteligente SPCP355.300 a las baterías en el siguiente orden:

   - En primer lugar, conecte el cable positivo (rojo).

   - En segundo lugar, conecte el cable negativo (negro).

PELIGRO: Al retirar los conectores de la batería, desconecte siempre primero el conector negativo (negro) antes de desconectar el conector positivo (rojo).

7.1.2.2 Comprobación de voltaje de la batería

La fuente de alimentación inteligente SPCP355.300 realiza una comprobación de carga en cada batería colocando una resistencia de carga en los terminales de la batería y midiendo el voltaje resultante. Esta comprobación de la batería se realiza cada cinco segundos.

7.1.2.3 Protección contra descarga mínima

Si la alimentación de la red eléctrica a la fuente de alimentación inteligente SPCP355.300 falla durante un tiempo prolongado, cada batería suministra alimentación a las salidas de potencia de 12 V C.C. de la fuente de alimentación durante un tiempo limitado. Las baterías pueden llegar a descargarse. Para evitar que las baterías se descarguen hasta el punto de que no se puedan recuperar, la fuente de alimentación inteligente SPCP355.300 desconecta la batería si el voltaje medido cae por debajo de los 10,5 V CC. A continuación, tras restaurarse la alimentación de la red principal, la batería se puede recargar.

7.1.2.4 Tiempos de espera de la batería

Consulte *Calcular los requisitos de alimentación de la batería* en la página 378 para obtener información sobre batería en espera.

7.1.3 Cableado de la interfaz X-BUS

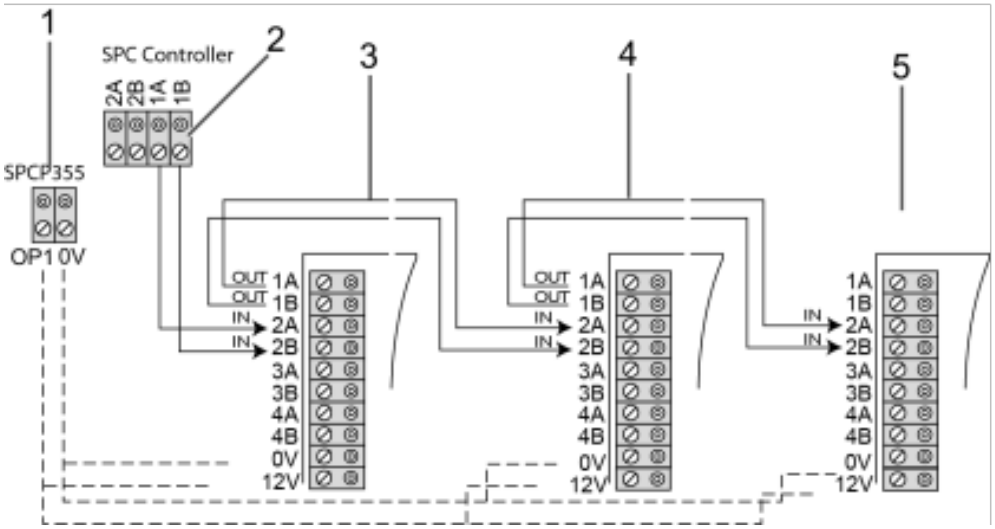
La interfaz X-BUS permite conectar módulos de expansión y teclados al controlador SPC. El X-BUS se puede cablear con un gran número de configuraciones diferentes según los requisitos de la instalación.

En la siguiente tabla se muestra una lista de los tipos de cable y las distancias recomendadas:

Longitud máxima de cables = (número de módulos de expansión y teclados del sistema) x (distancia máxima para cada tipo de cable)

Tipo de cable	Distancia
Cable de alarma estándar CQR	200 m
UTP Cat-5 núcleo sólido	400 m
Belden 9829	400 m
IYSTY 2x2x0,6 (mín.)	400 m

En el siguiente diagrama se muestra un ejemplo de cableado de X-BUS:



Número	Descripción
1	Salidas de fuente de alimentación inteligente SPCP355.300
2	Controlador SPC
3	Módulo de expansión de entrada/salida SPCP355.300
4	Módulo de expansión posterior
5	Módulo de expansión posterior

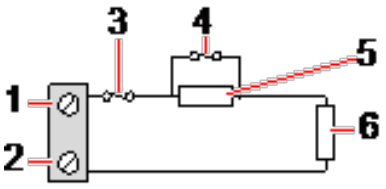
7.1.3.1 Cableado de las entradas

El módulo de expansión tiene 8 entradas de zona incorporadas que se pueden configurar como una de las siguientes:

- Sin resistencia final de línea
- Una resistencia final de línea
- Dos resistencias finales de línea
- Antienmascaramiento PIR

Configuración por defecto

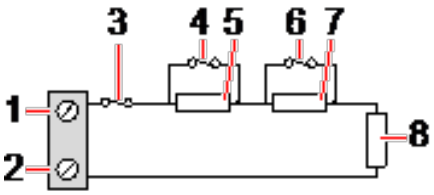
En el siguiente diagrama se muestra la configuración por defecto, 2 RFL 4k7:



Número	Descripción
1	Entrada 1
2	COM
3	Tamper
4	Alarma
5	4k7
6	RFL 4k7

Antienmascaramiento PIR

En el siguiente diagrama se muestra la configuración del PIR antienmascaramiento:



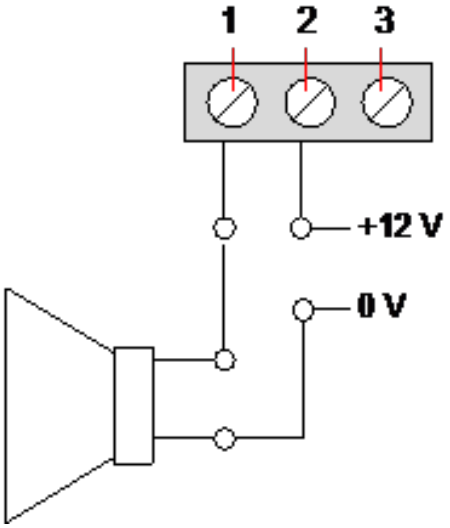
Número	Descripción
1	Entrada 2
2	COM
3	Tamper
4	Alarma
5	4k7
6	Fallo de detector
7	2K2
8	RFL 4k7

7.1.3.2 Cableado de las salidas

Las salidas de relé lógicas del módulo de expansión y de la fuente de alimentación se pueden asignar a cualquiera de las salidas del sistema SPC. Las salidas de relé pueden conmutar una tensión nominal de 30 V C.C. a 1 A (carga no inductiva).

Cuando se activa el relé, la conexión de terminal «común» (COM) conmuta del terminal «Normalmente Cerrado» (NC) al «Normalmente Abierto» (NA).

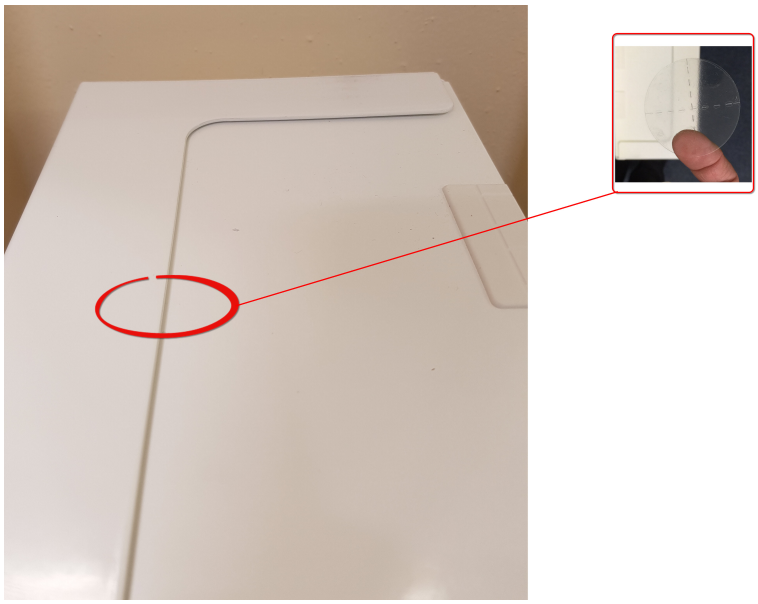
En el siguiente diagrama se muestra el cableado de una salida alta activa:



Número	Descripción
1	Terminal Normalmente Abierto
2	Conexión de terminal común (COM)
3	Terminal Normalmente Cerrado (NC)

7.1.4 Conformidad con las homologaciones NF y A2P

Dirección del organismo certificador	
Certificación CNPP	
Pôle Européen de Sécurité - Vernon	**Certificación AFNOR**
Route de la Chapelle Réanville	11 rue François de Pressensé
CD 64 - CS 22265	93571 Saint Denis La Plaine Cedex
F-27950 SAINT MARCEL	www.marque-nf.com
www.cnpp.com	



Para cumplir con las regulaciones de instalación NF y A2P, esta carcasa debe estar sellada con la etiqueta de tamper adjunta luego de la instalación.

Los productos SPC que se listan han sido probados de conformidad con la norma NF324 - H58, con referencia a RTC50131-6 y RTC50131-3, y las certificaciones EN vigentes. Consulte *Conformidad con las certificaciones EN50131* en la página 23.

Tipo de producto	Configuración	Estándar	Marca
SPC6350.320 + SPCP355.300 (Cert. 1233700001a)	60 h, sin supervisión	NF Grado 3, Clase 1	
SPC5350.320 + SPCP355.300 (Cert. 1233700001b)	60 h, sin supervisión		
SPC6330.320 + SPCP333.300 (Cert. 1232200003)	60 h, sin supervisión	NF Grado 3, Clase 1	
SPC5330.320 + SPCP333.300 (Cert. 1232200003)	60 h, sin supervisión		

7.1.5 LED de estado de la fuente de alimentación

En la siguiente tabla se muestra una lista con la información del LED de estado de la fuente de alimentación:

LED	RED C.A.	BAT. 1 y 2	FUSIBLE	LÍMITE	ESTADO
COLOR	verde	verde	rojo	rojo	verde
Condición					
Normal	ON	ON	Off	Off	ON
Red OK, batería cargando	ON	Parpadeando			ON
Fallo red, batería OK	Off	ON			ON
Red OK, batería defectuosa o ausente	ON	Off			ON
Red OK, batería defectuosa, ausente o en modo de protección contra descarga mínima	Todos los indicadores LED apagados.				
Fallo de fusible			ON		ON
Sobrepasada la corriente de carga total				ON	ON
Fallo interruptor fuente alim.	Off	Off	Off	Off	Parpadeando

7.1.6 Recuperación del sistema

Fallo de red y batería

En caso de fallo tanto en la red de CA como de la batería, el interruptor de arranque de la fuente de alimentación (elemento 25 en *Fuente de alimentación inteligente SPCP355.300* en la página 61) permite reiniciar el sistema si solo se restablece la alimentación de la batería. Para arrancar el sistema, haga lo siguiente:

Prerrequisitos

- La alimentación de C.A. ha fallado
- La alimentación de la batería ha fallado
- Hay baterías nuevas disponibles

1. Conecte los conductores de la batería.
2. Pulse y mantenga pulsado el botón de arranque de la fuente de alimentación.

   Todos los indicadores LED parpadean.
3. Mantenga pulsado el botón de arranque de la fuente de alimentación hasta que todos los LED dejen de parpadear.
4. Suelte el botón de arranque de la fuente de alimentación.

Restauración de fusible PTC

En caso de que se restablezca uno de los fusibles PTC, deberá desconectar manualmente y a continuación volver a conectar las conexiones de red de C.A. y de la batería.

8 Hardware del controlador

En esta sección se describe el hardware del controlador.

Consulte también

Suministrar alimentación a los módulos de expansión desde los terminales de alimentación auxiliar en la página 377

Cableado de la interfaz X-BUS en la página 81

Cableado de una sirena interior en la página 95

Cableado de entradas de zona en la página 91

Luces LED de estado del controlador en la página 376

Suministrar alimentación a los módulos de expansión desde los terminales de alimentación auxiliar en la página 377

Cableado de la interfaz X-BUS en la página 81

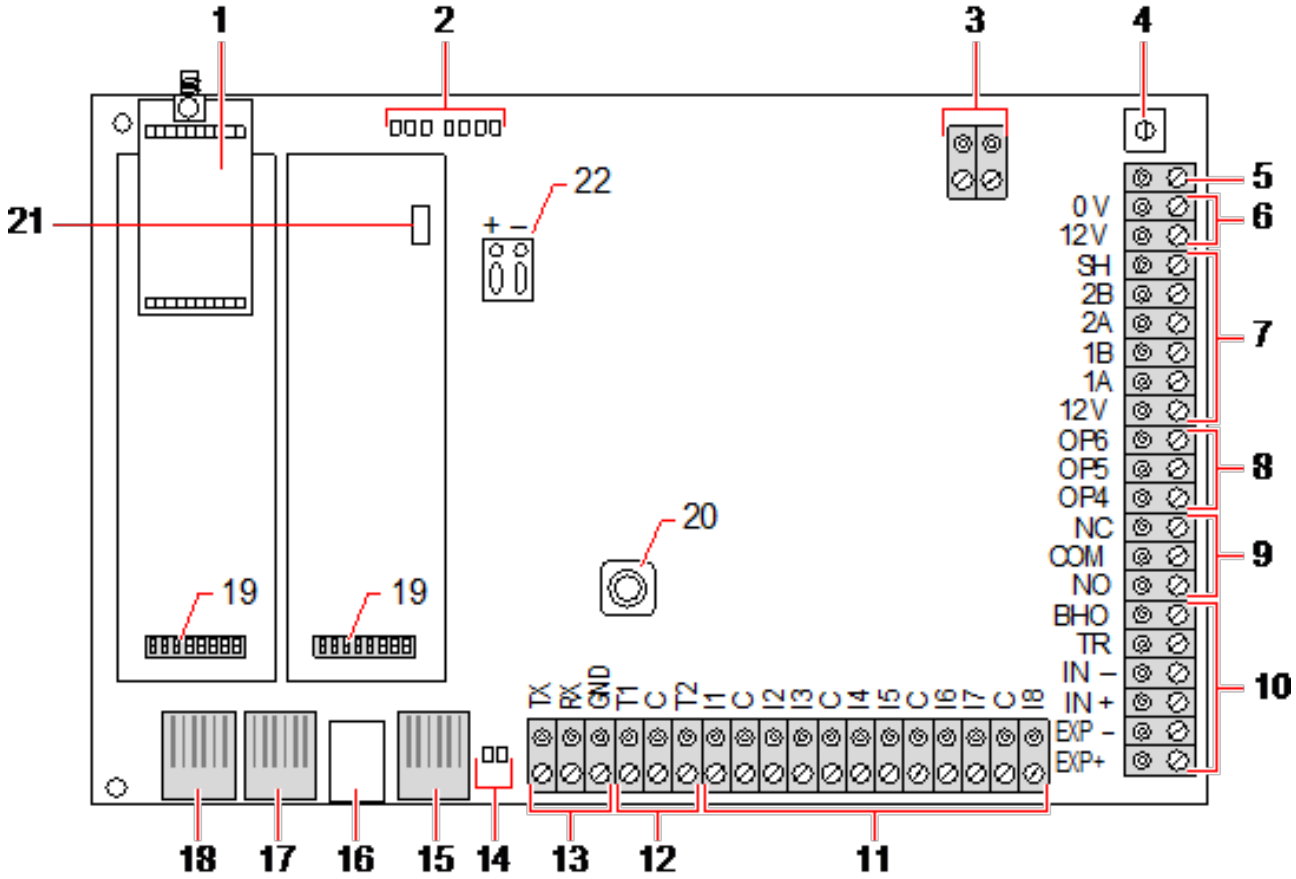
Cableado de una sirena interior en la página 95

Cableado de entradas de zona en la página 91

8.1 Hardware del controlador 42xx/43xx/53xx/63xx

En esta sección se describe el controlador para los modelos SPC42xx, 43xx, 53xx y 63xx. En *Hardware del controlador SPC5350 y 6350* en la página 76, se describen los modelos SPC5350 y 6350.

El controlador SPC ofrece ocho zonas cableadas y zonas vía radio opcionales.



Número	Nombre	Descripción
1	Módulo vía radio opcional	La placa del controlador puede venir de fábrica con un módulo vía radio integrado para los sensores vía radio (868 MHz).
2	LED de estado de SPC	Estos 7 LED muestran el estado de diversos parámetros del sistema según se describe en *Luces LED de estado del controlador* en la página 376.
3	Entrada de alimentación de CA	Entrada de red de CA: El voltaje de entrada de la red de CA se aplica a esta conexión de 2 clavijas a través del transformador integrado en la carcasa del SPC. La toma de tierra de la red de CA se ha cableado a un punto de conexión en la carcasa metálica. Referencia de reloj*: También se puede aplicar una señal de referencia de reloj a este conector de dos clavijas para mantener la hora exacta en el sistema.
4	Botón de Reset	• Para resetear el controlador: – Pulse este interruptor una vez. • Para resetear los ajustes de programación a los valores por defecto y reiniciar el controlador: – Presione el botón hacia abajo hasta que aparezca el mensaje sobre si desea restablecer los valores de fábrica. – Seleccione SÍ para restablecer los valores por defecto de fábrica. **Advertencia:** Si el controlador vuelve a los ajustes de fábrica, se borrarán todos los archivos de configuración guardados en el controlador, incluyendo las copias de respaldo. También se borran todos los aislamientos e inhibiciones. Se recomienda guardar una copia de seguridad en un PC antes de restablecer el controlador a los ajustes de fábrica. **Nota:** Esta función no está disponible si el bloqueo técnico está habilitado.
5	Terminal de conexión a tierra	No se requiere y no se debe conectar este terminal.
6	Salida de 12 V auxiliar	El controlador SPC proporciona una salida auxiliar de 12 V CC que se puede utilizar para alimentar los módulos de expansión y dispositivos como enclavamientos, sirenas, etc. Consulte *Suministrar alimentación a los módulos de expansión desde los terminales de alimentación auxiliar* en la página 377. La corriente máxima que se puede entregar es de 750 mA. **Nota:** La cantidad de corriente extraída depende del tiempo que tendrá que funcionar bajo las condiciones de la batería.
7	Interfaz X-BUS	Es el bus de comunicaciones de la central SPC que se utiliza para conectar entre sí los módulos de expansión en el sistema. Consulte *Cableado de la interfaz X-BUS* en la página 81. SPC4000 solo tiene una interfaz X-BUS.
8	Salidas integradas	Las salidas OP4, OP5 y OP6 son salidas resistivas de colector abierto de 12 V con una corriente de 400 mA y una salida auxiliar de 12 V. Si las salidas no están conectadas a 12 V del controlador y reciben alimentación de una fuente externa, los 0 V de la fuente de alimentación deben estar conectados a los 0 V del controlador y la fuente de alimentación externa no puede superar los 12 V.
9	Salida de relé	El controlador SPC proporciona un relé de conmutación de polo único de 1 A que se puede utilizar para activar la salida de flash de la sirena exterior.

Número	Nombre	Descripción
10	Sirena interior/Sirena exterior	Las salidas de sirena interior y exterior (INT+, INT-, EXT+, EXT-) son salidas resistivas con una corriente de 400 mA. Las salidas BHO (Bell Hold Off), TR (Tamper Return) y EXT se utilizan para conectar una sirena exterior al controlador. Los terminales l INT + INT- se utilizan para conectar con los dispositivos internos, como una sirena interior. Consulte *Cableado de una sirena interior* en la página 95.
11	Entradas de zona	El controlador incluye 8 entradas de zona integradas que pueden ser monitoreadas mediante una variedad de configuraciones de supervisión. Puede programar estas configuraciones desde la opción de programación del sistema. La configuración por defecto es Dos resistencias finales de línea (2RFL) con los valores de resistencia de 4k7. Consulte *Cableado de entradas de zona* en la página 91.
12	Terminales tamper	El controlador incluye 2 terminales de entrada tamper adicionales que pueden conectarse a los dispositivos tamper auxiliares para brindar una mayor protección. Cuando no están en uso, estos terminales deben ponerse en corto.
13	Bloque de terminales de puerto serie 2 	Puede utilizar el bloque de terminales de puerto serie 2 (TX, RX, GND) para conectar un módem externo o un programa de terminales de PC. El puerto serie 2 comparte el canal de comunicaciones con el módem de respaldo. Si instala un módem de respaldo, asegúrese de que no haya otros dispositivos conectados a este puerto serie.
14	 LED de conectividad Ethernet	Los 2 LED de conectividad Ethernet indican el estado de la conexión Ethernet. La luz LED izquierda indica la actividad de los datos en el puerto Ethernet; la luz LED derecha indica que el enlace Ethernet está activo.
15	 Interfaz Ethernet	La interfaz Ethernet sirve para la conexión de un PC al controlador con el fin de programar el sistema.
16	Interfaz USB	La interfaz USB se utiliza para acceder a la programación del navegador o al programa de un terminal.
17	Puerto serie 2 	Este puerto serie RS232 puede utilizarse para conectar con un módem externo o el programa de un terminal del PC. El puerto serie 2 comparte el canal de comunicaciones con el módem de respaldo. Si instala un módem de respaldo, asegúrese de que no haya otros dispositivos conectados a este puerto serie.
18	Puerto serie 1	Este puerto serie RS232 puede utilizarse para conectar con un dispositivo de protocolo X10.
19	Módulos enchufables opcionales	Se puede conectar un módulo principal (ranura izquierda) y un módulo de respaldo (ranura derecha) al controlador. Estos módulos pueden ser módems GSM o RTB que ofrecen una mayor funcionalidad de comunicación. El módem de respaldo no debe estar conectado si la interfaz del puerto serie 2 está conectada a un módem externo u otro dispositivo.
20	Tamper frontal	Este tamper frontal integrado (interruptor e interruptor) brinda protección de tamper a la carcasa. **Nota:** El tamper frontal no se utiliza en la carcasa G5.

Número	Nombre	Descripción
21	Selector de batería	J12: Coloque el puente para utilizar una batería de 17 Ah y retire la batería de 7 Ah. Nota: Este selector sólo está disponible en la revisión 2.3 de la placa del controlador. (No aplicable a las centrales SPC5350 y SPC5360).
22	Entrada de alimentación auxiliar	Entrada de 12 V desde batería o fuente de alimentación**.

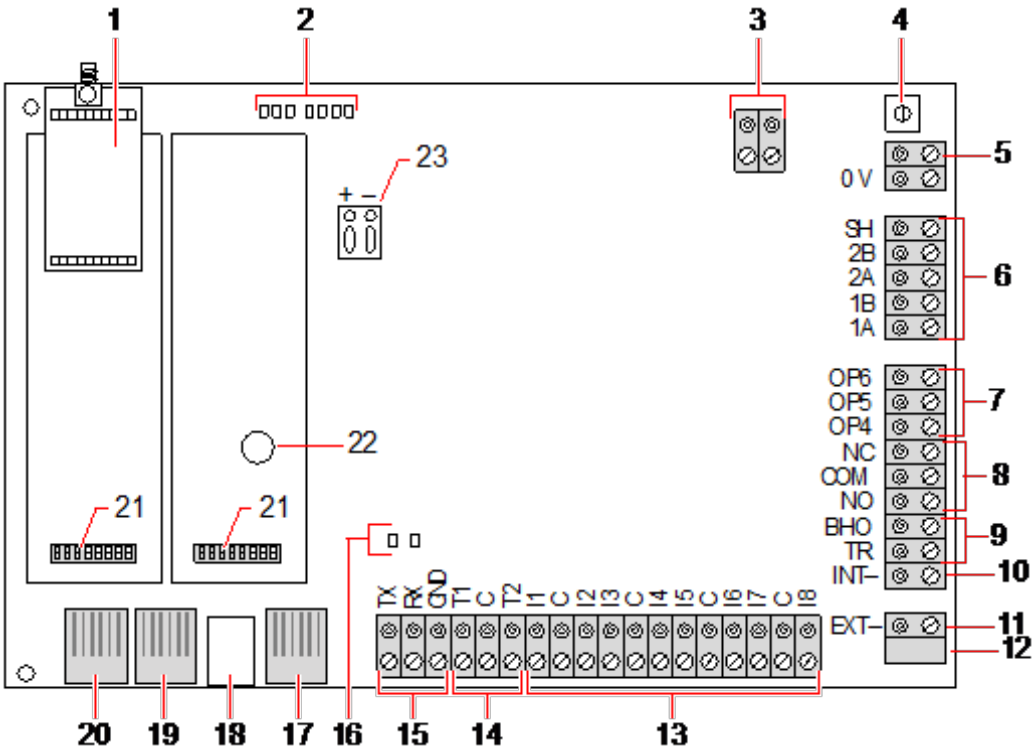
* Configuración por defecto para centrales SPC5350 y SPC5360

** La fuente de alimentación solo es aplicable a las centrales SPC5350 y SPC6350.

8.2 Hardware del controlador SPC5350 y 6350

En esta sección se describe el SPC5350 y el SPC6350.

El módulo de expansión que está conectado a la fuente de alimentación dentro de G5 está configurado como ID1 por defecto. No se debe cambiar este ajuste.



Número	Nombre	Descripción
1	Módulo vía radio opcional	La placa del controlador puede venir de fábrica con un módulo vía radio integrado para los sensores vía radio (868 MHz).

Número	Nombre	Descripción
2	LED de estado de SPC	Estos 7 LED muestran el estado de diversos parámetros del sistema según se describe en *Luces LED de estado del controlador* en la página 376.
3	Referencia de reloj	También se puede aplicar una señal de referencia de reloj a este conector de dos clavijas para mantener la hora exacta en el sistema. Conecte la referencia del reloj CN17 en la fuente de alimentación inteligente SPCP355.300.
4	Botón de Reset	• Para resetear el controlador: – Pulse este interruptor una vez. • Para resetear los ajustes de programación a los valores por defecto y reiniciar el controlador: – Presione el botón hacia abajo hasta que aparezca el mensaje sobre si desea restablecer los valores de fábrica. – Seleccione SÍ para restablecer los valores por defecto de fábrica. **Advertencia:** Si el controlador vuelve a los ajustes de fábrica, se borrarán todos los archivos de configuración guardados en el controlador, incluyendo las copias de respaldo. También se borran todos los aislamientos e inhibiciones. Se recomienda guardar una copia de seguridad en un PC antes de restablecer el controlador a los ajustes de fábrica. **Nota:** Esta función no está disponible si el bloqueo técnico está habilitado.
5	Terminal de conexión a tierra	No se requiere y no se debe conectar este terminal.
6	Interfaz X-BUS	Es el bus de comunicaciones de la central SPC que se utiliza para conectar entre sí los módulos de expansión en el sistema. Consulte *Cableado de la interfaz X-BUS* en la página 81. Las terminales 1B y 1A se deben conectar a los terminales del módulo de expansión de E/S SPCP355.300 2B y 2A, respectivamente. Los terminales 2A y 2B se deben conectar a los terminales 2A y 2B, respectivamente, del siguiente módulo de expansión del X-BUS.
7	Salidas integradas	Las salidas OP4, OP5 y OP6 son salidas resistivas de colector abierto de 12V con una corriente de 300mA. La carga de OP4 se debe conectar a la fuente de alimentación inteligente SPCP355.300.
8	Salida de relé	El controlador SPC proporciona un relé de conmutación de polo único de 1 A que se puede utilizar para activar la salida de flash de la sirena exterior.
9	Bell Hold-Off (BHO) y Tamper Return (TR)	Las salidas BHO (Bell Hold Off) y TR (Tamper Return) (y la salida EXT) se utilizan para conectar una sirena exterior al controlador. Consulte *Cableado de una sirena interior* en la página 95.
10	Sirena interior (negativo)	El terminal INT- se utiliza para conectar con los dispositivos internos, como una sirena interna. La alimentación para la sirena interna se debe conectar a la fuente de alimentación inteligente SPCP355.300.

Número	Nombre	Descripción
11	Sirena exterior (negativo)	El terminal EXT- sirve para conectar con los dispositivos externos, como una sirena exterior. La alimentación para la sirena exterior se debe conectar a la fuente de alimentación inteligente SPCP355.300.
12	No utilizar.	No utilizar.
13	Entradas de zona	El controlador incluye 8 entradas de zona integradas que pueden ser monitoreadas mediante una variedad de configuraciones de supervisión. Puede programar estas configuraciones desde la opción de programación del sistema. La configuración por defecto es Dos resistencias finales de línea (2RFL) con los valores de resistencia de 4k7. Consulte *Cableado de entradas de zona* en la página 91.
14	Terminales tamper	El controlador incluye 2 terminales de entrada tamper adicionales que pueden conectarse a los dispositivos tamper auxiliares para brindar una mayor protección. Cuando no están en uso, estos terminales deben ponerse en corto.
15	Bloque de terminales de puerto serie 2	Puede utilizar el bloque de terminales de puerto serie 2 (TX, RX, GND) para conectar un módem externo o un programa de terminales de PC. El puerto serie 2 comparte el canal de comunicaciones con el módem de respaldo. Si instala un módem de respaldo, asegúrese de que no haya otros dispositivos conectados a este puerto serie.
16	LED de conectividad Ethernet	Los 2 LED de conectividad Ethernet indican el estado de la conexión Ethernet. La luz LED izquierda indica la actividad de los datos en el puerto Ethernet; la luz LED derecha indica que el enlace Ethernet está activo.
17	Interfaz Ethernet	La interfaz Ethernet sirve para la conexión de un PC al controlador con el fin de programar el sistema.
18	Interfaz USB	La interfaz USB se utiliza para acceder a la programación del navegador o al programa de un terminal.
19	Puerto serie 2	Este puerto serie RS232 puede utilizarse para conectar con un módem externo o el programa de un terminal del PC. El puerto serie 2 comparte el canal de comunicaciones con el módem de respaldo. Si instala un módem de respaldo, asegúrese de que no haya otros dispositivos conectados a este puerto serie.
20	Puerto serie 1	Este puerto serie RS232 puede utilizarse para conectar con un dispositivo de protocolo X10.
21	Módulos enchufables opcionales	Se puede conectar un módulo principal (ranura izquierda) y un módulo de respaldo (ranura derecha) al controlador. Estos módulos pueden ser módems GSM o RTB que ofrecen una mayor funcionalidad de comunicación. El módem de respaldo no debe estar conectado si la interfaz del puerto serie 2 está conectada a un módem externo u otro dispositivo.
22	Batería de reloj de tiempo real	Batería para reloj de tiempo real (RTR).
23	Entrada de alimentación auxiliar	Entrada de 12 V desde A1 en fuente de alimentación inteligente SPCP355.300.

Consulte también

Suministrar alimentación a los módulos de expansión desde los terminales de alimentación auxiliar en la página 377

9 Módulo de expansión de puerta

El módulo de expansión de dos puertas puede gestionar hasta dos puertas y dos lectores de tarjetas. La configuración del modo de funcionamiento se realiza a través de las dos E/S de puerta. Cada una de las dos E/S de puerta es responsable de la funcionalidad de las dos entradas y una salida del controlador de puerta. Se puede asignar un número de puerta específico a una E/S de puerta, lo cual asigna una funcionalidad definida previamente a las entradas y la salida. Si no se asigna un número de puerta a ninguna de las E/S de puerta (la opción «Zonas» está seleccionada), las entradas y las salidas del controlador de puerta pueden utilizarse como entradas y salidas en la central de control. Por lo tanto, no habrá funcionalidad de acceso disponible en este controlador de dos puertas.

Si se asigna un número de puerta únicamente a la primera E/S de puerta del controlador de dos puertas, el primer lector se utilizará como lector de entrada para esta puerta. Si hay un segundo lector disponible, se utiliza como lector de salida para la puerta configurada. Dos entradas y una salida tienen funcionalidad definida previamente y el usuario puede configurar dos entradas y una salida. Además, la entrada del sensor de posición de puerta de la primera puerta puede utilizarse como zona de intrusión, pero solo con funcionalidad limitada.

Si se asigna un número de puerta a cada una de las dos E/S de puertas, las dos puertas se gestionarán independientemente. El primer lector de tarjetas se utiliza como lector de entrada para la primera puerta y el segundo lector de tarjetas se utiliza como lector de entrada para la segunda puerta. Todas las entradas y salidas tienen funcionalidad definida previamente. Además, las entradas del sensor de posición de puerta de las dos puertas pueden utilizarse como zonas de intrusión, pero solo con funcionalidad limitada.

Para obtener más información sobre los lectores de tarjetas y formatos de tarjetas soportados actualmente, consulte *Lectores de tarjeta y formatos de tarjeta admitidos* en la página 404.

Cada número de zona libre puede ser asignado a las zonas. Sin embargo, la asignación no es fija. Si se ha asignado el número 9 a una zona, dicha zona y un módulo de expansión de entrada con la dirección 1 se conectan al X-Bus (que está utilizando los números de zona 9–16). La zona asignada desde el controlador de dos puertas se trasladará al siguiente número de zona libre. La configuración se adaptará en consecuencia.

10 Cableado del sistema

Este capítulo abarca:

10.1 Cableado de la interfaz X-BUS

La interfaz X-BUS permite conectar módulos de expansión al controlador. El X-BUS se puede cablear con un gran número de configuraciones diferentes según los requisitos de la instalación. La velocidad de baudios de la interfaz X-BUS es 307 kb.

AVISO: El X-BUS es un bus RS-485 con una velocidad de baudios de 307 kb. El rendimiento completo solo se admite en una configuración de cableado en lazo (consulte *Configuración en lazo* en la página siguiente) y punta (consulte *Configuración en punta* en la página 83) (la mejor calidad de señal debido a la configuración en cadena de tipo margarita de secciones aisladas con 1 transmisor/1 receptor y resistencias de terminación equilibradas en cada extremo).

El rendimiento en el cableado con configuración en estrella o multipunto (consulte *Configuración en estrella y multipunto* en la página 84) es limitado debido a que las condiciones de la especificación de bus RS-485 no son las óptimas (calidad de la señal reducida debido a múltiples receptores/transmisores en paralelo con resistencias de terminación no equilibradas).

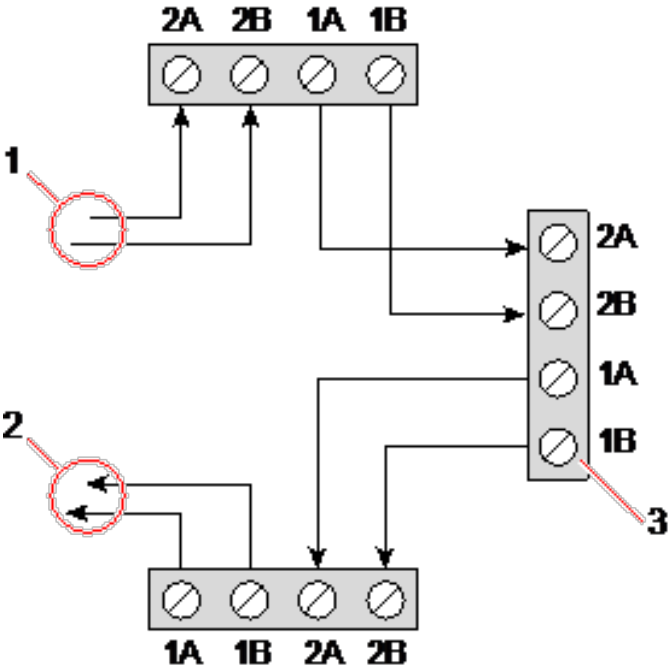
AVISO: Se recomienda el uso de la configuración en lazo (consulte *Configuración en lazo* en la página siguiente) o en punta (consulte *Configuración en punta* en la página 83).

La tabla a continuación muestra las distancias máximas entre controlador/módulo de expansión o módulo de expansión/módulo de expansión para todos los tipos de cable con configuración en lazo o en punta.

Tipo de cable	Distancia
Cable de alarma estándar CQR	200 m
UTP Categoría: 5 (núcleo sólido)	400 m
Belden 9829	400 m
IYSTY 2 x 2 x 0,6 (mín.)	400 m

Cada dispositivo incluye cuatro terminales (1A, 1B, 2A y 2B) para conectar a los módulos de expansión a través del cable X-BUS. El controlador inicia un procedimiento de detección al encenderse para determinar

la cantidad de módulos de expansión conectados en el sistema y la topología mediante la cual están conectados.



Cableado de módulos de expansión

Número	Descripción
1	Módulo de expansión anterior
2	Módulo de expansión posterior
3	Controlador SPC

La mayoría de los módulos de expansión posee terminales adicionales 3A/3B y 4A/4B para el cableado de módulos de expansión de bifurcación. Consulte *Cableado de un módulo de expansión de bifurcación* en la página 89 para obtener instrucciones sobre el cableado de módulos de expansión de bifurcación.

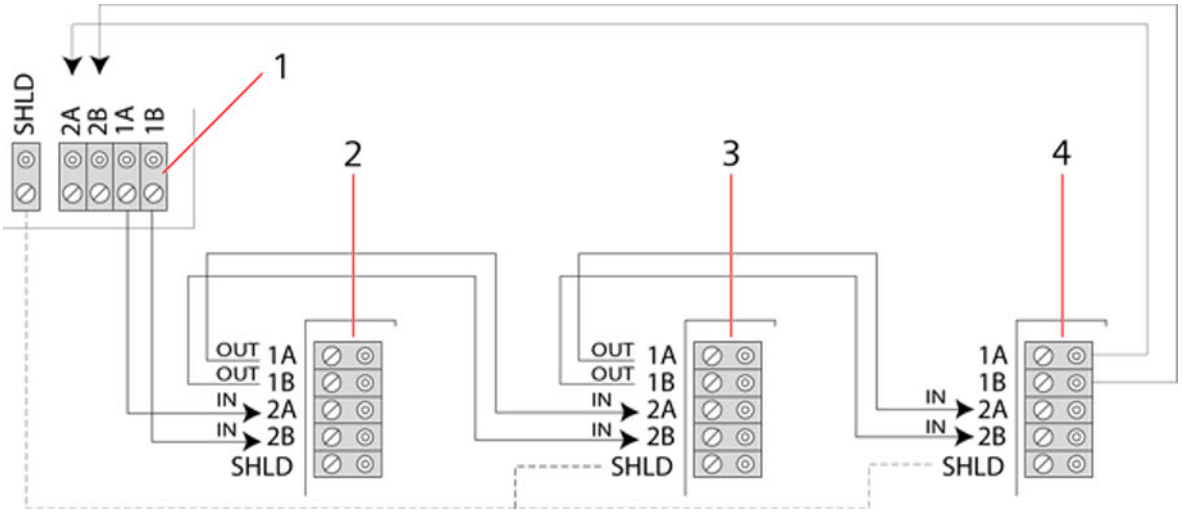
10.1.1 Configuración en lazo

AVISO: El SPC42xx/43xx no admite configuración en lazo (solo 1 puerto X-BUS).

AVISO: Todos los módulos de expansión/teclados por defecto tienen un jumper de terminación. La configuración en lazo requiere el uso de estos jumpers.

El método de cableado en lazo (o anillo) ofrece la máxima seguridad al proporcionar comunicaciones con tolerancia a fallos en el X-BUS. Todos los teclados y módulos de expansión son supervisados y, en caso de fallo o discontinuidad del X-BUS, el sistema continúa funcionando y todos los detectores se controlan. Eso se logra al conectar 1A, 1B en el controlador a 2A, 2B en el primer teclado o módulo de expansión. El cableado continúa con la conexión de 1A, 1B a 2A, 2B en el siguiente módulo de expansión y así sucesivamente hasta el último teclado o módulo de expansión. La última conexión es 1A, 1B del último

módulo de expansión a 2A, 2B del controlador. Consulte la información de configuración de cableado en la figura a continuación.



Número	Descripción
1	Controlador
2-4	Módulos de expansión

10.1.2 Configuración en punta

AVISO: SPC52xx/53xx/63xx admite 2 puntas (2 puertos X-BUS).

SPC42xx/43xx admite 1 punta (1 puerto X-BUS).

AVISO: Todos los módulos de expansión/teclados por defecto tienen un jumper de terminación. La configuración en punta requiere el uso de estos jumpers.

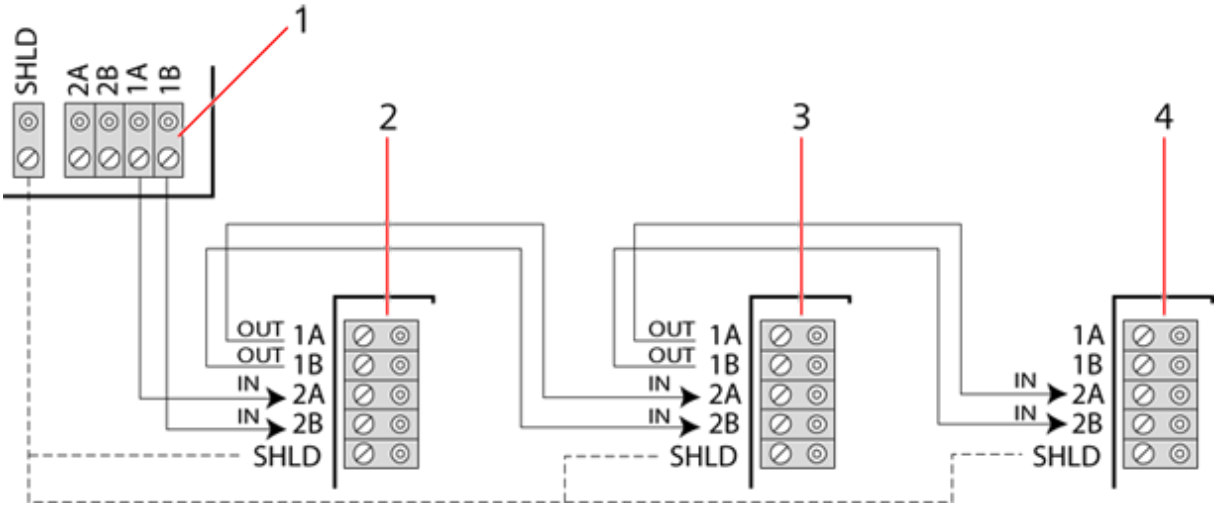
El método de cableado en punta (o lazo abierto) ofrece un alto nivel de tolerancia de fallos, y podría ser más conveniente para determinadas instalaciones. En caso de fallo o discontinuidad de un X-BUS, todos los módulos de expansión y detectores hasta el punto del fallo continúan siendo supervisados.

En esta configuración, el controlador SPC utiliza un único puerto X-BUS (1A/1B o 2A/2B) para admitir un grupo de módulos de expansión. Consulte la información de configuración de cableado en la figura a continuación. El último módulo de expansión en una configuración en lazo abierto no está cableado hacia el controlador y puede ser identificado por la luz LED que destella rápidamente (un flash cada 0,2 segundos aprox.) cuando se trabaja en programación en modo de técnico completo.

En modo automático, la numeración del módulo de expansión comienza en el módulo de expansión más cercano al controlador y finaliza con el módulo de expansión conectado más alejado del controlador. Por ejemplo, si hay seis dispositivos conectados en una configuración de lazo abierto, el módulo de expansión más próximo en la conexión del X-BUS es el módulo de expansión 1, el segundo más próximo es el módulo de expansión 2, etc., hasta el módulo de expansión conectado más lejos del controlador, que es el módulo de expansión 6.

Por defecto, todos los módulos de expansión/teclados tienen jumpers de terminación, lo que permite la terminación de todos los dispositivos. Esto es obligatorio para la configuración en punta (cadena), porque el jumper actúa como una terminación resistente que cancela los ecos de la línea.

Con la configuración de cableado en lazo, por defecto, todos los módulos de expansión/teclados tienen un jumper, lo que permite la terminación en el dispositivo.



Configuración en punta

Número	Descripción
1	Controlador
2-4	Módulos de expansión

10.1.3 Configuración en estrella y multipunto

AVISO: Consulte *Ejemplos de cableado correcto* en la página 87, *Ejemplos de cableado incorrecto* en la página 88 y *Apantallado* en la página 89 antes de comenzar la instalación.

Los métodos de cableado en estrella y multipunto permiten la utilización de los cableados existentes con cables de cuatro núcleos en edificios pequeños (generalmente, casas) con un entorno de ruido eléctrico bajo. Estos métodos de cableado están limitados a las especificaciones que se muestran a continuación:

	SPC42xx/SPC43xx	SPC52xx/SPC53xx/SPC63xx
Máx. módulos de expansión/teclados	8	16 (8 por puerto X-BUS)
Longitud total del cable	200 m	200 m

AVISO: El rendimiento en el cableado con configuración en estrella o multipunto es limitado debido a que las condiciones de la especificación de bus RS-485 no son las óptimas (calidad de la señal reducida debido a múltiples receptores/transmisores en paralelo con resistencias de terminación no equilibradas).

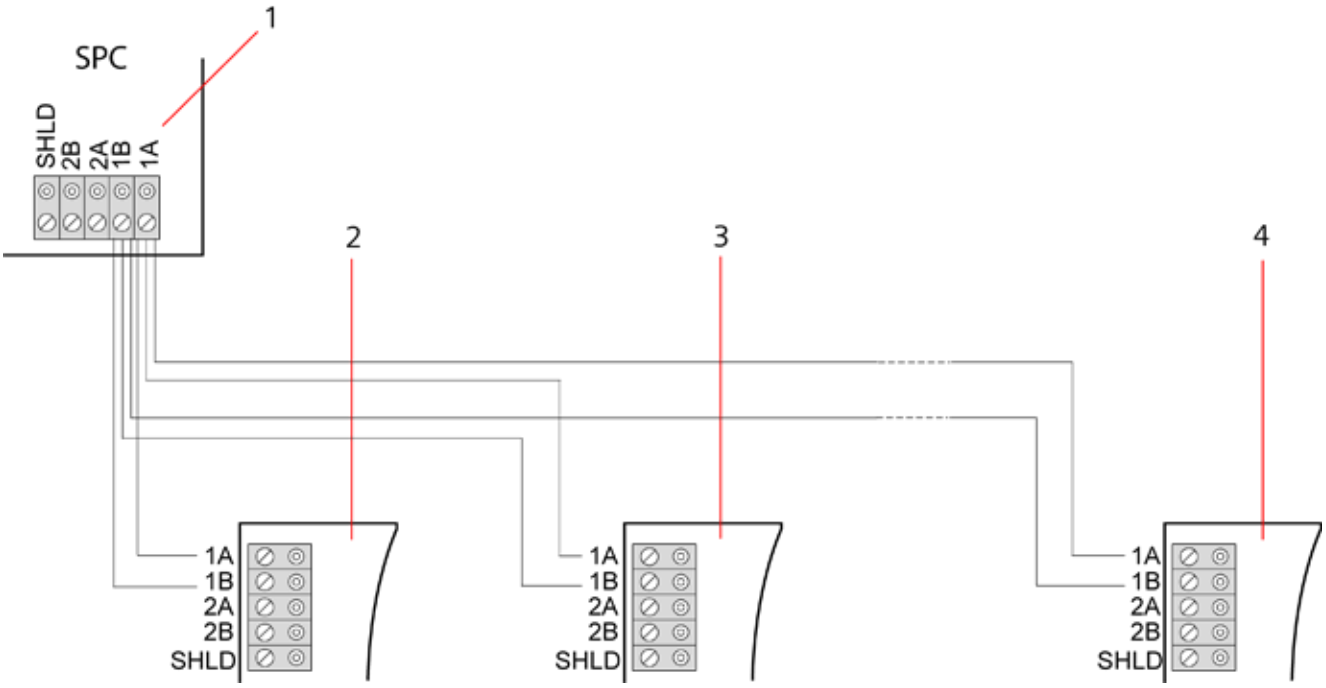
Configuración en estrella

AVISO: Todos los módulos de expansión/teclados por defecto tienen un jumper de terminación. En la configuración en estrella, se deben **retirar** estos jumper.

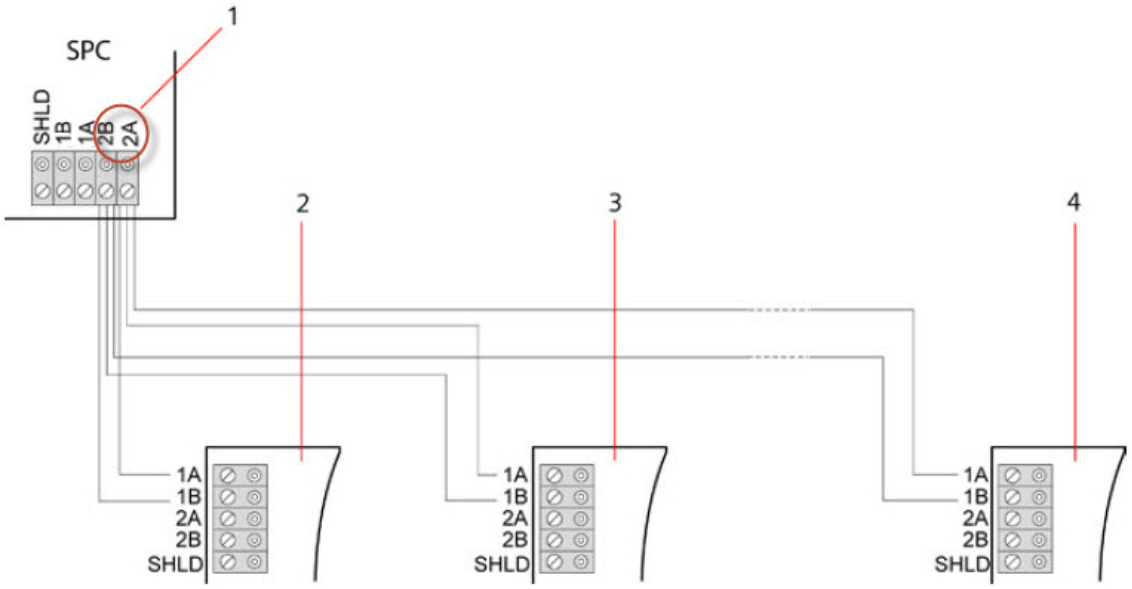
Una configuración en estrella se establece cuando varios módulos de expansión se vuelven a conectar al mismo puerto X-BUS en el controlador SPC. Según el tipo de controlador, es posible que haya 2 puertos

(1A/1B, 2A/2B). Sin embargo, se utiliza un solo puerto (1A/1B) para cada teclado o módulo de expansión.

En caso de discontinuidad de un X-BUS, el sencillo se desconectará, pero todos los demás módulos de expansión y detectores se seguirán supervisando. Si se produce un corto en el cable, se deshabilitarán todos los módulos de expansión.



Configuración en estrella



Configuración en estrella 2

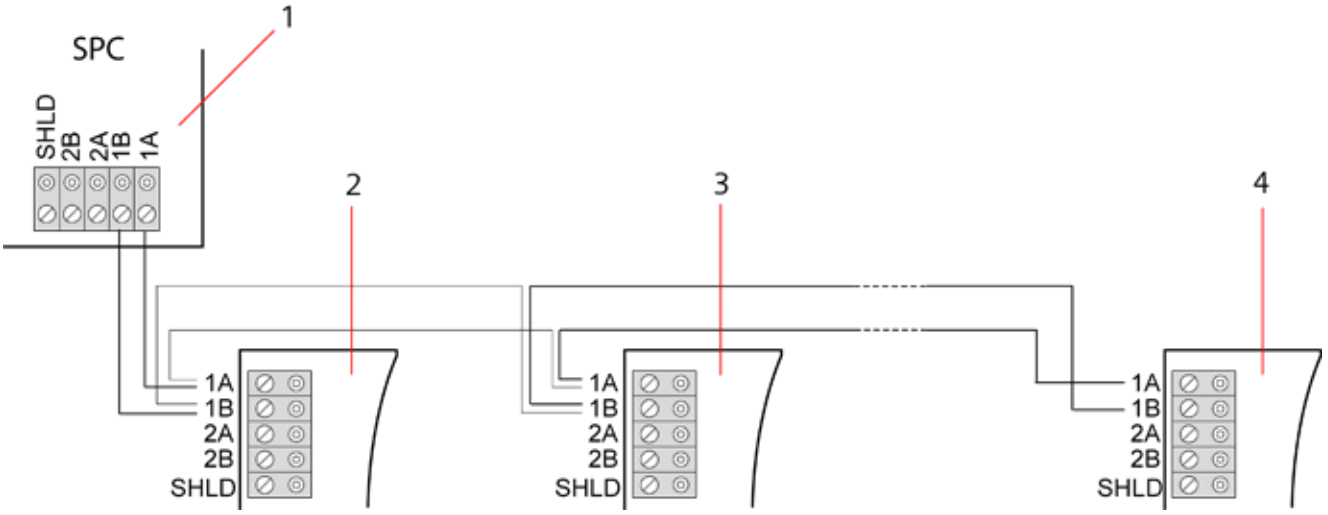
Número	Descripción
1	Controlador SPC
2-4	Módulos de expansión

Configuración multipunto

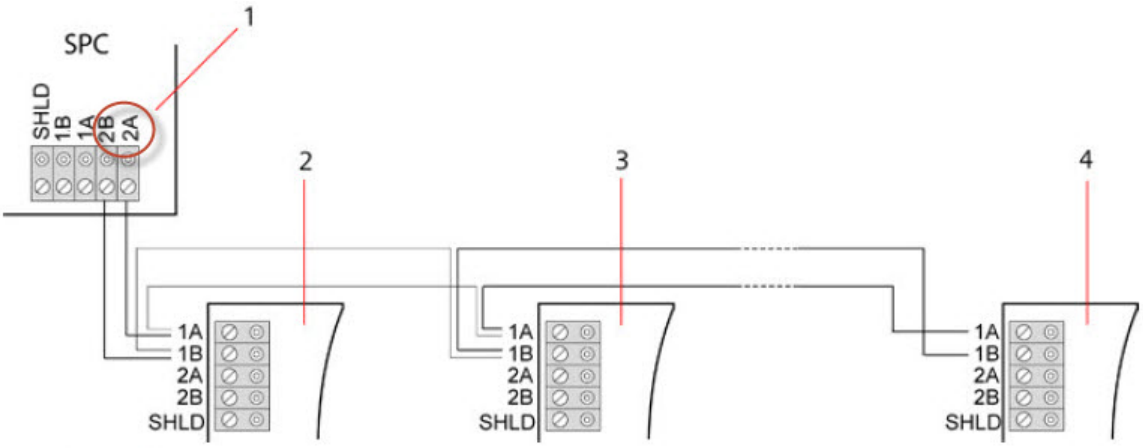
AVISO: Todos los módulos de expansión/teclados por defecto tienen un jumper de terminación. En la configuración multipunto, se deben **retirar** estos jumper con la excepción del último teclado o módulo de expansión.

La configuración multipunto varía en que cada módulo de expansión utiliza el mismo canal de comunicación al cablearse en el siguiente módulo de expansión, y todos los módulos de expansión utilizan el mismo canal de entrada. Consulte la información de configuración multipunto en la segunda imagen.

En caso de discontinuidad de un X-BUS, todos los módulos de expansión y detectores hasta el punto del fallo continúan siendo supervisados. Si se produce un corto en el cable, se deshabilitarán todos los módulos de expansión.



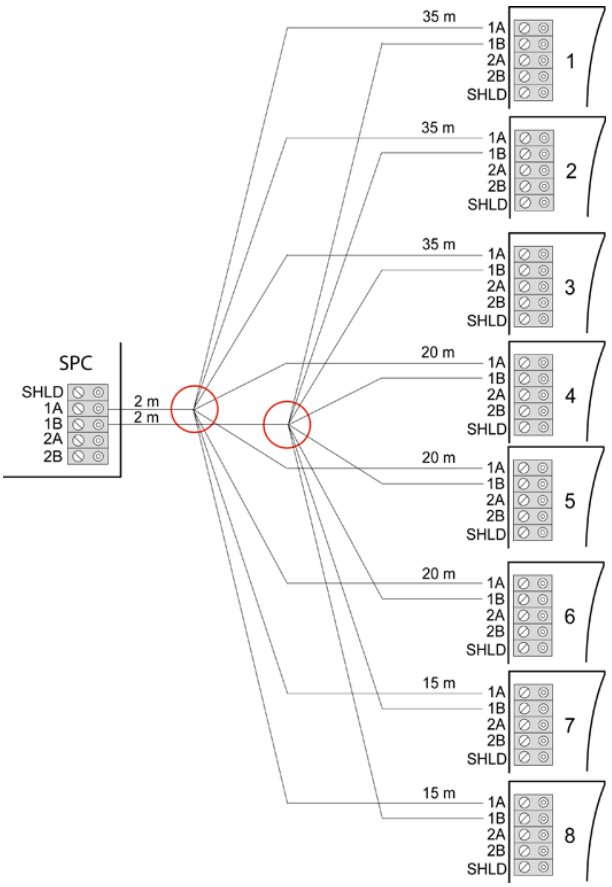
Configuración multipunto



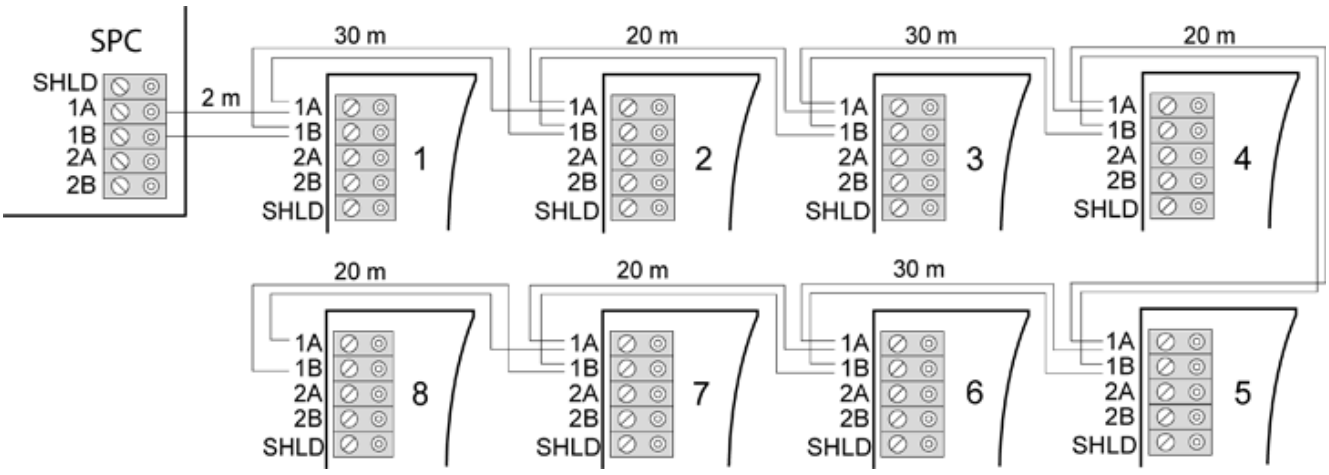
Configuración multipunto 2

Número	Descripción
1	Controlador SPC
2-4	Módulos de expansión

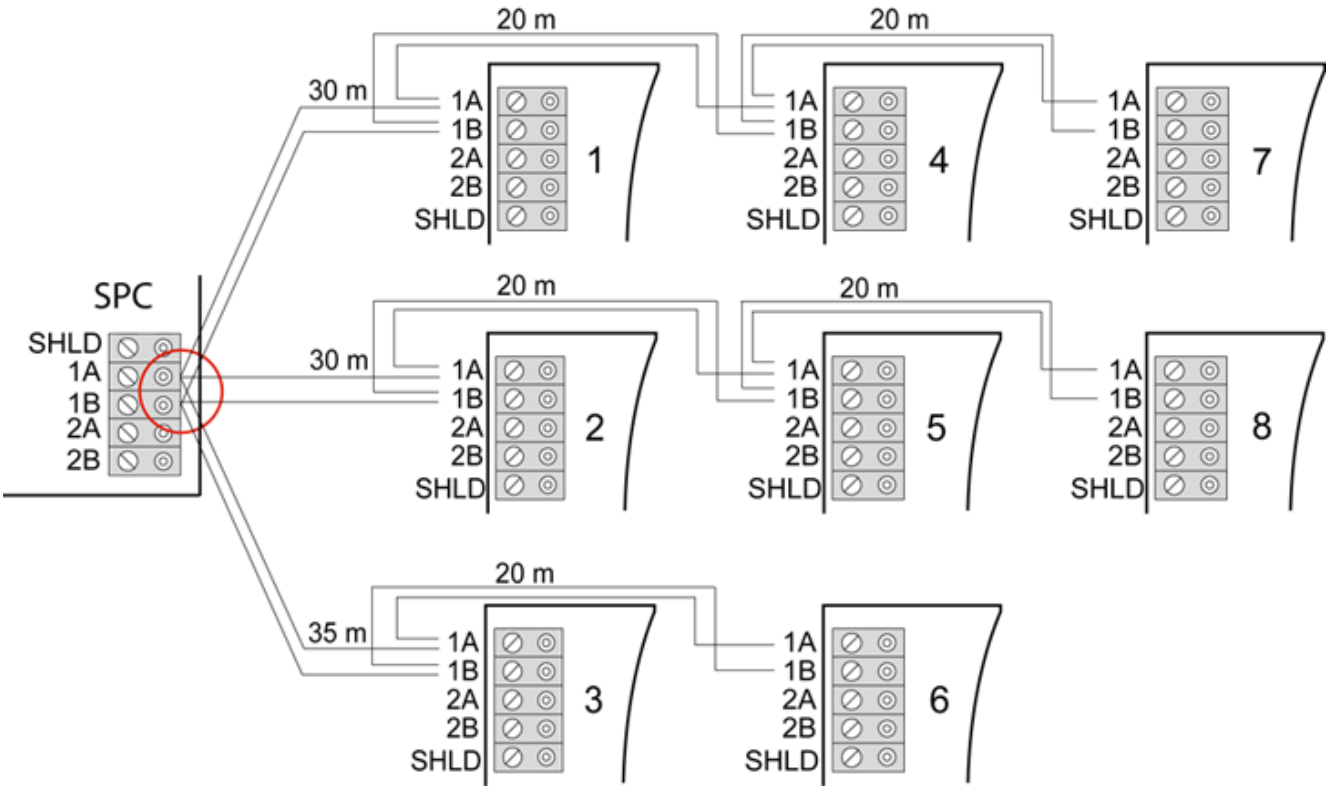
10.1.3.1 Ejemplos de cableado correcto



Cableado en estrella



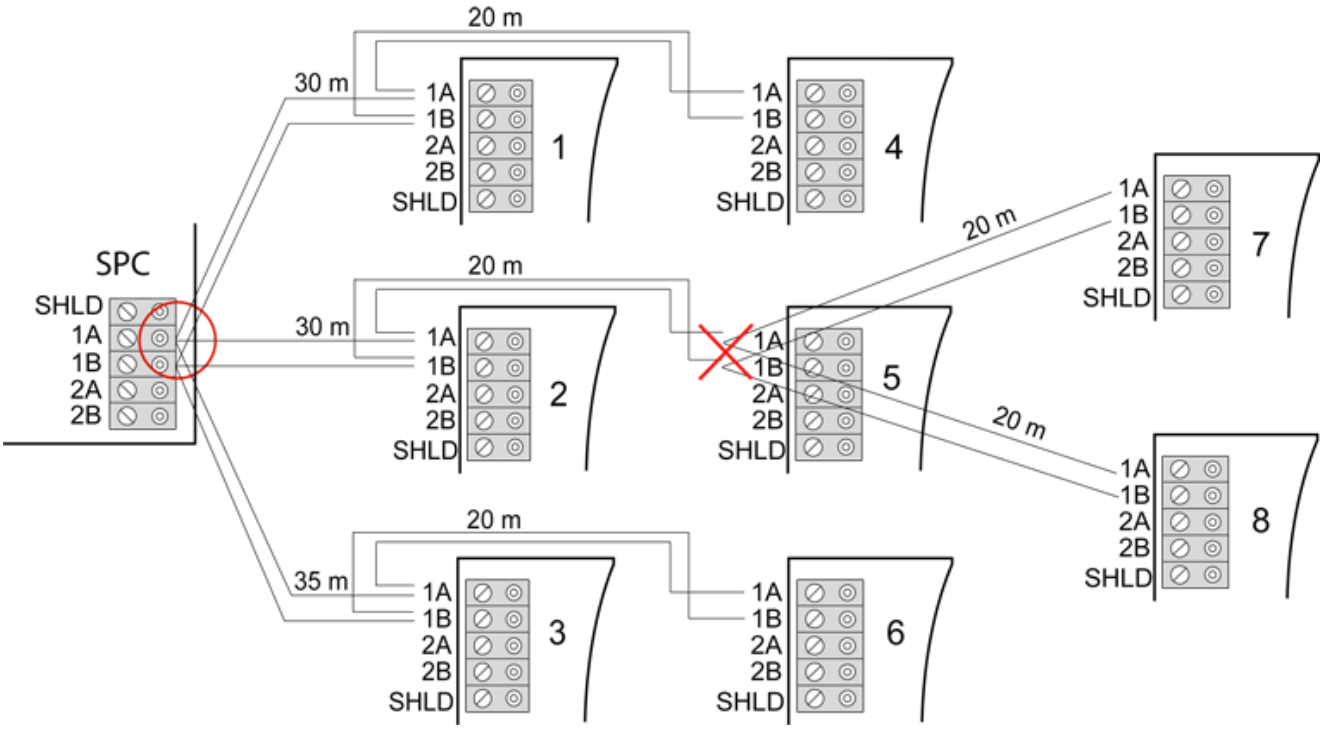
Cableado multipunto



Cableado mixto

10.1.3.2 Ejemplos de cableado incorrecto

AVISO: Solo se permite una configuración combinada de cableado en estrella y multipunto si el punto en estrella está en el puerto X-BUS del controlador. En este caso, se deben cablear todos los módulos de expansión/teclados en la configuración multipunto sin otros puntos en estrella en el cableado.



No se permite el cableado con un segundo punto en estrella.

AVISO: Si la configuración combinada de cableado en estrella y multipunto no está debidamente cableada, la calidad de señal reducida puede dar lugar a un tiempo de reacción lento de los dispositivos conectados (por ejemplo: funcionamiento del teclado) o, incluso, la pérdida de comunicación con los dispositivos. Si se detecta este comportamiento, se recomienda utilizar una configuración de cableado en lazo o en estrella.

10.1.4 Apantallado

Solo se deben utilizar terminales de apantallado (SHLD) para los tipos de cables que utilicen apantallado (por ejemplo: Belden 9829). Si se requiere apantallado (es decir, en instalaciones con muchas interferencias eléctricas): conecte el apantallado del cable a los terminales SHLD del controlador y a todos los módulos de expansión conectados. Si se debe conectar el apantallado a tierra, entonces, se debe conectar un cable del terminal SHLD del controlador al vástago a tierra del chasis. NO conecte a tierra el terminal SHLD de cualquiera de los módulos de expansión.

AVISO: Para cableado en estrella y multipunto

No se recomienda que utilice cables apantallados debido a las desventajas de las características eléctricas (mayor capacitancia) en la configuración en estrella y multipunto. Sin embargo, si se requiere el uso de apantallado (es decir, sitios con gran interferencia de campo eléctrico), se debe realizar un nuevo cableado, con configuración en punta o en lazo, con los cables de instalación adecuados.

10.1.5 Config. cabl.

La identificación y el orden de numeración de los módulos de expansión y los teclados difieren según sea un direccionamiento automático o manual de los módulos de expansión. Para obtener más información sobre la configuración manual y automática, consulte *X-BUS* en la página 136.

Para un sistema con direccionamiento manual, los módulos de expansión y los teclados tienen una secuencia de numeración por separado y los define el técnico manualmente. Es decir, los módulos de expansión están numerados como 01, 02, 03, etc., según se desee. Usando los mismos números, se puede enumerar los teclados según se desee.

En la configuración manual, el sistema asigna automáticamente zonas para cada módulo de expansión. Es por esto que los dispositivos sin zonas como, por ejemplo, los módulos de expansión de 8 salidas, deben direccionarse por último.

En un sistema con direccionamiento automático, los módulos de expansión y los teclados pertenecen al mismo grupo de numeración y los asigna el controlador. Es decir, los módulos de expansión y los teclados están enumerados de forma conjunta como 01, 02, 03, en el orden de detección relativo a la ubicación del controlador.

10.2 Cableado de un módulo de expansión de bifurcación

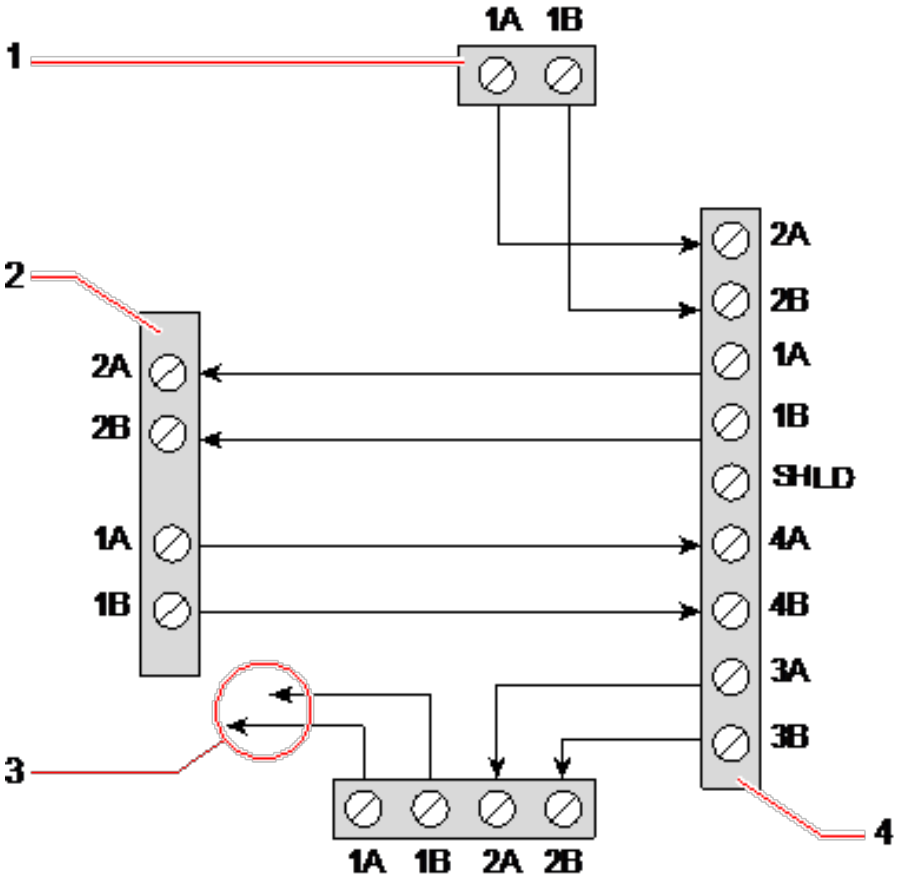
El cableado de la interfaz X-BUS con ocho terminales 1A/1B a 4A/4B hace posible la conexión de un módulo de expansión de bifurcación adicional.

Si no se utiliza la bifurcación, los terminales 1A/1B se utilizan para conectar el módulo de expansión/teclado siguiente. En ese caso, los terminales 3A/3B y 4A/4B no se utilizan.

Los siguientes módulos tienen capacidad de cableado de bifurcación (terminales adicionales 3A/B y 4A/B):

- Módulo de expansión de 8 entradas/2 salidas
- Módulo de expansión de 8 salidas
- Módulo de expansión de fuente de alimentación

- Módulo de expansión vía radio
- Módulo de expansión de 2 puertas



Cableado de un módulo de expansión de bifurcación

Número	Descripción
1	Módulo de expansión anterior
2	Módulo de expansión conectado a bifurcación
3	Módulo de expansión posterior
4	Módulo de expansión con bifurcación

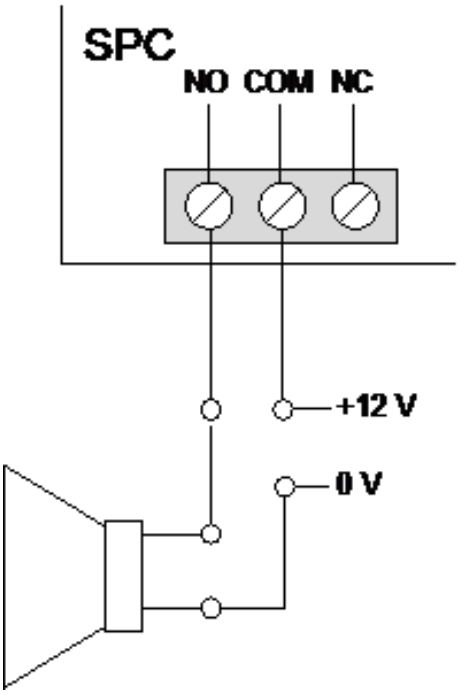
10.3 Cableado del sistema a tierra

El terminal 0 V de las fuentes de alimentación inteligentes, los teclados y los módulos de expansión deben conectarse al terminal 0 V (sistema a tierra) del controlador SPC.

10.4 Cableado de la salida del relé

El controlador SPC tiene incorporado un relé de conmutación de polo único de 1 A que se puede asignar a cualquiera de las salidas del sistema SPC. Esta salida de relé pueden conmutar una tensión nominal de 30 V CC (carga no inductiva).

Cuando se activa el relé, la conexión de terminal común (COM) conmuta del terminal **N**ormalmente **C**errado (NC) al terminal **N**ormalmente **A**bierto (NA).



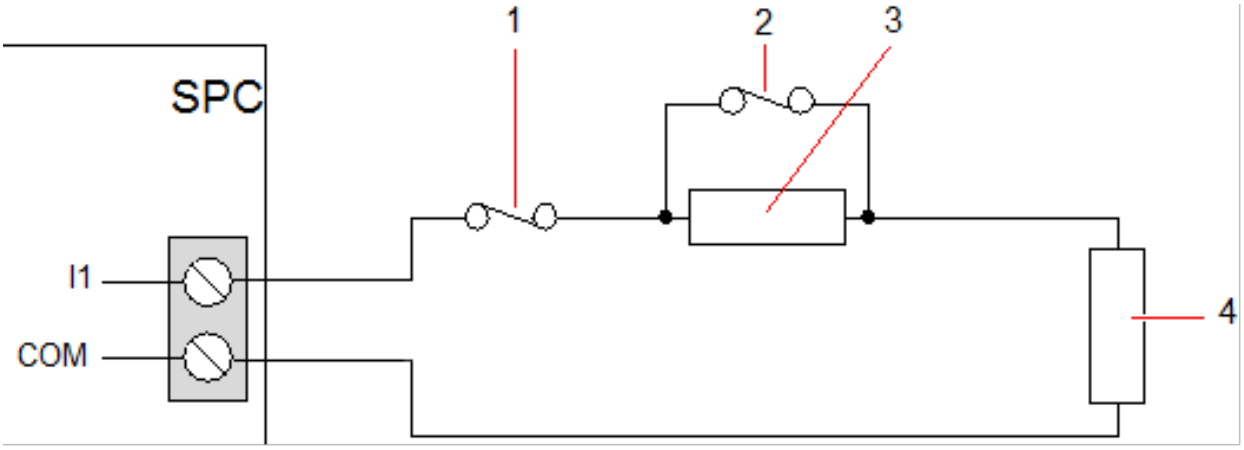
Cableado estándar

NA	Terminal normalmente abierto
COM	Conexión de terminal común
NC	Terminal normalmente cerrado

10.5 Cableado de entradas de zona

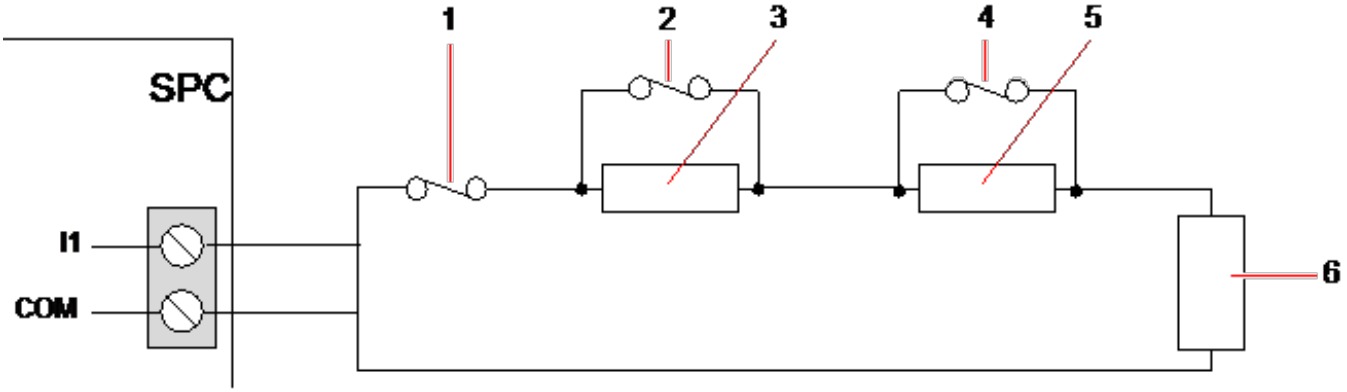
El controlador SPC cuenta con 8 entradas de zona incorporadas. Por defecto, estas entradas se controlan mediante la supervisión de final de línea. El instalador puede escoger una de las siguientes configuraciones cuando cablea las entradas:

- Sin resistencia final de línea (SRFL)
- Una resistencia final de línea (1RFL)
- Dos resistencias finales de línea (2RFL)
- Antienmascaramiento PIR



Configuración por defecto (2 RFL 4k7)

Número	Descripción
1	Tamper
2	Alarma
3	RFL 4k7
4	RFL 4k7



Configuración de PIR antienmascaramiento

Número	Descripción
1	Tamper
2	Alarma
3	RFL 4k7
4	Fallo
5	RFL 2K2
6	RFL 4k7

La tabla a continuación muestra los rangos de resistencia asociados a cada configuración.

1RFL

Tipo de RFL	Reposo			Alarma		
	Mín.	Nom.	Máx.	Mín.	Nom.	Máx.
Ninguna	0 Ω (-100%)	150 Ω	300 Ω (+100%)	300 Ω (+100%)	N/A	Infinito
SINGLE_1K	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	23 kΩ	N/A	Infinito
SINGLE_1K5	1,1 kΩ (-27%)	1,5 kΩ	2,1 kΩ (+40%)	23 kΩ	N/A	Infinito
SINGLE_2K2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	23 kΩ	N/A	Infinito
SINGLE_4K7	3,1 kΩ (-22%)	4,7 kΩ	6,3 kΩ (+24%)	23 kΩ	N/A	Infinito

Tipo de RFL	Reposo			Alarma		
	Mín.	Nom.	Máx.	Mín.	Nom.	Máx.
SINGLE_10K	7 kΩ (-30%)	10 kΩ	13 kΩ (+30%)	23 kΩ	N/A	Infinito
SINGLE_12K	8,5 kΩ (-30%)	12 kΩ	15,5 kΩ (+30%)	23 kΩ	N/A	Infinito

2RFL con enmascaramiento PIR y fallo

Tipo de RFL	Reposo			Alarma		
	Mín.	Nom.	Máx.	Mín.	Nom.	Máx.
Mask_1K_1K_6K8 (1K / 1K / 6K8)	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	1,5 kΩ (-25%)	2 kΩ	2,5 kΩ (+25%)
Mask_1K_1K_2K2 (1K / 1K / 2K2)	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	1,5 kΩ (-25%)	2 kΩ	2,6 kΩ (+30%)
Mask_4K7_4K7_2K2 (4K7 / 4K7 / 2K2)	3,9 kΩ (-18%)	4,7 kΩ	5,6 kΩ (+20%)	8,4 kΩ (-11%)	9,4 kΩ	10,3 kΩ (+10%)

Tipo de RFL	Fallo			Enmascaramiento		
	Mín.	Nom.	Máx.	Mín.	Nom.	Máx.
Mask_1K_1K_6K8	2.700 Ω (-69%)	8,8 kΩ	12,6 kΩ (+20%)	-	-	-
Mask_1K_1K_2K2	2,8 k (-13%)	3,2 k	3,6 k (+13%)	3,8 k (-10%)	4,2 k	4,8 k (+15)
Mask_4K7_4K7_2K2	6 k (-14%)	6,9 k	7,8 k (+14%)	10,8 k (-7%)	11,6 k	12,6 k (+9%)

2RFL

Tipo de RFL	Reposo			Alarma		
	Mín.	Nom.	Máx.	Mín.	Nom.	Máx.
DUAL_1K0_470	400 Ω (-20%)	470 Ω	700 kΩ (+40%)	1,1 kΩ (-27%)	1,5 kΩ	2 kΩ (+34%)
DUAL_1K0_1K0	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	1,5 kΩ (-25%)	2 kΩ	2,6 kΩ (+30%)
DUAL_1k0_2k2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	2,3 kΩ (-29%)	3,2 kΩ	4,2 kΩ (+32%)
DUAL_1k5_2k2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	2,7 kΩ (-28%)	3,7 kΩ	4,8 kΩ (+30%)
DUAL_2K2_2K2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	3,4 kΩ (-23%)	4,4 kΩ	5,6 kΩ (+28%)

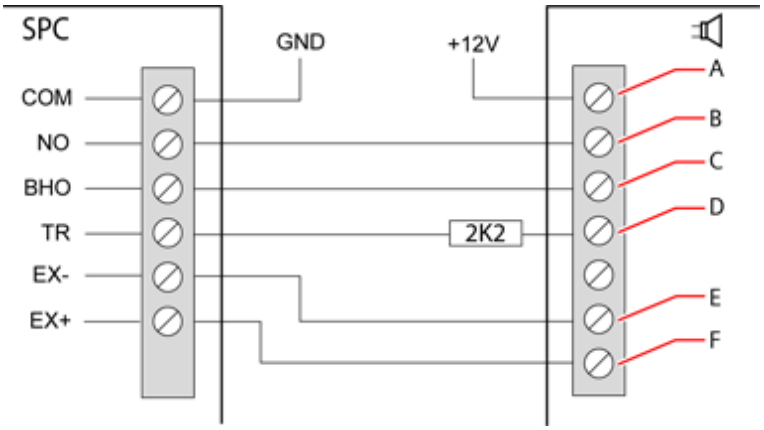
Tipo de RFL	Reposo			Alarma		
	Mín.	Nom.	Máx.	Mín.	Nom.	Máx.
DUAL_2k2_4k7	4,1 kΩ (-13%)	4,7 kΩ	5,4 kΩ (+15%)	6 kΩ (-14%)	6,9 kΩ	7,9 kΩ (+15%)
DUAL_2K7_8K2	7,2 kΩ (-13%)	8,2 kΩ	9,2 kΩ (+13%)	9,9 kΩ (-10%)	10,9 kΩ	11,9 kΩ (+10%)
DUAL_3K0_3K0	2,1 kΩ (-30%)	3,0 kΩ	3,9 kΩ (+30%)	4,5 kΩ (-25%)	6 kΩ	7,5 kΩ (+25%)
DUAL_3K3_3K3	2,3 kΩ (-26%)	3,3 kΩ	4,3 kΩ (+31%)	4,9 kΩ (-26%)	6,6 kΩ	8,3 kΩ (+26%)
DUAL_3K9_8K2	7,0 kΩ (-15%)	8,2 kΩ	9,5 kΩ (+16%)	10,5 kΩ (-14%)	12,1 kΩ	13,8 kΩ (+15%)
DUAL_4K7_2K2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	5 kΩ (-28%)	6,9 kΩ	8,8 kΩ (+28%)
DUAL_4K7_4K7	3,3 kΩ (-30%)	4,7 kΩ	6,1 kΩ (+30%)	7 kΩ (-26%)	9,4 kΩ	11,9 kΩ (+27%)
DUAL_5K6_5K6	4,0 kΩ (-26%)	5,6 kΩ	7,2 kΩ (+29%)	8,3 kΩ (-26%)	11,2 kΩ	14,1 kΩ (+26%)
DUAL_6K8_4K7	3,3 kΩ (-30%)	4,7 kΩ	6,1 kΩ (+30%)	8,1 kΩ (-30%)	11,5 kΩ	14,9 kΩ (+30%)
DUAL_2k2_10K	9,2 kΩ (-8%)	10 kΩ	10,8 kΩ (+8%)	11,3 kΩ (-8%)	12,2 kΩ	13,2 kΩ (+9%)
DUAL_10k_10k	7,5 kΩ (-25%)	10 kΩ	12,5 kΩ (+25%)	17 kΩ (-15%)	20 kΩ	23 kΩ (+15%)

Para todos los tipos de RFL, una resistencia inferior a 300 Ω se considera un cortocircuito. Si la resistencia no se encuentra dentro de los umbrales indicados, se considera una desconexión.

10.6 Cableado de una sirena SAB exterior

En una sirena exterior a la placa del controlador SPC, la salida de relé está conectada a la entrada de flash con las salidas Bell Hold Off (BHO) y TR (Tamper Return) conectadas a sus respectivas entradas en la interfaz de la sirena exterior.

Existe una resistencia (2K2) previamente ensamblada en la placa del controlador entre los terminales BHO y TR. Cuando se realiza el cableado de una sirena exterior, conecte esta resistencia en serie desde el terminal TR del controlador hacia el terminal TR de la interfaz de la sirena exterior.

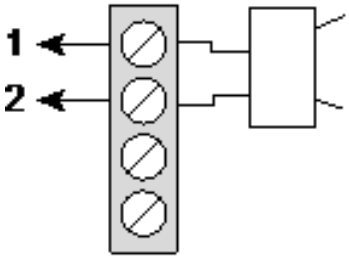


Cableado sirena exterior

Etiqueta	Descripción
A	Flash +
B	Flash –
C	Hold off
D	Tamper return
E	Sirena -
F	Sirena +

10.7 Cableado de una sirena interior

Para cablear una sirena interior hasta el controlador SPC, conecte los terminales IN+ e IN– directamente a la entrada de la sirena de 12 V.



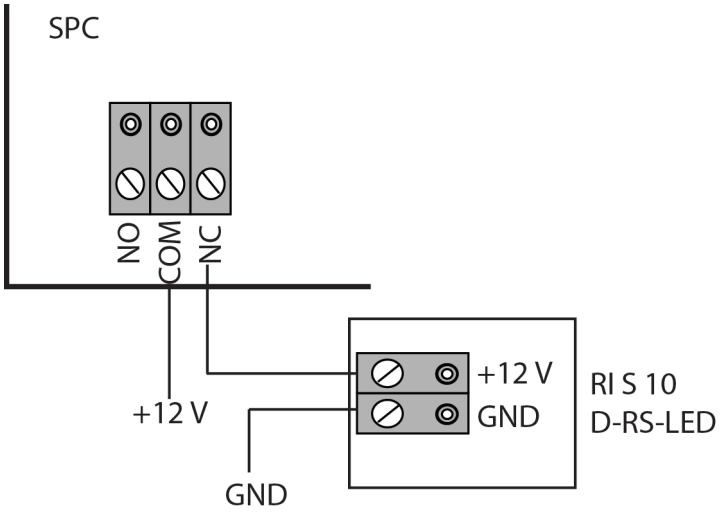
Cableado de sirena interior (12 V)

IN–	IN– (Controlador SPC)
IN+	IN+ (Controlador SPC)

10.8 Cableado para rotura de cristal

El SPC admite la interfaz de rotura de cristal RI S 10 D-RS-LED en combinación con detectores de rotura de cristal GB2001.

El siguiente diagrama muestra cómo se cablea la interfaz de rotura de cristal al controlador SPC para alimentación, o a un módulo de expansión de 8 entradas / 2 salidas:



Para más información sobre el cableado de la interfaz de rotura de cristal con una zona, véase la documentación específica del producto.

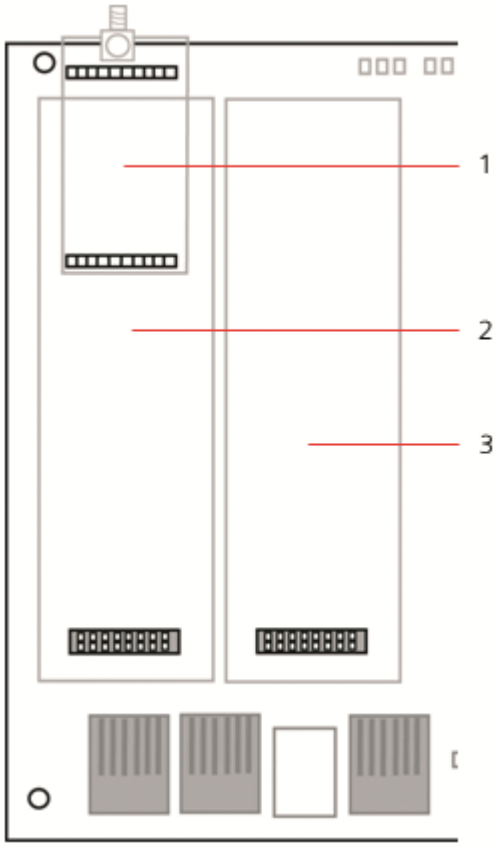
Para más información sobre el cableado de los sensores de rotura de cristal a la interfaz de rotura de cristal, véase la documentación específica del producto.

10.9 Instalación de módulos enchufables

Se pueden instalar dos módems (RTB o GSM) en la placa del controlador para incrementar la funcionalidad. La imagen a continuación muestra las 2 ranuras disponibles para cada módem: la ranura principal (izquierda) y la ranura de respaldo (derecha).

Si ambas ranuras del módem están disponibles, siempre debe conectar el módulo enchufable en la ranura principal. El sistema siempre intenta realizar llamadas RTB o GSM en un módem instalado en la ranura principal antes de intentar usar la ranura de respaldo.

ADVERTENCIA: Los módems no son del tipo plug-and-play. Debe iniciar sesión en la central en Modo técnico y, a continuación, apagar la placa del controlador antes de instalar, retirar o mover módems de una posición a otra. Tras completar la tarea del módem, vuelva a conectar el sistema a la fuente de alimentación y vuelva a iniciar sesión en el controlador en Modo técnico. Configure y guarde la configuración. Si no se sigue este proceso, se producirá un error de CRC.



Módulos enchufables

Número	Descripción
1	Ranura de receptor vía radio
2	Ranura del módem principal
3	Ranura de módem de respaldo

Para obtener información de instalación, consulte el manual de instrucciones de instalación que corresponda.

Encontrará las guías de instalación disponibles en http://www.spcsupportinfo.com/connectspcdata/userdata.

11 Alimentación del controlador SPC

El controlador SPC tiene dos fuentes de alimentación: el suministro de la red de CA y la batería de respaldo. Un electricista calificado debe realizar las conexiones a la red de CA, la cual debe estar conectada desde una punta que pueda ser aislada. Consulte *Cableado de la red CA al controlador* en la página 391 para obtener más información sobre los tamaños de conductores, las clasificaciones de fusibles, etc.

Luego, el SPC debe recibir alimentación desde la red de CA primero y, luego, desde la batería de respaldo. Para que se cumpla con la norma EN, se debe utilizar solo una batería de la capacidad adecuada.

11.1 Alimentación desde la batería únicamente

Se recomienda que, cuando se suministre alimentación a un sistema solo desde la batería, la batería esté completamente cargada (>13,0 V). El sistema no se encenderá cuando utilice una batería con menos de 12 V y no se aplique red de CA.

AVISO: La batería continuará alimentando el sistema hasta que se detecte un nivel de descarga mínimo (10,5 V a 10,8 V). El tiempo que permanecerá el sistema activo con la batería dependerá de la carga externa y de la clasificación de Ah de la batería.

12 Interfaz de usuario del teclado

Están disponibles los siguientes modelos de teclado:

- SPCK420/421: también denominado teclado LCD en todo este documento.
- SPCK620/623: también denominado teclado confort en todo este documento.

12.1 SPCK420/421

Esta sección abarca:

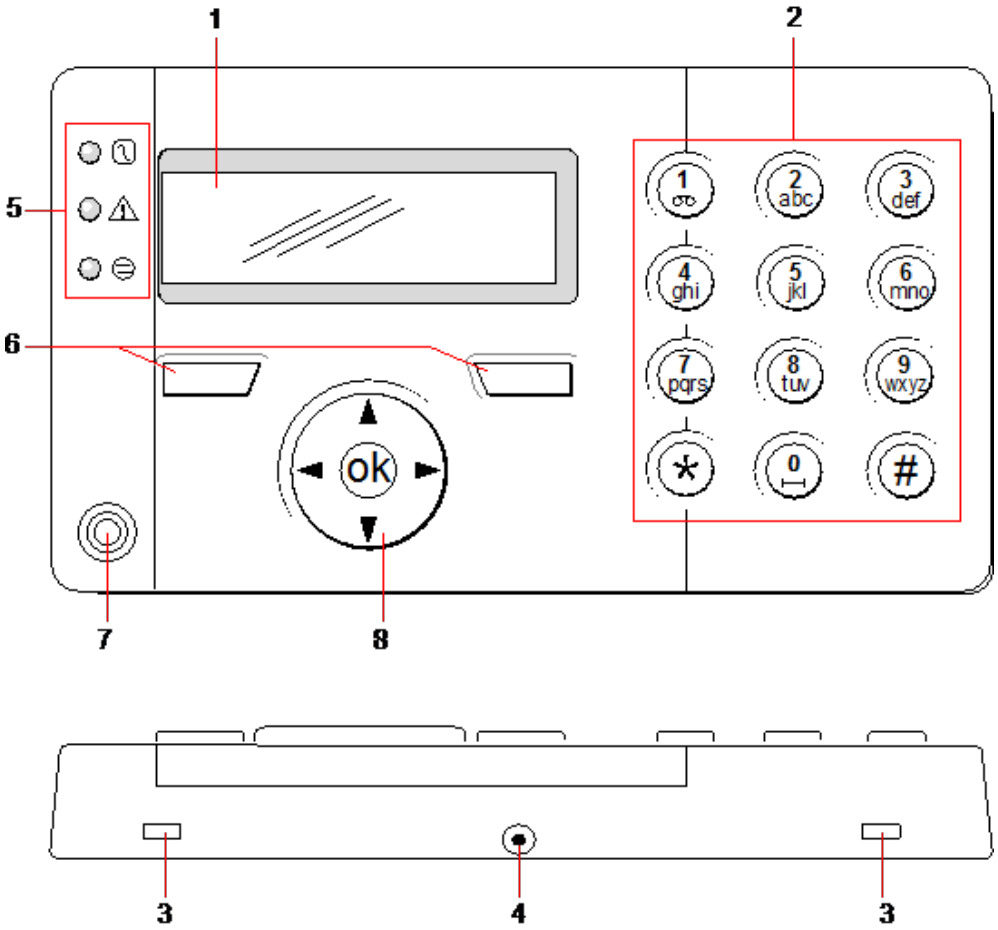
12.1.1 Acerca del teclado LDC

El teclado LCD es una interfaz de usuario montada en la pared que permite:

- **A los técnicos** programar el sistema a través de los menús de programación del técnico (protegidos con clave) y armar/desarmar el sistema; un usuario puede controlar el sistema a diario.
- **A los usuarios** acceder a los menús de programación para usuarios (protegidos con clave) y ejecutar procesos operacionales (armado/desarmado) en el sistema. (Consulte *Manual de usuario SPCK420/421* para obtener más información sobre la programación de usuarios).

La unidad del teclado LCD incluye un interruptor de tamper frontal integral y una pantalla de 2 líneas de 16 caracteres. También incluye una tecla de navegación sencilla para ayudar a localizar las opciones de programación requeridas, y dos teclas programables (izquierda y derecha) para seleccionar el menú o la configuración del programa requeridos. Tres indicadores LED en el teclado indican el estado de la alimentación de CA, de las alertas del sistema y de las comunicaciones.

El teclado LCD puede incorporar de fábrica un lector de dispositivos de proximidad Portable ACE (PACE) (consulte *Información general de tipos de teclados* en la página 389).



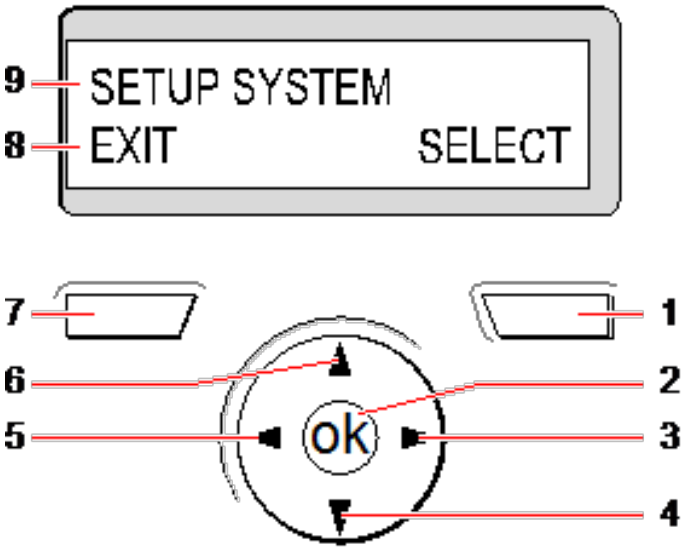
Teclado LCD

Número	Nombre	Descripción
1	Pantalla LCD	La pantalla del teclado (2 líneas de 16 caracteres) muestra todos los mensajes de incidencias y de advertencia, además de proporcionar una interfaz visual para la programación del sistema (sólo programación de técnico). De la pantalla se puede ajustar el contraste y las condiciones en las que se produce la retroiluminación.
2	Teclas alfanuméricas	El teclado alfanumérico permite la entrada tanto de datos numéricos como de texto durante la programación. Los caracteres alfabéticos se seleccionan pulsando la cantidad de veces adecuada las teclas correspondientes. Para alternar entre mayúsculas y minúsculas, pulse la tecla de almohadilla (#). Para introducir un carácter numérico, mantenga pulsada la tecla correspondiente durante 2 segundos.
3	Pestañas accesibles por palanca	Las pestañas accesibles por palanca proporcionan acceso a las pinzas de montaje posteriores del teclado. Los usuarios pueden abrir estas pinzas desde la parte frontal insertando un destornillador de 5 mm en las ranuras y empujando suavemente.
4	Tornillo de fijación de montaje posterior	Este tornillo fija los soportes frontal y posterior del teclado. Para abrir el teclado es necesario extraer este tornillo.
5	LED indicadores de estado	Los LED indicadores de estado proporcionan información acerca del estado actual del sistema, como se describe en la siguiente tabla.

Número	Nombre	Descripción
6	Teclas de función programables	Las teclas de función programables izquierda y derecha son teclas sensibles al contexto que permiten desplazarse por los menús y la programación.
7	Área del receptor de dispositivo en proximidad	Si el teclado incluye un receptor de dispositivos de proximidad (consulte *Información general de tipos de teclados* en la página 389), los usuarios deberán presentar el mando Portable ACE a una distancia de un 1 cm sobre esta área para ARMAR/DESARMAR el sistema.
8	Tecla multifunción de navegación	La tecla multifunción de navegación, en combinación con la pantalla del teclado, proporciona una interfaz para programar el sistema.

LED		Estado
Toma de CA general (Verde)		Indica la existencia de tensión de red o de un fallo en la red. PARPADEANDO: Fallo detectado en la red de CA. FIJO: Red de CA correcta.
Alerta del sistema (Amarillo)	⚠	Indica una alerta del sistema PARPADEANDO: Alerta del sistema detectada; la pantalla muestra la ubicación y la naturaleza de la alerta. Si el sistema se encuentra ARMADO, NO se muestra ningún indicador de alerta del sistema. APAGADO: No se han detectado alertas. Si se asigna un teclado a más de una zona, el LED no indica una condición de alerta si alguna de estas particiones está ARMADA.
Estado X Bus (Rojo)		Indica el estado de las comunicaciones de X-BUS durante la programación en modo TÉCNICO COMPLETO. Parpadea regularmente: (una vez cada 1,5 segundos aprox.) indica que el estado de las comunicaciones es correcto. Parpadea rápidamente: (una vez cada 0,25 segundos aprox.) indica que el teclado es el último módulo de expansión del X-BUS. Si se va a instalar el teclado por primera vez y se ha suministrado alimentación al mismo antes de conectarlo a la interfaz X-BUS del controlador, el LED permanece en estado ENCENDIDO.

12.1.2 Uso de la interfaz del teclado LCD



Pantalla del teclado

Número	Nombre	Descripción
1	TECLA PROGRAMABLE DERECHA	Esta tecla se utiliza para seleccionar la opción que se muestra en el lado derecho de la línea inferior de la pantalla. Estos son los valores posibles: • SELECC para seleccionar la opción que se muestra en la línea superior • INTRO para introducir los datos que se muestran en la línea superior • SIGUIENTE para ver la alerta siguiente después de la que se muestra en la línea superior • BORRAR para borrar la alerta que se muestra en la línea superior • SALVAR para salvar la configuración
2	OK	El botón OK actúa como una tecla de SELECC. para la opción de menú mostrada en la línea superior y también como tecla ENTER/SALVAR para los datos que aparecen en la línea superior.
3	▶	En el modo de programación, la tecla de la flecha hacia la derecha permite al usuario avanzar por los menús de la misma forma que al pulsar la opción SELECC. (tecla programable derecha). En el modo de entrada de datos, pulse esta tecla para mover el cursor una posición a la derecha.
4	▼	En el modo de programación, con la tecla de la flecha hacia abajo, el usuario se desplaza a la siguiente opción de programación del mismo nivel del menú. Si pulsa esta tecla de forma continuada, se desplazará por todas las opciones de programación disponibles en el nivel del menú actual. En el modo alfanumérico, si pulsa esta tecla sobre un carácter en mayúsculas, el carácter cambia a minúsculas. Cuando se muestran alertas, con la tecla de flecha hacia abajo, el usuario se desplaza al siguiente mensaje de alerta en orden de prioridad. (Consulte *Priorización de mensajes en pantalla* en la página opuesta.)

Número	Nombre	Descripción
5	◀	En el modo de programación, la tecla de la flecha hacia la izquierda permite que el usuario vuelva al nivel anterior del menú. Si pulsa esta tecla estando en el nivel del menú superior, el usuario saldrá de la programación. En el modo de entrada de datos, pulse esta tecla para mover el cursor una posición a la izquierda.
6	▲	En el modo de programación, la tecla de la flecha hacia arriba lleva al usuario a la opción de programación anterior del mismo nivel del menú. Si pulsa esta tecla de forma continuada, se desplazará por todas las opciones de programación disponibles en el nivel del menú actual. En el modo alfanumérico, si pulsa esta tecla sobre un carácter en minúsculas, el carácter cambia a mayúsculas.
7	TECLA PROGRAMABLE IZQUIERDA	Esta tecla se utiliza para seleccionar la opción que se muestra en el lado izquierdo de la línea inferior de la pantalla. Estos son los valores posibles: • SALIR para salir de la programación • ATRÁS para volver al menú anterior
8	LÍNEA INFERIOR DE LA PANTALLA	En estado INACTIVO, esta línea aparece en blanco. En el modo de programación, esta línea muestra las opciones disponibles para el usuario. Estas opciones se encuentran alineadas sobre las teclas programables izquierda y derecha, según sea necesario.
9	LÍNEA SUPERIOR DE LA PANTALLA	En estado INACTIVO, muestra la fecha y la hora actuales. En el modo de programación, esta línea muestra una de las siguientes opciones: • La función de programación que se va a seleccionar • La configuración actual de la función seleccionada • La naturaleza de la alerta actual durante una condición de alerta (Consulte *Priorización de mensajes en pantalla* abajo.)

Priorización de mensajes en pantalla

Los mensajes de problemas y las alertas se muestran en el teclado en el siguiente orden:

- Zona
  - – Alarmas
  - – Tamper
  - – Problema
- Alertas de partición
  - – Fallo al armar
  - – Tiempo de espera de entrada
  - – Tamper de código
- Estado sistema
  - – Red CA
  - – Batería
  - – Fallo fuente alimentación

– Fallo Aux.
– Fusible sirena exterior
– Fusible sirena interior
– Tamper de sirena
– Tamper de carcasa
– Tamper auxiliar 1
– Tamper auxiliar 2
– Interferencia vía radio
– Fallo módem 1
– Línea módem 1
– Fallo módem 2
– Línea módem 2
– Fallo comunicación
– Pánico usuario
– Fallo cable X-BUS
– Fallo comunicación X-BUS
– Fallo CA X-BUS
– Fallo batería X-BUS
– Fallo fuente alimentación X-BUS
– Fallo fusible X-BUS
– Fallo tamper X-BUS
– Fallo antena X-BUS
– Interferencia vía radio X-BUS
– Pánico X-BUS
– Incendio X-BUS
– Alarma médica X-BUS
– Enlace fuente alimentación X-BUS
– Tamper de salida X-BUS
– Bajo voltaje X-BUS
– Restauración de técnico requerida
– Autoarmado

- Información del sistema
  – Zonas en prueba
  – Zonas abiertas
  – Estado de partición
  – Batería baja (detector)
  – Sensor perdido
  – Batería baja APR
  – APR perdida

– Test APR retrasado

– Cámara fuera de línea

– Batería baja mando

– Sobrecorriente X-BUS

– Nombre del instalador

– Teléfono del instalador

– Técnico habilitado

– Fabr. habilitado

– Reiniciar

– Fallo de hardware

– Sobrecorriente Aux.

– Batería baja

– Enlace Ethernet

– Nombre del sistema

12.1.3 Introducción de datos en el teclado LCD

La introducción de datos y la exploración de los menús en el teclado LCD tienen lugar mediante el uso de la interfaz de programación. A continuación, se detalla el uso de la interfaz para cada tipo de funcionamiento.

Introducir valores numéricos

En el modo de Entrada numérica, solo se pueden introducir dígitos numéricos (0 a 9).

- Para mover la posición del cursor un carácter a la izquierda y a la derecha respectivamente, pulse las teclas de flecha a la izquierda y a la derecha.
- Para salir de la función sin salvar los cambios, pulse la tecla ATRÁS del menú.
- Para salvar la configuración programada, pulse INTRO o ACEPTAR.

Introducir texto

En el modo de Entrada de texto, se pueden introducir caracteres alfabéticos (A a Z) y dígitos numéricos (0 a 9).

- Para introducir un carácter alfabético, pulse la tecla que corresponde la cantidad de veces que sea necesaria.
- Para introducir un carácter especial específico de un idioma (ä, ü, ö…), pulse el botón 1 para avanzar por los caracteres especiales.
- Para introducir un espacio + caracteres especiales (+, -./[ ]…), pulse el botón 0.
- Para introducir un dígito, mantenga la tecla que corresponde presionada durante 2 segundos y suelte la tecla.
- Para mover la posición del cursor un carácter a la izquierda y a la derecha respectivamente, pulse las teclas de flecha a la izquierda y a la derecha.
- Para salir de la función sin salvar los cambios, pulse ATRÁS.
- Para salvar la configuración programada, pulse INTRO o ACEPTAR.
- Para alternar entre mayúscula y minúscula para un carácter, pulse las teclas hacia abajo y hacia arriba cuando el carácter esté resaltado por el cursor.
- Para alternar entre mayúsculas y minúsculas para el resto de los caracteres, pulse la tecla de almohadilla (#).
- Para eliminar un carácter a la izquierda del cursor, pulse la tecla asterisco (*).

Seleccionar una opción de programación

En el modo Navegación, el técnico/usuario selecciona una opción de una lista de opciones de programación definidas previamente.

- Para desplazarse por las opciones disponibles y realizar la selección, pulse las flechas hacia abajo y hacia arriba.
- Para salir de la función sin salvar los cambios, pulse ATRÁS.
- Para salvar la configuración seleccionada, pulse INTRO o ACEPTAR.

12.2 SPCK620/623

Esta sección abarca:

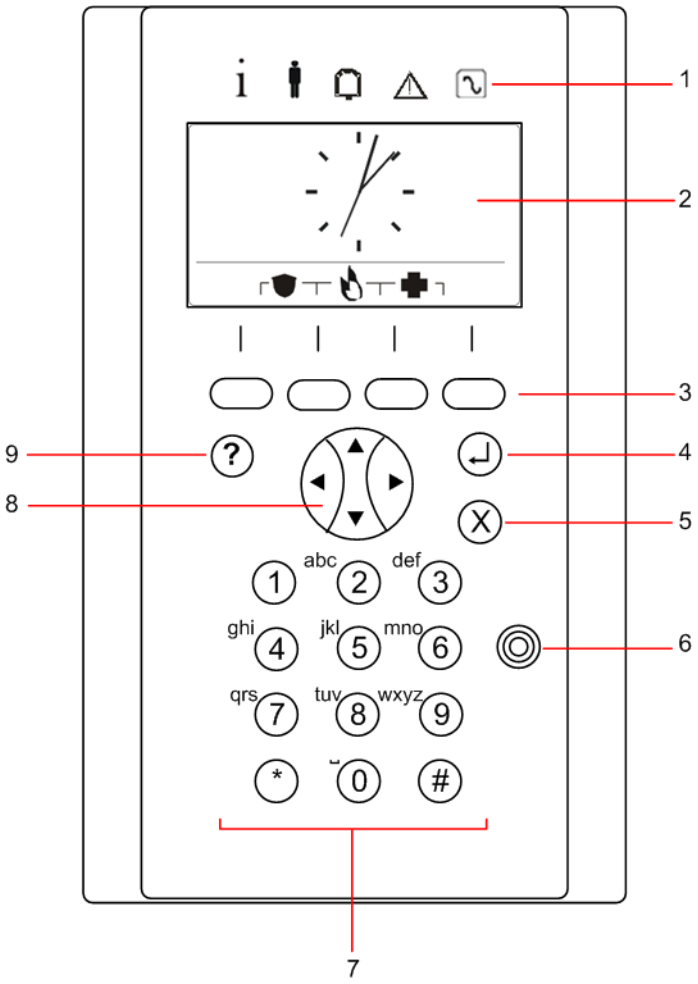
12.2.1 Acerca del teclado Comfort

El teclado Comfort es una interfaz de usuario montada en la pared que permite:

- A los técnicos programar el sistema a través de los menús de programación del técnico (protegidos con clave) y armar/desarmar el sistema; un usuario puede controlar el sistema a diario.
- A los usuarios acceder a los menús de programación para usuarios (protegidos con clave) y ejecutar procesos operacionales (armado/desarmado) en el sistema. (Consulte *Manual de usuario SPC620/623* para obtener más información sobre la programación de usuarios)

El SPCK620 está equipado con teclas programables y una amplia pantalla LCD, lo que facilita su manejo. Sus funciones se pueden mejorar con un módulo de expansión de interruptor de llave SPCE110 ó un módulo de expansión de indicación SPCE120.

El SPCK623 está equipado con un lector de tarjeta de proximidad (125 kHz EM 4102) para un acceso más fácil del usuario, teclas programables, una amplia pantalla LCD y soporte de ayuda vocal. Sus funciones se pueden mejorar con un módulo de expansión de interruptor de llave SPCE110 ó un módulo de expansión de indicación SPCE120.



Número	Nombre	Descripción
1	LED indicadores de estado	Los LED indicadores de estado proporcionan información acerca del estado actual del sistema, según se describe en *Descripción de LED* en la página 112.
2	Pantalla LCD	La pantalla del teclado muestra todos los mensajes de alerta y de advertencia, además de proporcionar una interfaz visual para la programación del sistema (sólo programación de técnico). (Consulte *Priorización de mensajes en pantalla* en la página siguiente). Se pueden configurar las condiciones en las que se produce la retroiluminación de la pantalla.
3	Teclas de función programables	Teclas sensibles al contexto que permiten desplazarse por los menús y la programación.
4	Tecla Enter	Confirmar pantalla o entrada.
5	Tecla de menú Atrás	Volver al menú. Restablecer los zumbadores, las sirenas y las alarmas de la memoria.
6	Área del receptor de dispositivo en proximidad	Sólo SPCK 623: Si el teclado incluye un receptor de dispositivos de proximidad, los usuarios deberán presentar el mando Portable ACE a una distancia de un 1 cm sobre esta área.

Número	Nombre	Descripción
7	Teclas alfanuméricas	El teclado alfanumérico permite la entrada tanto de datos numéricos como de texto durante la programación. Los caracteres alfabéticos se seleccionan pulsando la cantidad de veces adecuada las teclas correspondientes. Para alternar entre mayúsculas y minúsculas, pulse la tecla de almohadilla (#). Para introducir un carácter numérico, mantenga pulsada la tecla correspondiente durante 2 segundos.
8	Tecla multifunción de navegación	Navegación a través de menús y para desplazarse por los mensajes de alerta. (Consulte *Priorización de mensajes en pantalla* abajo.)
9	Tecla de información	Muestra información.

Priorización de mensajes en pantalla

Los mensajes de problemas y las alertas se muestran en el teclado en el siguiente orden:

- Zona
  - – Alarmas
  - – Tamper
  - – Problema
- Alertas de partición
  - – Fallo al armar
  - – Tiempo de espera de entrada
  - – Tamper de código
- Estado sistema
  - – Red CA
  - – Batería
  - – Fallo fuente alimentación
  - – Fallo Aux.
  - – Fusible sirena exterior
  - – Fusible sirena interior
  - – Tamper de sirena
  - – Tamper de carcasa
  - – Tamper auxiliar 1
  - – Tamper auxiliar 2
  - – Interferencia vía radio
  - – Fallo módem 1
  - – Línea módem 1
  - – Fallo módem 2
  - – Línea módem 2
  - – Fallo comunicación
  - – Pánico usuario

– Fallo cable X-BUS
– Fallo comunicación X-BUS
– Fallo CA X-BUS
– Fallo batería X-BUS
– Fallo fuente alimentación X-BUS
– Fallo fusible X-BUS
– Fallo tamper X-BUS
– Fallo antena X-BUS
– Interferencia vía radio X-BUS
– Pánico X-BUS
– Incendio X-BUS
– Alarma médica X-BUS
– Enlace fuente alimentación X-BUS
– Tamper de salida X-BUS
– Bajo voltaje X-BUS
– Restauración de técnico requerida
– Autoarmado

- Información del sistema
  – Zonas en prueba
  – Zonas abiertas
  – Estado de partición
  – Batería baja (detector)
  – Sensor perdido
  – Batería baja APR
  – APR perdida
  – Test APR retrasado
  – Cámara fuera de línea
  – Batería baja mando
  – Sobrecorriente X-BUS
  – Nombre del instalador
  – Teléfono del instalador
  – Técnico habilitado
  – Fabr. habilitado
  – Reiniciar
  – Fallo de hardware
  – Sobrecorriente Aux.
  – Batería baja
  – Enlace Ethernet
  – Nombre del sistema

12.2.2 Descripción de LED

Descripción	Símbolo	Color	Funcionamiento	Descripción
Información		Azul	ON	El sistema o la partición no se pueden armar. El armado forzado es posible (se pueden anular fallos o zonas abiertas).
			Parpadeante	El sistema o la partición no se pueden armar ni tampoco se puede realizar el armado forzado (no se pueden anular fallos o zonas abiertas).
			Off	El sistema o la partición se pueden armar.
		Ámbar	Parpadeante	Técnico en la instalación.
Operador		verde	ON	La partición asignada está desarmada.
			Parpadeante	La partición asignada está armada parcialmente A/B
			Off	La partición asignada está armada totalmente
Alarma		rojo	ON	Alarma
			Parpadeante	-
			Off	No hay alarma
Alerta		Ámbar	ON	-
			Parpadeante	Problema
			Off	No hay problema
Red CA		verde	ON	Sistema ok
			Parpadeante	Fallo red c. a.
			Off	Sin conexión de bus

AVISO: Las indicaciones de LED para información, estado de partición, alarma y fallo están desactivadas cuando el teclado está en estado de reposo. Se debe introducir un PIN de usuario válido. Es configurable si la indicación de energía se puede ver en estado inactivo.

12.2.3 Descripción de modo de visualización

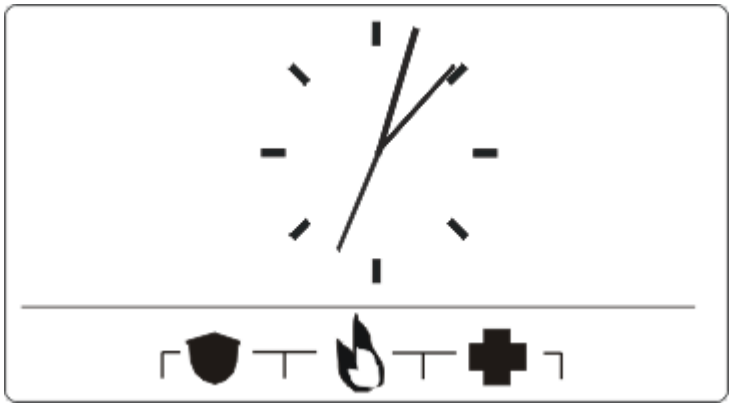
Existen dos modos de visualización (automático):

- Vista de particiones múltiples: El usuario tiene acceso a diversas particiones. La visualización de las particiones se realiza a través de grupos de particiones. Si no hay ningún grupo de partición configurado, solo se visualiza el grupo general «Todas mis particiones».
- Vista de partición simple: El usuario solo tiene derechos para 1 partición. En la vista de partición simple, solo se muestra una partición con fuentes de gran tamaño, y esta puede controlarse directamente.

Los derechos del usuario pueden estar restringidos por la configuración o los ajustes del teclado en el cual el usuario está iniciando sesión. Solo se mostrará la partición si el usuario y el teclado que está utilizando para iniciar sesión tienen derecho para esa partición. Si el usuario tiene derecho de acceso a diversas particiones, pero el teclado tiene derecho solo para una partición, el usuario solo verá una partición.

12.2.4 Teclas de función en reposo

Teclas de emergencia

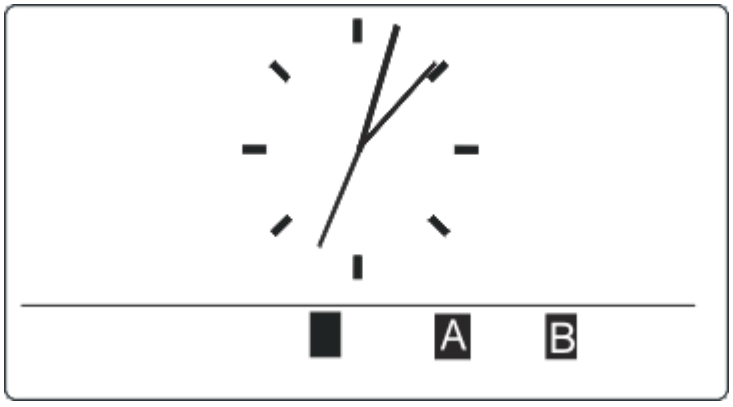


Las teclas de emergencia se muestran en función de la configuración. Al pulsar las teclas de forma simultánea, se activa una llamada de emergencia.

	Alarma de pánico
	Alarma incendio
	Alarma médica

El proceso activado depende de la configuración del sistema. Consulte al instalador para obtener más información.

Configuración directa



Dependiendo de la configuración, se visualiza la opción de armado directo. Se puede activar un armado forzado/armado parcial sin el código PIN de la partición a la cual está asignado el teclado.

13 Herramientas de software de apoyo

La siguiente herramienta de software para PC está disponible para la gestión remota de una central SPC:

- **SPC Manager**
  Permite crear, controlar y modificar de forma remota la funcionalidad basada en acceso dentro del sistema SPC.

14 Inicio del sistema

PRECAUCIÓN: El sistema SPC debe ser instalado por un técnico instalador autorizado.

1. Conecte el teclado a la interfaz X-BUS del controlador.
2. Acceda a la programación en modo de técnico al introducir el código PIN de técnico por defecto (1111). Para obtener más información, consulte *Código PIN de técnico* abajo.

14.1 Modos técnicos

El sistema SPC funciona con dos modos de programación para técnicos instaladores autorizados: Completo y Normal. En el navegador, solo se permite finalizar la sesión en modo técnico normal.

Modo técnico completo

Se debe aislar o borrar cualquier alerta, fallo y tamper antes de que se autorice la salida del modo técnico completo.

El modo técnico completo proporciona una funcionalidad de programación más completa. Sin embargo, el modo técnico completo deshabilita todos los ajustes de alarmas, informes y programación de salidas para el sistema. Para obtener una descripción completa de todas las opciones del menú Técnico completo, consulte *Programación de técnico a través del teclado* en la página 125.

Modo técnico normal

El modo técnico normal proporciona menos funciones de programación y no afecta las salidas programadas en el sistema. Para obtener una descripción completa de todas las opciones del menú Técnico normal, consulte *Programación de técnico normal a través del teclado* en la página 123.

14.1.1 Código PIN de técnico

El código PIN de técnico para programación por defecto para la puesta en marcha es ‘1111’.

Si, tras la puesta en marcha, la instalación cambia de Grado 2 a Grado 3, todos los códigos PIN tienen el prefijo 0. Por lo tanto, el código PIN de técnico por defecto será ‘01111’.

El aumento de la cantidad de dígitos para el código PIN (consulte *Opciones* en la página 254) agregará la cantidad relevante de ceros adelante del código PIN existente (por ejemplo: 001111 para un código PIN de 6 dígitos).

AVISO: Si se habilita por defecto el código PIN 1111, por ejemplo, y se realiza una nueva instalación de SPC, debe cambiar el código PIN de técnico en la central. Si no cambia el código PIN, recibirá un mensaje de información que le solicitará que cambie el código PIN por defecto antes de salir del modo técnico completo.

14.2 Programación con el teclado

El teclado proporciona acceso rápido in situ a los menús y a la programación del sistema. El técnico de instalación autorizado debe establecer la configuración por defecto con el teclado. También se debe realizar la programación del lector de tarjetas/dispositivos de proximidad y la asignación de usuarios a través del teclado.

14.3 Configurar ajustes de puesta en marcha

Puede cambiar los ajustes de puesta en marcha en otro momento cuando programe la funcionalidad del sistema.

Si se está alimentando la central, en el teclado se mostrará el número de versión del sistema SPC.

Requisito previo

- Para iniciar la configuración de inicio, mantenga pulsado el botón de restablecimiento en la placa durante al menos 6 segundos.

1. Pulse una tecla del teclado.

   - Después de cada ajuste, pulse SIGUIENTE para desplazarse al siguiente ajuste.

2. Seleccione el IDIOMA en el que se mostrará el asistente de configuración.
3. Seleccione la REGIÓN que corresponda.

   - EUROPA, SUECIA, SUIZA, BÉLGICA, ESPAÑA REINO UNIDO, IRLANDA, ITALIA, CANADÁ, EE. UU.

4. Seleccione el TIPO de instalación:

   - DOMÉSTICA: es adecuada para un uso doméstico (casas y apartamentos).

   - INDUSTRIAL: proporciona tipos de zona adicionales y descripciones de zona comercial por defecto para las primeras ocho zonas.

   - FINANCIERA: específica para bancos e instituciones financieras, incluye funciones como autoarmado, bloqueos temporales, grupos de interbloqueos y tipo de zona sísmica.

   Para obtener más información sobre las descripciones de las zonas por defecto, consulte *Ajustes por defecto de modo doméstico, comercial y financiero* en la página 380.

5. Seleccione el grado de seguridad de su instalación.
6. IDIOMA Se muestran los idiomas disponibles por defecto en el sistema. A continuación se muestran los idiomas disponibles por defecto para cada región:

   - IRLANDA/REINO UNIDO: inglés, francés, alemán

   - EUROPA/SUIZA/ESPAÑA/FRANCIA/ALEMANIA: inglés, francés, alemán, italiano, español

   - BÉLGICA: inglés, holandés, flamenco, francés, alemán

   - SUECIA: inglés, sueco, danés, francés, alemán

   AVISO: Si el sistema se encuentra en su configuración por defecto y la REGIÓN se modifica al iniciarse, solo estarán disponibles para la nueva REGIÓN los idiomas que estén actualmente en el sistema para la REGIÓN anterior.

7. Seleccione los idiomas que requiere para su instalación. Los idiomas seleccionados aparecen marcados con un asterisco (*) delante. Para eliminar o seleccionar un idioma, pulse almohadilla (#) en el teclado.

   Los idiomas que no se hayan seleccionado se borran del sistema, y no estarán disponibles si restablece el sistema al estado por defecto.

Para añadir otros idiomas a la central, consulte *Actualización de idiomas* en la página 351. Para añadir otros idiomas al teclado, consulte la documentación de ese teclado. Encontrará las guías de instalación disponibles en http://www.spcsupportinfo.com/connectspcdata/userdata.

8. Introduzca la FECHA y la HORA.

   El sistema explora el X-BUS en busca de módems.

9. Habilite SPC CONNECT para que la central se comunique con https://www.spcconnect.com tras haber configurado la dirección IP.
10. Habilite la opción DHCP para asignar automáticamente una dirección IP de red disponible a la central. Si habilitó SPC CONNECT Y DHCP, se agrega un ATS SPC CONNECT a la central para completar la conexión a https://www.spcconnect.com
11. Para las centrales habilitadas para DHCP, la dirección IP asignada automáticamente aparece en el menú DIRECCIÓN IP. Si la opción DHCP no está habilitada, aparece la dirección IP por defecto. Pulse SELECC. para continuar. En el modo Programación de técnico, debajo de COMUNICACIONES, debe introducir manualmente la dirección IP estática de la central.
12. Seleccione el modo de direccionamiento X-BUS:

    - MANUAL: recomendado para la mayoría de los tipos de instalación, especialmente cuando se realiza una preconfiguración.

    - AUTOMÁTICO: se recomienda solo para instalaciones muy pequeñas.

13. Seleccione la topología de instalación: LAZO (anillo) o PUNTA (cadena).

    El sistema escanea la cantidad de teclados, módulos de expansión, controladores de puertas y entradas de zona disponibles.

14. Pulse SIGUIENTE para explorar todos los dispositivos X-BUS.

    Aparecerá el MODO DE PROGRAMACIÓN.

    Los ajustes de puesta en marcha están completos.

15. Marque las alertas en el menú ESTADO DEL SISTEMA > ALERTAS. De lo contrario, no podrá salir del modo técnico.
16. Configure el sistema a través del teclado o del navegador web.

Consulte también

Ajustes por defecto de modo doméstico, comercial y financiero en la página 380

14.4 Crear usuarios del sistema

Por defecto, el sistema SPC sólo permite al técnico acceder al sistema. El técnico debe crear Usuarios para permitir al personal armar, desarmar y realizar operaciones básicas en el sistema según sea necesario. Los usuarios tienen el uso restringido a una serie de operaciones de la central al asignárseles perfiles de usuario específicos.

El sistema admite todos los códigos PIN de usuario dentro del rango de códigos PIN permitido; p. ej., si se usa un código PIN de 4 dígitos, se permitirían todos los códigos PIN de usuario del 0000 al 9999.

Consulte *Usuarios* en la página 173 o *Usuarios* en la página 209.

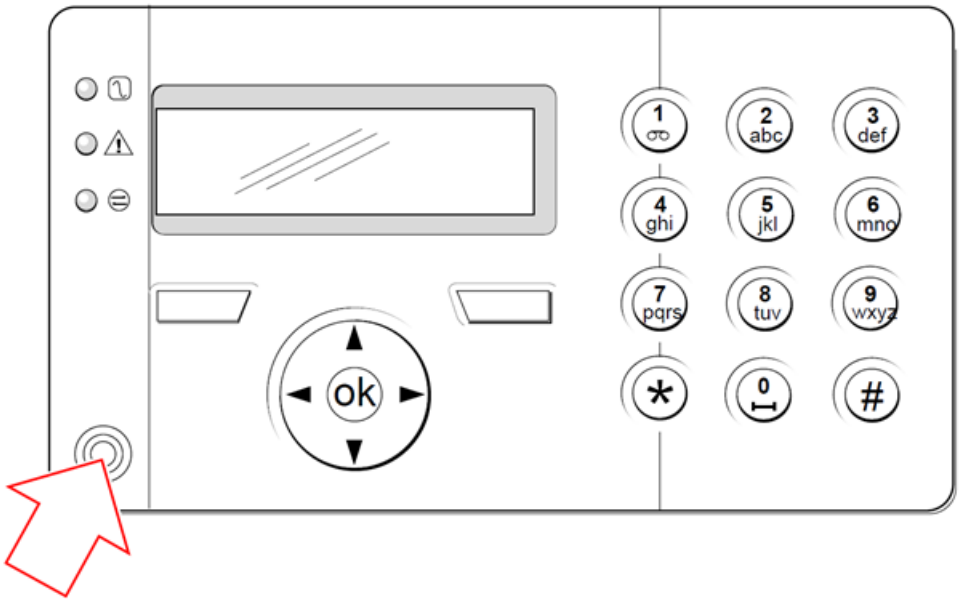
La capacidad de permitir al fabricante el acceso al sistema (por ejemplo, a realizar una actualización de firmware de la central) se configura como un derecho del usuario para un perfil de usuario. Si a un usuario se le va a permitir actualizar el firmware, asegúrese de que dicho usuario posee el perfil adecuado para este propósito.

Consulte también

Código PIN de técnico en la página 117

14.5 Programación de ACE portátil

El teclado SPC se puede configurar con un lector de tarjetas/dispositivos de proximidad. Los usuarios con determinados perfiles configurados pueden armar o desarmar el sistema de forma remota, así como también programarlo, según el nivel del perfil. Cuando se programa un dispositivo de proximidad en el teclado, el usuario puede armar o desarmar el sistema o introducir programación de usuario al presentar el dispositivo a una distancia de un 1 cm sobre el área del receptor del teclado.



Área del receptor del teclado

Para programar un ACE portátil en el teclado:

1. Introduzca el código PIN de programación de técnico. (El código por defecto es 1111. Consulte *Código PIN de técnico* en la página 117).
2. Desplácese hasta USUARIOS.
3. Pulse SELECC.
4. Seleccione EDITAR y seleccione USER1 de la lista.
5. Desplácese hasta PACE y pulse SELECC.
6. Desplácese entre HABILITAR y DESHABILITAR para la funcionalidad PACE.

   El teclado destella PRESENTAR PACE en la línea superior de la pantalla.
7. Coloque el dispositivo PACE a una distancia de un 1 cm del área del receptor en el teclado.

   El teclado indica que se ha registrado el dispositivo al mostrar PACE CONFIGURADO.

Para deshabilitar un ACE portátil en el sistema:

1. Introduzca el código PIN de programación de técnico. (El código por defecto es 1111. Consulte *Código PIN de técnico* en la página 117).
2. Desplácese hasta USUARIOS.
3. Pulse SELECC.
4. Seleccione EDITAR y seleccione USER1 de la lista.
5. Desplácese hasta PACE y pulse SELECC.
6. Desplácese hasta DESHABILITADO.

   El teclado indicará ACTUALIZADO.

14.6 Configuración de dispositivos de mando vía radio

Si se instala un módulo receptor vía radio de 868 MHz en el teclado o el controlador, se puede programar un dispositivo de mando vía radio con el teclado.

Para programar un dispositivo de mando vía radio en el sistema:

1. Introduzca el código PIN de programación de técnico. (El código por defecto es 1111. Consulte *Código PIN de técnico* en la página 117.)
2. Con las flechas arriba/abajo, desplácese hasta la opción USUARIOS.
3. Pulse SELECC.
4. Seleccione la opción EDITAR y pulse SELECC.
5. Desplácese hasta el usuario deseado y pulse SELECC.
6. Desplácese hasta la opción MANDO V.R. y pulse SELECC.
7. Desplácese hasta la opción HABILITADO y pulse SELECC.

   El mensaje PULSE TEC.MANDO parpadea en la línea superior.
8. Coloque el mando vía radio dentro de una distancia de 8 metros del teclado y presione una de las teclas.

   Aparecerá el mensaje MANDO V.R.CONFDO para indicar que se ha registrado el dispositivo.

Para deshabilitar un dispositivo de mando vía radio en el sistema:

1. Introduzca el código PIN de programación de técnico. (El código por defecto es 1111. Consulte *Código PIN de técnico* en la página 117.)
2. Con las flechas arriba/abajo, desplácese hasta la opción USUARIOS.
3. Seleccione la opción EDITAR y pulse SELECC.
4. Desplácese hasta el usuario deseado y pulse SELECC.
5. Desplácese hasta la opción MANDO V.R. y pulse SELECC.
6. Desplácese hasta DESHABILITADO y pulse SALVAR.

Si no se detecta un receptor vía radio de 868 MHz en el sistema, no se mostrará la opción MANDO V.R. en el menú del teclado.

Cantidad de mandos vía radio por usuario: Se puede programar un solo dispositivo de mando vía radio por cada usuario. Para cambiar los dispositivos entre los usuarios, repita el procedimiento de programación para los dispositivos nuevos. Los dispositivos de mando vía radio estarán disponibles para uso por parte de otros usuarios.

14.6.1 Borrado de alertas utilizando el mando

Las alertas en el sistema SPC normalmente se borran mediante la opción RESTAURAR del teclado. También se puede borrar las alertas desde el dispositivo de mando vía radio.

Si se muestra una alerta activa en el teclado con el sistema DESARMADO, la alerta se puede borrar o restaurar pulsando la tecla DESARMAR en el mando vía radio, cinco segundos después de que se haya desarmado el sistema.

Para habilitar esta funcionalidad, la opción RESTAUR.TECLADO debe estar habilitada en Opciones del sistema:

1. Inicie sesión en el teclado con un código de técnico.
2. Desplácese a TÉCNICO TOTAL > OPCIONES.

3. Pulse SELECC.
4. Desplácese hasta RESTAURACIÓN MANDO y pulse SELECC.
5. Desplácese hasta la opción HABILITADO y pulse SALVAR.

15 Programación de técnico normal a través del teclado

Esta sección brinda opciones de programación en modo técnico [normal] con el teclado LCD.

Para cada opción de menú, el teclado debe estar en programación en modo técnico:

1. Introduzca un código PIN de técnico válido. (El código PIN de técnico por defecto es 1111. Para obtener más información, consulte *Código PIN de técnico* en la página 117).
2. Con las flechas arriba/abajo, desplácese hasta la opción de programación deseada.
3. También es posible seleccionar una opción de programación empleando los dígitos del teclado, introduzca el código de programación de técnico más el dígito, tal como se muestra en la tabla que figura a continuación.

   Si modifica alguna de las opciones de programación, el teclado muestra ACTUALIZADO momentáneamente.

Número	Nombre	Descripción
1	ARMADO	Realiza un desarmado, armado total o armado parcial en el sistema.
2	ANULAR	Muestra una lista de las zonas inhibidas en el sistema.
3	INHIBIR	Permite al técnico aislar zonas en el sistema. Consulte *Aislar* en la página 171.
4	REGISTRO INCIDENCIAS	Muestra una lista de las incidencias más recientes en el sistema. Consulte *Regt.incidenc.* en la página 172.
5	REGISTRO DE CONTROL DE ACCESOS	Muestra una lista de los accesos más recientes en el sistema. Consulte *Registro de control de accesos* en la página 172.
6	REGISTRO ALARMAS	Muestra una lista de alarmas recientes. Consulte *Registro alarmas* en la página 172.
7	CAMBIO COD.TECN.	Permite al técnico cambiar el código del técnico. Consulte *Cambiar código PIN de técnico* en la página 173.
8	USUARIOS	Permite al técnico añadir, editar o borrar usuarios. Consulte *Usuarios* en la página 173.
9	Envío SMS	Permite al usuario añadir, editar o borrar detalles de SMS para usuarios. Consulte *Envío SMS* en la página 177.

Consulte también

Test en la página 167

Control de puertas en la página 180

Programación de técnico a través del teclado en la página 125

Texto del instalador en la página 180

Configurar fecha/hora en la página 180

Envío SMS en la página 177

16 Programación de técnico a través del teclado

Esta sección brinda opciones de programación en modo técnico [completo] con el teclado LCD.

Para cada opción de menú, el teclado debe estar en programación en modo técnico completo:

1. Introduzca un código PIN de técnico válido. (El código PIN de técnico por defecto es 1111. Para obtener más información, consulte *Código PIN de técnico* en la página 117).
2. Pulse SELECC. para la programación de TÉCNICO COMPLETO.
3. Con las flechas arriba/abajo, desplácese hasta la opción de programación deseada.
4. Se implementa una función de selección rápida. Pulse # para seleccionar un parámetro (por ejemplo: un atributo de zona). El parámetro seleccionado aparece con un * (por ejemplo: *Inhibición).

   Cuando termine con las opciones de programación, el teclado muestra ACTUALIZADO momentáneamente.

16.1 Estado del sistema

La opción de estado de sistema muestra todos los fallos del sistema.

Para ver estos fallos:

1. Desplácese a ESTADO SISTEMA.
2. Pulse SELECC.

   Se mostrará el estado de los siguientes elementos.

   Haga clic en cada elemento para ver más detalles.

ZONAS ABIERTAS	Muestra todas las zonas abiertas.
INCIDENCIAS	Se muestran las alarmas actuales en el sistema
PRUEBAS	Se muestran todas las zonas en prueba.
ELEMENT.AISLADOS	Se muestran las zonas que están aisladas.
FALLO AL ARMAR	Se muestran todas las particiones que han fallado al armar. Seleccione cada partición para ver detalles de por qué no se ha conseguido armar la partición.
BATERÍA	Muestra el tiempo de duración de la batería, el voltaje y la corriente. Debe introducir los valores de **Capacidad de la batería** y **Corriente máxima** en OPCIONES para ver el tiempo de batería restante en el teclado en caso de fallo de la red de CA. Esto se indica en el menú ESTADO > BATERÍA > DURACIÓN BATERÍA. Este menú también indica si hay un fallo de la batería.
AUX	Se muestra el voltaje y la corriente de la alimentación auxiliar.

AVISO: Los usuarios no pueden salir de la programación en modo TÉCNICO TOTAL si existen condiciones de fallo. El primer fallo aparecerá en el teclado cuando intente salir del modo técnico. Puede ver y aislar todas las fallas dentro del menú Estado del sistema, debajo de Alertas y Zonas abiertas.

16.2 Opciones

1. Desplácese hasta OPCIONES y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

   Las opciones de programación que se muestran en el menú OPCIONES variarán según el grado de seguridad del sistema (véase columna derecha).

ADVERTENCIA: Para cambiar la región en su central, se recomienda restaurar la central y seleccionar una nueva región como parte del asistente de inicio.

Variable	Descripción	Default
Grado EN50131	Determina el grado de seguridad de la instalación SPC. • Irlanda y regiones europeas: – EN50131 Grado 2 – EN50131 Grado 3 – Libre • Región del Reino Unido: – PD6662 (basada en EN50131 Grado 2) – PD6662 (basada en EN50131 Grado 3) – Libre • Región sueca: – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Libre • Región belga: – TO-14 (basada en EN50131 Grado 2) – TO-14 (basada en EN50131 Grado 3) – Libre • Región suiza: – SWISSI Cat 1 – SWISSI Cat 2 – Libre • Región española – EN50131 Grado 2 – EN50131 Grado 3 • Región alemana – VdS Clase A – VdS Clase C – Libre • Francia – NFtyp2 – NFtyp3 – Libre	Grado 2 País: n/d

Variable	Descripción	Default
REGIÓN	Determina los requisitos regionales específicos con los que cumple la instalación. Las opciones son GB, IRLANDA, EUROPA, SUECIA, SUIZA, BÉLGICA, ALEMANIA y FRANCIA	
TIPO INSTALACIÓN	Determina si el SPC se está instalando para utilizar en un negocio comercial o en una residencia privada. Elija entre COMERCIAL (consulte *Funcionamiento en modo doméstico* en la página 362), DOMÉSTICA (consulte *Funcionamiento en modo comercial* en la página 361) o FINANCIERA.	Hogar

Consulte *Opciones* en la página 254 para obtener más información sobre las siguientes OPCIONES.

ARMADO PARCIAL A	RENOMBRE TEMPORIZADO ACCESO A E/S E/S CON ALARMA LOCAL
ARMADO PARCIAL B	RENOMBRE TEMPORIZADO ACCESO A E/S E/S CON ALARMA LOCAL
MOSTRAR MENSAJE CRA	MOSTRAR MENSAJE (HABILITADO/DESHABILITADO)
CONFIRMACIÓN	VDS DD243: GARDA EN50131-9
Confirm.zonas	Seleccione CANT. DE ZONAS
RESTAURACIÓN AUTOMÁTICA	HABILITADO/DESHABILITADO
RESET ALARMA MANDO	HABILITADO/DESHABILITADO
CÓDIGO COACCIÓN	Deshabilitar PIN +1 Código + 2
Redisp. sirena	HABILITADO/DESHABILITADO
SIRENA INMEDIATA	HABILITADO/DESHABILITADO
SIRENA POR FTS	HABILITADO/DESHABILITADO
FLASH POR FTS	HABILITADO/DESHABILITADO

ALARMA AL SALIR	HABILITADO/DESHABILITADO Solo disponible en modo CONFIG. TÉCNICO porque la configuración no cumple con la EN50131.
IDIOMA	IDIOMA SISTEMA REPOSO: IDIOMA
DÍGITOS PIN	4 DÍGITOS 5 DÍGITOS 6 DÍGITOS 7 DÍGITOS 8 DÍGITOS
Restauración coded	HABILITADO/DESHABILITADO
ACCESO WEB	HABILITADO/DESHABILITADO Permite/Restringe el acceso al navegador web.
ZONAS ABIERTAS	HABILITADO/DESHABILITADO
PERMITIR TÉCNICO	HABILITADO/DESHABILITADO
PERMITIR FABRICANTE *	HABILITADO/DESHABILITADO
MOSTRAR ESTADO	HABILITADO/DESHABILITADO

RESIST. FL	NINGUNO 1 RFL 1K 1 RFL 1K5 1 RFL 2K2 1 RFL 4K7 1 RFL 10K 1 RFL 12K 2 RFLs 1K/470 2 RFLs 1K/1K 2 RFLs 2K2/1K0 2 RFLs 2K2/1K5 2 RFLs 2K2/2K2 2 RFLs 2K2/4K7 2 RFLs 2K7/8K2 2 RFLs 2K2/10K 2 RFLs 3K0/3K0 2 RFLs 3K3/3K3 2 RFLs 3K9/8K2 2 RFLs 4K7/2K2 2 RFLs 4K7/4K7 2 RFLs 5K6/5K6 2 RFLs 6K8/4K7 2 RFLs 10K/10K MASK_1K_1K_6K8 MASK_1K_1K_2K2 MASK_4K7_4K7_2K2
MODO AUT.SMS	Solo código Solo ID llam. Cod.+ID llam. Solo cod.SMS Cod.SMS+ID llam.
PACE y código PIN	HABILITADO/DESHABILITADO
Rest.con des.	HABILITADO/DESHABILITADO **Nota:** Para cumplir con la norma PD6662, se debe deshabilitar esta opción.
Restaur.técnico	HABILITADO/DESHABILITADO
Tamp.fuera línea	HABILITADO/DESHABILITADO
BLOQUEO TÉCNICO	HABILITADO/DESHABILITADO Si esta opción está habilitada, el sistema no se puede restaurar con el botón amarillo del controlador, a no ser que se introduzca un código PIN de técnico en el teclado.
Código generado	HABILITADO/DESHABILITADO
CONFIG. RELOJ	DST AUTOMÁTICO SINC. HORA RED CA
SOSPECHA AUDIBLE	HABILITADO/DESHABILITADO

MOSTRAR CÁMARAS	HABILITADO/DESHABILITADO
Test sísmicos ON	HABILITADO/DESHABILITADO
IMPEDIR ARMADO TRAS ALERTA	HABILITADO/DESHABILITADO
Arm. antienmasc.	Deshabilitar TAMPER FALLO ALARMA
DES. ANTIENMASC.	Deshabilitar TAMPER FALLO ALARMA
REDISPARO COACCIÓN	HABILITADO/DESHABILITADO
Rearme pánico	HABILITADO/DESHABILITADO
SIL.VERIF.AUDIO	HABILITADO/DESHABILITADO
SALIDA M.TECNICO	HABILITADO/DESHABILITADO

* No disponible para SPC42xx, SPC43xx.

16.3 Temporizaciones

1. Desplácese hasta TEMPORIZADORES y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

Temporizaciones

Designación de las funciones en el siguiente orden:

- Primera fila: web
- Segunda fila: teclado

Temporizador	Descripción	Default
Audible		
Sirenas interiores TIEMPO SIR. INT.	Tiempo durante el cual las sirenas interiores sonarán cuando se active la alarma. (0-999 minutos; 0 = nunca)	15 min.
Sirenas exteriores TIEMPO SIR. EXT.	Tiempo durante el cual las sirenas exteriores sonarán cuando se active la alarma. (0-999 minutos; 0 = nunca)	15 min.

Temporizador	Descripción	Default
Retardo sirena exterior RET.SIR.EXT.	Esto generará un retardo en la activación de la sirena exterior. (0-999 segundos)	0 seg.
Chime TEMP.CHIME	Cantidad de segundos durante la cual se activará una salida chime al abrirse una zona con atributo de chime. (1-10 segundos)	2 seg.
Confirmación		
Confirmar TIEMPO CONFIRM.	**Nota:** Esta opción está disponible únicamente para determinadas combinaciones de opción de **Grado** y **Confirmación**. (Consulte *Opciones* en la página 254 y *Estándares* en la página 271). Este temporizador se aplica a la función de confirmación de alarma y se define como el tiempo máximo entre las alarmas de dos zonas no solapadas que dispararán una alarma confirmada. (0-60 minutos)	30 min.
Atraco confirmado	**Nota:** Esta opción está disponible únicamente para determinadas combinaciones de opción de **Grado** y **Confirmación**. (Consulte *Opciones* en la página 254 y *Estándares* en la página 271). Este temporizador se aplica a la función de atraco confirmado y se define como el tiempo máximo entre las alarmas de dos zonas no solapadas que dispararán una alarma confirmada. (480-1200 minutos)	480 min.
Retardo marcación RETARDO MARCACIÓN	Cuando está programado, el retardo de marcación inicia un período de retardo predefinido antes de que el sistema se comunique con una central de recepción de alarmas (CRA). Esto está diseñado específicamente para reducir las respuestas innecesarias de las centrales de recepción de alarmas y la policía. En caso de que otra zona se active, se ignorará el período de retardo de marcación y la marcación se realizará de inmediato. (0-999 segundos)	30 seg.
Abortar alarma ABORTAR ALARMA	Tiempo tras alarma informada en el que se puede informar un mensaje de alarma abortada. (0-999 segundos)	30 seg.
Configuración		
Autorización de armado AUTORIZ. ARMADO	Período durante el cual es válida la autorización de armado. (10-250 segundos)	20 seg.
Fin de salida SALIDA FINAL	El tiempo de salida final es la cantidad de segundos que se retarda el armado tras cerrarse una zona con el atributo de salida final. (1-45 segundos)	7 seg.
Sirena con armado total SIR.ARM.TOTAL	Activa momentáneamente la alarma exterior para indicar una condición de armado total. (0-10 segundos)	0 seg.
Fallo al armar FALLO AL ARMAR	Cantidad de segundos que se muestra este fallo en los teclados (0: Hasta la introducción de un PIN válido). (0-999 segundos)	10 seg.

Temporizador	Descripción	Default
Flash con armado total FLAH.ARM.TOTAL	Activa momentáneamente el flash de la alarma exterior para indicar una condición de armado total. (0-10 segundos)	0 seg.
Alarma		
Doble detección DOBLE DETECCIÓN	El máximo retardo entre la activación de zonas con el atributo de doble detección que generará una alarma. (1-99 segundos)	10 seg.
Pruebas DIAS PRUEBAS	La cantidad de días durante los cuales una zona permanece a prueba antes de retornar automáticamente al funcionamiento normal. (1-99 días)	14 días
Intervalo de test sísmico AUTOTEST SÍSMICO	El período promedio entre los tests automáticos del sensor sísmico. (12-240 horas) **Nota:** Para habilitar el test automático, se debe habilitar el atributo de **Test de sensor automático** para una zona sísmica.	168 horas
Duración test sísmico DUR. TEST SISM.	Tiempo máximo (en segundos) que tarda el sensor sísmico en disparar una alarma en respuesta a una salida de 'test sísmico'. (3-120 segundos)	30 seg.
Retardo reposición automática	Tiempo que se retardará una restauración automática después de que el estado de una zona vuelva a ser normal. (0-9999 segundos)	0 seg.
Bloqueo post-alarma BLOQUEO POST-ALARMA	El tiempo después de una alarma antes de que el usuario pueda tener acceso. (1-120 minutos)	0 min.
Tiempo de acceso	El tiempo durante el cual un usuario con acceso con alarma puede acceder al sistema tras finalizar el tiempo de bloqueo. (10-240 minutos)	
Flash exterior TIEMPO FLASH	Tiempo durante el cual la salida flash estará activa cuando se active la alarma. (1-999 minutos; 0 = indefinidamente)	15 min.
Avisos		
Retardo red CA RETAR.FALLO C.A.	El tiempo después de detectarse un fallo en la red de CA y antes de que el sistema active un aviso. (0-60 minutos)	0 min.
Retardo interferencia RF	El tiempo después de detectarse el retardo de interferencia RF y antes de que el sistema active un aviso. (0-999 segundos)	0 min.
Técnico		
Acceso de técnico ACCESO DE TÉCNICO	El temporizador para el acceso del técnico comienza tan pronto como el usuario habilita el acceso del técnico. (0-999 minutos; 0 indica sin limitación de tiempo para el acceso al sistema)	0 min.
Salida modo técnico automática SAL.AUTO.M.TÉC.	Tiempo de inactividad tras el cual se cerrará automáticamente la sesión del técnico. (0-300 minutos)	0 min.

Temporizador	Descripción	Default
Teclado		
Tiempo espera teclado TIEMPO ESP. TECL.	La cantidad de segundos que un RKD esperará la introducción de teclas antes de salir del menú actual. (10-300 segundos)	30 seg.
Idioma teclado IDIOMA TECLADO	El tiempo que un teclado esperará en reposo antes de cambiar al idioma por defecto. (0 -9999 seg.; 0 = nunca)	10 seg.
Incendio		
Prealarma incendio PREALARMA INCENDIO	Número de segundos que se debe esperar antes de notificar una alarma de incendio para zonas con el atributo «Prealarma incendio» seleccionado. Consulte *Editar una zona* en la página 274. (1-999 segundos)	30 seg.
Reconocimiento de alarma de incendio RECONOCIMIENTO ALARMA INCENDIO	Tiempo adicional de espera antes de informar una alarma de incendio para las zonas con los atributos de «Prealarma incendio» y «Reconocimiento de incendio». Consulte *Editar una zona* en la página 274. (1-999 segundos)	120 seg.
Código		
PIN Válido PIN VÁLIDO	Período durante el cual el PIN es válido. (1-330 días)	30 días
Límite cambios de PIN LÍMITE CAMBIOS DE PIN	Cantidad de cambios dentro de un período válido. (1-50)	5
Aviso PIN AVISO EXP. PIN	Tiempo antes de caducar un PIN tras el cual se mostrará una advertencia. (1-14 días)	5 días
Configuración general		
Tiempo salida RF SALIDA RF	El tiempo que la salida RF permanecerá activa en el sistema. (0-999 segundos)	0 seg.
Límite tiempo sincronismo LÍMITE TIEMPO SINCRONISMO	Límite de tiempo dentro del cual no se llevará a cabo la sincronización. La sincronización de tiempo solo se produce si la hora del sistema y la hora de actualización están fuera de este límite. (0-300 segundos)	0 seg.
T. fallo link T. Fallo Link	Tiempo de espera para fallo de enlace Ethernet. (0 -250 seg.; 0 = deshabilitado)	0 seg.
Cámara fuera de línea CAM.NO EN LÍNEA	Tiempo hasta que la cámara pase a estar fuera de línea. (10-9999 segundos)	10 seg.

Temporizador	Descripción	Default
Supervisada SUPERVISADA ⓘ	Este atributo solo se aplica a servicios remotos. La cantidad de horas durante las cuales una zona debe abrirse si la zona está programada con el atributo **Frecuente**. (1-9999 horas)	336 h (2 semanas)
Silencio por coacción	Tiempo durante el cual una alarma de coacción continuará silenciada y no podrá restaurarse desde el teclado. (0-999 minutos)	0 min.
Silencio por atraco/pánico	Cantidad de minutos durante los cuales una alarma de atraco/pánico continuará silenciada y no podrá restaurarse desde el teclado. (0-999 minutos)	0 min.

Los tiempos por defecto dependen de la configuración del técnico. Los tiempos por defecto pueden o no ser permisibles, y dependen de la configuración establecida por el técnico.

Los rangos/ajuste válidos podrían depender del grado de seguridad especificado en **Configuración > Sistema > Estándares**.

16.4 Particiones

1. Desplácese hasta PARTICIONES y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

AÑADIR	Para el modo Doméstico y Comercial, el tipo de partición por defecto es Estándar. En el modo Financiero, seleccione el tipo de partición ESTÁNDAR, CAJERO AUTOMÁTICO, CÁMARA ACORAZADA o AVANZADO. Introduzca el nombre de la partición y el horario de entrada/salida preferido.

EDITAR	Edite los siguientes ajustes: • DESCRIPCIÓN • ENTRADA SALIDA – TEMPOR. ENTRADA – TEMPOR. SALIDA – SIN TEMPOR. SALIDA – ENTR. MANDO V. R. ACTIVA • ARMADO PARCIAL A/B – HABILITADO/DESHABILITADO – TEMPORIZADO – ACCESO A E/S – E/S A ALARMA – LOCAL – SIN SIRENAS • PARTIC. ENLAZADAS – PARTIC. – ARMADO TOTAL – ARMADO TOTAL TODO – IMPEDIR ARMADO TOTAL – IMPEDIR ARMADO TOTAL TODO – DESARMADO – DESARMADO TODO – IMPEDIR DESARMADO – IMPEDIR DESARMADO TODO • PROGRAMACIÓN – CALENDARIO – ARMADO/DESARMADO AUTOMÁTICO – BLOQUEO TIEMPO – ACC.CAM.ACORAZ. • INFORMES – ARMADO PREMATURO – ARMADO TARDÍO – DESARMADO PREMATURO – DESARMADO TARDÍO • ARMADO/DESARMADO – AVISO ARMADO AUTOMÁTICO – CANCELACIÓN ARMADO AUTOMÁTICO – RETARDO ARMADO AUTOMÁTICO – CONMUTADOR LLAVE – INTERVALO DE RETARDO – CONTADOR DE RETARDO – DESARMADO RETARDADO – DURACIÓN DESARMADO – INTERBLOQUEO – CÓDIGO PIN DOBLE • SALIDA RF
BORRAR	Seleccione la partición que borrará.

Consulte *Añadir/Editar una partición* en la página 275 para obtener más información sobre estas opciones.

16.5 Grupos de particiones

1. Desplácese hasta GRUPOS PARTICIONES y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

AÑADIR	Introduzca el nombre del grupo de particiones.
EDITAR	Nombre grupo: Renombre el grupo según sea necesario. Particiones: Desplácese a una partición y selecciónela. Seleccione HABILITADO o DESHABILITAR para añadirla o eliminarla del grupo. Un asterisco (*) indica que una partición forma parte del grupo.
BORRAR	Seleccione la partición que borrará.

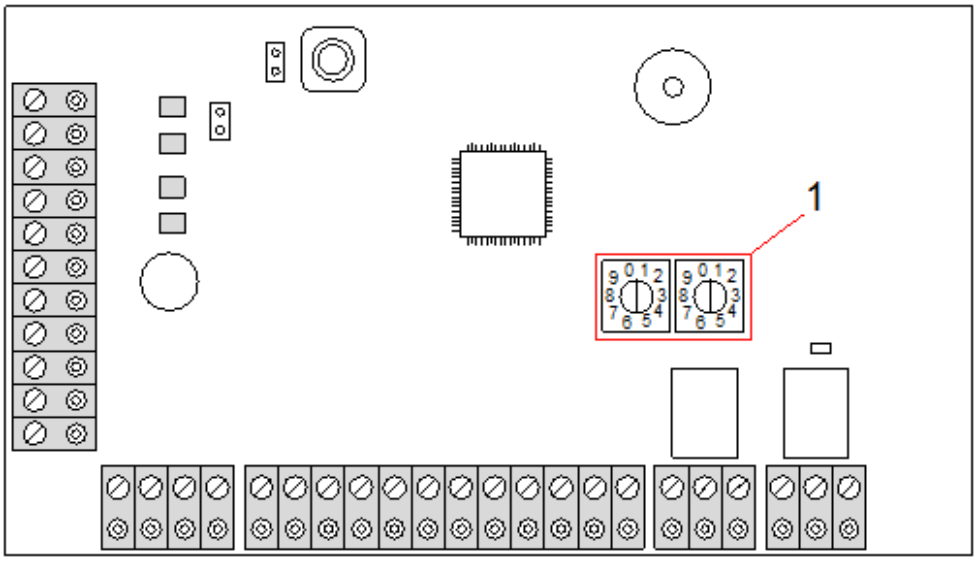
16.6 X-BUS

1. Desplácese hasta X-BUS y pulse SELECC.
2. Desplácese hasta las opciones de programación deseadas:

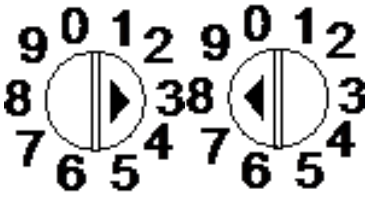
16.6.1 Direccionamiento X-BUS

Se pueden configurar, localizar y controlar los módulos de expansión, teclados y zonas subsiguientes mediante los pasos que se explican en esta sección. En este menú también puede acceder a la configuración de X-BUS, como tipo, horarios de comunicación y reintentos.

Las imágenes a continuación muestran la ubicación de los conmutadores rotativos, y cada conmutador rotativo con el símbolo de una flecha que apunta a un número para su identificación (es decir: 3, 8). El interruptor derecho es el primer dígito de la unidad y el interruptor izquierdo es el décimo dígito. El módulo de expansión en la figura a continuación se identifica con el número 38.



Conmutadores rotativos

Número	Descripción
1	 Conmutadores rotativos que identifican al módulo de expansión como 38.

En un sistema con direccionamiento automático, los módulos de expansión y los teclados se asignan a la misma secuencia de numeración. Por ejemplo, el controlador numera automáticamente los módulos de expansión y teclados como 01, 02, 03, etc., en el orden en que son detectados, o sea, por su posición relativa al controlador. En esta configuración, las zonas están asignadas a cada módulo de expansión de entrada.

El SPC41xx no admite los módulos de expansión direccionados automáticamente.

16.6.2 Actualiz. X-Bus

La utilidad de actualización de X-Bus descubre el estado actual del X-Bus y muestra su configuración actual.

Para actualizar el estado del X-Bus:

1. Desplácese a Actualiz. X Bus.
2. Pulse SELECC.

   Se muestra una lista de teclados en línea.
3. Pulse la tecla programable derecha del teclado tras cada visualización para ver los módulos de expansión, las zonas y los elementos fuera de línea.
4. Vuelve a pulsar esta misma tecla para salir.

La función de **Actualizar** no produce cambios en el sistema, pero es útil para detectar fallos en el sistema, como conexiones sueltas o módulos de expansión inactivos, antes de **Reconfigurar**.

16.6.3 Reconfigurar

AVISO: La reconfiguración solo se aplica a zonas cableadas en el módulo de expansión. Las zonas vía radio en un módulo de expansión y las zonas de controladores no se pondrán en línea tras la reconfiguración. Para poner las zonas de controladores en línea, debe aplicar un tipo de zona que no sea 'Sin utilizar' mediante el menú de zonas en el teclado o el navegador web.

Si el sistema tiene una combinación de tipos de módulos de expansión (con o sin conmutadores rotativos), el sistema puede reconfigurarlos automáticamente. Si el sistema tiene todos los módulos de expansión con conmutadores rotativos, este todavía puede ser reconfigurado automáticamente, y el sistema ignorará los conmutadores rotativos y redireccionará todos los módulos de expansión en el sistema.

Se recomienda **Actualizar** antes de **Reconfigurar**.

Para reconfigurar teclados/módulos de expansión:

1. Desplácese hasta RECONFIGURAR.
2. Pulse SELECC.

   Se muestra una lista de teclados en línea.
3. Pulse SIGUIENTE.

   Se muestra la cantidad de módulos de expansión en línea.
4. Pulse SIGUIENTE

   Se muestra la cantidad de zonas en línea.
5. Pulse ATRÁS para salir.

16.6.4 Teclados/módulos de expansión/controladores de puertas

16.6.4.1 Localizar

Para localizar un teclado/módulo de expansión/controlador de puerta:

1. Desplácese hasta TECLADOS, MÓDULOS DE EXPANSIÓN o CONTROLADORES DE PUERTA y pulse SELECC.
2. Desplácese hasta LOCALIZAR y pulse SELECC.
3. Desplácese hasta el módulo de expansión/teclado/controlador de puerta que desea localizar y pulse SELECC.

   El dispositivo seleccionado emite un pitido y la luz LED parpadea para que el técnico pueda localizarlo.
4. Pulse ATRÁS para salir.

   Localice los teclados utilizando los mismos menús y siguiendo la opción de teclado en lugar del módulo de expansión.

16.6.4.2 Monitor

Para ver una descripción general de los teclados/módulos de expansión/controladores de puerta conectado al sistema:

1. Desplácese hasta TECLADOS, MÓDULOS DE EXPANSIÓN o CONTROLADORES DE PUERTA y pulse SELECC.
2. Desplácese hasta CONTROL y pulse SELECC.
3. Desplácese hasta la opción de programación de control deseada.
4. Pulse SELECC.

   Se muestra una lista de teclados/módulos de expansión detectados.
5. Desplácese por la lista y pulse SELECC. en el módulo de expansión/teclado/controlador de puerta deseado.

   Los parámetros y datos, según corresponda, se muestran para su edición como se indica en la tabla a continuación.

ESTADO	En línea o fuera de línea

Núm.serie	Número de serie (se utiliza para rastrear e identificar)
VER	Versión
ALIMENTACIÓN	Parámetros de alimentación: lecturas de tensión y corriente en tiempo real
Info dirección	El modo de direccionamiento y la dirección del teclado/módulo de expansión/controlador de puerta.
Fusible auxiliar	El estado del fusible auxiliar en el módulo de expansión/controlador de puerta
F.alimentación	El tipo y el estado de la fuente de alimentación. (Sólo módulos de expansión de fuente de alimentación). Desplácese para ver el voltaje y la carga actual en las salidas, además del estado de la batería. También está disponible la opción de Modo enlace, que muestra el ajuste de jumper en la central para el ajuste de Ah. Las opciones disponibles son 7 Ah y 17 Ah. (El jumper no está presente en los modelos 5350 ni 6350) Si utiliza el SPC 5360 o 6350, este menú muestra el estado de la batería y el de los fusibles de las salidas.
BATERÍA	Voltaje de la batería: nivel de voltaje de la batería (sólo módulos de expansión de fuente de alimentación)
ESTADO ENTRADA	Estado de entrada de cada zona asociada a un módulo de expansión de la forma siguiente: C: Cerrado A: Abierto D: Desconectado S: Cortocircuito (módulos de expansión con entradas únicamente)

6. Pulse ATRÁS para salir.

16.6.4.3 Editar teclados

Para editar teclados:

1. Desplácese hasta TECLADOS > EDITAR.
2. Pulse SELECC.
3. Desplácese hasta el dispositivo que desea editar y pulse SELECC.

   Los ajustes de configuración para un teclado estándar y un teclado Comfort se describen en las secciones a continuación.
4. Pulse ATRÁS para salir del menú.

Configuración del teclado LCD

Configure los siguientes ajustes para el teclado.

Configuración	Descripción
Descripción	Introduzca una descripción única para identificar el teclado.
Teclas de función (en estado de reposo)	
Pánico	Seleccione Habilitar, Deshabilitar o Habilitado silencioso. En caso de estar habilitada, la alarma de pánico se activa al pulsar simultáneamente ambas teclas.
Verificación	Si asigna una zona de verificación al teclado, cuando se dispara una alarma de pánico por pulsar simultáneamente las dos teclas o por introducir un código de coacción, se activan las incidencias de audio y vídeo.

Configuración	Descripción
Indicaciones visuales	
Backlight	Seleccione cuándo se enciende la retroiluminación del teclado. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Indicadores	Habilite o deshabilite los LED en el teclado.
Estado armado	Seleccione esta opción si el estado de armado debe indicarse en reposo.
Indicaciones audibles	
Zumbador	Habilite o deshabilite el zumbador en el teclado.
Zumbador armado parcial	Habilite o deshabilite el zumbador de armado parcial durante el tiempo de salida.
Pulsación tecla	Seleccione si se debe activar el volumen del altavoz para las pulsaciones de teclas.
Desactivación	
Calendario	Seleccione si el teclado debe estar limitado por calendario. Consulte *Calendarios* en la página 289.
Puerta de mapeo	Seleccione si el teclado debe estar limitado por una puerta de mapeo.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador llave.
Entrada con dispositivo PACE	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay un dispositivo PACE configurado en el teclado.
Particiones	
Localización	Seleccione la partición segura donde está ubicado el teclado.
Particiones	Seleccione las particiones que pueden ser controladas por el teclado.
Opciones	
Retardo armado total	Seleccione para configurar un armado con retardo en todos los teclados. Se ignora la ubicación del teclado y todas las particiones realizarán una cuenta regresiva del tiempo de salida total.

AVISO: Una partición debe estar asignada a un teclado solo si el teclado está dentro de la partición asignada y si la ruta de entrada/salida está definida. Si se asigna una partición, cuando esa partición en particular se arme o desarme, se utilizarán los temporizadores de entrada y salida (en caso de estar configurados). También estarán disponibles otras funciones relacionadas con las rutas de entrada/salida. Si no hay una partición asignada, la partición se armará o desarmará inmediatamente y las otras funciones de entrada/salida no estarán disponibles.

Configuración del teclado Comfort

Configure los siguientes ajustes para el teclado Comfort.

Configuración	Descripción
Descripción	Introduzca una descripción única para identificar el teclado.
Teclas de función (en estado de reposo)	
Pánico	Seleccione Habilitar, Deshabilitar o Habilitado silencioso. En caso de estar habilitada, la alarma de pánico se activa al pulsar simultáneamente F1 y F2.
Incendio	Habilite esta opción para que la alarma de incendio se active al pulsar simultáneamente F2 y F3.
Alarma médica	Habilite esta opción para que la alarma médica se active al pulsar simultáneamente F3 y F4.
Armado total	Habilite esta opción para que el armado total se active al pulsar F2 dos veces.
Armado parcial A	Habilite esta opción para que el armado parcial A se active al pulsar F3 dos veces.
Armado parcial B	Habilite esta opción para que el armado parcial B se active al pulsar F4 dos veces.
Verificación	Si asigna una zona de verificación al teclado Comfort, cuando se dispara una incidencia médica, de pánico o de incendio, o si el usuario introduce un código de coacción, se activan las incidencias de audio y vídeo.
Indicaciones visuales	
Backlight	Seleccione cuándo se enciende la retroiluminación del teclado. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Nivel retroilum.	Seleccione la intensidad de la retroiluminación. Rango de 1 a 8 (alto).
Indicadores	Habilite o deshabilite los LED en el teclado.
Estado armado	Habilite esta opción si el estado de armado debe indicarse en reposo. (LED)
Marca	Seleccione esta opción si el logo debe estar visible en reposo.
Reloj analógico	Seleccione la posición del reloj en caso de estar visible en reposo. Las opciones son: Alineado a la izquierda, Centrado, Alineado a la derecha o Deshabilitado.
Emergencia	Habilite esta opción si las teclas de función de Pánico, Incendio o Emergencia médica deben aparecer indicadas en la pantalla LCD.
Armado directo	Habilite esta opción si las teclas de función de Armado total/Armado parcial deben aparecer indicadas en la pantalla LCD.
Indicaciones audibles	
Alarmas	Seleccione el volumen del altavoz para las indicaciones de alarma o deshabilite el sonido.
Entrada/salida	El rango es de 0 a 7 (volumen máx.).
Chime	Seleccione el volumen del altavoz para las indicaciones de entrada y salida o deshabilite el sonido.
Pulsación tecla	El rango es de 0 a 7 (volumen máx.).
Mensajes hablados	Seleccione el volumen del altavoz para el chime o deshabilite el sonido.

Configuración	Descripción
Zumbador armado parcial	El rango es de 0 a 7 (volumen máx.).
Desactivación	
Calendario	Seleccione si el teclado debe estar limitado por calendario. Consulte Calendario.
Puerta de mapeo	Seleccione si el teclado debe estar limitado por una puerta de mapeo.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador llave.
Entrada con dispositivo PACE	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay un dispositivo PACE configurado en el teclado.
Particiones	
Localización	Seleccione la partición segura donde está ubicado el teclado.
Particiones	Seleccione las particiones que pueden ser controladas por el teclado.
Opciones	
Retardo armado total	Seleccione para configurar un armado con retardo en todos los teclados. Se ignora la ubicación del teclado y todas las particiones realizarán una cuenta regresiva del tiempo de salida total.

AVISO: Una partición debe estar asignada a un teclado solo si el teclado está dentro de la partición asignada y si la ruta de entrada/salida está definida. Si se asigna una partición, cuando esa partición en particular se arme o desarme, se utilizarán los temporizadores de entrada y salida (en caso de estar configurados). También estarán disponibles otras funciones relacionadas con las rutas de entrada/salida. Si no hay una partición asignada, la partición se armará o desarmará inmediatamente y las otras funciones de entrada/salida no estarán disponibles.

16.6.4.4 Editar módulos de expansión

Para editar los módulos de expansión:

1. Desplácese hasta MÓDULOS DE EXPANSIÓN > EDITAR.
2. Pulse SELECC.
3. Desplácese hasta el dispositivo que desea editar y pulse SELECC.

   Los parámetros y datos, si procede, se muestran para su edición.
4. Pulse ATRÁS para salir del menú.

Para darles nombre e identificarlos, se asignan zonas a los módulos de expansión (en grupos de 8) con identidades consecutivas entre 1 y 512 (El número más alto para la identificación de zonas es 512). Por lo tanto, todo módulo de expansión con nombre o identificado por un número mayor que 63 no tiene zonas asignadas.

Edición de módulos de expansión de E/S

En la siguiente tabla se muestra una lista de las opciones disponibles para los módulos de expansión de E/S:

Función	Descripción
Descripción	Se edita la descripción del módulo de expansión.

Edición de módulos de expansión de audio

En la siguiente tabla se muestran las opciones disponibles en el menú **Editar** para los módulos de expansión de audio:

Nombre	Descripción
DESCRIPCIÓN	Introduzca o edite una descripción para el módulo de expansión de audio.
INPUT	Seleccione la zona.
Límite volumen	Seleccione el límite de volumen.

Edición de módulos de expansión vía radio

En la siguiente tabla se muestra una lista de las opciones disponibles para los módulos de expansión vía radio:

Función	Descripción
Descripción	Se edita la descripción del módulo de expansión.

Edición de módulos de expansión de E/S analizados

En la siguiente tabla se muestra una lista de las opciones disponibles para los módulos de expansión de E/S analizados:

Nombre	Descripción
Descripción	Se edita la descripción del módulo de expansión.

Edición de módulos de expansión de indicador

En la siguiente tabla se muestra una lista de las opciones disponibles para los módulos de expansión de indicador:

Nombre	Descripción
DESCRIPCIÓN	Introduzca o edite una descripción para el módulo de expansión.
Localización	Seleccione una ubicación para el módulo de expansión en la lista de particiones disponibles.

Nombre	Descripción
Teclas de función	Le permite asignar un comportamiento a teclas específicas para particiones específicas. Seleccione una partición y asigne una de las siguientes opciones a esa partición: • Ninguno • Desarmado • Armado parcial A • Armado parcial B • Armado total • Cambio desarmado/armado total • Cambio desarmado/armado parc. A • Cambio desarmado/armado parc. B • Todo OK • Autorización de armado
INDICACIONES VISUALES (sólo en modo flexible)	Le permite asignar un comportamiento específico a cada LED del módulo indicador Cada LED tiene las siguientes opciones: • FUNCIÓN: Están disponibles las siguientes opciones: – CONMUTADOR LLAVE: Seleccione un conmutador llave y la posición de la llave. – DESHABILITADO: Seleccione esta opción para deshabilitar el LED. – SISTEMA: Seleccione el tipo de alarma que disparará el LED. – PARTICIÓN: Seleccione la partición que disparará el LED. – ZONA: Seleccione la zona que disparará el LED – PUERTA: Seleccione la puerta y la opción de puerta que disparará el LED. • ON – COLOR: Especifique el color de activación • ON - PARPADEO: Especifique el comportamiento del LED en estado activo. Las opciones disponibles son: – Continuo: Siempre encendido. – Parpadeo rápido/medio/lento: Velocidad variable del parpadeo. • OFF – COLOR: Especifique el color de desactivación. • OFF - PARPADEO: Especifique el comportamiento del LED en estado inactivo. Las opciones disponibles son: – Continuo: Siempre encendido. – Parpadeo rápido/medio/lento: Velocidad variable del parpadeo.
LED SIEMPRE	Habilite esta opción si los indicadores LED permanecen activos cuando las teclas están desactivadas.
Indicad. audible (sólo en modo flexible)	Seleccione los indicadores audibles para alarmas, entrada/salida, y pulsación de teclas,

Nombre	Descripción
Desactivación (sólo en modo flexible)	Selecciona una o varias de las siguientes opciones de desactivación: • Calendario: Seleccione un calendario de entre las opciones disponibles. • Conmutador llave: Seleccione un conmutador de llave de entre las opciones disponibles. • Teclado: Seleccione un teclado de entre las opciones disponibles. • Lector de tarjetas: Habilite o deshabilite la desactivación mediante un teclado.
MODE	Seleccione Ligado o Flexible. El modo Ligado reduce el número de opciones disponibles en el menú de Editar módulo de expansión.
INPUT	Seleccione la zona

Edición de módulos de expansión de conmutador de llave

En la siguiente tabla se muestra una lista de las opciones disponibles para los módulos de expansión de conmutador de llave:

Nombre	Descripción
DESCRIPCIÓN	Introduzca o edite una descripción para el módulo de expansión.
Localización	Seleccione una ubicación para el módulo de expansión en la lista de particiones definidas.
ENCLAVAMIENTO	Habilite o deshabilite el enclavamiento en la posición de la llave.
INDICACIONES VISUALES (sólo en modo flexible)	Le permite asignar un comportamiento específico a cada LED del módulo de expansión de conmutador de llave. Cada LED tiene las siguientes opciones: • FUNCIÓN: Están disponibles las siguientes opciones: – CONMUTADOR LLAVE: Seleccione un conmutador llave y la posición de la llave. – DESHABILITADO: Seleccione esta opción para deshabilitar el LED. – SISTEMA: Seleccione el tipo de alarma que disparará el LED. – PARTICIÓN: Seleccione la partición que disparará el LED. – ZONA: Seleccione la zona que disparará el LED – PUERTA: Seleccione la puerta y la opción de puerta que disparará el LED. • ON – COLOR: Especifique el color de activación • ON - PARPADEO: Especifique el comportamiento del LED en estado activo. Las opciones disponibles son: – Continuo: Siempre encendido. – Parpadeo rápido/medio/lento: Velocidad variable del parpadeo. • OFF – COLOR: Especifique el color de desactivación. • OFF - PARPADEO: Especifique el comportamiento del LED en estado inactivo. Las opciones disponibles son: – Continuo: Siempre encendido. • Parpadeo rápido/medio/lento: Velocidad variable del parpadeo.
Desactivación (sólo en modo flexible)	Seleccione un método de desactivación de entre las opciones disponibles: • Calendario: Seleccione un calendario.

Nombre	Descripción
Posiciones llave	Le permite asignar un comportamiento a posiciones específicas del conmutador de llave para particiones específicas. Seleccione una partición para la posición de la llave, y asigne una de las siguientes opciones a esa partición: • Ninguno • Desarmado • Armado parcial A • Armado parcial B • Armado total • Cambio desarmado/armado total • Cambio desarmado/armado parc. A • Cambio desarmado/armado parc. B • Todo OK • Autorización de armado

16.6.4.5 Editar controladores de puertas

Para obtener más información sobre controladores de puertas, consulte *Módulo de expansión de puerta* en la página 79.

1. Desplácese hasta CONTROLADORES DE PUERTA > EDITAR.
2. Pulse SELECC.
3. Desplácese hasta el dispositivo que desea editar y pulse SELECC.

   Los parámetros y datos, según corresponda, se muestran para su edición como se indica en la tabla a continuación.

DESCRIPCIÓN	Nombre del controlador de puerta
PUERTAS	Configuración de E/S de puerta 1 y E/S de puerta 2.
LECTORES	Configuración de los perfiles de lector

Para editar una E/S de PUERTA:

1. Desplácese hasta PUERTAS.
2. Pulse SELECC.
3. Desplácese hasta la E/S de PUERTA que desea editar y pulse SELECC.

   Los parámetros y datos, según corresponda, se muestran para su edición como se indica en la tabla a continuación.

ZONAS	No se completa ninguna funcionalidad de acceso. Se puede usar las entradas y las salidas normalmente.
PUERTA 1 – PUERTA 64	El número de puerta seleccionado se asigna a la E/S de PUERTA.

Si se selecciona la opción «ZONAS» para una E/S de PUERTA, se deben configurar las dos entradas de esta E/S de PUERTA:

Para editar las dos zonas de una E/S de PUERTA:

1. Desplácese hasta la E/S de PUERTA que desea editar y pulse SELECC.

   La opción «Zonas» se encuentra seleccionada.
2. Pulse SELECC.
3. Seleccione la zona que desea editar (zona DPS o DRS).
4. Pulse SELECC.

   Los parámetros y datos, según corresponda, se muestran para su edición como se indica en la tabla a continuación.

SIN ASIGNAR	Esta zona no está asignada y no se puede usar.
ZONA 1 – ZONA 512	La zona que se edita se asigna a este número de zona. Si la zona está asignada a un número de zona especifico, puede configurarla como una zona normal.

Puede asignar las zonas a cada número de zona libre. Sin embargo, la asignación no es fija. Si se ha asignado el número 9 a una zona y se conecta un módulo de expansión de entrada con la dirección 1 al X-Bus (que está utilizando los números de zona 9-16), la zona asignada desde el controlador de dos puertas se trasladará al siguiente número de zona libre. La configuración se adaptará en consecuencia.

Para editar un PERFIL DE LECTOR:

1. Desplácese hasta LECTORES.
2. Pulse SELECC.
3. Desplácese hasta el LECTOR que desea editar y pulse SELECC.

   Seleccione uno de los siguientes perfiles para el lector:

1	Para lectores con LED verde y rojo.
2	Para lectores VANDERBILT con LED amarillo (AR618X).
3	El Perfil 3 se utiliza con lectores HID que envían un código PIN a la central como una lectura de tarjeta con un código de lugar predefinido (0).
4	El Perfil 4 se utiliza con lectores HID que envían un código PIN a la central como una lectura de tarjeta con un código de lugar predefinido (255).
5	Seleccionar para activar los lectores Sesam. Para cumplir con las homologaciones VdS, asegúrese de seleccionar la opción **Anular perfil de lector** para proporcionar información sobre el proceso de configuración.

Consulte también

Módulo de expansión de puerta en la página 79

16.6.5 Modo direccionamiento

El direccionamiento X-BUS se puede configurar de una de las dos maneras siguientes:

Direccionamiento automático

Con el direccionamiento automático, el controlador anula los conmutadores rotativos y asigna automáticamente los módulos de expansión y los teclados en los ID exclusivos del sistema en orden secuencial.

Direccionamiento manual

El direccionamiento manual permite determinar manualmente el ID de cada módulo de expansión o teclado en un sistema. Todos los dispositivos deben instalarse donde sea necesario y cada ID debe establecerse manualmente utilizando los conmutadores rotativos. Las zonas a identificar pueden calcularse usando la siguiente fórmula: ((valor de ID x 8) + 1)= primero el número de la zona y luego las siguientes 7 zonas secuenciales. Por ejemplo: ((ID2 x 8) + 1) = 17. La zona 17 tiene asignada la entrada 1 en ID2. Cada entrada tiene la siguiente zona secuencial asignada, en este caso hasta la zona 24.

Aviso: Límite de ID para asignación de zona SPC 4000 - Módulo de expansión ID 1–3. SPC 5000: Módulo de expansión ID 1–15. SPC 6000: Módulo de expansión ID 1–63.

ID	Zona	ID	Zona	ID	Zonas	ID	Zonas	ID	Zonas
1	9-16	14	113-120	27	217-224	40	321-328	53	425-432
2	17-24	15	121-128	28	225-232	41	329-336	54	433-440
3	25-32	16	129-136	29	233-240	42	337-344	55	441-448
4	33-40	17	137-144	30	241-248	43	345-352	56	449-456
5	41-48	18	145-152	31	249-256	44	353-360	57	457-464
6	49-56	19	153-160	32	257-264	45	361-368	58	465-472
7	57-64	20	161-168	33	265-272	46	369-376	59	473-480
8	65-72	21	169-176	34	273-280	47	377-384	60	481-488
9	73-80	22	177-184	35	281-288	48	385-392	61	489-496
10	81-88	23	185-192	36	289-296	49	393-400	62	497-504
11	89-96	24	193-200	37	297-304	50	401-408	63	505-512
12	97-104	25	201-208	38	305-312	51	409-416		
13	105-112	26	209-216	39	313-320	52	417-424		

Si se configuran 2 dispositivos del mismo tipo (por ejemplo, módulos de expansión) con el mismo ID, luego de la configuración, ambos módulos de expansión emitirán un pitido y las luces LED intermitentes indicarán un conflicto. Restablezca los conmutadores y el sistema realizará un nuevo escaneo.

En un dispositivo, si ambos conmutadores rotativos están configurados en cero (0, 0), toda la configuración se convertirá en la configuración de direccionamiento automático.

Para seleccionar el MODO DE DIRECCIONAMIENTO:

1. Desplácese a MODO DE DIRECCIONAMIENTO.
2. Pulse SELECC.
3. Seleccione el modo de direccionamiento adecuado: AUTOMÁTICO o MANUAL
4. Pulse SELECC. para actualizar la configuración.

16.6.6 Tipo de X-BUS

Para programar el tipo de X-BUS desde el teclado:

1. Desplácese hasta TIPO X-BUS.
2. Pulse SELECC.

3. Desplácese hasta la configuración deseada:
   - LAZO
   - PUNTA
4. Pulse SELECC. para actualizar la configuración.

16.6.7 Reintentos bus

Para programar el número de veces que el sistema intenta retransmitir datos en la interfaz X-BUS antes de generar un fallo de comunicación:

1. Desplácese hasta REINTENTOS BUS.
2. Pulse SELECC.
3. Introduzca la cantidad de veces que desea que el sistema intente retransmitir datos.
4. Pulse SELECC. para actualizar la configuración.

16.6.8 Temporizador de comunicación

Para designar el período de tiempo antes del registro de un fallo de comunicación:

1. Desplácese hasta TEMP. COMUNICACIÓN.
2. Pulse SELECC.
3. Introduzca el horario preferido.
4. Pulse INTRO para actualizar la configuración.

16.7 Vía radio

1. Desplácese hasta VÍA RADIO y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

SENSORES	Podría ser necesario cambiar el tipo de sensor dado de alta en el sistema si se identificó el tipo de sensor incorrecto durante el proceso de alta. Si no se dieron de alta detectores vía radio, el teclado mostrará SIN SENSORES ACTIVOS. Están disponibles las siguientes opciones para los sensores: • AÑADIR Consulte *Añadir sensores* en la página siguiente • EDITAR (Cambiar asignación de zona) Consulte *Editar sensores (asignación de zonas)* en la página siguiente • ELIMINAR Seleccione el dispositivo o sensor que borrará.
APR	Añada, edite o elimine una APR (alarma personal vía radio). • AÑADIR Consulte *Añadir APR* en la página 151 • EDITAR Consulte *Editar APR* en la página 151 • ELIMINAR Seleccione la APR que borrará.
ANTENA EXTERIOR	Habilite o deshabilite la antena exterior.

SUPERVISIÓN	Habilite o deshabilite la supervisión de tamper.
FILTRO SEÑAL BAJA	Habilite o deshabilite el filtro de señal baja (intensidades RF 0 y 1).
DET.INTERF.RF	Habilite o deshabilite la interferencia RF.
PÁNICO VÍA RADIO	Habilite o deshabilite el pulsador de pánico vía radio o habilite el modo silencioso para el pulsador de pánico vía radio.
CRONOGRAMA TEST APR	Introduzca el período máximo (en días) entre los test de APR. El máximo es 365 días.
TIEMPO IMPEDIMENTO ARMADO	Introduzca el tiempo en minutos tras el cual, si un sensor o una APR no envía informes, se debe impedir el armado para una partición donde está la zona vía radio. El máximo es 720 minutos.
TIEMPO PÉRDIDA DISPOSITIVO	Introduzca la cantidad de minutos tras la cual un dispositivo vía radio se informa como perdido en caso de no envíe informes dentro de este período de tiempo. (el mínimo es 20 y el máximo es 720 minutos)

16.7.1 Añadir sensores

Para añadir un sensor vía radio:

1. Desplácese hasta AÑADIR y pulse SELECC.

   Se mostrará la opción ACTIVAR ALTA.
2. Pulse SELECC.

   En la línea superior de la pantalla, aparecerá el texto parpadeante ACTIVAR DISPOSITIVO.
3. Active el dispositivo vía radio entre 3 y 5 veces seguidas para permitir que el receptor del teclado detecte la transmisión vía radio del dispositivo.

   La pantalla indica que se ha detectado el dispositivo al mostrar el texto parpadeante SENSOR ENCONTRADO. Alternativamente, se mostrará la información de ID y TIPO del dispositivo.
4. Pulse ALTA.

   Aparecerá una opción para seleccionar el tipo de zona.
5. Pulse SELECC.
6. Desplácese hasta el tipo de zona requerido y presione SELECC.

Para añadir un dispositivo mediante ALTA TAMPER, desplácese hasta esta opción en el paso 2. El proceso de alta es idéntico con la excepción de que se le solicita que defina un tipo de partición antes del tipo de zona.

16.7.2 Editar sensores (asignación de zonas)

Podría ser necesario cambiar la asignación de zona de un sensor registrado en el sistema.

Para cambiar la asignación de zona de un detector vía radio:

1. Desplácese hasta EDITAR y pulse SELECC.
2. Desplácese hasta el sensor que desea cambiar y pulse SELECC.
3. Desplácese hasta ZONA.
4. Desplácese hasta el número de zona apropiado (solo se muestran los números de zona disponibles).
5. Pulse SELECC.

16.7.3 Añadir APR

AVISO: Solo puede configurar una APR o verificar su estado en el teclado si cuenta con un módulo vía radio en la central o si alguno de los módulos de expansión y la central tienen licencia para el tipo de módulo utilizado.

No se asignó una APR a un usuario. Generalmente, varias personas comparten una APR (por ejemplo, guardias de seguridad que trabajan en turnos) o, alternativamente, las APR pueden estar ancladas de forma permanente a una superficie, como debajo de un escritorio o detrás de una caja registradora.

Se permite un máximo de 128 APR por central.

Para configurar una APR con el teclado:

1. Seleccione VÍA RADIO y luego APR.
2. Seleccione AÑADIR para añadir una APR.
3. Seleccione MANUALMENTE para introducir un ID de APR de forma manual.
   La central también puede introducir automáticamente el ID seleccionando la opción ALTA APR. Se debe presionar uno de los botones de APR cuando aparece el mensaje ACTIVAR APR, de manera que la central pueda identificar la APR. La central no admitirá una APR si el ID es el mismo de una APR ya configurada.
4. Salga del menú AÑADIR y seleccione el menú EDITAR para configurar la APR.

16.7.4 Editar APR

Para configurar una APR con el teclado:

1. Seleccione VÍA RADIO y luego APR.
2. Seleccione EDITAR para configurar una APR.

DESCRIPCIÓN	Introduzca una descripción para identificar la APR.
ID DE TRANSMISOR	Introduzca el ID de la APR. La central no admitirá una APR si el ID es el mismo de una APR ya configurada.
Func. a pulsad.	Use esta sección para asignar funciones a las combinaciones de botones. Las funciones disponibles son Pánico, Pánico silencioso, Atraco, Sospecha, Salida RF usuario y Alarma médica. Se puede seleccionar más de una combinación de botones para la misma función. Por ejemplo: • Amarillo - Sospecha● • Rojo + Verde – Atraco • Para instalaciones comerciales o domésticas, la configuración por defecto es: Rojo + Verde – Pánico **Nota:** Si una combinación de botones no tiene asignada ninguna función, aún es posible usar esta combinación mediante un disparador. Consulte *Disparadores* en la página 295.

SUPERVISAR	Puede configurar la APR para que envíe señales de supervisión periódicas. Si se habilita la supervisión en la APR (con el puente), la APR enviará un mensaje de supervisión cada 7,5 minutos. El tiempo entre mensajes será aleatorio para reducir las probabilidades de cruce con otras APR. La función de supervisión también debe estar habilitada en la central para la APR específica para que pueda llevarse a cabo correctamente. Si la central no recibe la señal de supervisión, emite una alarma que aparece en el teclado y queda registrada. Si no se habilita la supervisión, la APR envía un mensaje de supervisión cada 24 horas para transmitir el estado de la batería de la APR a la central. Este mensaje también se envía de forma aleatoria para reducir las probabilidades de cruce con otras APR. Seleccione HABILITAR si se habilitó la supervisión para esa APR específica.
TEST	Permite comprobar la señal del PAT.

Consulte también

Disparadores en la página 295

Vía radio en la página 149

Test PAT en la página 170

16.8 Zonas

1. Desplácese hasta ZONAS y pulse SELECC.
2. Desplácese hasta la zona deseada (ZONA 1-x).
3. Desplácese hasta la opción de programación deseada:

DESCRIPCIÓN	Se utiliza para ayudar a identificar la zona; introduzca un nombre específico y descriptivo
TIPO DE ZONA	Determina el tipo de zona. Consulte *Tipos de zona* en la página 393.
ATRIBUTOS	Determina los atributos de la zona. Consulte *Atributos de zona* en la página 399.
A PARTICIÓN	Determina qué zona está asignada a qué partición. Esta opción del menú solo se muestra si hay múltiples particiones definidas en el sistema. Seleccionar esta función les permite a los usuarios formar un grupo de zonas identificas con esa partición del edificio en particular.

La cantidad y el tipo de atributos que se muestran en los menús del teclado para una zona en particular varían según el tipo de zona seleccionada.

16.9 en puertas

1. Desplácese hasta PUERTAS y pulse SELECC.
2. Desplácese hasta la puerta que desea programar y pulse SELECC.
3. Los parámetros y datos, si procede, se muestran para su edición de la siguiente manera:
   - Descripción
   - Entradas de puerta

- Grupo de puertas
- Atributos de puerta
- Temporizadores de puerta
- Información del lector (solo se muestra - formato de la última tarjeta utilizada con el lector configurado)

Entradas de puerta

Cada puerta tiene 2 entradas con funcionalidad definida previamente. Se pueden configurar estas dos entradas, el sensor de posición de puerta y el interruptor de liberación de puerta.

Nombre	Descripción
Zona	La entrada del sensor de posición de puerta también se puede utilizar para la parte de intrusión. Si se utiliza la entrada del sensor de posición de puerta para la parte de intrusión, se debe seleccionar el número de zona a la cual está asignada. Si se utiliza la entrada del sensor de posición de puerta para la parte de acceso, se debe seleccionar la opción «SIN ASIGNAR». Si se asigna el sensor de posición de puerta a una zona de intrusión, puede configurarse como una zona normal, pero con funcionalidad limitada (por ejemplo: no se pueden seleccionar todos los tipos de zonas). Si una partición o el sistema está configurado con un lector de tarjetas, la entrada del sensor de posición de puerta debe estar asignada a un número de zona y a la partición o el sistema que se debe armar.
Descripción (Web únicamente)	Descripción de la zona a la cual está asignado el sensor de posición de puerta.
Tipo de zona (Web únicamente)	Tipo de zona de la zona a la cual está asignado el sensor de posición de puerta (no todos los tipos de zonas están disponibles).
Atributos de zona (Web únicamente)	Se pueden modificar los atributos para la zona a la cual está asignado el sensor de posición de puerta.
Particiones (Web únicamente)	La partición a la cual están asignados la zona y el lector de tarjeta. (Si se utiliza el lector de tarjetas para el armado y desarmado, esta partición se armará/desarmará).
Posición de puerta (web) RFL posic.puerta (teclados)	La resistencia utilizada con el sensor de posición de puerta. Seleccione el valor o la combinación de resistencia utilizada.
DPS normalmente abierto	Seleccione si el interruptor de liberación de puerta debe ser una entrada normalmente abierta o normalmente cerrada.

Nombre	Descripción
Liberar puerta (web) RFL LIBER.PUERTA (teclados)	La resistencia utilizada con el interruptor de liberación de puerta. Seleccione el valor o la combinación de resistencia utilizada.
DRS normalmente abierto	Seleccione si el interruptor de liberación de puerta es una entrada abierta normalmente o no.
Sin DRS (Web únicamente)	Seleccione esta opción para ignorar DRS. Si se utiliza un DC2 en la puerta, se DEBE seleccionar esta opción. Si no se selecciona, la puerta se abrirá.
Localización lector (Entrada/salida) (Web únicamente)	Seleccione la ubicación de los lectores de entrada y salida.
Formatos de lector (web) INFORMACIÓN DEL LECTOR (teclados)	Se muestra el formato de la última tarjeta utilizada con cada lector configurado.

Cada número de zona libre puede ser asignado a las zonas, pero la asignación no es fija. Si se asigna el número 9 a una zona, dicha zona y un módulo de expansión de entrada con la dirección '1' se conectan al X-Bus (que está utilizando los números de zona 9–16). La zona asignada desde el controlador de dos puertas se trasladará al siguiente número de zona libre. La configuración se adaptará en consecuencia.

Grupos de puertas

Las distintas puertas pueden asignarse a grupos de puertas. Esto es necesario si una de las siguientes funcionalidades está activada:

- Custodia
- Retorno laxo
- Evitar retorno
- Bloqueo de puerta

Atributos de puerta

Si no hay ningún atributo activado, se puede usar una tarjeta válida.

Atributo	Descripción
Nulo	La tarjeta se bloquea temporalmente.
Grupo de puertas	Se utiliza cuando se asignan diversas puertas a la misma partición y/o se requiere funcionalidad de anti-retorno, custodia o interbloqueo.
Tarjeta y PIN	Se requiere tarjeta y código PIN para entrar.
Solo código PIN	Se requiere código PIN. No se aceptará ninguna tarjeta.
Código PIN o tarjeta	Se requiere código PIN o tarjeta para entrar.
Código PIN para salir	Se requiere código PIN en lector de salida. Se requiere puerta con lector de entrada y salida.
PIN para desarmar	Se requiere PIN para armar y desarmar la partición vinculada. Antes de introducir el código PIN, se debe presentar la tarjeta.
Desarmado desde exterior (navegador)	Cuando se presente la tarjeta en el lector de entrada, la partición/área se desarmará.
Desarmado desde interior (navegador)	Cuando se presente la tarjeta en el lector de salida, la partición/área se desarmará.
Anular alarma	Se permite el acceso si la partición está armada y la puerta es un tipo de zona de entrada o con alarma.
Armado total desde exterior (navegador)	Cuando se presente dos veces la tarjeta en el lector de entrada, la partición/área se armará totalmente.
Armado total desde interior	Cuando se presente dos veces la tarjeta en el lector de salida, la partición/área se armará totalmente.
Armado total forzado	Si el usuario cuenta con los derechos necesarios, puede forzar el armado desde el lector de entrada.
Emergencia	La puerta bloqueada se abre si se detecta una alarma de incendio dentro de la partición asignada.
Otra emergencia	Una alarma de incendio en cualquier otra partición desbloqueará la puerta.
Acompañante	La función de Visita obliga a los titulares de tarjetas con este privilegio a acompañar a otros titulares de tarjetas por puertas específicas. Si esta función está asignada a una puerta, se debe presentar primero una tarjeta con derecho de Visita para permitir abrir la puerta a otros titulares de tarjeta sin este derecho. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con derecho de Visita; se puede configurar individualmente para cada puerta.

Atributo	Descripción
Evitar retorno*	Se debe reforzar la funcionalidad anti-retorno en la puerta. Todas las puertas deben tener lectores de entrada y salida, y deben estar asignadas a un grupo de puertas. En este modo, los titulares de tarjeta deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta válido presentó su tarjeta de acceso para entrar a un grupo de puertas y no presentó la tarjeta para salir, el titular está incumplimiento las normas de anti-retorno. La próxima vez que el titular de tarjeta intente acceder al mismo grupo de puertas, se disparará una alarma de anti-retorno estricta y el titular no tendrá autorización para entrar al grupo de puertas.
Retorno laxo*	Los incumplimientos de las normas anti-retorno solo se registran. Todas las puertas deben tener lectores de entrada y salida, y deben estar asignadas a un grupo de puertas. En este modo, los titulares de tarjeta deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta válido presentó su tarjeta de acceso para entrar a un grupo de puertas y no presentó la tarjeta para salir, el titular está incumplimiento las normas de anti-retorno. La próxima vez que el titular de tarjeta intente acceder al mismo grupo de puertas, se disparará una alarma de anti-retorno laxa. Sin embargo, el titular de la tarjeta seguirá teniendo autorización para entrar al grupo de puertas.
Custodia*	La función Custodia le permite al titular de la tarjeta con derecho de Custodia (el custodia) conceder a otros titulares de tarjetas (que no son custodia) acceso a la sala. El usuario Custodia debe ser el primero en entrar en la sala. Los usuarios que no son custodia solo pueden ingresar si el custodia está en la sala. El custodia no podrá salir hasta que todos los usuarios que no son custodia hayan salido de la sala.
Sirena puerta	La sirena integrada en la placa del controlador de puerta suena cuando se activan las alarmas de puerta.
Ignorar forzado	La apertura forzada de la puerta no se procesa.
Interrelacionada* (navegador)	Solo se permitirá la apertura de una sola puerta de la partición a la vez. Requiere Grupo de puertas.
Prefijo de armado	Autorización con prefijo de clave (A, B, * o #) para armar el sistema
* Requiere Grupo de puertas	

Temporizadores de puerta

Temporizador	Mín.	Máx.	Descripción
Acceso autorizado	1 s	255 s	El período de tiempo durante el cual la cerradura permanecerá abierta tras la autorización de acceso.
Acceso denegado	1 s	255 s	Período de tiempo tras la cual el controlador estará listo para leer la siguiente incidencia tras una incidencia no válida.
Puerta abierta	1 s	255 s	Período de tiempo dentro del cual la puerta debe estar cerrada para evitar una alarma de «puerta abierta tiempo excesivo».
Puerta dejada abierta	1 min	180 min	Período de tiempo dentro del cual la puerta debe estar cerrada para evitar una alarma de «puerta dejada abierta».
Extendido	1 s	255 s	Tiempo adicional tras la autorización de acceso a una tarjeta con un atributo de tiempo extendido.

Temporizador	Mín.	Máx.	Descripción
Acompañante	1 s	30 s	Período de tiempo después de presentar una tarjeta con atributo de Visita dentro del cual un usuario sin atributo de Visita puede acceder por la puerta.

16.10 Salida

Cada tipo de zona del sistema SPC tiene un tipo de salida asociado (un indicador o una marca interna). Cuando se activa un tipo de zona, es decir, cuando se abre una puerta o una ventana, se detecta humo, se detecta una alarma, etc., se activa la salida correspondiente.

1. Desplácese hasta SALIDAS y pulse SELECC.
2. Desplácese hasta CONTROLADOR o MÓDULO DE EXPANSIÓN y pulse SELECC.
3. Desplácese hasta el módulo de expansión/salida que desea programar y pulse SELECC.

   Si se registran las activaciones de salida en el registro de incidencias del sistema (es decir, habilitadas, elementos registrados/deshabilitados, etc.), las opciones de programación están disponibles según se indica en la tabla a continuación.

NOMBRES	Se utilizan para ayudar a identificar la salida; introduzca un nombre específico y descriptivo.
TIPO DE SALIDA	Determina el tipo de salida; consulte la tabla en *Tipos de salidas y puertos de salida* abajo para obtener una descripción de los tipos de salida.
MODO SALIDA	Determina el estilo de la salida: Continua, Temporizada o Impulso.
POLARIDAD	Determina si la salida está activada con polaridad positiva o negativa.
REGISTRO	Determina si el registro del sistema está habilitado o deshabilitado.

Para conocer el procedimiento de test de salida, consulte *Test salida* en la página 169.

16.10.1 Tipos de salidas y puertos de salida

Cada tipo de salida puede asignarse a uno de los seis puertos de salida físicos del controlador SPC o a una salida en uno de los módulos de expansión conectados. Los tipos de salida que no están asignados a salidas físicas funcionan como indicadores de incidencias en el sistema y pueden registrarse y/o informarse a las estaciones centrales en caso de ser necesario.

Los puertos de salida en los módulos de expansión son todas salidas de tipo relé unipolar (NA, COM, NC). Por lo tanto, es posible que los dispositivos de salida requieran fuentes de alimentación externas para activarse si están cableados a las salidas de módulos de expansión.

La activación de un tipo de salida concreto depende del tipo de zona (consulte *Tipos de zona* en la página 393) o de condición de la alerta que provoca la activación. Si se definen varias particiones en el sistema, las salidas en el SPC se agrupan en salidas del sistema y salidas de partición; las salidas del sistema se activan para indicar una incidencia que afecta a todo el sistema (como un fallo en la red de CA), mientras que las salidas de partición indican incidencias detectadas en una o más de las particiones definidas en el sistema. Cada partición tiene su propio conjunto de salidas de partición. Si la partición es común para otras particiones, entonces las salidas indicarán el estado de todas las particiones en común, incluyendo el estado propio. Por ejemplo, si la partición 1 es común para las particiones 2 y 3, y Sirena Exterior está Si la sirena está activa, entonces la salida de sirena exterior de la Partición 1 también está activa.

Algunos tipos de salidas solo pueden indicar incidencias que afectan a todo el sistema (no específicas de particiones). Consulte la tabla a continuación para obtener más información.

Tipo de salida	Descripción
Sirena exterior	Este tipo de salida se utiliza para activar la sirena exterior del sistema y está activa cuando hay una sirena exterior activa. Por defecto, la salida está asignada a la primera salida de la placa del controlador (EXT+, EXT-). **Nota:** Se activa automáticamente una sirena exterior cuando una zona que está programada como zona de alarma dispara una alarma en modo Armado total o Armado parcial.
Flash exterior	Este tipo de salida se utiliza para activar el flash de la sirena exterior del sistema y está activa cuando hay un flash de partición activo. Por defecto, la salida está asignada a la salida de relé de flash (Salida 3) de la placa del controlador (NA, COM, NC). **Nota:** Se activa automáticamente una salida de flash exterior cuando una zona que está programada como zona de alarma dispara una alarma en modo Armado total o Armado parcial. El flash de sirena exterior se activa en una condición 'Fallo al armar' si el flash en la opción 'Fallo al armar' está marcada en las opciones del sistema.
Sirena interior	Este tipo de salida se utiliza para activar la sirena interior y está activa cuando hay una sirena interior activa. Por defecto, la salida está asignada a la segunda salida de la placa del controlador (INT+, INT-). **Nota:** Se activa automáticamente una sirena interior cuando una zona que está programada como zona de alarma dispara una alarma en modo Armado total o Armado parcial. La sirena interior se activa en una condición «Fallo al armar» si en las opciones del sistema está seleccionada la opción «Fallo al armar».
Alarma	Esta salida se activa tras la activación de una zona de alarma en el sistema o desde cualquier partición definida en el sistema.
Alarma confirmada	Esta salida se activa cuando se ha confirmado una alarma. Una alarma se confirma cuando se activan 2 zonas independientes en el sistema (o dentro de la misma partición) dentro de un período de tiempo específico.
Pánico*	Esta salida se activa tras la activación de tipos de zona de alarma de pánico desde cualquier partición. También se genera una salida de alarma de pánico si se produce una incidencia de coacción o si se habilita la opción de pánico para el teclado.
Atraco	Esta salida se activa cuando una zona programada como de tipo atraco dispara una alarma desde cualquier partición.
Incendio	Esta salida se activa tras la activación de una zona de incendio en el sistema (o desde cualquier partición).
Tamper	Esta salida se activa cuando se detecta una condición de tamper desde cualquier parte del sistema. Para un sistema de Grado 3, si se pierde la comunicación hacia un dispositivo X-BUS durante más de 100 segundos, se genera un tamper y las incidencias informadas de SIA y CIR enviarán un tamper.
Alarma médica	Esta salida se activa cuando se activa una zona de alarma médica.
Fallo	Esta salida se activa cuando se detecta un fallo técnico.

Tipo de salida	Descripción
Técnico	Esta salida se activa con actividad de una zona técnica.
Fallo red CA*	Esta salida se activa cuando se interrumpe la red de CA.
Fallo de batería*	Esta salida se activa cuando hay un problema con la batería de respaldo. Si el voltaje de la batería es inferior a 11 V, se activa esta salida. La opción 'Restaurar' para este fallo solo se presenta cuando el nivel de tensión asciende hasta por encima de 11,8 V.
Armado parcial A	Esta salida se activa si el sistema o cualquier partición definida en el sistema está en modo Armado parcial A.
Armado parcial B	Esta salida se activa si el sistema o cualquier partición definida en el sistema está en modo Armado parcial B.
Armado total	Esta salida se activa si el sistema está en modo Armado total.
Fallo al armar	Esta salida se activa si no se pudo armar el sistema o cualquier partición definida en el sistema. Se borra cuando se restaura la alarma.
Entrada/salida	Esta salida se activa si se ha activado una zona de entrada/salida, es decir, si se está ejecutando un temporizador de entrada o salida de una partición o del sistema.
Enclavamiento	Esta salida se activa según lo definido en la configuración de salida de enclavamiento del sistema (consulte *Configurar enclavamiento y autoarmado de salidas del sistema* en la página 232). Esta salida puede utilizarse para resetear los sensores de enclavamiento al igual que los sensores de humo o inerciales.
Salida incendio	Esta salida se activa si se activa alguna de las zonas de salida de emergencia.
Chime	Esta salida se activa momentáneamente cuando se activa el atributo chime de cualquier zona del sistema.
Humo	Esta salida se enciende momentáneamente (3 segundos) cuando un usuario desarma el sistema; puede utilizarse para restablecer detectores de humo. La salida también se activará cuando se restaure la zona. Cuando se utiliza la zona para restaurar detectores de humo bloqueados, la primera vez que se introduzca el código no se activarán las salidas de humo, sino que se silenciarán las sirenas; la siguiente vez que se introduzca el código, si la zona de incendio está en estado abierto, la salida de humo se activará momentáneamente. Este proceso se puede repetir hasta que se cierre la zona de incendio.
Test de paseo*	Esta salida se activa momentáneamente cuando se realiza un test de intrusión y se activa una zona. Esta salida se puede utilizar, por ejemplo, para activar tests funcionales de detectores conectados (si está disponible).
Armado automático	Esta salida se activa cuando se activa la función de armado automático en el sistema.
Coacción de usuario	Esta salida se activa si se ha activado el estado de coacción de usuario (si se introdujo un código PIN + 1 en el teclado).

Tipo de salida	Descripción
PIR enmascarado	Esta salida se activa si hay zonas PIR enmascaradas en el sistema. Genera una salida de fallo en la luz LED del teclado. Esta salida se bloquea y permanecerá activa hasta que sea restablecida por un usuario de nivel 2. Se registra el enmascaramiento PIR por defecto. La cantidad de entradas del registro no supera 8 entre los períodos de armado.
Zona omitida	Esta salida se activa si hay zonas inhibidas, aisladas o zonas de test de intrusión en el sistema.
Comunicación	Esta salida se activa si hay un fallo de comunicación con la estación central.
Test hombre caído	Esta salida se activa en un dispositivo vía radio de 'hombre caído', el cual se activa cuando se realiza el test de 'hombre caído'.
Desarmado	Esta salida se activa si el sistema está en modo Desarmado.
Aborto de alarmas	Esta salida se activa si se aborta una alarma, es decir, cuando se introduce un código de usuario válido a través del teclado luego de una alarma confirmada o no confirmada. Se utiliza, por ejemplo, con marcadores externos (SIA, CID, FF).
Test sísmico	Esta salida se utiliza para activar una prueba manual o automática en una zona sísmica. Los sensores sísmicos tienen un vibrador pequeño que se fijará a la misma pared que el sensor y estará cableado a una salida en la central o uno de sus módulos de expansión. Durante la prueba, la central espera hasta 30 segundos para que la zona sísmica se abra. Si esto no sucede, el test falla. Si se abre dentro de los 30 segundos, la central espera a que la zona se cierre dentro de un período de 10 segundos. Si esto no sucede, el test falla. Luego, la central espera otros 2 segundos antes de informar el resultado del test. El resultado del test, ya sea manual o automático, se almacena en el registro de incidencias del sistema.
Alarma local	Esta salida activa una alarma de intrusión local.
Salida RF	Esta salida se activa cuando se pulsa un botón de una APR o dispositivo de mando vía radio.
Fallo línea TX 1	Esta salida se activa cuando hay un fallo en la línea del módem principal.
Fallo TX 1	Esta salida se activa cuando falla el módem principal.
Fallo línea TX 2	Esta salida se activa cuando hay un fallo en la línea del módem secundario.
Fallo TX 2	Esta salida se activa cuando falla el módem secundario.
Batería baja	Esta salida se activa cuando la batería está baja.
Estado de entrada	Esta salida se activa si se implementa un procedimiento de entrada 'Todo OK' y no se genera una alarma, es decir, cuando se pulsa el botón 'Todo OK' dentro del período de tiempo configurado tras haber introducido el código de usuario.
Estado de aviso	Esta salida se activa si se implementa un procedimiento de entrada 'Todo OK' y se genera una alarma silenciosa, es decir, cuando no se pulsa el botón 'Todo OK' dentro del período de tiempo configurado tras haber introducido el código de usuario.
Listo para armar	Esta salida se activa cuando una partición está lista para el armado.

Tipo de salida	Descripción
Config. ACK	Esta salida señala el estado de armado. La salida alterna durante 3 segundos para indicar que el armado ha fallado. La salida permanece activa durante 3 segundos si el armado se ha realizado correctamente.
Arm. total hecho	Esta salida se activa durante 3 segundos para indicar que el sistema se ha armado completamente.
Blockschloss 1	Se utiliza para dispositivos Blockschloss normales. Cuando todas las zonas de una partición están cerradas, y no hay errores pendientes, la salida «Blockschloss 1» se activa. Si la cerradura del Blockschloss está cerrada, se activa una entrada de «Llave A/D», se arma la partición relevante y se activa la salida Config. ACK durante 3 segundos para indicar que el armado se ha realizado satisfactoriamente. «Blockschloss 1» no está desactivado. Si el Blockschloss está desbloqueado, el dispositivo Blockschloss desactiva la entrada de Llave A/D dejándola en estado desarmado (cerrado), y la partición queda desarmada. A continuación, «Blockschloss 1» se desactiva.
Blockschloss 2	Se utiliza para dispositivos de tipo Blockschloss: Bosch Blockschloss, Sigmalock Plus, E4.03. Cuando todas las zonas de una partición están cerradas, y no hay errores pendientes, la salida «Blockschloss 2» se activa. Si la cerradura del Blockschloss está cerrada, se activa una entrada de «Llave A/D», se arma la partición relevante y se activa la salida Config. ACK durante 3 segundos para indicar que el armado se ha realizado satisfactoriamente. A continuación, «Blockschloss 2» se desactiva. Si el Blockschloss está desbloqueado, la zona de Llave A/D pasa a quedar desarmada (cerrada) y la partición queda desarmada. «Blockschloss 2» está activado (si la partición está lista para el armado).
Elemento bloqueo	Se activa si el elemento de bloqueo está en la posición «bloqueada».
Elemento desbloqueo	Se activa si el elemento de bloqueo está en la posición «desbloqueada».
Código tamper	Se activa si hay un código tamper en la partición. Se desactiva cuando se restaura el estado.
Problema	Se activa si hay alguna zona con problemas.
Link Ethernet	Se activa si hay algún fallo en el link de Ethernet.
Fallo red	Se activa si hay algún fallo de comunicación de EDP.
Reset cristal	Sirve para conectar la alimentación para el módulo de interfaz de rotura de cristal y para desconectarla a fin de reiniciar el dispositivo. La salida se reinicia si un usuario introduce su código, la zona no está en estado cerrado y las campanas están desactivadas.

Tipo de salida	Descripción
Atraco confirmado	Se activa en los siguientes casos para cumplir con PD6662: • se producen dos activaciones de zona de atraco con una diferencia de más de dos minutos entre sí • se produce la activación de una zona de atraco y una zona de pánico con una diferencia de más de dos minutos entre sí • Si se produce la activación de una zona de atraco y una zona de tamper o una zona de pánico y una zona de tamper dentro del período de dos minutos.
Modo técnico completo	Se activa si hay un técnico in situ y el sistema se encuentra en modo técnico completo.

**Este tipo de salida sólo puede indicar incidencias que afectan a todo el sistema (no específicas de particiones).*

Consulte también

Configurar enclavamiento y autoarmado de salidas del sistema en la página 232

16.11 Comunicación

1. Desplácese hasta COMUNICACIÓN y pulse SELECC.
2. Desplácese a la opción de programación deseada.

16.11.1 Puertos serie

Los puertos serie admiten la conexión de PC antiguas al sistema u otros equipos periféricos tales como impresoras.

1. Desplácese hasta PUERTOS SERIE.
2. Pulse SELECC.
3. Desplácese hasta el puerto serie que desea programar.
4. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.

TIPO	Determina si el tipo es TERMINAL (información del sistema) o IMPRESORA (registro de incidencias del SPC).
VELOCIDAD DE BAUDIOS	Determina la velocidad de la comunicación entre la central y los equipos periféricos. Tenga en cuenta que la velocidad de baudios debe ser igual en ambos equipos.
BITS DE DATOS	Determina el tamaño del paquete de datos que se debe transferir entre la central y los equipos periféricos. Tenga en cuenta que los bits de datos deben ser iguales en ambos equipos.
BITS DE PARADA	Determina la cantidad de bits de parada al final del paquete de datos. Tenga en cuenta que los bits de parada deben ser iguales en ambos equipos.
PARIDAD	Determina la paridad (par/impar) del paquete de datos. Tenga en cuenta que la paridad debe ser igual en ambos equipos.
CONTROL DE FLUJO	Determina si los datos se encuentran bajo control de hardware (RTS. CTS) o de software (ninguno). Tenga en cuenta que el control de flujo debe ser igual en ambos equipos.

5. Pulse ATRÁS para salir.

16.11.2 Puertos Ethernet

Para programar el puerto Ethernet:

1. Desplácese hasta PUERTO ETHERNET.
2. Pulse SELECC.

   Se mostrará la opción DIRECCIÓN IP, XXX.XXX.XXX.XXX (Para números de una cifra, se necesitan ceros delante, por ejemplo: 001).
3. Pulse SELECC. e introduzca la dirección IP preferida.

   Cuando pulse la tecla INTRO, el sistema emitirá un sonido dos veces y aparecerá el mensaje ACTUALIZADO si la dirección IP es válida. Si introduce la dirección IP manualmente, debe ser la única en la red LAN o VLAN conectada a la central. Si se utiliza la opción DCHP, no se completa el campo.
4. Desplácese hasta IP DE MÁSCARA DE SUBRED.
5. Pulse SELECC. e introduzca la MÁSCARA SUBRED con formato XXX.XXX.XXX.XXX. (Para números de una cifra, se necesitan ceros delante, por ejemplo: 001). Cuando pulse la tecla INTRO, el sistema emitirá un sonido dos veces y aparecerá el mensaje ACTUALIZADO si la IP DE MÁSCARA DE SUBRED es válida.
6. Desplácese hasta PUERTA DE ENLACE. Tenga en cuenta que la puerta de enlace debe estar programada para el acceso fuera de la red (para uso con el Portal).
7. Pulse SELECC. e introduzca el formato XXX.XXX.XXX.XXX. de la PUERTA DE ENLACE. (Para números de una cifra, se necesitan ceros delante, por ejemplo: 001). Cuando pulse la tecla INTRO, el sistema emitirá un sonido dos veces y aparecerá el mensaje ACTUALIZADO si la PUERTA DE ENLACE es válida.
8. Desplácese hasta DHCP. El DHCP está habilitado si la red LAN tiene un servidor DHCP para asignar la dirección IP. La dirección IP debe habilitarse manualmente. Tenga en cuenta que la puerta de enlace debe estar programada si la central requiere acceso fuera de la red (para servicio del Portal).
9. Pulse SELECC. e introduzca el formato XXX.XXX.XXX.XXX. de la PUERTA DE ENLACE. (Para números de una cifra, se necesitan ceros delante, por ejemplo: 001).

   Cuando pulse la tecla INTRO, el sistema emitirá un sonido dos veces y aparecerá el mensaje ACTUALIZADO si la PUERTA DE ENLACE es válida.

   Se muestra la opción DHCP.
10. Desplácese entre DHCP HABILITADO y DESHABILITADO para seleccionar la opción preferida.
11. Pulse SELECC.

16.11.3 Transmisores

El sistema SPC es compatible con los transmisores inteligentes SPC para comunicaciones con líneas analógicas e interfaz de redes móviles para comunicaciones y conectividad mejoradas. El sistema SPC debe configurarse en consecuencia.

16.11.3.1 Control de la interfaz de red de transmisión

El sistema de alarma SPC envía un polling a SPC Com XT, el cual responde con un reconocimiento (ACK) de polling. Al recibir un ACK de polling válido, el sistema de alarma SPC actualiza el estado a OK y resetea el temporizador de intervalo de polling (según la categoría de ATP).
Si el sistema de alarma SPC no recibe un ACK de polling dentro del período de tiempo especificado (según la categoría de ATP), el sistema de alarma SPC actualiza el estado a CAÍDO.

SPC admite las siguientes interfaces de transmisión:

- Ethernet
- Módem GSM con GPRS habilitado
- Módem RTB

AVISO: Antes de cambiar el código PIN o de usar una nueva tarjeta SIM, asegúrese de que todas las fuentes de alimentación estén desconectadas (red de CA y batería) o la tarjeta no se activará.

AVISO: Tras restablecer los valores por defecto de fábrica, durante el proceso de configuración inicial del sistema con el teclado, la central detecta si hay un módem principal o de respaldo y, en caso de ser así, muestra el tipo de módem y lo habilita automáticamente con la configuración por defecto. No se permite otro tipo de configuración en esta etapa.

16.11.3.2 Configurar módems

Para configurar un módem GSM o RTB:

1. Desplácese hasta MÓDEMS y pulse SELECC.
2. Desplácese entre PRINCIPAL y RESPALDO para seleccionar el módem que corresponde y pulse SELECC.

   Se muestra la opción HABILITAR MÓDEM.
3. HABILITE o INHIBA el módem según sea necesario.
4. Desplácese a ESTADO TX, TIPO, VERSIÓN FIRMWARE y NIVEL DE SEÑAL, y pulse SELECC. para ver detalles del módem.
5. Configure los siguientes ajustes del módem desde el menú, tal como se indica a continuación, y pulse INTRO después de cada selección:

Opción de menú	Descripción
CÓDIGO PAÍS	Seleccione un país de la lista.
CÓDIGO GSM	(Sólo módem GSM) Introduzca un código GSM para la tarjeta SIM.
MODO RESPUESTA	Elija esta opción para seleccionar el modo en que el módem responderá a las llamadas entrantes: NO RESPONDER NUNCA O RESPONDER SIEMPRE.
RESP. ACC. TÉCNICO	Seleccione HABILITAR para responder sólo con código de técnico autorizado.

Opción de menú	Descripción
CONFIG. SMS	Seleccione HABILIT. SMS para habilitar el SMS para este módem. **Sólo módem RTB** Seleccione Servidor SMS para introducir un número de teléfono apropiado del proveedor de servicios de SMS accesible donde usted se encuentra, si es necesario. Este número muestra automáticamente el número por defecto para SMS en el país seleccionado. Para comprobar manualmente el SMS, seleccione TEST e introduzca el NÚMERO DE SMS. Para probar automáticamente un SMS a intervalos específicos, seleccione TEST AUTOMÁTICO, seleccione un INTERVALO DE TEST e introduzca el NÚMERO DE SMS.
MARCACIÓN DE PREFIJO	**Sólo módem RTB** Introduzca el número de prefijo que se debe incluir antes del número de SMS, si es necesario.
Supervisión de línea	**Sólo módem RTB** Habilite esta opción para controlar la tensión de la línea conectada al módem. **Sólo módem GSM** Habilite esta opción para controlar el nivel de señal del módulo GMS conectado al módem. Seleccione un modo de control (SIEMPRE ACTIVADO, ARMADO TOTAL, DESHABILITAR). La opción ARMADO TOTAL solo permite esta función cuando el sistema está en Armado total. Introduzca la cantidad de segundos para el TEMPORIZADOR de supervisión (0 -9999 segundos). **Nota:** Configuración de confirmación EN 50131-9 Para que la confirmación según EN50131-9 funcione correctamente, la supervisión de línea debe estar habilitada. (Consulte *Opciones del sistema* en la página 254.)
USSD	**Sólo módem GSM** Introduzca el código del Servicio Suplementario de Datos no Estructurados (**USSD**) para su proveedor de servicios para habilitar la comprobación de crédito mediante SMS gratuito para tarjetas SIM prepagas. Nota: Esta función no está disponible universalmente. Verifique con su proveedor del servicio.
COMP. CRÉDITO SIM	Habilite esta función para recibir información sobre saldo de crédito para tarjetas SIM prepagas (donde esté disponible por parte de su proveedor del servicio).

Sólo módem GSM

Si la mensajería SMS está habilitada y se envía un código PIN incorrecto a la tarjeta SIM tres veces, la tarjeta SIM se bloqueará. En este caso, Vanderbilt recomienda que se retire la tarjeta SIM y se desbloquee con un teléfono móvil. Si se cambia la tarjeta SIM del módulo GSM o si se utiliza una tarjeta SIM con un código PIN, Vanderbilt recomienda que se programe el código PIN antes de que se coloque la tarjeta SIM en el soporte de la tarjeta. Esto garantiza que no se envíen códigos PIN incorrectos a la tarjeta SIM. Cuando se coloca la tarjeta SIM en el soporte, se debe desconectar la alimentación (red de CA y batería).

16.11.4 Estación central

Esta sección abarca:

16.11.4.1 Agregar

Para programar la configuración de la estación central:

1. Desplácese hasta ESTACIÓN CENTRAL > AÑADIR.
2. Pulse SELECC.
3. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.

ID ABONADO	Esta información debe estar disponible desde la estación de recepción y se utiliza para identificar a los usuarios cada vez que se realiza una llamada a la CRA.
NOMBRE ABONADO	Descripción de la central de recepción de alarmas remota.
PROTOCOLO	El protocolo de comunicación que se utilizará (SIA, Contact ID, Formato rápido).
TELÉFONO 1	El primer número que se debe marcar para contactarse con la CRA.
TELÉFONO 2	El segundo número que se debe marcar para contactarse con la CRA. El sistema sólo intenta contactar con la CRA mediante este número si el primer número de contacto no pudo conectar con éxito.
PRIORIDAD	El módem (primario o de respaldo) que se utilizará para comunicarse con la CRA.

4. Una vez que se complete la programación, en el teclado aparecerá la opción de realizar una llamada de test a la estación.

16.11.4.2 Editar

Par editar la configuración de la estación central:

1. Desplácese hasta ESTACIÓN CENTRAL > EDITAR.
2. Pulse SELECC.
3. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.

ID ABONADO	Esta información debe estar disponible desde la estación de recepción y se utiliza para identificar a los usuarios cada vez que se realiza una llamada a la CRA.
NOMBRE ABONADO	Descripción de la central de recepción de alarmas remota.
PROTOCOLO	El protocolo de comunicación que se utilizará (SIA, Contact ID, Formato rápido).
TELÉFONO 1	El primer número que se debe marcar para contactarse con la CRA.
Teléfono 2	El segundo número que se debe marcar para contactarse con la CRA. El sistema sólo intenta contactar con la CRA mediante este número si el primer número de contacto no pudo conectar con éxito.
INTENTOS DE MARCACIÓN	Introduzca la cantidad de veces que el sistema intentará realizar una llamada al receptor.
INTERVALO DE MARCACIÓN	Introduzca la cantidad de segundos de retardo entre intentos fallidos de marcación. (0-999)

Partic.asignadas	Asigne las particiones para las que se enviarán incidencias a la CRA.
INCIDENCIAS ENVIADAS	Defina los tipos de incidencias enviadas a la CRA.
PRIORIDAD	El módem (primario o de respaldo) que se utilizará para comunicarse con la CRA.
TEST AUTOMÁTICO	Define una programación para comprobar la conexión a la CRA. Los posibles valores oscilan entre cada hora y una vez cada 30 días.

4. Una vez que se complete la programación, en el teclado aparecerá la opción de realizar una llamada de test a la estación.

16.11.4.3 Borrar

Le permite borrar una CRA configurada.

16.11.4.4 Iniciar llamada de test

Le permite comprobar la conexión con la CRA.

Para realizar una llamada de prueba, haga lo siguiente:

1. Seleccione Llamad. test
2. Seleccione el nombre de la CRA.
3. Haga clic en Selecc.
4. Seleccione el módem que se utilizará para la llamada de prueba.

   Se realiza la llamada de prueba.

16.11.5 SPC Connect PRO

SPC Connect PRO es una aplicación de escritorio diseñada para brindar asistencia técnica para la instalación y el mantenimiento de los sistemas SPC. Si usa SPC Connect PRO, puede crear instalaciones y configurarlas antes de llegar al lugar. La herramienta puede utilizarse en conjunto con el servicio en la nube SPC Connect para conectarse de forma remota a sitios y brindar asistencia técnica.

Para habilitar y configurar el soporte para SPC Connect PRO:

1. Desplácese hasta SPC CONNECT PRO y pulse SELECC.
2. Habilite la opción SPC CONNECT PRO.
3. Desplácese hasta INTERFACES y pulse SELECC.
4. Habilite/Deshabilite la opción ETHERNET, USB, SERIE (X10) y MÓDEM según corresponda.
5. Para habilitar la interfaz TCP, seleccione PUERTO TCP, introduzca el número de puerto y pulse SELECC.

16.12 Test

1. Desplácese a TEST y pulse SELECC.
2. Desplácese a la opción de programación deseada.

16.12.1 Test sirena

Para realizar un test de sirena:

1. Desplácese hasta TEST > TEST DE SIRENA.
2. Pulse SELECC.

Cuando se selecciona la opción TEST DE SIRENA, encontrará las siguientes opciones disponibles: SIRENAS EXTERIORES, FLASH, SIRENAS INTERIORES y ZUMBADOR. Al seleccionar cada una de estas opciones, el dispositivo suena para comprobar que funciona correctamente.

16.12.2 Test de intrusión

Un test de intrusión garantiza que los detectores están funcionando correctamente en el sistema SPC.

Para realizar un test de intrusión:

1. Desplácese a TEST > TEST INTRUSIÓN.
2. Pulse SELECC.
3. La pantalla indica el número total de zonas del sistema donde se realizará la prueba con el texto PARA PRUEBA XX (donde XX representa el número de zonas válidas para test de intrusión). Coloque el sensor en la primera zona y actívelo (abra la puerta o la ventana).

   El zumbador del teclado suena continuamente durante unos dos segundos para indicar que se ha detectado la activación de la zona, a la vez que desciende el número de zonas que quedan por someterse al test (se muestran en el teclado).
4. Prosiga con las zonas que quedan en el sistema hasta que todas se hayan probado. Si el sistema no reconoce la activación de una zona, revise el cableado del detector o sustitúyalo por otro detector si fuera necesario.

AVISO: Todas las zonas se pueden incluir en un test de intrusión de técnico.

16.12.3 Control de zonas

La opción Control de zonas muestra la información de estado de cada una de las zonas del sistema.

Para ver más información sobre el estado de zonas:

1. Desplácese hasta TEST > CONTROL DE ZONAS.
2. Pulse SELECC.
3. Desplácese hasta la zona preferida y pulse SELECC.

   Se mostrará el estado de la zona y el valor de resistencia asociado.
4. Pulse SIGUIENTE para localizar la zona (por ejemplo: CONTROLADOR 1 = primera zona del controlador).

   Consulte la tabla a continuación para ver la información de estado (válido para resistencias 2RFL).

Estado de zona	Abreviatura
DESCONOCIDO	UK
CERRADO	CE
Alarma	OP
CORTO	SH
DESCONECTADO	DI
IMPULSO	PU

Estado de zona	Abreviatura
DET.VIBRACIÓN	GR
ENMASCARADO	AM
FALLO	FA
SUSTITUCIÓN C.C.	DC
FUERA DE LÍMITES	OB
INESTABLE	IN

Se pueden controlar todas las zonas del sistema y determinar si están funcionando correctamente al realizar un test de control.

Para realizar un test de control de zonas:

1. Desplácese hasta CONTROL DE ZONAS.
2. Pulse SELECC.
3. Desplácese hasta la zona preferida y pulse SELECC, o bien introduzca el número de zona directamente.

   Si la zona se encuentra ubicada cerca del teclado, se puede ver el estado del teclado cuando cambia. En la parte superior derecha se muestran el estado de la zona y el valor de resistencia.
4. Cambie el estado del sensor, por ejemplo, para un sensor de contacto de puerta, abra la puerta.

   El zumbador del teclado emite un pitido y el estado del sensor cambia de CL (Cerrado) a OP (Abierto). El valor de resistencia correspondiente cambia a un valor que depende del esquema de resistencia RFL.

Se recomienda que verifique el funcionamiento de todas las zonas del sistema una vez que finalizó la instalación. Para localizar la zona, seleccione SIGUIENTE (botón derecho) en el teclado. Un valor de estado de zona SH o DI indica que hay un cortocircuito en la zona o que está desconectada.

16.12.4 Test salida

Para realizar un test de salida:

1. Desplácese hasta TEST SALIDA.
2. Pulse SELECC.
3. Desplácese entre CONTROLADOR y MÓDULO DE EXPANSIÓN para seleccionar la opción preferida.
4. Si está comprobando las salidas del controlador, desplácese hasta la salida correspondiente y pulse SELECC. Si está comprobando las salidas del módulo de expansión, seleccione el módulo de expansión y luego la salida.

   La pantalla del teclado indica el estado actual de la salida en la línea superior.
5. Alterne entre los estados de salida ACT/DES.
6. Verifique que el dispositivo conectado a la salida seleccionada cambie de estado según corresponda.

16.12.5 Pruebas

La opción Pruebas ofrece un método para comprobar las zonas seleccionadas. Las zonas en prueba no disparan alarmas, pero sí quedan registradas en el registro de incidencias. Las zonas en prueba

permanecerán a prueba hasta que finalice el período de prueba según lo establecido en los valores por defecto (14 días).

Para realizar la prueba:

1. Desplácese hasta PRUEBAS y pulse SELECC.
2. Desplácese entre HABILITAR PRUEBA y CANCELAR PRUEBA para seleccionar la opción preferida.
3. Desplácese hasta la zona preferida y pulse SELECC.

   Aparecerá un mensaje para que confirme que la zona está en prueba.

AVISO: Se pueden incluir todos los tipos de zona en la prueba.

16.12.6 Opciones audibles

Las opciones audibles se aplican como indicadores dentro de un test de intrusión.

Para establecer las opciones audibles:

1. Desplácese a OPCIONES AUDIBLES.
2. Pulse SELECC.
3. Desplácese hasta una de las siguientes opciones: TODO, SIR. INT., SIR. EXT., TECLADO.
4. Pulse SALVAR.
5. Pulse ATRÁS para salir.

16.12.7 Indicadores visuales

Esta prueba sirve para comprobar todos los píxeles en el teclado LCD y todos los píxeles e indicadores LED en el teclado Confort, el módulo de indicador y el conmutador de llave.

Para probar un teclado:

1. Desplácese a Indic. visuales.
2. Pulse SELECC.
3. Pulse Habilitar.

En el teclado LCD se muestran dos filas de caracteres que cambian continuamente.

En el teclado Confort, se encienden todos los indicadores LED y se muestran todos los píxeles de la pantalla.

1. Pulse ATRÁS para deshabilitar la comprobación.
2. Pulse ATRÁS para salir.

16.12.8 Test PAT

AVISO: Solo un técnico o un usuario que tenga derecho de 'Test APR' asignado puede realizar esta prueba. Consulte *Derechos de usuario* en la página 213.

Para comprobar un APR desde el teclado:

1. Desplácese hasta TEST APR y pulse SELECC.
2. Cuando se le solicite ACTIVAR APR, pulse los tres botones simultáneamente en la APR.

Si el test fue exitoso, aparecerá el mensaje *n* OK, donde *n* indicará la cantidad de APR comprobadas.

3. Repita el test en caso de ser necesario.
4. Pulse ATRÁS o X para finalizar el test.

16.12.9 Test sísmico

Para realizar un test sísmico:

1. Desplácese a TEST > TEST SÍSMICO.
2. Pulse SELECC.
3. Seleccione TEST TODAS PART., o seleccione una partición concreta para comprobar.
4. Si selecciona una partición individual para comprobar, puede seleccionar TEST TODAS ZONAS o bien una zona sísmica específica para comprobar.

   Mientras se está realizando el test, en el teclado se muestra el mensaje 'TEST SÍSMICO'.

   Si el test falla, se muestra el mensaje «FALLO SÍSMICO». Si se pulsa la tecla «i» o «VER», se muestra una lista de las zonas con fallo por la que es posible desplazarse.

   Si el test es satisfactorio, se muestra «SÍSMICO OK».

Consulte también

Test de sensor sísmico en la página 368.

16.13 Utilidades

1. Desplácese hasta UTILIDADES y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

Versión software	Para ver la versión actual del software.
PARÁM.FÁBRICA	Para resetear los usuarios o restablecer la configuración de fábrica.
CONFIG.BACKUP	Para realizar una copia de respaldo de la configuración.
RESTAUR.CONFIG.	Para restaurar la configuración.
REINICIO SISTEMA	Para reiniciar el sistema.
LICENCIA	Introduzca un número de licencia para cambiar la clave de licencia de SPC. El sistema no registra o informa un cambio de licencia.

16.14 Aislar

Las zonas, alertas de sistema o alertas desde dispositivos X-BUS se pueden inhibir manualmente desde el teclado. Al inhibirse una zona se elimina la misma del sistema hasta que el usuario la restaura.

Para inhibir zonas, alertas de sistema o alertas desde dispositivos X-BUS:

1. Desplácese a INHIBICIÓN y pulse SELECC.
2. Desplácese a la opción deseada de la siguiente tabla y pulse SELECC.

ZONA	Seleccione la zona correspondiente y cambie la configuración de NO INHIBIDA a INHIBIDA.

Sistema	Inhiba la alerta del sistema deseada.
XBUS	Inhiba la alerta que desee desde MÓDULOS DE EXPANSIÓN o TECLADOS: • Perdida comunic. • FALLO FUSIBLE XBUS (sólo módulos de expansión) • Tamper X-Bus
Ver aislam.	Para ver una lista de las zonas, alertas del sistema y alertas de dispositivos X-BUS que se hayan inhibido.

16.15 Regt.incidenc.

Las incidencias recientes del sistema se muestran en la opción REG.INCIDENCIAS. Las incidencias parpadean a intervalos de un segundo.

1. Desplácese a Reg.incidencias y pulse SELECC.
2. Para ver una incidencia de una fecha determinada, especifique la fecha con las teclas numéricas.

   Las incidencias más recientes se muestran en la parte inferior de la pantalla. Todas las incidencias anteriores se van mostrando por orden durante un segundo.

16.16 Registro de control de accesos

El acceso a las diferentes zonas en el sistema se muestra en la opción REG.ACC.PUERTAS.

1. Desplácese a REG.ACC.PUERTAS y pulse SELECC.
2. Seleccione una puerta en el sistema para la que desee mostrar las incidencias de acceso.

   Las incidencias de acceso más recientes se muestran con la fecha y la hora.
3. Para buscar una incidencia de acceso en particular, desplácese por las incidencias de acceso o introduzca una fecha y pulse INTRO.

16.17 Registro alarmas

El registro de alarmas muestra una lista de las incidencias de alarma.

- Seleccione **Registro > Registro del sistema > Registro de alarmas**.

En este registro se muestran los siguientes tipos:

- Zonas
  – Alarma
  – Pánico
- Incidencias del sistema
  – Alarma confirmada
  – Coacción de usuario
  – Pánico X-Bus
  – Pánico usuario
  – Pánico RPA

16.18 Cambiar código PIN de técnico

Para cambiar el código de técnico:

1. Desplácese hasta CAMBIO COD.TECN. y pulse SELECC.

   Aparecerá un código generado de forma aleatoria.

2. Introduzca un nuevo código, si es necesario, sobreescribiendo el código mostrado y pulsando INTRO.

   El número mínimo de dígitos necesario para este código depende de la configuración de seguridad del sistema o de la longitud programada para los dígitos PIN en el navegador (**Config. central > Config. sistema > Opciones**). El sistema no aceptará un código PIN con un número menor de dígitos que el que se ha configurado.

3. Confirme el código PIN nuevo y pulse SALVAR.
4. Pulse ATRÁS para volver a la pantalla anterior y corregir el código.

   Si se agota el tiempo de la pantalla durante el proceso, el código antiguo seguirá siendo válido.

16.19 Usuarios

Solo los usuarios con el derecho de usuario adecuado habilitado en su perfil pueden añadir, editar o borrar .

16.19.1 Agregar

Para añadir usuarios al sistema:

1. Desplácese a USUARIOS > AÑADIR.

   Seleccione un ID de usuario de los ID disponibles en el sistema y pulse SELECT.

2. Pulse ENTER para aceptar el nombre de usuario por defecto o introduzca un nombre de usuario personalizado y pulse ENTER.
3. Desplácese al tipo de perfil de usuario deseado y pulse ENTER para seleccionarlo.

   El sistema genera un código por defecto para cada nuevo usuario.

4. Pulse ENTER para aceptar el código de usuario por defecto o bien introduzca un código de usuario nuevo y pulse ENTER.

El teclado confirma que se ha creado el nuevo usuario.

16.19.2 Editar

Para editar usuarios en el sistema:

1. Desplácese a USUARIOS > EDITAR.
2. Pulse SELECC.
3. Edite la configuración de usuario deseada que se muestra en la siguiente tabla.

CAMBIAR NOMBRE	Editar el nombre de usuario actual
PERFIL DE USUARIO	Seleccione el perfil adecuado para este usuario.
CÓDIGO COACCIÓN	Habilitar o deshabilitar coacción para este usuario.

FECHA LIMITE	Habilite esta opción si el usuario solo puede acceder al sistema durante un período de tiempo especificado. Introduzca una fecha DESDE y otra fecha HASTA, y pulse INTRO.
ACCESO TARJETA	Habilitar o deshabilitar la capacidad de la tarjeta
Mando vía radio	Habilitar o deshabilitar el acceso al mando vía radio (teclado vía radio, control remoto).
HOMB.CAÍDO [HCD]	Se habilita el test de hombre caído.
CONTROL DE ACCESOS	Si no hay ninguna tarjeta asignada al usuario: • AÑADIR TARJETA • ALTA TARJETA Si el usuario tiene una tarjeta asignada: • EDITAR TARJETA – NÚMERO TARJETA – ATRIBUTOS TARJETA (consulte Control de accesos) • Reset tarjeta • BORRAR TARJETA
IDIOMA	Seleccione un idioma para este usuario que se mostrará en el sistema.

16.19.2.1 Control de accesos

Se puede asignar una tarjeta de acceso a cada uno de los usuarios en la central de control.

Para configurar el control de acceso para un usuario:

1. Desplácese a USUARIOS > EDITAR.
2. Pulse SELECC.
3. Seleccione el usuario que se desee configurar y pulse SELECC.
4. Desplácese a CONTROL ACCESOS y pulse SELECC.

Las siguientes secciones indican los pasos de programación que se encuentran en la opción de control de acceso del usuario seleccionado.

Añadir tarjeta manualmente

Si se conoce el formato del número de la tarjeta, ésta se puede crear manualmente.

El código local de la tarjeta está configurado para el perfil de usuario asignado para este usuario.

1. Desplácese a AÑADIR TARJETA
2. Pulse SELECC.

   Se ha añadido una tarjeta nueva y ahora se puede editar.

Alta tarjeta

AVISO: Sólo se pueden dar de alta tarjetas con formatos soportados.

Si el número o el formato de la tarjeta es desconocido, ésta se puede leer y su información se puede dar de alta.

1. Desplácese a ALTA TARJETA.
2. Pulse SELECC.
3. Seleccione la puerta en la que se presentará la tarjeta.
4. Pulse SELECC.

AVISO: La nueva tarjeta se puede presentar en el lector de entrada o en el de salida de la puerta seleccionada.

5. Presente la tarjeta en un lector de tarjetas en la puerta seleccionada.

   La información para la nueva tarjeta se da de alta.

Editar tarjeta

Si ya hay una tarjeta de acceso asignada a un usuario, se puede cambiar mediante el teclado:

1. Desplácese a EDITAR TARJETA.
2. Pulse SELECC.
3. Edite la configuración de usuario deseada que se muestra en la tabla en *Control de accesos* abajo.
4. Pulse ATRÁS para salir.

Control de accesos

Atributo	Descripción
Número tarjeta	Número de la tarjeta de CCAA Introduzca 0 para dejar sin asignar esta tarjeta.
Tarjeta vacía	Inhibición temporal de tarjeta
Tiempo ampliado	Ampliación de la temporización de la puerta al presentar la tarjeta.
Anulación de Código	Acceso a puerta sin PIN en una puerta con lector de PIN.
Prioridad	Las tarjetas prioritarias se almacenan localmente en los controladores de puertas y permiten el acceso en caso de fallo técnico allí donde el controlador de puerta no se puede comunicar con la central de control. El número máximo de usuarios prioritarios es: • SPC4xxx – todos los usuarios • SPC5xxx – 512 • SPC6xxx – 512
Acompañante	La función de Visita obliga a los titulares de tarjetas con este privilegio a acompañar a otros titulares de tarjetas por puertas específicas. Si esta función está habilitada en una puerta, se debe presentar primero una tarjeta con la atribución de Visita para permitir abrir la puerta a otros titulares de tarjeta sin este atributo. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con derecho de Visita; se puede configurar individualmente para cada puerta.

Atributo	Descripción
Custodia	La función de Custodia impone a un titular de tarjeta con dicho privilegio a estar siempre dentro de una estancia (grupo de puertas) cuando otros titulares de tarjetas están dentro. El usuario Custodia debe ser el primero en entrar en la sala. Sólo podrán entrar otros titulares de tarjetas si hay un responsable en la estancia. El titular de la tarjeta con atributo de Custodia no podrá salir hasta que todas las tarjetas que no sean de responsable hayan salido de la estancia. Identifica al titular de esta tarjeta como responsable. El usuario con atributo de Custodia debe ser el primero en entrar en un grupo de puertas que requiera un titular de tarjeta de Custodia, y debe ser el último en abandonar dicho grupo de puertas.

Borrar tarjeta

Si una tarjeta de acceso ya no se necesita, se puede borrar mediante el teclado.

1. Desplácese a BORRAR TARJETA.
2. Pulse SELECC.

Reset tarjeta

Si la función de «Evitar retorno» está activada en una estancia y un usuario sale de dicha estancia sin utilizar el lector de tarjetas, no se le permitirá volver a entrar en esa estancia. La tarjeta del usuario se puede resetear para permitirle volver a presentar su tarjeta una vez sin necesidad de comprobación de retorno.

Para resetear la tarjeta mediante el teclado:

1. Desplácese a RESET TARJETA.
2. Pulse SELECC.

16.19.3 Borrar

Para borrar usuarios del sistema:

1. Desplácese a USUARIOS > BORRAR.
2. Pulse SELECC.

   Se muestra una ventana para confirmar la orden de eliminar.
3. Pulse SÍ para borrar al usuario.

16.20 Perfiles de usuario

Consulte también

Añadir/Editar perfiles de usuario en la página 212

16.20.1 Agregar

Para añadir perfiles de usuario al sistema:

El creador debe tener un perfil de usuario de tipo MAESTRO.

1. Desplácese a PERF. USUARIOS > AÑADIR.

   Se muestra la opción NUEVO NOMBRE. Pulse SELECC.

2. Introduzca un nombre de perfil de usuario personalizado y pulse INTRO.

   El teclado confirma que se ha creado el nuevo perfil de usuario.

16.20.2 Editar

Para editar perfiles de usuario en el sistema:

1. Desplácese a PERF. USUARIOS > EDITAR.
2. Pulse SELECC.
3. Edite la configuración de perfil de usuario deseada que se muestra en la siguiente tabla.

CAMBIAR NOMBRE	Edite el nombre del perfil si es necesario.
CAMBIAR PARTICIONES	Seleccione las particiones relevantes para este perfil.
CALENDARIO	Seleccione un calendario configurado o NINGUNO.
DERECHO	Habilita o deshabilita características del sistema para este perfil. Consulte *Derechos de usuario* en la página 213.
Puerta	Seleccione el tipo de acceso disponible para este perfil para las puertas configuradas. Las opciones son NINGUNA, SIN LÍMITE o CALENDARIO.
CÓDIGO LUGAR	Introduzca un código de lugar para todas las tarjetas que utilicen este perfil.

16.20.3 Borrar

Para borrar perfiles de usuario del sistema:

1. Desplácese a PERF. USUARIOS > BORRAR.
2. Desplácese por los perfiles de usuario hasta llegar al perfil requerido.
3. Pulse SELECC.

   Se le solicitará que confirme el borrado.
4. Pulse SELECC para borrar el perfil de usuario.

16.21 Envío SMS

El sistema SPC admite la comunicación de alertas por SMS desde la central al técnico y a teléfonos móviles de usuarios selectos (Incidencias SMS), además de permitir a los usuarios controlar el sistema SPC de forma remota a través de SMS (Control SMS). Estas dos funciones están relacionadas entre sí, pues permiten al usuario responder a una notificación por SMS sin necesidad de encontrarse físicamente en las instalaciones.

Se puede configurar un máximo de 32 (SPC4xxx), 50 (SPC5xxx) o 100 (SPC6xxx) ID de SMS para cada central. Para habilitar las comunicaciones por SMS se requiere un módem con SMS habilitado, así como un sistema y una configuración de usuarios adecuados.

Dependiendo del modo de AUTENTICACIÓN SMS seleccionado (consulte *Opciones* en la página 126), la autenticación de usuario por SMS se puede configurar para usar diferentes combinaciones del código PIN e ID llamada del usuario, o el código PIN de SMS y código PIN de llamada.

La notificación por SMS puede funcionar con un módem RTB si el operador de RTB admite SMS a través de RTB, mientras que para el control por SMS se necesita un módem GSM en la central. Un módem GSM admite tanto notificación como control por SMS.

Control SMS

El control por SMS se puede configurar de manera que un usuario remoto pueda enviar un mensaje SMS para realizar las siguientes acciones en la central:

- Armado/desarmado
- Habilitar/deshabilitar técnico
- Habilitar/deshabilitar acceso de fabricante
- Salida de usuario on/off.

Incidenc.SMS

La notificación por SMS se puede configurar para enviar un rango de incidencias que ocurran en el sistema, como por ejemplo:

- Alarmas
- Alarm.confirmd.
- Fallos y tampers
- Armado y desarmado
- Inhibición y aislamiento
- Todos los demás tipos de incidencias

16.21.1 Agregar

Para añadir un usuario

Prerrequisitos

- Hay un módem instalado e identificado por el sistema.
- La función **Autenticación SMS** está activada en OPCIONES (consulte *Opciones* en la página 126).

1. Desplácese hasta SMS > AÑADIR y pulse SELECC.
2. Seleccione un usuario para añadir a la función SMS.
3. Introduzca un NÚMERO DE SMS para este usuario y pulse INTRO.
4. Introduzca un PIN SMS para este usuario y pulse INTRO.

   El teclado indica que los detalles de SMS se han actualizado.

16.21.2 Editar

Prerrequisitos

- Hay un módem instalado e identificado por el sistema.
- La función **Autenticación SMS** está activada en OPCIONES (consulte *Opciones* en la página 126).

1. Desplácese hasta SMS > EDITAR y pulse SELECC.
2. Seleccione un ID SMS de técnico o de usuario para editar.

NÚMERO DE SMS	Introduzca el número al que se enviarán los SMS (requiere un prefijo de código de país de tres dígitos). **Nota:** El número de SMS del técnico se puede borrar reseteándolo a 0. Los números de SMS de los usuarios no se pueden borrar.
EDITAR USUARIO	Seleccione un nuevo usuario para este ID de SMS si es necesario.
FILTRO DE INCIDENCIAS	Seleccione las incidencias de la central que el usuario o el técnico recibirán a través de SMS. Seleccione HABILITADO o DESHABILITADO. Las incidencias que están habilitadas se indican con un * antes de la incidencia en la lista.
DERECHOS CONTROL	Seleccione las operaciones que el usuario o el técnico podrán realizar de forma remota en la central a través de SMS. Consulte *Comandos de SMS* en la página 218

AVISO: Las incidencias de alarma de ATRACO no se transmiten por SMS.

Si la línea telefónica está conectada a la red RTB a través de un PBX, debe insertarse el dígito de acceso a la línea adecuado antes del número de la parte a la que se llama. Asegúrese de que **I**dentidad de **L**ínea **L**lamante (CLI) esté activada en la línea seleccionada para realizar llamadas a la red SMS. Consulte al administrador de PBX para obtener más información.

16.21.3 Borrar

1. Desplácese hasta SMS > BORRAR.
2. Desplácese al ID de SMS requerido.
3. Pulse SELECC.

   El teclado indica que la información de SMS se ha actualizado.

16.22 X-10

A la fecha de la versión 3.4, X-10 se encuentra en servicio. Esta funcionalidad se mantiene en el producto para conservar la compatibilidad retroactiva.

X-10 es una tecnología que permite al sistema controlar dispositivos periféricos, tales como luces o equipos, y las incidencias del sistema pueden utilizarse para disparar salidas en los dispositivos X-10. El controlador SPC ofrece un puerto serie dedicado (puerto serie 1) para conectarse directamente con un equipo X-10 estándar.

1. Desplácese hasta X-10 y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

HABILITAR X-10	Para habilitar o deshabilitar la funcionalidad X-10 en el sistema.
DISPOSITIVOS	Para añadir, editar, eliminar o comprobar dispositivos X-10.
REGISTRO	Para habilitar o deshabilitar el registro de X-10.

16.23 Configurar fecha/hora

La fecha y la hora se pueden introducir manualmente en el sistema. La información de hora y fecha se muestra en el teclado y en el explorador, y se utiliza en funciones de programación relacionadas con el tiempo.

1. Desplácese a la opción FECHA Y HORA y pulse SELECC.

   La fecha aparecerá en la línea superior de la pantalla.
2. Para introducir una fecha nueva, pulse las teclas numéricas correspondientes. Para mover el cursor a la izquierda y a la derecha, pulse las teclas de flecha a la izquierda y a la derecha.
3. Pulse SELECC. para guardar la nueva fecha.

   Si se intenta guardar un valor de fecha incorrecto, aparecerá el texto VALOR NO VÁLIDO durante un segundo y se solicitará al usuario que introduzca una fecha válida.
4. Para introducir una nueva hora, pulse las teclas numéricas correspondientes. Para mover el cursor a la izquierda y a la derecha, pulse las teclas de flecha a la izquierda y a la derecha.
5. Pulse SELECC. para guardar la nueva hora.

   Si se intenta guardar un valor de hora incorrecto, aparecerá el texto VALOR NO VÁLIDO durante un segundo y se solicitará al usuario que introduzca una hora válida.

16.24 Texto del instalador

Esta configuración le permite al técnico introducir información del sistema e información de contacto del técnico.

1. Desplácese hasta TEXTO DEL INSTALADOR y pulse SELECC.
2. Desplácese hasta la opción de programación deseada:

NOMBRE DEL SISTEMA	Se utiliza para ayudar a identificar el sistema. Utilice un nombre claro y descriptivo para la instalación.
ID DEL SISTEMA	Se utiliza para identificar la instalación cuando está conectado a una estación central (máx. 10 dígitos).
NOMBRE DEL INSTALADOR	Se utiliza para fines de contacto.
TELÉFONO DEL INSTALADOR	Se utiliza para fines de contacto.
MOSTRAR INSTALADOR	Configuración para mostrar los detalles del instalador en estado de reposo.

Los detalles de contacto del instalador programados en estas opciones del menú también deben introducirse en la etiqueta del teclado al finalizar la instalación.

16.25 Control de puertas

Esta opción le permite controlar todas las puertas del sistema.

1. Desplácese a CONTROL PUERTA y pulse SELECC.
2. Seleccione la puerta que desee controlar y pulse SELECC.

3. Seleccione uno de los estados de la puerta listados a continuación como nuevo estado de puerta y pulse SELECC.

Normal	La puerta está en modo de funcionamiento normal. Se necesita una tarjeta con los correspondientes atributos de acceso para abrir la puerta.
Temporizada	La puerta se abre para permitir el acceso solo durante un intervalo temporizado.
Bloqueado	La puerta está bloqueada. La puerta permanece cerrada aunque se presente una tarjeta con los correspondientes atributos de acceso.
Desbloqueada	La puerta está desbloqueada.

16.26 SPC Connect

Añada un ATS SPC Connect para configurar una conexión entre una central y el sitio web de SPC Connect https://www.spcconnect.com. Esto le permite a un usuario de una central registrar y acceder a su central de forma remota a través del sitio web de SPC Connect. Si no se habilita la opción SPC Connect durante la secuencia del asistente de inicio, puede utilizar este menú para añadir el ATS SPC Connect. Si se habilitó la opción SPC Connect durante el inicio, este menú muestra el ID de registro de la central.

AÑADIR	Si se deshabilitó la opción SPC Connect durante el asistente de inicio, aparecerá el menú AÑADIR. Seleccione AÑADIR para crear un ATS SPC Connect. Esto le permite a un usuario de una central registrar y acceder a su central de forma remota a través del sitio web de SPC Connect: https://www.spcconnect.com.
ID DE REGISTRO	Si se habilitó la opción SPC CONNECT durante el asistente de inicio, aparecerá el ID de registro de la central. Brinde esta información a un usuario final para permitirle registrar su central en el sitio web de SPC Connect, https://www.spcconnect.com, y acceder de forma remota a la central.
ID EMPRESA	Para uso futuro.
BORRAR	Para eliminar un ATS SPC Connect de una central, seleccione BORRAR.

17 Programación de técnico a través del navegador

Se puede acceder a las opciones de programación de técnico en la central SPC a través de cualquier navegador web estándar de un PC, con el acceso protegido por un código PIN.

Para acceder a la programación del técnico a través del navegador, introduzca el código de técnico por defecto (1111). Para obtener más información, consulte *Código PIN de técnico* en la página 117.

Este servidor web proporciona acceso al conjunto completo de funciones de programación que se utilizan para instalar y configurar el sistema SPC.

Esta opción de programación sólo se debe proporcionar a instaladores autorizados del sistema SPC.

Las funciones de programación en modo técnico en el sistema SPC se dividen en las siguientes categorías:

Funciones de modo técnico normal

Es posible programar estas funciones sin que sea necesario desactivar el sistema de alarma. Se puede acceder a las funciones directamente al ingresar al modo técnico.

Funciones de modo técnico completo

Estas funciones requieren que se desactive el sistema de alarma antes de que comience la programación. Podrá acceder a estas funciones dentro del menú Técnico completo.

AVISO: Si la opción 'Salida de modo técnico' está habilitada en las opciones del sistema, el técnico puede salir del modo técnico completo con las alertas activas, pero debe aceptar todas las alertas que se listan en el teclado o en el navegador antes de cambiar de modo técnico completo a modo técnico normal.

Se puede acceder al servidor web del controlador SPC a través de la interfaz USB o de Ethernet.

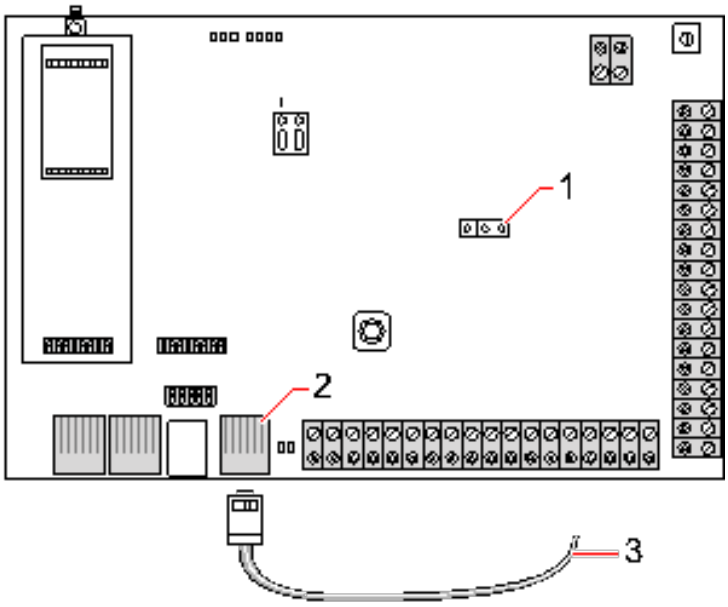
Si se está programando con una interfaz de navegador, haga clic en **Salvar** cuando se realicen cambios.
Haga clic en **Actualizar** para ver los valores de programación actuales en una página web.

17.1 Información del sistema

Haga clic en el icono **?** para ver el menú Ayuda, el cual proporciona información actualizada sobre la central y la funcionalidad autorizada actualmente en el sistema.

17.2 Interfaz Ethernet

IP



Connect (conectar)

Número	Descripción
1	JP9 SPC4xxx
2	Puerto Ethernet
3	A puerto Ethernet en el PC

Si la interfaz Ethernet del SPC está conectada a una red de área local (LAN) existente, consulte con el administrador de red de dicha LAN antes de conectarse a la central. Dirección IP por defecto: 192.168.1.100.

Conectar el cable

- Conecte un cable Ethernet desde la interfaz Ethernet en el PC al puerto Ethernet en la placa del controlador
  – O BIEN –
  Si está realizando la conexión directamente desde un PC, debe utilizar un cable cruzado. Consulte *Conexiones de cable de red* en la página 375.

  Las luces LED a la derecha de la interfaz Ethernet indican una conexión de datos exitosa (luz LED derecha encendida) y el tráfico de datos de Ethernet (luz LED izquierda parpadeante).

Determinar la dirección IP del controlador SPC

1. Acceda al modo técnico (consulte *Código PIN de técnico* en la página 117).
2. Con las flechas ARRIBA y ABAJO, desplácese hasta la opción COMUNICACIÓN y pulse SELECC.
3. Desplácese hasta PUERTO ETHERNET y pulse SELECC.
4. Desplácese hasta DIRECCIÓN IP y pulse SELECC.

17.3 Conexión a la central a través de USB

Si se resetea la central con el cable USB conectado, deberá desenchufar el cable y volverlo a enchufarlo.

El puerto USB del controlador se conecta a un PC a través de un USB estándar tipo A o un cable tipo B. Deben instalarse controladores para establecer una conexión USB desde el controlador al PC.

Prerrequisitos

- Su PC debe estar conectado con la central a través de un cable USB.

1. Conecte el cable USB del controlador a una interfaz USB del PC.

   Aparecerá el asistente **Nuevo hardware encontrado**.
2. Haga clic en **Next (siguiente)**.

   Windows XP detecta una unidad USB genérica.
3. Haga clic en **Finalizar**.

   Windows XP detecta la central SPC – Sistema Avanzado de Seguridad en el puerto COM N, siendo N el número del puerto COM asignado al dispositivo.
4. Anote el puerto COM asignado al dispositivo; lo necesitará más adelante.

   Vuelve a aparecer el asistente de **Nuevo hardware encontrado**.
5. Seleccione **Instalar el software automáticamente**.
6. Si el asistente de instalación de unidad de Windows XP le pide que seleccione la opción que mejor se ajuste de una lista, elija la siguiente opción:

   Conexión local USB a la SPC Vanderbilt Intrunet
7. Haga clic en **Next (siguiente)**.

   Aparecerá un cuadro de diálogo respecto de la certificación de Windows. Vanderbilt considera que es aceptable para continuar. Si tiene más dudas, póngase en contacto con el administrador de la red o con un técnico de Vanderbilt.
8. Haga clic en **Continuar de todos modos**.

   La instalación finaliza.
9. Haga clic en **Finalizar**.

   El controlador está instalado.

Configuración de la conexión en Windows XP

Configure la nueva conexión en el PC:

1. Haga clic en **Inicio**.
2. Seleccione **Conectar a > Mostrar todas las conexiones > Crear una conexión nueva**.
3. En el asistente para nueva conexión, seleccione **Configurar una conexión avanzada**.
4. Seleccione las Opciones de conexión avanzadas, **Conectar directamente a otro equipo**.
5. Seleccione **Invitado** como rol para este PC.
6. Introduzca un nombre para la conexión.
7. Seleccione un puerto de serie disponible para su uso con la conexión. Este debe corresponderse con el puerto COM que está utilizando el dispositivo USB.
8. Seleccione si esta conexión estará disponible para todos los usuarios o solo para usted.

9. En el último cuadro de diálogo del asistente, haga clic en **Finalizar**.
10. El PC solicitará un nombre de usuario y clave para la conexión USB. Introduzca la siguiente información:

    - Nombre de usuario SPC

    - Clave: password (por defecto)
11. Haga clic en **Conectar**.

    El PC inicia un enlace de datos con el controlador. Cuando establece el enlace, aparece un icono de conexión en la barra de tareas en la parte inferior de la pantalla del PC.
12. Haga clic con el botón derecho y seleccione **Estado**.

    Aparecerá la dirección IP del servidor en la ventana de información.
13. Introduzca esta dirección en la barra de direcciones de un navegador de Internet con el protocolo de transferencia de hipertexto seguro (por ejemplo: https://192.168.5.1).
14. Inicie sesión en la aplicación de navegador del SPC con su código de usuario.

Debe cambiar inmediatamente y anotar su código por defecto. Si olvida su código, la única solución es volver a la configuración predeterminada de fábrica del sistema, reseteando toda la configuración del sistema. La configuración se puede recuperar si hay una copia de seguridad disponible.

Windows 7

Prerrequisitos

- Debe contar con derechos de Administrador Local para ejecutar las acciones de esta tarea.

1. Abra el Panel de Control de Windows 7.
2. Seleccione **Teléfono y módem**.

   Se abrirá la página **Teléfono y módem**.
3. Seleccione la pestaña **Módems** y haga clic en **Añadir**.

   Se abrirá la página **Asistente para agregar hardware - Instalar nuevo módem**.
4. Haga clic en **Siguiente** dos veces.

   El asistente de **Agregar nuevo hardware** muestra una lista de módems.
5. Seleccione **Cable de comunicación entre dos ordenadores**.
6. Haga clic en **Next (siguiente)**.
7. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.
8. Vuelva a la pestaña **Módems** en la página **Teléfono y módem**.
9. Seleccione el nuevo módem y haga clic en **Propiedades**.

   Se abrirá la página **Cable de comunicaciones entre dos ordenadores - Propiedades**.
10. En la pestaña **General**, haga clic en **Cambiar configuración** para que se puedan editar las propiedades.
11. Seleccione la pestaña **Módem**.
12. Modifique el valor de **Velocidad máxima del puerto** a **115200** y haga clic en **Aceptar**.
13. En el **Panel de control**, abra **Centro de redes y recursos compartidos**.
14. Haga clic en **Modificar configuración del adaptador**. Si hay un nuevo módem en la lista de conexiones disponibles, continúe con el paso 22. Si el módem *no* está presente, continúe con los siguientes pasos.

15. En el **Centro de redes y recursos compartidos**, haga clic en **Configurar una nueva conexión o red**.
16. Seleccione **Configurar una conexión de acceso telefónico** y haga clic en **Siguiente**.
17. Introduzca los valores que desee en los campos **Número de teléfono**, **Nombre de usuario** y **Clave**, e indique un nombre en el campo **Nombre de conexión**.
18. Haga clic en **Conectar**.

    Windows 7 crea la conexión.
19. Sáltese el proceso de **Comprobación de la conexión a Internet**.
20. Haga clic en **Cerrar**.
21. En el **Centro de redes y recursos compartidos**, haga clic en **Cambiar configuración del adaptador**.
22. Haga doble clic en el nuevo módem.

    Se abre la página **Conectar *NombreDeConexión***, siendo *NombreDeConexión* el nombre que usted ha definido para el módem.
23. Haga clic en **Propiedades**.
24. Compruebe que el campo **Conectarse mediante**: contiene la información correcta, por ejemplo, Cable de comunicación entre dos ordenadores (COM3).
25. Abra su navegador e introduzca la dirección IP del controlador, con https como protocolo de conexión.
26. Si el navegador muestra una página de error de certificado, haga clic en **Continuar de todos modos**.
27. Inicie sesión en la central.

17.4 Inicio de sesión en el navegador

Para iniciar sesión en el navegador:

1. Cuando se haya establecido el enlace Ethernet o USB y se haya determinado la dirección IP del controlador, abra el navegador del PC.
2. Introduzca la dirección IP en la barra de direcciones del navegador con el protocolo de transferencia de hipertexto seguro. (Por ejemplo: https:// 192.168.1.100.) Consulte la tabla en *Configuración por defecto para la dirección del servidor WEB* en la página siguiente.

   Se mostrará una página con un mensaje de seguridad.
3. Haga clic en **Continuar a este sitio web**.

   Aparecerá la página de inicio de sesión.

4. Introduzca la siguiente información:

   - **ID de usuario**: Nombre de usuario o de técnico

   - **Clave**: Código PIN de usuario o de técnico.

5. Seleccione el idioma en el que desea visualizar las páginas del navegador. Con la configuración de idioma por defecto «Autom.» se cargará automáticamente el idioma asignado a este ID de usuario.
6. Haga clic en **Iniciar sesión**.

Configuración por defecto para la dirección del servidor WEB

Conexión	Dirección IP del servidor web
Ethernet	192.168.1.100 (por defecto)
RS232	192.168.2.1 (fija)
Módem de respaldo/RS232	192.168.3.1 (fija)
Módem principal	192.168.4.1 (fija)
USB	192.168.5.1 (fija)

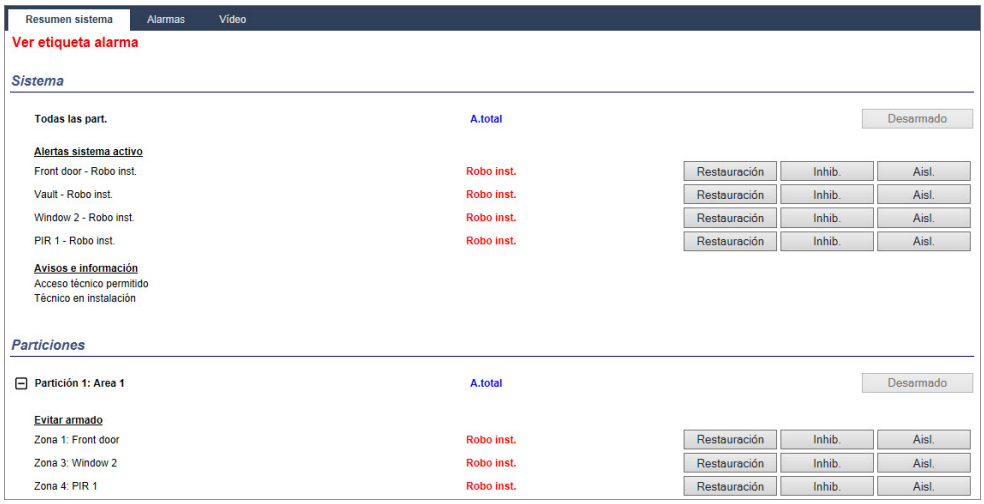
17.5 Inicio de SPC

La página de inicio de SPC tiene una pestaña **Resumen del sistema**, una pestaña **Alarmas** y una pestaña **Vídeo**.

17.5.1 Resumen sistema

La pestaña **Resumen del sistema** está dividida en estas tres secciones:

- **Sistema:** Muestra el estado de todas las particiones, las alertas del sistema activas, las advertencias y la información del sistema.
- **Particiones:** Muestra el estado de cada partición definida en el sistema con un máximo de 20 incidencias de alarma. Puede armar o desarmar una partición, y el estado de la partición se mostrará aquí.
- **Inhibiciones y aislamientos:** Muestra una lista de todas las zonas aisladas y le permite restaurar o inhibir antes de armar.



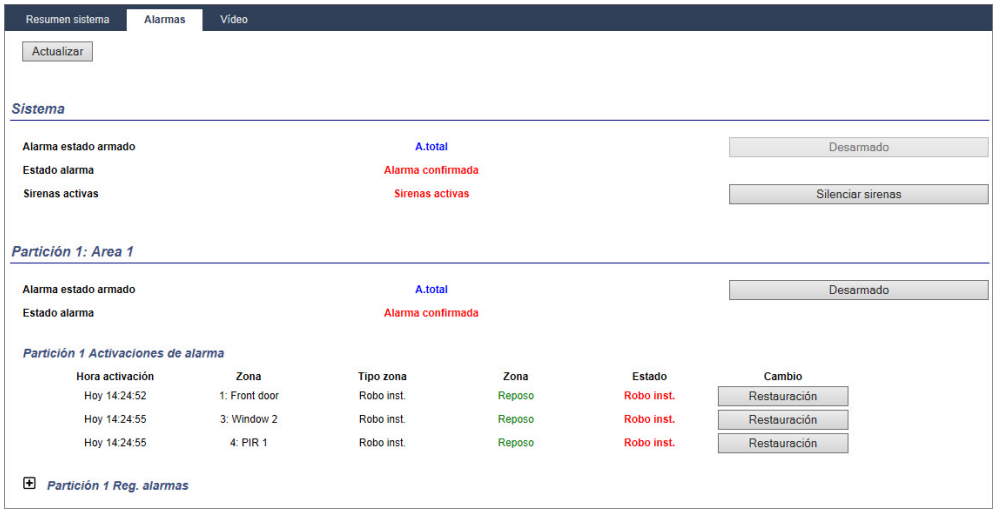
AVISO: Si hay alarmas en el sistema, se muestra el mensaje de información **Ver alarma**.

17.5.2 Descripción general de alarmas

En la pestaña **Alarmas** se mostrará la siguiente información:

- **Estado armado de alarma:** Muestra si el sistema estaba parcialmente o totalmente armado al momento de la activación de la alarma.
- **Estado de alarma:** Muestra el tipo de alarma (alarma, alarma confirmada, etc.)
- **Sirenas activas:** Muestra si la alarma activó las sirenas. Haga clic en el botón **Silenciar sirenas** para cancelar.

Para cada partición, se muestra **Estado de armado de alarma**, **Estado de alarma**, **Activaciones de alarma** y **Registro de alarma**. **Activaciones de alarma** muestra una lista de las zonas en estado de alarma ordenadas por activación. Haga clic en el botón **Restaurar** para borrar. El **Registro de alarma** muestra hasta 20 incidencias.

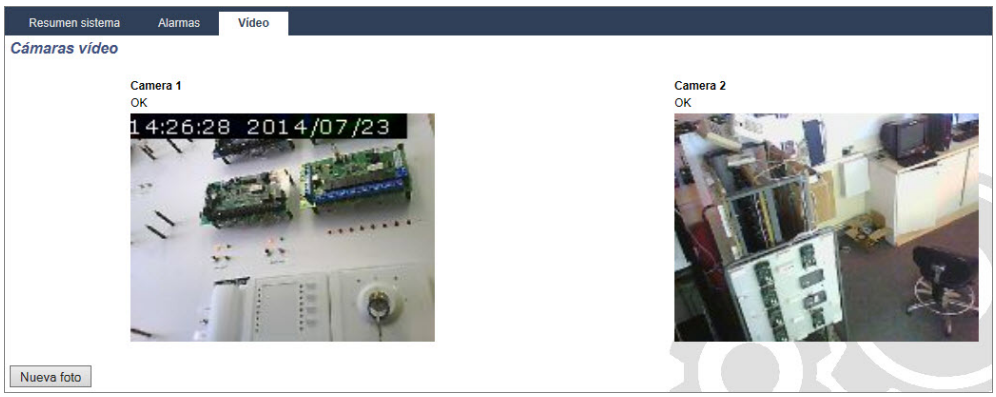


17.5.3 Ver vídeo

La pestaña **Vídeo** muestra imágenes de hasta 4 cámaras IP.

- En modo técnico completo, técnico normal y usuario, seleccione **SPC General > Vídeo**.

  Todas las cámaras configuradas y operativas (hasta 4 máx.) se muestra en la página **Cámaras de vídeo**. Solo dos cámaras están disponibles en el ejemplo a continuación.



Las imágenes se actualizan automáticamente según la configuración del intervalo de la cámara. (Consulte *Configurar vídeo* en la página 298.)

Haga clic en el botón **Pausar actualización** para mantener la imagen actual en pantalla y pausar la actualización. Haga clic en el botón **Reiniciar actualización** para permitir que la central actualice las imágenes.

Nota: Asegúrese de que la resolución seleccionada sea de 320 x 240 para las cámaras que se mostrarán en el navegador. De lo contrario, es posible que las imágenes no se visualicen correctamente. Se puede utilizar la resolución más alta de 640 x 480 para el funcionamiento con SPC Com.

Transmisión de fallo de vídeo

Encima de la imagen de la cámara se muestra un informe de fallo de vídeo. En la siguiente tabla se muestra una lista de los posibles mensajes:

Mensaje	Descripción
OK	La cámara se está comportando normalmente
Timeout	Ha terminado el tiempo de conexión de la cámara
Socket no válido	Error de manipulación de ranura interna
Imagen demasiado pequeña	Imagen recibida demasiado pequeña
Búfer demasiado pequeño	La imagen recibida es demasiado grande. Baje la resolución en la configuración de la cámara.
Formato incorrecto	Formato recibido no válido.
Abortar	Conexión TCP desconectada
Interna	La central de alarmas no tiene memoria suficiente para completar la petición.
Petición incorrecta	Se ha enviado a la cámara una petición mal formulada. Compruebe los ajustes de configuración de su cámara.
Error del cliente	La cámara ha notificado un error del cliente. Compruebe la configuración de su cámara.

Mensaje	Descripción
Error de autorización	El nombre de usuario y/o la contraseña son incorrectos.
Desconocido	Se ha notificado un error desconocido. Puede que el modelo de la cámara no sea compatible.

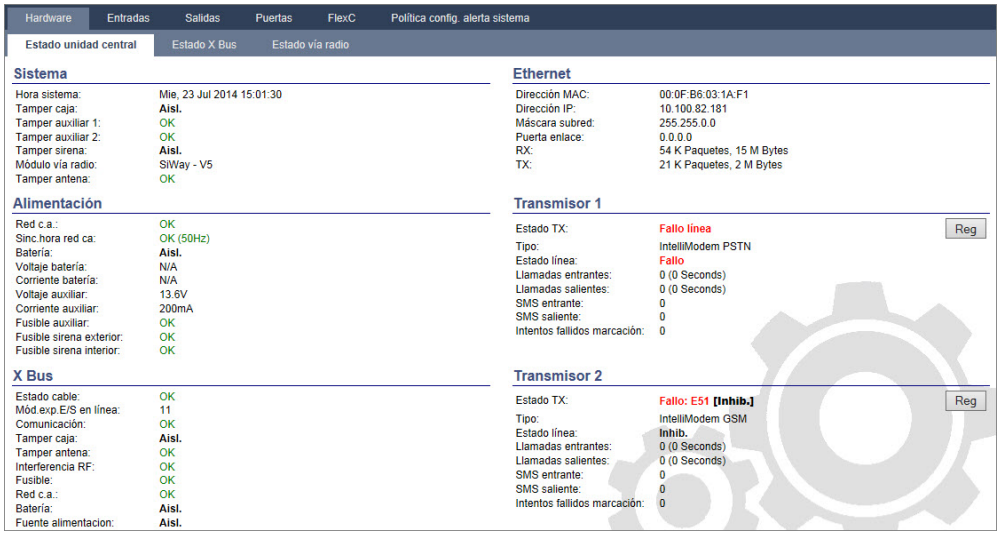
17.6 Estado de la central

Esta sección abarca:

17.6.1 Estado

Esta página muestra el estado y un resumen de los principales componentes de SPC, incluyendo el sistema, alimentación, X-BUS y comunicaciones.

1. Seleccione **Estado > Hardware > Estado del controlador**.
2. Consulte las secciones a continuación para obtener más información.



Acciones ejecutables

Las siguientes acciones solo son posibles si se ha establecido una conexión.

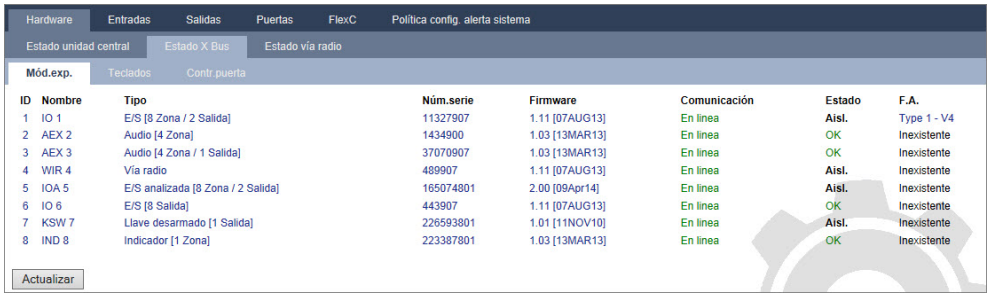
Restaurar todas las alertas	Restaura todas las alertas activas en la central. Estos mensajes de alerta se muestran en texto en rojo frente al elemento pertinente.
Refresh	Actualiza los cambios en el estado de la central. Debe actualizar la página de estado para mostrar el estado de la central en un momento en particular.

Técnico completo/Técnico normal	Para alternar entre los modos técnico completo y técnico normal. El modo de técnico completo deshabilita las alarmas y evita que se informen las incidencias a la estación central.

17.6.2 Estado de X-BUS

1. Seleccione **Estado > Hardware > Estado X-Bus**.

   Se muestra la siguiente página con el estado de los diferentes dispositivos X-Bus. Todos los módulos de expansión detectados aparecen listados por defecto.



ID	Nombre	Tipo	Núm.serie	Firmware	Comunicación	Estado	F.A.
1	IO 1	E/S [8 Zona / 2 Salida]	11327907	1.11 [07AUG13]	En línea	Aisl.	Type 1 - V4
2	AEX 2	Audio [4 Zona]	1434900	1.03 [13MAR13]	En línea	OK	Inexistente
3	AEX 3	Audio [4 Zona / 1 Salida]	37070907	1.03 [13MAR13]	En línea	OK	Inexistente
4	WIR 4	Vía radio	489907	1.11 [07AUG13]	En línea	Aisl.	Inexistente
5	IOA 5	E/S analizada [8 Zona / 2 Salida]	165074801	2.00 [09Apr14]	En línea	Aisl.	Inexistente
6	IO 6	E/S [8 Salida]	443907	1.11 [07AUG13]	En línea	OK	Inexistente
7	KSW 7	Llave desarmado [1 Salida]	226593801	1.01 [11NOV10]	En línea	Aisl.	Inexistente
8	IND 8	Indicador [1 Zona]	223387801	1.03 [13MAR13]	En línea	OK	Inexistente

2. Seleccione una de las siguientes pestañas:

   - Módulos de expansión (para programar módulos de expansión, consulte *Módulos de expansión* en la página 235).

   - Teclados (para programar teclados, consulte *Teclados* en la página 240).

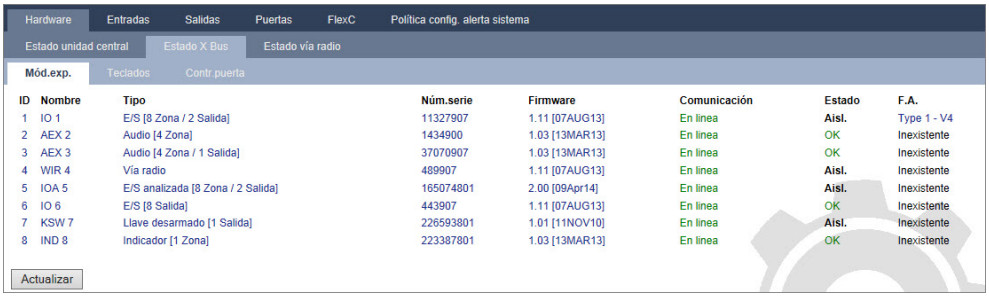
   - Controladores de puerta (para programar controladores de puerta, consulte *Controladores de puertas* en la página 245).

3. Haga clic en cualquiera de los parámetros de identificación del teclado / módulo de expansión / controlador de puerta (ID, descripción, tipo, número de serie) para ver más detalles sobre su estado.

17.6.2.1 Estado del módulo de expansión

1. Seleccione **Estado > Hardware > Estado X-Bus**.
2. Seleccione la pestaña **Módulos de expansión**.

   Se muestra una lista de módulos de expansión detectados y fuentes de alimentación asociadas.



ID	Nombre	Tipo	Núm.serie	Firmware	Comunicación	Estado	F.A.
1	IO 1	E/S [8 Zona / 2 Salida]	11327907	1.11 [07AUG13]	En línea	Aisl.	Type 1 - V4
2	AEX 2	Audio [4 Zona]	1434900	1.03 [13MAR13]	En línea	OK	Inexistente
3	AEX 3	Audio [4 Zona / 1 Salida]	37070907	1.03 [13MAR13]	En línea	OK	Inexistente
4	WIR 4	Vía radio	489907	1.11 [07AUG13]	En línea	Aisl.	Inexistente
5	IOA 5	E/S analizada [8 Zona / 2 Salida]	165074801	2.00 [09Apr14]	En línea	Aisl.	Inexistente
6	IO 6	E/S [8 Salida]	443907	1.11 [07AUG13]	En línea	OK	Inexistente
7	KSW 7	Llave desarmado [1 Salida]	226593801	1.01 [11NOV10]	En línea	Aisl.	Inexistente
8	IND 8	Indicador [1 Zona]	223387801	1.03 [13MAR13]	En línea	OK	Inexistente

ID mód. expansión	Este número de ID es un identificador único para el módulo de expansión.
Descripción	Descripción del módulo de expansión. Este texto aparecerá en el navegador y el teclado.
Tipo	El tipo de módulo de expansión detectado (E/S, F.A., teclado, etc.).
Núm.serie	El número de serie del módulo de expansión.
Versión	La versión de firmware del módulo de expansión.

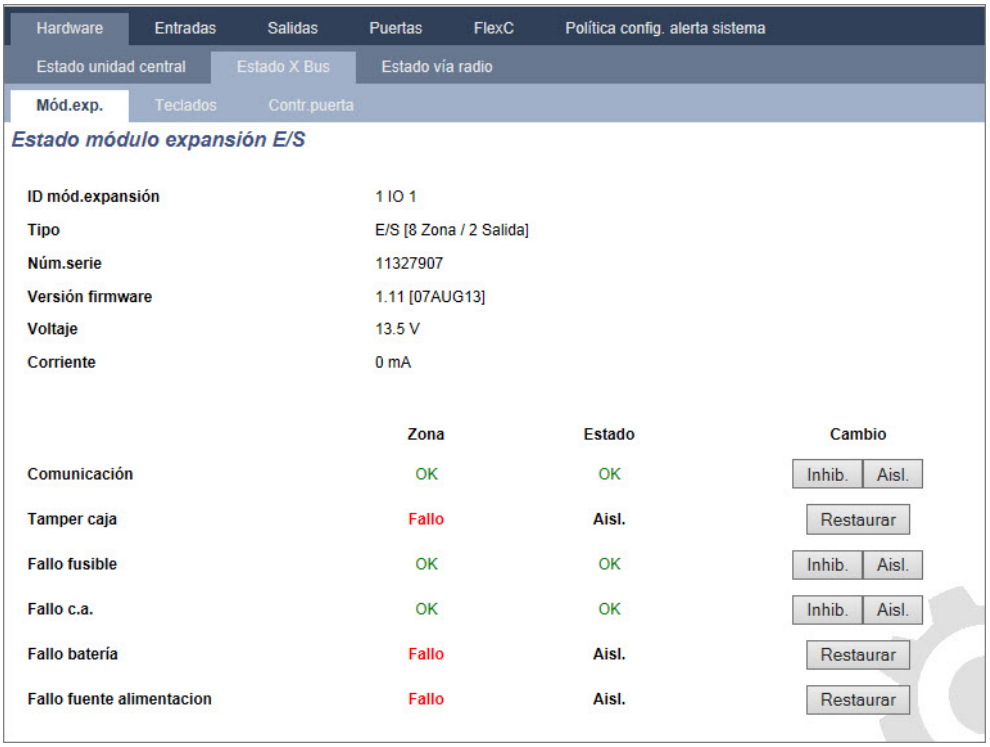
Comunicación	El estado del módulo de expansión (en línea o fuera de línea).
Estado	El estado del módulo de expansión (OK, Fallo, Ab, Tamper).
F.alimentación	El tipo de fuente de alimentación conectada al módulo de expansión, si procede. Haga clic en la fuente de alimentación para ver su estado.

Acciones ejecutables

Refresh	Haga clic en el botón para actualizar el estado del X-BUS.

Para ver más información de estado:

- Haga clic en cualquiera de los parámetros de identificación del módulo de expansión (ID, descripción, tipo, número de serie) para ver más detalles sobre su estado.



Nombre	Descripción
Comunicación	El estado físico (OK, Fallo) y el estado programado (OK, Aislado, Inhibido) de la conexión del cable del X-BUS al módulo de expansión.
Tamper de carcasa	El estado físico y programado del tamper de carcasa del módulo de expansión.
Fallo fusible	El estado físico y programado del fusible del módulo de expansión.
Red CA central	El estado físico y programado de la alimentación eléctrica al controlador.
Fallo batería	El estado físico y programado de la batería
Fallo fuente alimentación	El estado físico y programado de la fuente de alimentación.
Ab Tamper	El estado físico y programado de las salidas de tamper en la fuente de alimentación.
Bajo voltaje	Indicación del estado de bajo voltaje de la batería.

Acciones ejecutables

Nombre	Descripción
Restaurar alertas	Haga clic en el botón para restaurar todas las alertas en la central.
Inhibir ⓘ	Haga clic en este botón para inhibir una condición de fallo. La operación de anulación deshabilitará dicho fallo o zona sólo durante un periodo de armado. La operación de anulación no está disponible en el grado de seguridad EN 50131 Grado 3.
Aislar	Haga clic en este botón para aislar esa zona. Al aislar una zona, ésta se desactiva hasta que transcurre el tiempo necesario para que la zona se vuelva a restaurar explícitamente. Es aconsejable actuar con cautela al aislar zonas, ya que dichas zonas no estarán activas siempre que el sistema esté ARMADO.

Consulte también

Estado de la fuente de alimentación abajo

17.6.2.2 Estado de la fuente de alimentación

La página **Estado de la fuente de alimentación** muestra detalles sobre el estado actual de la fuente de alimentación y sus salidas, además de sobre el estado de cualquiera de las baterías conectadas.

Son compatibles los siguientes tipos de fuentes de alimentación:

- Fuente de alimentación inteligente SPCP332/333
- Fuente de alimentación inteligente SPCP355.300

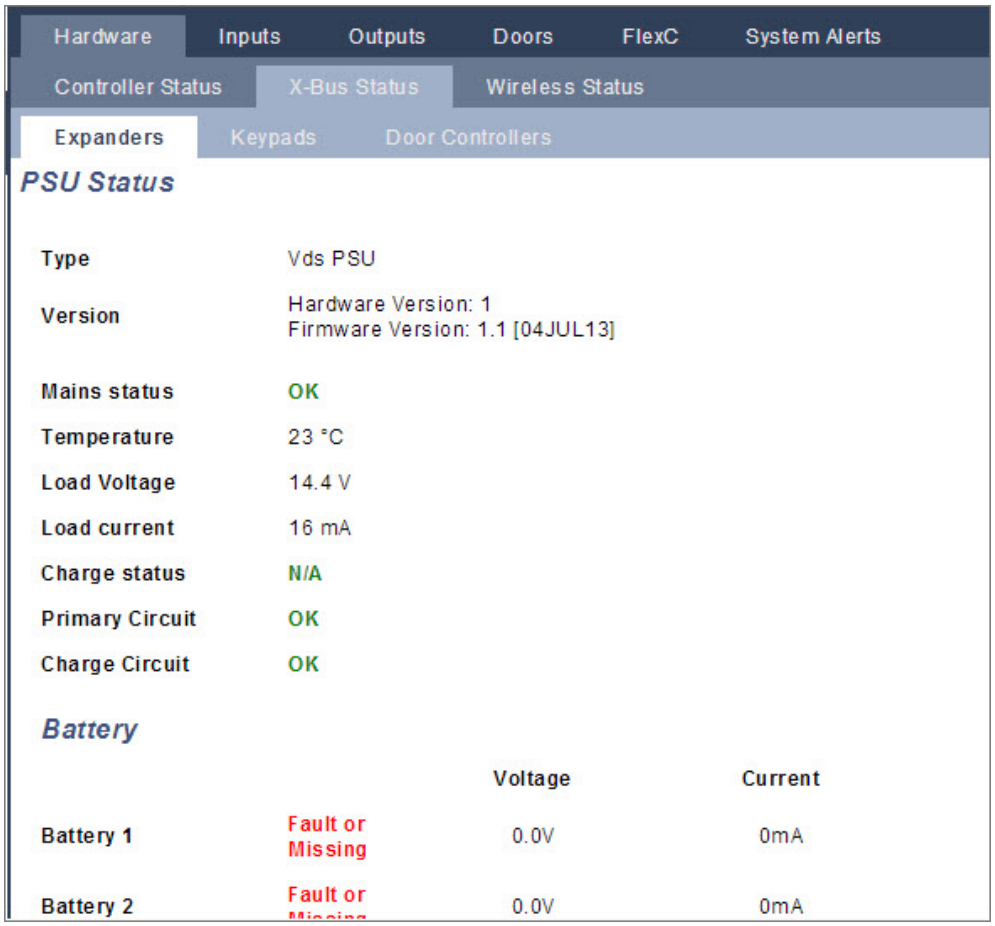
Estado de fuente de alimentación inteligente SPCP332/333

En la siguiente imagen se muestra el estado de la fuente de alimentación inteligente:

Nombre	Descripción
Tipo	El tipo de fuente de alimentación.
Versión	La versión de la fuente de alimentación.
Estado red de c.a.	Se muestra el estado de la conexión de C.A. Los posibles valores son Fallo y OK.
Enlace batería	Se muestra el tipo de batería conectada.
Estado batería	Se muestra el estado de la conexión de la batería. Los posibles valores son Fallo y OK.
Voltaje batería	Se muestra la lectura de voltaje de la batería.
Corriente de batería	Se muestra la corriente obtenida de la batería.
Salida	Se muestra el voltaje en las salidas, la corriente absorbida por la salida y el estado del fusible en la salida.

Estado de la fuente de alimentación inteligente SPCP355.300

En la siguiente imagen se muestra el estado de la fuente de alimentación inteligente SPCP355.300.



Nombre	Descripción
Tipo	El tipo de fuente de alimentación.
Versión	La versión de la fuente de alimentación.

Nombre	Descripción
Estado red de c.a.	Se muestra el estado de la conexión de C.A. Los posibles valores son Fallo y OK.
Temperatura	Se muestra la temperatura de la fuente de alimentación.
Voltaje de carga	El voltaje en la fuente de alimentación
Corriente de carga	La corriente absorbida por la fuente de alimentación.
Estado de carga	Se muestra el estado de la carga de la batería.
Circuito primario	Se muestra el estado del circuito primario que suministra energía cuando la red de C.A. está conectada.
Circuito de carga	Se muestra el estado del circuito primario que carga las baterías cuando la red de C.A. está conectada.
Batería	Se muestra el estado de carga, el voltaje y la corriente disponible de las baterías.
Salida	Se muestra el voltaje, el estado del fusible y el estado del tamper de las salidas de la fuente de alimentación.

17.6.2.3 Estado del teclado

1. Seleccione **Estado > Hardware > Estado X-Bus**.
2. Seleccione la pestaña **Teclados**.

   Se muestra una lista de teclados detectados.

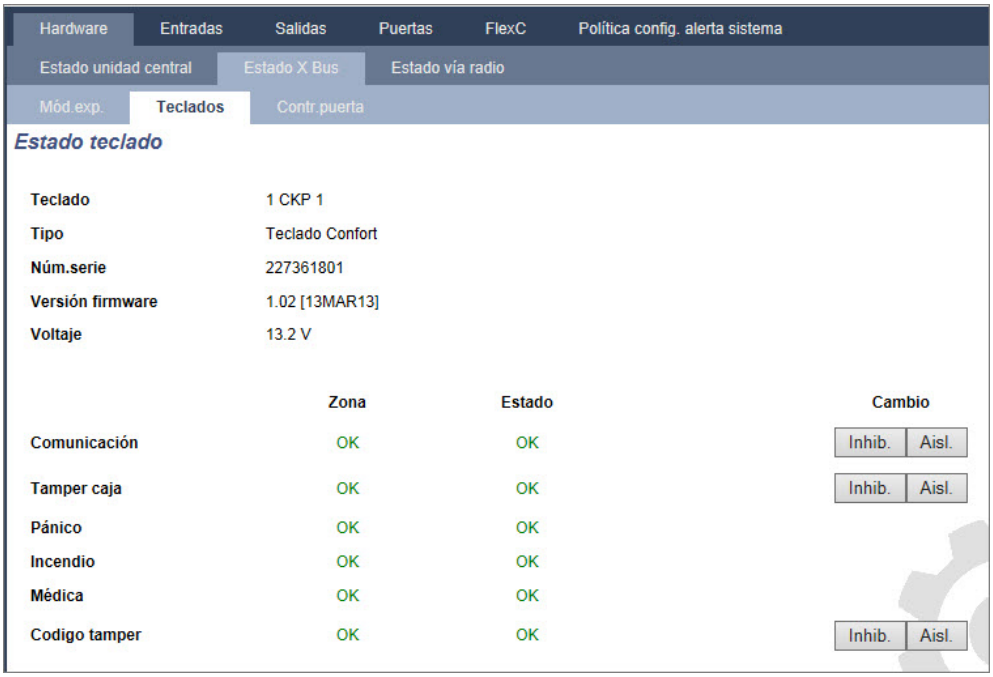
Nombre	Descripción
ID mód. expansión	Este número de ID es un identificador único para el teclado.
Descripción	El texto de la descripción del teclado (máx. 16 caracteres).
Tipo	El tipo de módulo de expansión detectado (=teclado).
Núm.serie	El número de serie del teclado.
Versión	La versión de firmware del teclado.
Comunicación	El estado del teclado (en línea o fuera de línea).
Estado	El estado del teclado (OK, Fallo).

Acciones ejecutables

Refresh	Haga clic en el botón **Actualización** para actualizar la lista de teclados detectados y su estado.

Para ver más información de estado:

- Haga clic en los parámetros de identificación de un teclado (ID, descripción, tipo, número de serie) para ver más información sobre su estado.



Comunicación	El estado físico (OK, Fallo) y el estado programado (OK, Aislado, Inhibido) de la conexión del cable del teclado al módulo de expansión.
Tamper de carcasa	El estado físico y programado del tamper de carcasa del módulo de expansión.
ACCESO TARJETA	Se aplica solo a los teclados con un receptor PACE instalado.
Pánico	Estado de alarma de pánico desde teclado.
Incendio	Estado Alarma pánico teclado.
Alarma médica	Estado de Alarma médica teclado.
Código tamper	Código teclado estado de alarma de tamper

Acciones ejecutables

Restaurar alertas	Haga clic en el botón para restaurar todas las alertas en la central.
Inhibir ⓵	Haga clic en este botón para inhibir una condición de fallo. La operación de anulación deshabilitará dicho fallo o zona sólo durante un periodo de armado. La operación de anulación no está disponible en el grado de seguridad EN 50131 Grado 3.
Aislar	Haga clic en este botón para aislar esa zona. Al aislar una zona, ésta se desactiva hasta que transcurre el tiempo necesario para que la zona se vuelva a restaurar explícitamente. Es aconsejable actuar con cautela al aislar zonas, ya que dichas zonas no estarán activas siempre que el sistema esté ARMADO.

17.6.2.4 Estado de controlador de puerta

1. Seleccione **Estado > Hardware > Estado X-Bus**.
2. Seleccione la pestaña **Controladores de puerta.**

   Se muestra una lista de los controladores de puerta detectados.

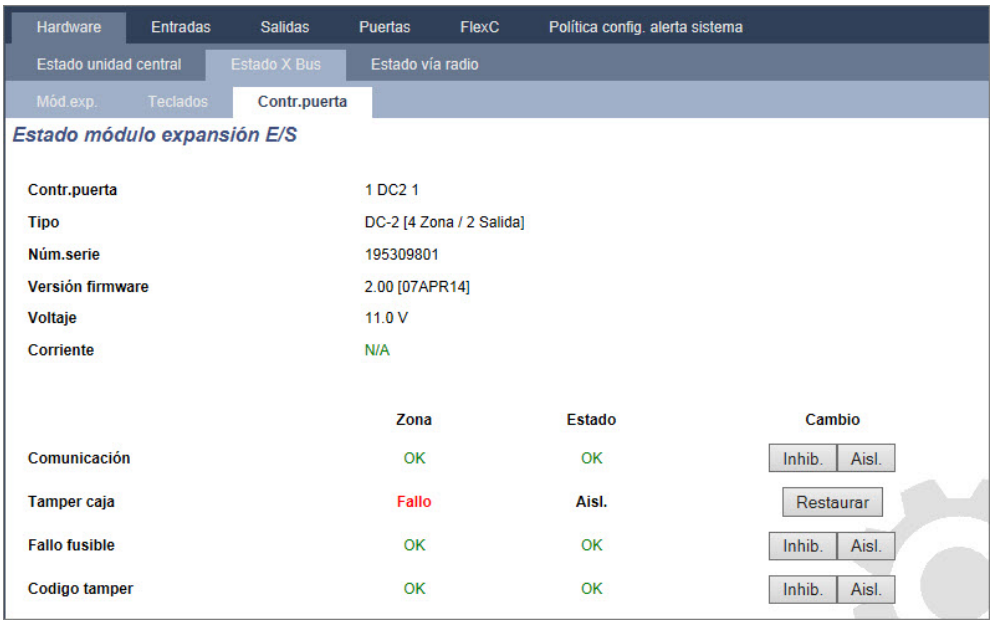
ID mód. expansión	Este número de ID es un identificador único para el controlador de puerta.
Descripción	El texto de la descripción del controlador de puerta (máx. 16 caracteres).
Tipo	El tipo de módulo de expansión detectado (=controlador de puerta).
Núm.serie	El número de serie del controlador de puerta.
Versión	La versión de firmware del controlador de puerta.
Comunicación	El estado del controlador de puerta (en línea o fuera de línea).
Estado	El estado del controlador de puerta (OK, Fallo)
F.alimentación	Especifica si el controlador de puerta tiene una fuente de alimentación.

Acciones ejecutables

Refresh	Haga clic en el botón **Actualizar** para actualizar el estado de las alertas del sistema.

Para ver más información de estado:

- Haga clic en los parámetros de identificación de un controlador de puerta (ID, descripción, tipo, número de serie) para ver más información sobre su estado.



Comunicación	El estado físico (OK, Fallo) y el estado programado (OK, Aislado, Inhibido) de la conexión del cable del teclado al módulo de expansión.

Tamper de carcasa	El estado físico y programado del tamper de carcasa del módulo de expansión.
Fallo fusible	El estado físico y programado del fusible del controlador de puerta.
Código tamper	Estado del código de usuario. Múltiples intentos fallidos provocan una incidencia.

Acciones ejecutables

Restaurar alertas	Haga clic en el botón para restaurar todas las alertas en la central.
Inhibir	Haga clic en este botón para inhibir una condición de fallo. La operación de anulación deshabilitará dicho fallo o zona sólo durante un periodo de armado. La operación de anulación no está disponible en el grado de seguridad EN 50131 Grado 3.
Aislar	Haga clic en este botón para aislar esa zona. Al aislar una zona, ésta se desactiva hasta que transcurre el tiempo necesario para que la zona se vuelva a restaurar explícitamente. Es aconsejable actuar con cautela al aislar zonas, ya que dichas zonas no estarán activas siempre que el sistema esté ARMADO.

17.6.3 Vía radio

La detección con sensores vía radio (868 MHz) en la central PSC se realiza mediante módulos receptores vía radio que pueden venir montados de fábrica en el teclado o el controlador, o instalando un módulo de expansión vía radio.

1. Seleccione **Configuración > Hardware > Vía radio > Vía radio**.

2. Consulte la tabla a continuación para obtener más información.

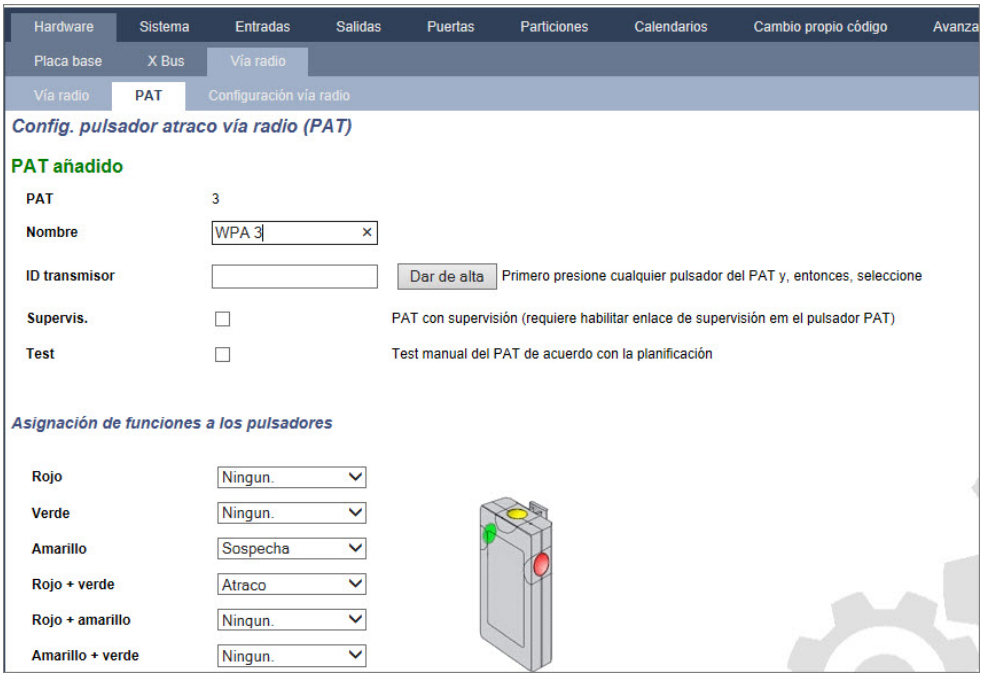
Sensor	El número del sensor registrado en el sistema (1 = primero; 2 = segundo; etc.).
ID	Un número de identidad único para ese sensor.
Tipo	El tipo de sensor vía radio detectado (contacto magnético, inercial/shock, etc.).
Zona	La zona a la cual ha sido dado de alta el sensor.
Batería	El estado de la batería conectada al sensor (si aplica).
Supervisar	El estado de la operación de supervisión (OK = señal de supervisión recibida; Sin supervisión = sin operación de supervisión).

Señal	La intensidad de la señal recibida desde el detector (01=baja, 09=alta). **Nota:** Aunque no es posible dar de alta un dispositivo con una intensidad de señal inferior a 3, los dispositivos cuya señal cae por debajo de 3 después de su registro no se anulan.

Acciones ejecutables

Registro	Haga clic para ver el Registro de sensor vía radio. *Registro - Sensor vía radio X* abajo.
Dar de alta	Haga clic para abrir la lista de dispositivos vía radio sin estar dados de alta.

1. Seleccione **Configuración > Hardware > Vía radio > APR**.
2. Se muestran la identidad de cada APR registrada y el estado.



17.6.3.1 Registro - Sensor vía radio X

Para ver un registro rápido de las incidencias para un sensor vía radio:

1. Haga clic en el botón **Registro**.
2. Consulte la tabla a continuación para obtener más información.

Fecha/Hora	La fecha y la hora de la incidencia registrada.
Receptor	La ubicación del receptor vía radio, es decir, el módulo vía radio montado en el teclado, controlador o módulo de expansión vía radio.
Señal	La intensidad de la señal recibida desde el detector (01=baja, 09=alta).
Estado	El estado físico del detector.
Batería	El estado de la batería conectada al sensor (OK, Fallo).

3. Cree un archivo de texto del registro haciendo clic en **Archivo de texto**.

17.6.4 Zonas

Para ver la configuración, consulte *Editar una zona* en la página 274.

1. Para ver todas las zonas, seleccione **Estado > Entradas > Todas las zonas**. Para ver solamente las zonas que solo son X-BUS, seleccione la pestaña **Zonas X Bus**, y para ver las zonas que solo son vía radio, seleccione la pestaña **Zonas vía radio**.

2. Consulte la tabla a continuación para obtener más información.

Actualización automática de estado	Marque este botón para activar la actualización automática del resumen de zona. Solo puede hacer esto para todas las zonas y no para zonas de filtro.
Descripción de zona	El texto de la descripción de la zona (máx. 16 caracteres).
Particiones	Particiones a las que será asignada esta zona.
Tipo de zona	El tipo de zona (alarma, entrada/salida, etc.).
RFL	Muestra la calidad de RFL para el rango de resistencia del estado de zona. Estos son los valores posibles: • Buena: valor nominal +/-25% del rango definido. • OK: valor nominal +/- 50% del rango definido. • Pobre: valor nominal +/- 75% del rango definido. • No satisfactoria: cualquier otro valor. • Ruidosa: indica un problema de detección de la señal. El cableado puede que esté próximo a un cable de alimentación u otra fuente de interferencia. Esta columna solo está visible en modo Técnico. Para más información sobre valores de resistencia nominal y sus rangos definidos, véase *Cableado de entradas de zona* en la página 91.

Entrada	El estado de entrada detectado de esa zona (Desconocido, Abierto, Cerrado, Desconectado, Corto, Impulso, Det. vibración, Enmascarado, Fallo, Fuera de límites, Inestable, Sustitución c.c., Ruidoso). Sustitución c.c. es una alerta de tamper de entrada. Sustitución c.c. realiza una comprobación periódica para garantizar que no se aplican voltajes externos a ese circuito. Inestable: Se detecta un estado inestable cuando el valor de resistencia de entrada de zona no es estable a lo largo de un período de muestreo definido. Ruidoso: Se detecta un estado ruidoso cuando se induce una interferencia externa en el circuito de entrada a lo largo de un período de muestreo definido. Fuera de límites: Se detecta un estado de fuera de límites cuando el valor de resistencia en la entrada de zona no se encuentra dentro de las tolerancias aceptadas de los valores RFL vigentes.
Estado	El estado programado de esa zona. Un valor de estado de Normal significa que la zona está programada para funcionar con normalidad. A continuación se muestra una lista de los valores posibles: Aislar, Probar, Inhibir, Tamper, Alarma, Salida incendio, Fallo aviso, Fallo atraco, Fallo detector, Fallo línea, Pánico, Atraco, Técnica, Médica, Bloqueo, Incendio, Problema, Enmascaramiento PIR, Normal, Accionado, Tamper, Post-alarma. Una zona se encuentra en un estado de post-alarma si se produjo una alarma y finalizó el tiempo de espera de alarma confirmada. Esto restablece la zona, pero indica que se produjo una alarma.

Acciones ejecutables

Refresh	Actualiza la información de estado que se muestra para la central.
Registro	Haga clic en el botón **Registro** para ver un registro del estado de entrada de esa zona.
Inhibir ⓵	Haga clic en este botón para inhibir un fallo o una zona abierta. La operación de anulación deshabilitará dicho fallo o zona sólo durante un periodo de armado. La operación de anulación no está disponible en el grado de seguridad EN 50131 Grado 3.
Restaurar	Haga clic en este botón para restaurar la condición de alarma de la central.
Aislar	Zona. Al aislar una zona, esta se desactivará hasta que transcurra el tiempo necesario para que la zona se restaure nuevamente de forma explícita. Es aconsejable actuar con cautela al aislar zonas, ya que dichas zonas no estarán activas siempre que el sistema esté ARMADO.
Pruebas	Seleccione una zona y haga clic sobre este botón para realizar una prueba en esa zona.
Test sísmico	Haga clic en este botón para iniciar una comprobación del detector sísmico seleccionado. Para más información sobre detectores sísmicos, véase *Sensores sísmicos* en la página 367.
Ocultar cerrado	Haga clic en este botón para ocultar todas las entradas cerradas.
Filtrado estado zonas	Seleccione un tipo de zona dl menú desplegable. Solo se mostrará el resumen de este tipo de zona.

17.6.5 en puertas

1. Seleccione **Estado > Puertas**.

2. Consulte la tabla a continuación para obtener más información.

Puerta	Este número de ID es un identificador único para la puerta.
Zona	El número de zona al cual el sensor de posición de puerta está acoplado (solo si la entrada del sensor de posición de puerta también se utiliza como zona de intrusión).
Particiones	La partición a la cual están asignados la entrada del sensor de posición de puerta y el lector de tarjetas.
DPS	Estado de sensor de posición de puerta.
DRS	Estado de interruptor de liberación de puerta.
Estado	El estado de la puerta (OK, Fallo).
Modo de puerta	Especifica el modo de funcionamiento de la puerta.

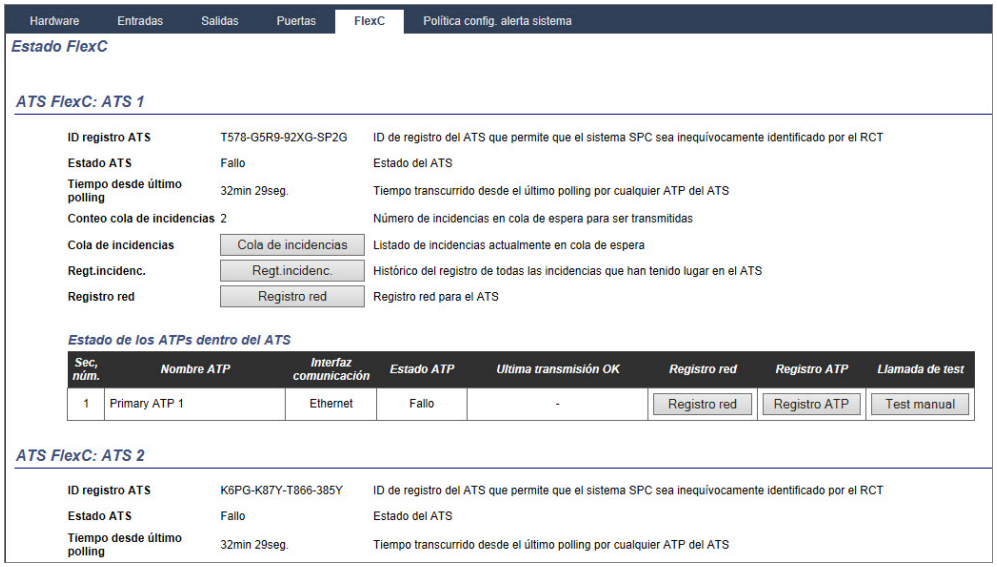
Acciones ejecutables

Refresh	Actualiza el resumen de puerta.
Registro	Muestra un registro de las incidencias para la puerta seleccionada.
Bloquear	Bloquea la puerta seleccionada.
Desbloquear	Desbloquea la puerta seleccionada.
Normal	Hace que el control del sistema de la puerta vuelva a ser normal.
Moment.	Desbloquea la puerta durante un intervalo de tiempo.

17.6.6 Estado ATS y ATP de FlexC

Esta página muestra el estado de cada uno de los ATS configurados en el sistema.

1. Para ver el estado de un ATS, acceda a **Estado > FlexC**.



2. La tabla a continuación muestra los criterios de estado disponibles para cada ATS.

ID de registro de ATS	El ID de registro único del ATS identifica inequívocamente a la central en el RCT.
Estado del ATS	El estado del ATS, por ejemplo, inicializando.
Tiempo desde último polling	Tiempo transcurrido desde el último polling por cualquier ATP en el ATS.
Cantidad de incidencias en cola	Número de incidencias en la cola de incidencias esperando a ser transmitidas.
Cantidad de incidencias en cola	N.º de incidencias en la cola de incidencias esperando a ser transmitidas.
Cola de incidencias	Listado de incidencias actualmente en la cola de incidencias. La tabla muestra lo siguiente: • N.º en secuencia de incidencias • Fecha y hora • Descripción de incidencia • Información adicional de la incidencia • Fecha/hora inicio • Informar duración

Regt.incidenc.	Historial del registro de todas las incidencias que han tenido lugar en el ATS. La tabla muestra los mismos campos que la cola de incidencias mencionada anteriormente y el siguiente campo adicional: • N.º en secuencia de incidencias • Fecha y hora • Descripción de incidencia • Información adicional de la incidencia • Resultado • ATP informada • Fecha/hora inicio • Fecha/hora recon./fallo • Informar duración
Registro de red	Registro de red para el ATS que muestra el intervalo de polling configurado.
Estado de ATP dentro del ATS	Esta tabla muestra cada ATP en el ATS. Para cada ATP, la tabla muestra el número de secuencia de la ATP, el nombre de la ATP, la interfaz de comunicaciones, el estado de la ATP, la última transmisión exitosa, el registro de red, el registro de la ATP y el botón de la llamada de test. **Registro de red:** Haga clic en el botón para mostrar el registro de red. **Registro de ATP:** Muestra una lista de las transmisiones de polling. Haga clic en el botón **Actualizar** para actualizar el registro. Haga clic en el botón **Ultimo el más reciente** para cambiar el orden de visualización. Por defecto, se muestra primero la incidencia más reciente. Botón **Test manual**: Haga clic en este botón para forzar una llamada de test. La incidencia se añade a la cola de incidencias.

17.6.7 Alertas del sistema

1. Seleccione **Estado > Alertas del sistema**.

2. Consulte la tabla a continuación para obtener más información.

Alerta	Descripción de la alerta del sistema.

Entrada	El estado real de la alerta que se detectó en la central (OK, Fallo).
Estado	El estado programado de la alerta del sistema, es decir, si se aisló o se inhibió la alerta. El valor de estado OK se muestra si no se deshabilitó la condición de alerta.

Acciones ejecutables

Refresh	Haga clic en este botón para actualizar el estado de las alertas del sistema.
Restaurar	Haga clic en este botón para restaurar una alerta en la central.
Inhibir	Haga clic en este botón para inhibir una condición de fallo. La operación de anulación deshabilitará dicho fallo o zona sólo durante un periodo de armado. La operación de inhibición no está disponible en el grado seguridad EN 50131 Grado 3.
Aislar	Haga clic en este botón para aislar la zona. Al aislar una zona, ésta se desactiva hasta que transcurre el tiempo necesario para que la zona se vuelva a restaurar explícitamente. Es aconsejable actuar con cautela al aislar zonas, ya que dichas zonas no estarán activas siempre que el sistema esté ARMADO.

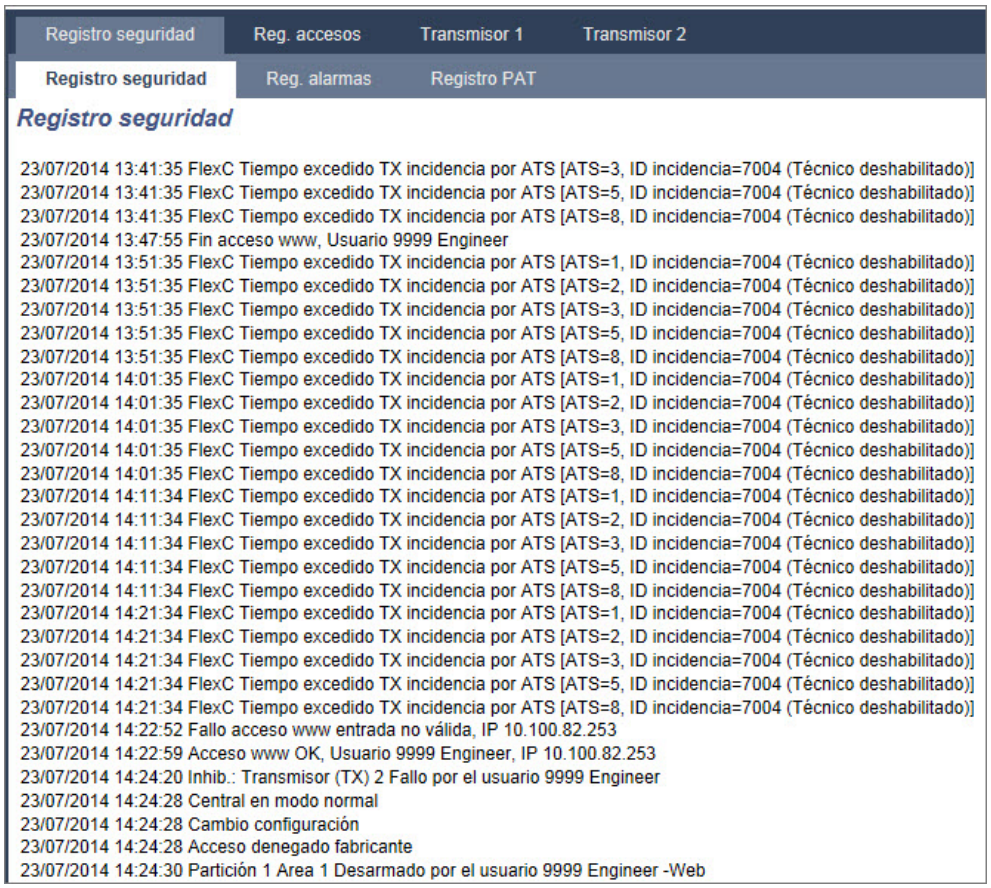
17.7 Registros

Esta sección abarca:

17.7.1 Registro del sistema

Este registro muestra todas las incidencias del sistema SPC.

1. Seleccione **Registro > Registro del sistema > Registro del sistema**.
2. Cree un archivo de texto del registro haciendo clic en **Archivo de texto**.
3. El registro de los cambios de estado de una zona individual se habilita configurando el atributo de registro para dicha zona en la página de configuración de atributos de zona.



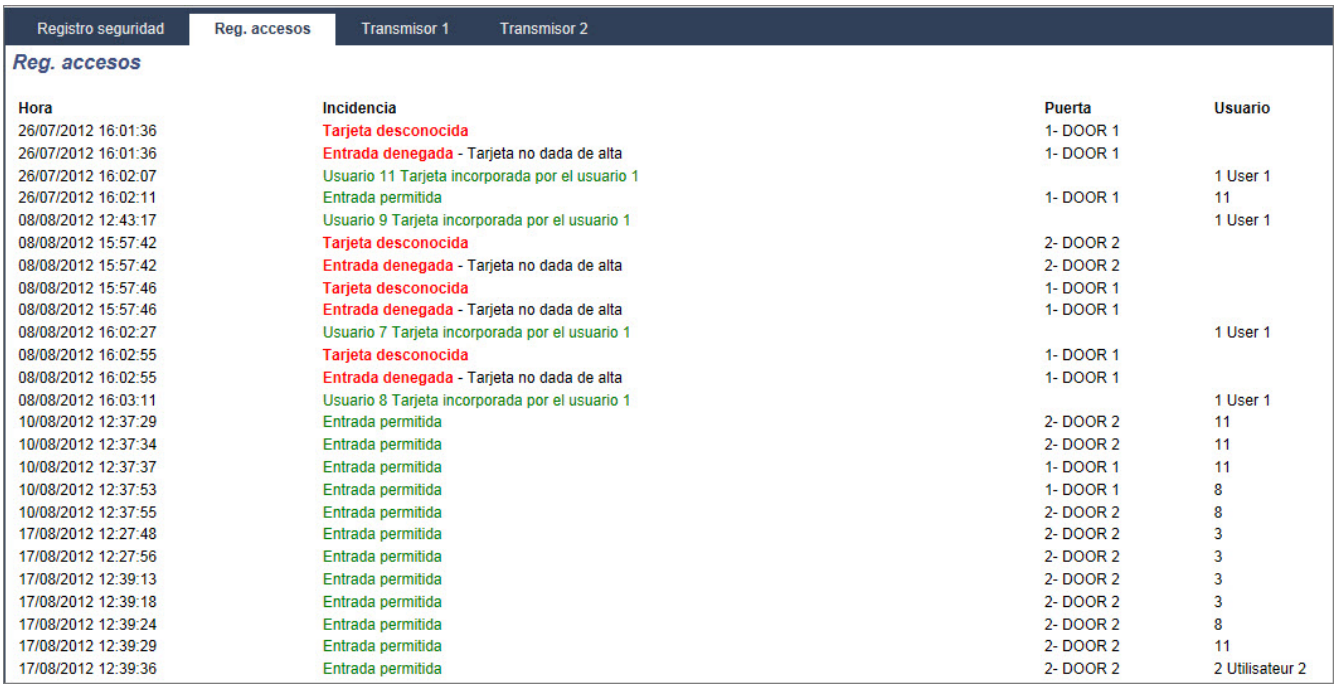
Con el fin de evitar que varias incidencias de una misma fuente llenen el registro, el sistema SPC, según los estándares, sólo permite el registro de 3 activaciones de la misma zona en un período establecido.

17.7.2 Registro de control de accesos

El registro recoge todas las incidencias de acceso del sistema SPC.

- Seleccione **Registro > Registro acceso**.

  Se mostrará la siguiente página:



Hora	Incidencia	Puerta	Usuario
26/07/2012 16:01:36	Tarjeta desconocida	1- DOOR 1	
26/07/2012 16:01:36	Entrada denegada - Tarjeta no dada de alta	1- DOOR 1	
26/07/2012 16:02:07	Usuario 11 Tarjeta incorporada por el usuario 1		1 User 1
26/07/2012 16:02:11	Entrada permitida	1- DOOR 1	11
08/08/2012 12:43:17	Usuario 9 Tarjeta incorporada por el usuario 1		1 User 1
08/08/2012 15:57:42	Tarjeta desconocida	2- DOOR 2	
08/08/2012 15:57:42	Entrada denegada - Tarjeta no dada de alta	2- DOOR 2	
08/08/2012 15:57:46	Tarjeta desconocida	1- DOOR 1	
08/08/2012 15:57:46	Entrada denegada - Tarjeta no dada de alta	1- DOOR 1	
08/08/2012 16:02:27	Usuario 7 Tarjeta incorporada por el usuario 1		1 User 1
08/08/2012 16:02:55	Tarjeta desconocida	1- DOOR 1	
08/08/2012 16:02:55	Entrada denegada - Tarjeta no dada de alta	1- DOOR 1	
08/08/2012 16:03:11	Usuario 8 Tarjeta incorporada por el usuario 1		1 User 1
10/08/2012 12:37:29	Entrada permitida	2- DOOR 2	11
10/08/2012 12:37:34	Entrada permitida	2- DOOR 2	11
10/08/2012 12:37:37	Entrada permitida	1- DOOR 1	11
10/08/2012 12:37:53	Entrada permitida	1- DOOR 1	8
10/08/2012 12:37:55	Entrada permitida	2- DOOR 2	8
17/08/2012 12:27:48	Entrada permitida	2- DOOR 2	3
17/08/2012 12:27:56	Entrada permitida	2- DOOR 2	3
17/08/2012 12:39:13	Entrada permitida	2- DOOR 2	3
17/08/2012 12:39:18	Entrada permitida	2- DOOR 2	3
17/08/2012 12:39:24	Entrada permitida	2- DOOR 2	8
17/08/2012 12:39:29	Entrada permitida	2- DOOR 2	11
17/08/2012 12:39:36	Entrada permitida	2- DOOR 2	2 Utilisateur 2

- Cree un archivo de texto del registro haciendo clic en el botón **Archivo de texto**.

17.7.3 Registro APR

Este registro muestra todas las incidencias de APR en el sistema.

- Seleccione **Registro > Registro del sistema > Registro de APR**.

  Se mostrará la siguiente página:

17.7.4 REGISTRO ALARMAS

El registro de alarmas muestra una lista de las incidencias de alarma.

- Seleccione **Registro > Registro del sistema > Registro de alarmas**.

En este registro se muestran los siguientes tipos:

- Zonas
  – Alarma
  – Pánico
- Incidencias del sistema
  – Alarma confirmada
  – Coacción de usuario

– Pánico X-Bus
– Pánico usuario
– Pánico RPA

17.8 Usuarios

La siguiente tabla muestra el número máximo de usuarios, los perfiles de usuario y los dispositivos de usuarios para la central:

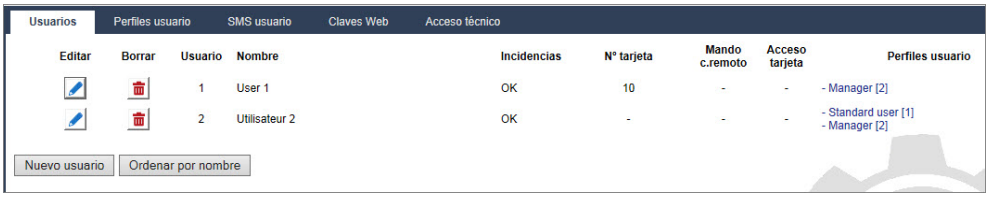
N.º máximo	SPC4xxx	SPC5xxx	SPC6xxx
Usuarios	100	500	2500
Perfiles de usuario	100	100	100
Perfiles de usuario por usuario	5	5	5
Dispositivos PACE	32	250	250
ID SMS	32	50	100
Claves web	32	50	100
Mandos vía radio	32	50	100
Dispositivos HCD	32	32	32

ADVERTENCIA: Si se actualiza desde una versión de firmware anterior a la 3.3, tenga en cuenta lo siguiente:
- La clave web del técnico, si estaba configurada, se borra, por lo que debe volver a introducirse tras la actualización.
- Todos los usuarios existentes se asignarán a perfiles de usuario nuevos correspondientes a sus niveles de acceso de usuario previos. Si se sobrepasa el número máximo de perfiles de usuarios, no se asignará ningún perfil (consulte *Añadir/Editar perfiles de usuario* en la página 212). Revise toda la configuración de usuario tras actualizar el firmware.
- El ID de técnico por defecto cambia de 513 a 9999.

17.8.1 Añadir/Editar un usuario

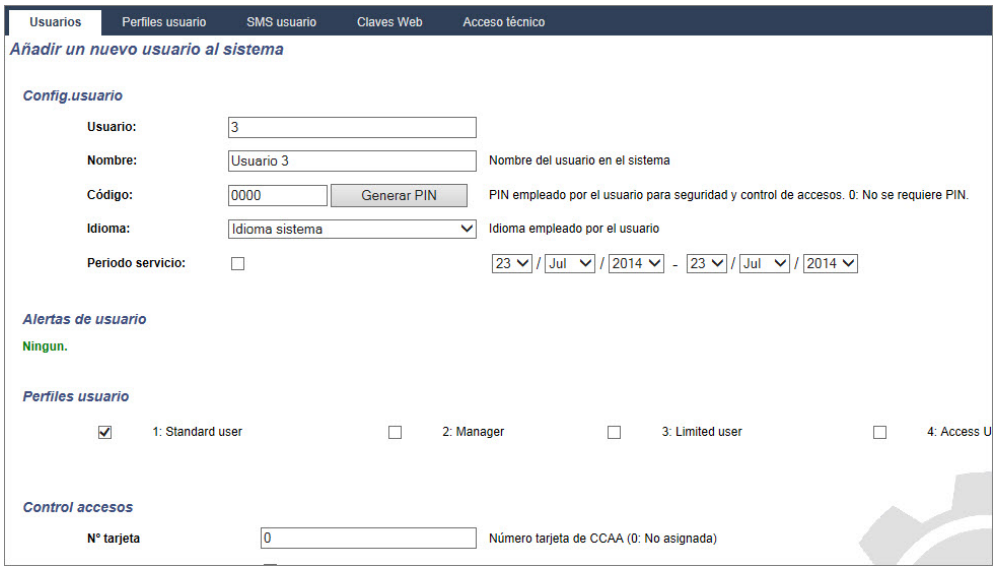
1. Seleccione **Usuarios > Usuarios**.

   Se muestra una lista de usuarios configurados.



2. Haga clic en el botón **Añadir usuario** o en el botón **Editar** del usuario requerido.

   Aparecerá la siguiente página.



3. Introduzca un **ID de usuario** que no se esté utilizando actualmente. Si introduce un ID que ya está en uso, aparecerá el mensaje «ID no disponible».
4. Indique un **Nombre de usuario** (máximo 16 caracteres, distingue entre mayúsculas y minúsculas).
5. Para generar automáticamente un **Código PIN de usuario** para un usuario nuevo, haga clic en el botón **Generar código PIN**. Modifique el código si es necesario. Introduzca 0 si no se requiere ningún código.

   Nota: Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.
6. También puede limitar el acceso al sistema para este usuario marcando la casilla **Periodo servicio** e introduciendo las fechas en los campos **Hasta** y **Desde**.

   En **Alertas de usuario** se muestra el estado del código de usuario. Por ejemplo, se muestra el número de días que quedan para que expire el código, si están habilitados los cambios periódicos en la Política de PIN del sistema.
7. Puede habilitar la opción **Acceso con alarma** para permitirle a este usuario acceder al sistema durante un período de tiempo específico.

   Los límites de tiempo para esta opción se establecen en la página **Temporizadores del sistema**. Vaya a **Configuración > Sistema > Temporizadores del sistema** para configurar esta opción. Consulte *Temporizaciones* en la página 266.

En modo normal, todo usuario que tenga este atributo seleccionado no podrá acceder al sistema.

8. Seleccione el perfil de usuario adecuado (consulte *Añadir/Editar perfiles de usuario* en la página 212) para este usuario.
9. Seleccione **Habilit. coacción** para este usuario si es necesario. La cantidad de códigos PIN asignados para coacción (PIN+1 o PIN+2) está configurada en las opciones del sistema (consulte *Opciones* en la página 254).

La opción **Coacción** solo está disponible en esta página si **Coacción usuario** está habilitado para el sistema en **Opciones del sistema**. Si la opción **Coacción** está habilitada para este usuario, no se permiten códigos PIN de usuario consecutivos para otros usuarios (por ejemplo: 2906, 2907), ya que introducir este PIN desde el teclado activaría una incidencia de coacción de usuario.

Control de accesos

Atributo	Descripción
Número tarjeta	Número de la tarjeta de CCAA Introduzca 0 para dejar sin asignar esta tarjeta.
Tarjeta vacía	Inhibición temporal de tarjeta
Tiempo ampliado	Ampliación de la temporización de la puerta al presentar la tarjeta.
Anulación de Código	Acceso a puerta sin PIN en una puerta con lector de PIN.
Prioridad	Las tarjetas prioritarias se almacenan localmente en los controladores de puertas y permiten el acceso en caso de fallo técnico allí donde el controlador de puerta no se puede comunicar con la central de control. El número máximo de usuarios prioritarios es: • SPC4xxx – todos los usuarios • SPC5xxx – 512 • SPC6xxx – 512
Acompañante	La función de Visita obliga a los titulares de tarjetas con este privilegio a acompañar a otros titulares de tarjetas por puertas específicas. Si esta función está habilitada en una puerta, se debe presentar primero una tarjeta con la atribución de Visita para permitir abrir la puerta a otros titulares de tarjeta sin este atributo. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con derecho de Visita; se puede configurar individualmente para cada puerta.
Custodia	La función de Custodia impone a un titular de tarjeta con dicho privilegio a estar siempre dentro de una estancia (grupo de puertas) cuando otros titulares de tarjetas están dentro. El usuario Custodia debe ser el primero en entrar en la sala. Sólo podrán entrar otros titulares de tarjetas si hay un responsable en la estancia. El titular de la tarjeta con atributo de Custodia no podrá salir hasta que todas las tarjetas que no sean de responsable hayan salido de la estancia. Identifica al titular de esta tarjeta como responsable. El usuario con atributo de Custodia debe ser el primero en entrar en un grupo de puertas que requiera un titular de tarjeta de Custodia, y debe ser el último en abandonar dicho grupo de puertas.

17.8.1.1 Dispositivos desconocidos

Si un dispositivo desconocido, como un mando, un dispositivo PACE o una tarjeta, se ha escaneado pero no se ha asignado a un usuario, se muestra un botón en la sección correspondiente de la página de usuarios.

- Botón **Mando vía radio – Mando desconocido** o, si el dispositivo está asignado al usuario, botón **Borrar mando vía radio**
- Botón **Dispositivo PACE – PACE desconocido** o, si el dispositivo está asignado al usuario, botón **Borrar PACE**
- Botón **Control de accesos – Tarjeta desconocida**

Para asignar un mando, un dispositivo PACE o una tarjeta al usuario:

1. Haga clic en el botón **Desconocido** para el dispositivo. La página Usuario muestra una lista de dispositivos desconocidos.
2. Haga clic en **Agregar** para asignar el dispositivo al usuario.

Nota: Para asignar una tarjeta al usuario, el perfil de usuario asociado debe tener definido el código de lugar correcto.

Para desasignar un mando o un dispositivo PACE de un usuario:

1. Haga clic en el botón **Borrar**.
   El dispositivo se desasigna del usuario y también se borra del sistema.
2. Para volver a añadir el dispositivo, deberá volver a escanearlo.

Para desasignar una tarjeta de un usuario:

1. Cambie el número de tarjeta a cero (0).
2. Haga clic en **Salvar**.
   La tarjeta se desasigna del usuario y también se borra del sistema.
3. Para volver a añadir la tarjeta, deberá volver a escanearla.

17.8.2 Añadir/Editar perfiles de usuario

AVISO: Los perfiles de usuario globales no se pueden editar en el navegador, sino que deben editarse en SPC Manager.

1. Seleccione **Usuarios > Perfiles usuario**.

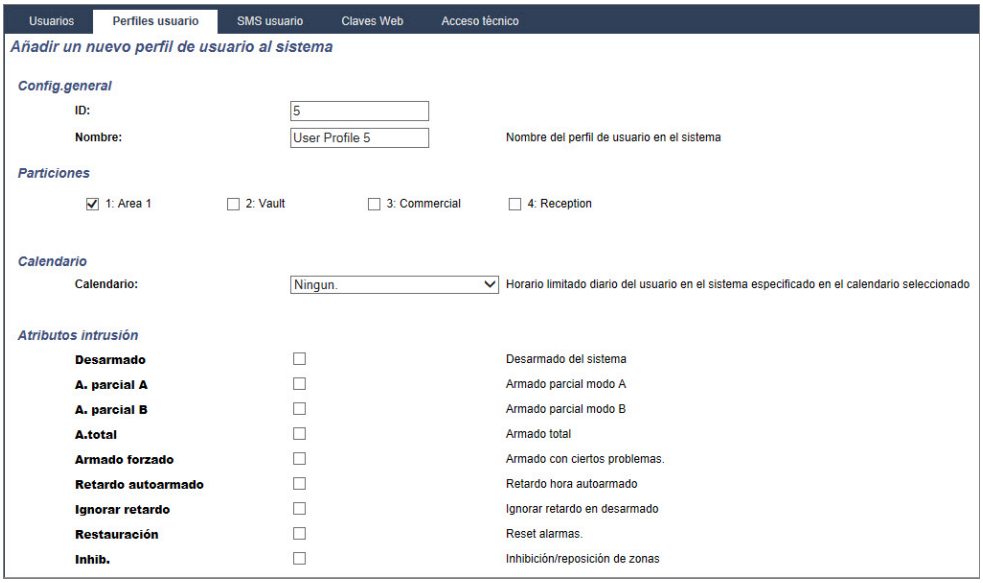
   Se muestra una lista de los perfiles configurados, con el número de usuarios asignados a cada perfil.

2. Haga clic en **Añadir perfil de usuario** o haga clic en el botón **Editar** del perfil requerido.
   Se muestra la siguiente página con las opciones de configuración categorizadas de la siguiente manera:

   - Configuración general

   - Derechos de usuario/central

- Control de accesos



Configuración general

1. Introduzca un **ID perfil de usuario** que no se esté utilizando actualmente. Si introduce un ID que ya está en uso, aparecerá el mensaje «ID no disponible».
2. Indique un **Nombre del perfil de usuario** (máximo 16 caracteres, diferenciando entre mayúsculas y minúsculas).
3. Seleccione todas las **Particiones** que serán controladas por este perfil de usuario.
4. Seleccione un **Calendario** para establecer las limitaciones temporales de este perfil en el sistema.

Derechos de usuario/central

- Seleccione los derechos de usuario requeridos que se asignarán a este perfil de usuario.

Derechos de usuario

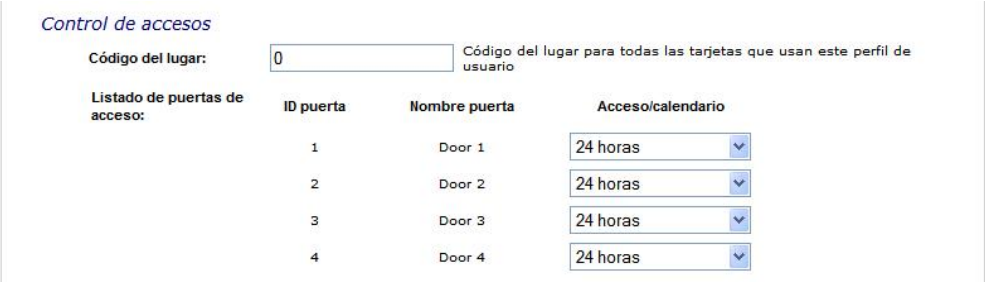
Derecho	Tipo de perfil de usuario por defecto	Descripción
Derechos de usuario: Intruso		
Armado total	Limitado Estándar Gerente	El modo ARMADO TOTAL arma completamente el sistema de alarma y proporciona protección total a un edificio (la apertura de cualquier zona de alarma activa la alarma). Al seleccionarse ARMADO TOTAL, el zumbador suena y el teclado muestra la cuenta atrás del período de tiempo de salida. Debe salir del edificio antes de que transcurra este período de tiempo. Una vez transcurrido dicho tiempo, el sistema se arma y la apertura de las zonas de entrada/salida inicia el temporizador de entrada. Si el sistema no se desarma antes de que termine el temporizador de entrada, la alarma se activa.

Derecho	Tipo de perfil de usuario por defecto	Descripción
Armado parcial A	Estándar Gerente	La opción ARMADO PARCIAL A proporciona protección al perímetro de un edificio, a la vez que permite el movimiento libre por las particiones de acceso. Las zonas clasificadas como Excl.A.Parc.A continúan sin protección en este modo. Por defecto, no existe tiempo de salida; el sistema lo establece al instante al seleccionar este modo. Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial A.
Armado parcial B	Estándar Gerente	La opción ARMADO PARCIAL B proporciona protección a todas las zonas, con excepción de aquellas clasificadas como Excl.A.Parc.B. Por defecto no existe tiempo de salida; el sistema lo establece al instante al seleccionar este modo. Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial B.
Armado forzado	Maestro estándar	La opción ARMADO FORZADO se muestra en la pantalla del teclado cuando se intenta armar el sistema y existe una zona de alarma con fallos o que permanece abierta (la línea superior de la pantalla muestra la zona abierta). Al seleccionarse esta opción, se arma la alarma y se anula la zona para ese período establecido.
Desarmado	Limitado Estándar Gerente	La operación DESARMADO desarma la alarma. Esta opción de menú sólo aparece en el teclado tras activarse una zona de entrada/salida e introducirse un código de usuario válido.
Retardo autoarmado	Estándar* Gerente	El usuario puede retardar o cancelar el autoarmado.
Ignorar retardo	Estándar Gerente	El usuario puede anular automáticamente el Retardo desarmado. Sólo disponible para instalaciones Financieras. Consulte *Armado/Desarmado* en la página 281.
Restaurar	Estándar Gerente	La operación RESTAURAR restaura la condición de alerta en el sistema y borra el mensaje de alerta asociado a dicha condición. Una condición de alerta se puede borrar únicamente tras restaurar las zonas o fallos, que la hayan activado, a su estado de funcionamiento normal y una vez seleccionada, en la programación del usuario, la opción BORRAR ALERTA para esa zona.
Inhibir	Estándar Gerente	Al inhibir una zona, dicha zona se desactiva para el período establecido de la alarma. Éste es el método preferido para desactivar una zona abierta o con fallos, ya que la condición abierta o con fallos se muestra en el teclado cada vez que el sistema se arma para recordar al usuario que tenga en cuenta esa zona.
Aislar	Estándar* Gerente	Al aislar una zona se desactiva la misma hasta que transcurra el tiempo establecido para anular el aislamiento. Es posible aislar todos los tipos de zona del controlador. Esta función de desactivación de zonas abiertas o con fallos se debe utilizar con mucho cuidado; cuando una zona está inhibida, el sistema la ignora, y se podría pasar por alto al armarse el sistema en el futuro, poniendo así en peligro así la seguridad de las instalaciones.

Derecho	Tipo de perfil de usuario por defecto	Descripción
Derechos de usuario: Sistema		
Acceso web	Estándar* Gerente	El usuario puede acceder a la central a través del navegador web.
Ver registro	Estándar Gerente	Esta opción de menú muestra la incidencia más reciente en la pantalla del teclado. El registro de incidencias (consulte *Regt.incidenc.* en la página 172) informa sobre la hora y la fecha de cada incidencia registrada.
Usuarios	Gerente	Este usuario puede crear y editar otros usuarios en la central, pero solo con los mismos derechos o menos que él.
Envío SMS	Estándar* Gerente	Esta característica permite a los usuarios configurar el servicio de mensajes SMS si se ha instalado un módem en el sistema.
Configurar Fecha	Estándar Gerente	Utilice esta opción de menú para programar la hora y la fecha en el sistema (consulte *Configurar fecha/hora* en la página 180). Asegúrese de que la información sobre la hora y la fecha es precisa. Estos campos se muestran en el registro de incidencias al notificar las incidencias del sistema.
Cambio de código	Estándar Gerente	Esta opción de menú permite a los usuarios cambiar sus códigos PIN de usuario (consulte *Cambiar código PIN de técnico* en la página 173). **Nota:** Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.
Ver vídeo / Vídeo en navegador	Estándar Gerente	El usuario puede ver imágenes de vídeo mediante el navegador web. **Aviso:** Para esta función, también debe estar habilitado el derecho de acceso web.
Chime	Estándar Gerente	Todas las zonas con el atributo CHIME generan, al abrirlas, una ráfaga corta de tonos audibles en el zumbador del teclado (cuando el sistema está desarmado). Esta opción de menú permite habilitar o deshabilitar la función de Chime en todas las zonas.
Técnico	Gerente	Esta opción permite a los usuarios conceder acceso a la programación del técnico. Para los requisitos regionales suizos CAT1 y CAT2, cuando se permite el acceso al técnico, todas las particiones deben estar desarmadas; de lo contrario, se le denegará el acceso al técnico.
Actualizado	Gerente	El usuario puede autorizar al fabricante el acceso a la central para actualizar el firmware.
Derechos de usuario: Control		
Salida	Estándar Gerente	Activación/desactivación de las salidas configuradas (actuaciones). Consulte *Editar una salida* en la página 226.

Derecho	Tipo de perfil de usuario por defecto	Descripción
X-10	Estándar Gerente Control de accesos	Activación y desactivación de los dispositivos X-10 configurados. **Aviso:** X-10 está en mantenimiento. Esta funcionalidad se mantiene en el sistema para conservar la compatibilidad retroactiva.
Control de puertas	Estándar* Gerente Control de accesos	El usuario puede bloquear/desbloquear puertas.
Control RF	Estándar Gerente Control de accesos	El usuario puede controlar la salida RF
Derechos de usuario: Test		
Test sirena (s):	Estándar Gerente	El usuario puede realizar un test de sirenas para comprobar las sirenas exteriores, el flash, las sirenas interiores y el zumbador y, así, garantizar su funcionamiento correcto.
Test de intrusión	Estándar Gerente	El usuario puede realizar un test de intrusión que le permitirá comprobar el funcionamiento de todos los detectores de alarma de un sistema.
Test PAT	Estándar Gerente	El usuario puede comprobar un PAT.
Test sísmico	Estándar Gerente	El usuario puede comprobar el detector sísmico.
Derechos de usuario: Técnico de servicio		
Configurar usuarios (maestro)		El usuario puede crear y editar otros usuarios en el sistema sin restricción de los atributos de usuario.
Configurar perfiles de usuario		El usuario puede crear y editar perfiles de usuario en el sistema.
Configurar calendarios		El usuario puede configurar calendarios.
Configurar puertas		El usuario puede editar puertas.
Acceso de nivel 3		Permitir al usuario llevar a cabo tareas de técnico con nivel 3. Esta función solo está disponible en modo «Sin restricción» (EN50131 requiere que las operaciones previas solo estén autorizadas por un usuario de nivel 3 para un sistema de grado 3).
* Estas funciones no están habilitadas por defecto para este usuario, pero se pueden seleccionar.		

Control de accesos



1. Introduzca un **Código de lugar**, si es necesario, para todas las tarjetas asignadas a este perfil de usuario. Consulte *Lectores de tarjeta y formatos de tarjeta admitidos* en la página 404.
2. Seleccione los derechos de **Acceso** de este perfil de usuario para las puertas configuradas en el sistema. Las opciones son:

   - Sin acceso

   - Sin límite de tiempo (es decir, acceso las 24 horas)

   - Calendario (si está configurado)

Usuarios

Se muestra una lista de usuarios asignados a este perfil. Haga clic en un usuario para ver o editar sus detalles.

Puede crear un nuevo perfil de usuario basado en un perfil existente haciendo clic en **Replicar**. Se muestra una nueva página de **Perfil de usuario**.

Consulte también

Añadir/Editar perfiles de usuario en la página 212

Añadir/Editar una partición en la página 275

17.8.3 Configuración de SMS

El sistema SPC permite la mensajería (SMS) remota en sistemas que tengan un módem instalado.

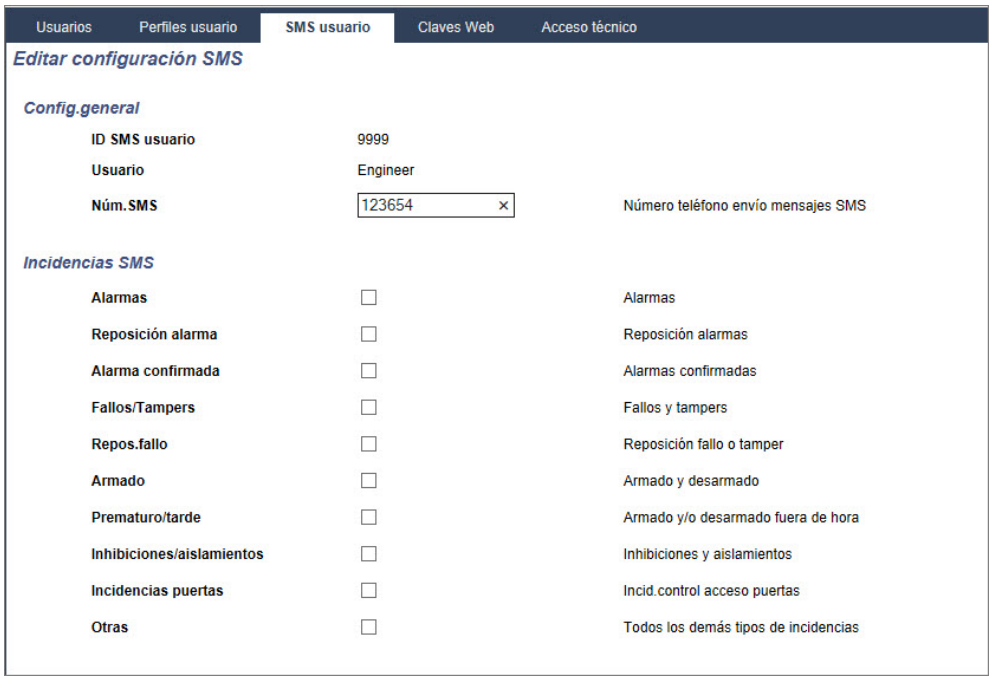
Prerrequisitos

- Hay un módem instalado e identificado por el sistema.
- La función **Autentificación SMS** está activada. (Consulte *Opciones* en la página 254.)

1. Seleccione **Usuarios > Usuarios SMS**.

   Al hacerlo, se muestra el ID de SMS del técnico y una lista de ID de SMS de usuarios con los correspondientes detalles de SMS.

2. Haga clic en el botón **Test** para comprobar un número de SMS.
3. Haga clic en **Añadir** para añadir un nuevo ID de SMS, o haga clic en **Editar** junto al ID de SMS deseado.



4. Configure los detalles de SMS tal como se indica a continuación:

ID de SMS	ID generado por el sistema.
Número de SMS	Introduzca el número al que se enviarán los SMS (requiere un prefijo de código de país de tres dígitos). **Nota:** El número de SMS del técnico se puede borrar reseteándolo a 0. Los números de SMS de los usuarios no se pueden borrar.
Operador	Seleccione un nuevo usuario para este ID de SMS si es necesario.
Incidencias SMS	Seleccione las incidencias de la central que el usuario o el técnico recibirán a través de SMS.
Control SMS	Seleccione las operaciones que el usuario o el técnico podrán realizar de forma remota en la central a través de SMS. Consulte *Comandos de SMS* abajo.

AVISO: Las incidencias de alarma de ATRACO no se transmiten por SMS.

Si la línea telefónica está conectada a la red RTB a través de un PBX, debe insertarse el dígito de acceso a la línea adecuado antes del número de la parte a la que se llama. Asegúrese de que **I**dentidad de **L**ínea **L**lamante (CLI) esté activada en la línea seleccionada para realizar llamadas a la red SMS. Consulte al administrador de PBX para obtener más información.

17.8.4 Comandos de SMS

Una vez finalizada la configuración de SMS, pueden activarse sus funciones. Los comandos, dependiendo de la configuración de SMS, se envían mediante un código PIN o un identificador de llamada. El tipo de código PIN depende de lo que se haya configurado para Autentificación de SMS.

La tabla siguiente muestra todos los comandos de SMS disponibles. La acción y la respuesta posteriores también se indican.

Los comandos de SMS se envían en forma de texto al número de teléfono de la tarjeta SIM del controlador.

Para los comandos que usan un código PIN, el formato del texto es:

****.comando o **** comando,

siendo **** el código PIN y «comando» el comando, es decir, el código PIN seguido de un espacio o un punto. Por ejemplo, el comando «ATOT» se introduce como: **** ATOT o ****.ATOT. También se puede utilizar la versión completa del comando, si aparece en la lista. Por ejemplo, ****.Armado total.

Si el usuario no dispone de derechos suficientes para ejecutar un comando, en el sistema se indica Acceso denegado.

Si está habilitado el ID de quien llama, y está configurado el número de SMS de la persona que envía el mensaje, no es necesario el prefijo del código.

COMANDOS (** = código)**

Utilización del código	Identificación número teléfono llamada entrante	Acción	Respuesta
**** AYUD ****.AYUD	AYUD	Se muestran todos los comandos disponibles.	Todos los comandos disponibles
**** ATOT ****.ATOT ****.A.TOTAL	ATOT A.TOTAL	Se arman todas las particiones a las que tiene acceso el usuario.	Hora/fecha de armado del sistema. Si fuera aplicable, responde con zonas abiertas o de armado forzado
****.APA ****.APA		Permite armado parcial A de alarma por SMS. También es posible especificar el nombre personalizado definido en el campo de renombre ARMADO PARCIAL de la página de **Opciones**. Consulte *Opciones* en la página 254.	Sistema armado
****.APB ****.APB		Permite armado parcial B de alarma por SMS. También es posible especificar el nombre personalizado definido en el campo de renombre ARMADO PARCIAL de la página de **Opciones**. Consulte *Opciones* en la página 254. Por ejemplo: ****.APA Noche	Sistema armado

Utilización del código	Identificación número teléfono llamada entrante	Acción	Respuesta
**** DESM ****.DESM ****.DESARMADO	DESM Desarmado comun	Se desarman todas las particiones a las que tiene acceso el usuario.	Desarmado sistema
**** ESTD ****.ESTD ****.ESTADO	ESTD ESTADO	Recupera el estado de las particiones.	Estado del sistema y particiones aplicables • Para un sistema de partición única, el sistema y el modo se recuperan cuando el modo es el estado de armado del sistema. • Para un sistema de particiones múltiples, se recupera el estado de cada partición.
**** XA1.ON ****.XA1.ON		Donde el dispositivo X-10 se identifica como «A1», se activa.	Estado de «A1»
**** XA1.OFF ****.XA1.OFF		Donde el dispositivo X-10 se identifica como «A1», se desactiva.	Estado de «A1»
**** LOG ****.LOG		Se muestran hasta 10 incidencias recientes.	Incidencias recientes
**** ATEC.ON ****.ATEC.ON	ATEC.ON	Habilita el acceso de técnico.	Permitir técnico
**** ATEC.OFF ****.ATEC.OFF	ATEC.OFF	Deshabilita el acceso de técnico.	Acceso retirado a técnico
**** AFAB.ON ****.AFAB.ON		Habilita el acceso de fabricante.	Estado de fabricante
**** AFAB.OFF ****.AFAB.OFF		Deshabilita el acceso de fabricante.	Estado de fabricante

Utilización del código	Identificación número teléfono llamada entrante	Acción	Respuesta
**** ABT.5.ON ****.ABT.5.ON ****.SALIDA		Cuando la salida de usuario (puerta de mapeo) se identifica como «O5», se activa.	Estado de «ABT.5» Por ejemplo: • Salida ABT.5 activada. • Calefacción de salida activada (siendo Calefacción el nombre de la salida).
**** ABT.5.OFF ****.ABT.5.OFF		Cuando la salida de usuario (puerta de mapeo) se identifica como «O5», se desactiva.	Estado de «ABT.5» Por ejemplo: Salida O5 desactivada
****.BORR ****.RESTAURAR		Permite el borrado de alertas por SMS.	

Para el reconocimiento de SMS, la identificación de la salida (puerta de mapeo) utiliza el formato ONNN, donde O se refiere a la salida y NNN son los espacios numéricos, de los cuales no todos son necesarios.
(Por ejemplo: O5 para salida 5)

Para el reconocimiento de SMS, el dispositivo X-10 utiliza el formato XYNN, donde X significa X-10; Y se refiere a la identidad alfabética y NN son los espacios numéricos disponibles. (Ejemplo: XA1)

El SMS funciona utilizando un protocolo estándar que se utiliza en teléfonos con SMS. Tenga en cuenta que algunos operadores RTB no ofrecen el servicio de SMS a través de RTB. Para que los SMS funcionen con RTB han de cumplirse los siguientes criterios:

- El ID de quien llama debe estar habilitado en la línea telefónica.
- La línea telefónica debe ser directa, no a través de PABX u otro equipo de comunicaciones.
- Tenga en cuenta también que la mayoría de los proveedores de servicios solo permite los SMS a un teléfono registrado en el mismo país. (Esto se debe a cuestiones de facturación).

17.8.5 Borrado de claves web

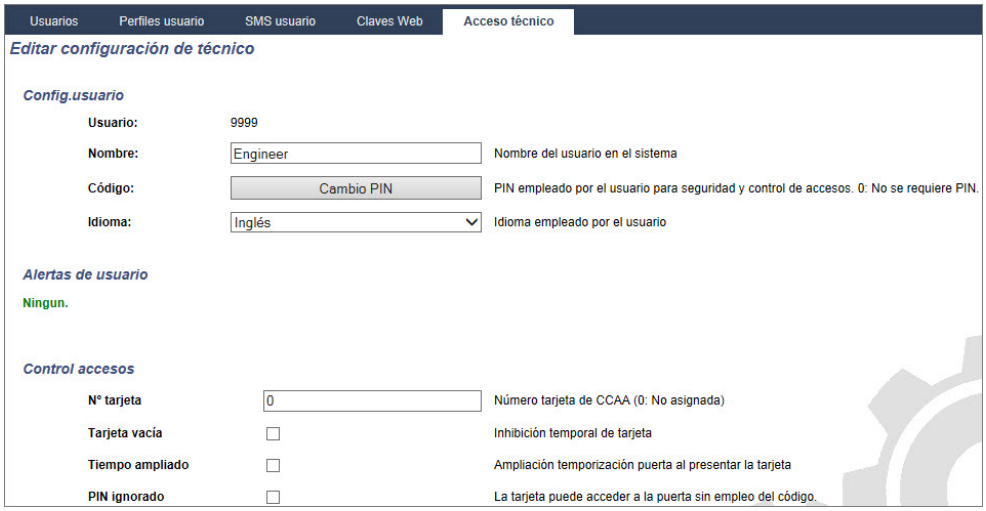
En esta página aparece una lista de claves de técnico y de cualquier otro usuario, así como la clave de técnico que se ha creado para acceder al navegador de Internet.

1. Seleccione **Usuarios > Claves web**.

2. Haga clic en el botón **Borrar** junto al técnico o el usuario para borrar la clave.

17.8.6 Ajustes de configuración de técnico

1. Seleccione **Usuarios > Técnico**.



2. Cambie el **Nombre usuario** del «Técnico» si es necesario.
3. Haga clic en el botón **Cambiar código PIN** para cambiar el PIN de técnico (consulte *Cambio de código de técnico y de clave web* en la página opuesta).

   Nota: Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.
4. Seleccione el **Idioma** que utilizará el técnico. (Solo se muestra si están disponibles múltiples idiomas. Consulte *Actualización de idiomas* en la página 351).

Control de accesos

Atributo	Descripción
Número tarjeta	Número de la tarjeta de CCAA Introduzca 0 para dejar sin asignar esta tarjeta.
Tarjeta vacía	Inhibición temporal de tarjeta
Tiempo ampliado	Ampliación de la temporización de la puerta al presentar la tarjeta.
Anulación de Código	Acceso a puerta sin PIN en una puerta con lector de PIN.
Prioridad	Las tarjetas prioritarias se almacenan localmente en los controladores de puertas y permiten el acceso en caso de fallo técnico allí donde el controlador de puerta no se puede comunicar con la central de control. El número máximo de usuarios prioritarios es: • SPC4xxx – todos los usuarios • SPC5xxx – 512 • SPC6xxx – 512

Atributo	Descripción
Acompañante	La función de Visita obliga a los titulares de tarjetas con este privilegio a acompañar a otros titulares de tarjetas por puertas específicas. Si esta función está habilitada en una puerta, se debe presentar primero una tarjeta con la atribución de Visita para permitir abrir la puerta a otros titulares de tarjeta sin este atributo. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con derecho de Visita; se puede configurar individualmente para cada puerta.
Custodia	La función de Custodia impone a un titular de tarjeta con dicho privilegio a estar siempre dentro de una estancia (grupo de puertas) cuando otros titulares de tarjetas están dentro. El usuario Custodia debe ser el primero en entrar en la sala. Sólo podrán entrar otros titulares de tarjetas si hay un responsable en la estancia. El titular de la tarjeta con atributo de Custodia no podrá salir hasta que todas las tarjetas que no sean de responsable hayan salido de la estancia. Identifica al titular de esta tarjeta como responsable. El usuario con atributo de Custodia debe ser el primero en entrar en un grupo de puertas que requiera un titular de tarjeta de Custodia, y debe ser el último en abandonar dicho grupo de puertas.

17.8.6.1 Cambio de código de técnico y de clave web

Esta página le permite cambiar el código PIN para acceder al teclado, así como la clave para acceder al navegador web (únicamente para el nivel de técnico).

1. Cambie el código PIN como se indica a continuación:

Código PIN anterior	Introduzca el código PIN de técnico actual. (solo dígitos numéricos)
Código PIN nuevo	Introduzca el código PIN de técnico nuevo. (solo dígitos numéricos)
Confirmar código PIN nuevo	Vuelva a introducir el código PIN de técnico nuevo.

2. Haga clic en el botón **Cambiar código PIN** para activar el código PIN nuevo.

El número mínimo de dígitos necesario para este código depende de la configuración de seguridad del sistema o de la longitud programada para los **dígitos PIN** en el menú **Config. central > Config. sistema > Opciones**.

3. Cambie la clave web a una clave más segura para acceder al navegador web.

Nueva clave	Introduzca la nueva clave de acceso web (caracteres alfabéticos de la A a la Z y dígitos numéricos del 0 al 9).
Confirme nueva clave	Vuelva a introducir la nueva clave de acceso web.

4. Haga clic en el botón **Cambiar clave** para activar la nueva clave.

Esta clave distingue entre mayúsculas y minúsculas; así pues, compruebe si introduce caracteres en mayúsculas o en minúsculas en su nueva clave.

17.9 Configuración

Esta sección abarca:

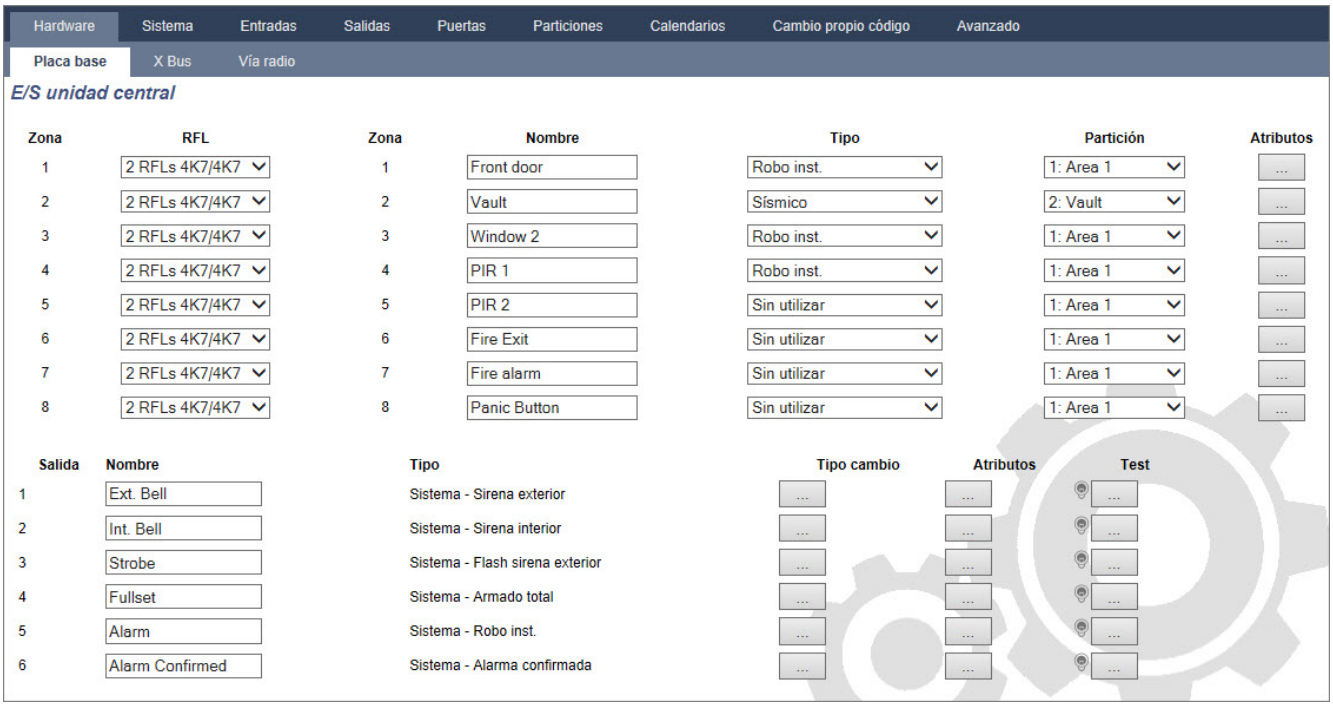
17.9.1 Configurar entradas y salidas de controlador

Esta sección abarca:

17.9.1.1 Editar una entrada

1. Seleccione **Configuración> Hardware > Controlador**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

Entrada	El número se muestra para referencia y no puede programarse.
RFL	Seleccione Final de línea (RFL) para la entrada de zona (por defecto: 4K7).
Analizada	Muestra si el sensor es un sensor de tipo inercial/shock.
Cantidad de pulsos	La cantidad de pulsos programada en la central que disparará una alarma de un sensor de tipo inercial/shock.
Sensibilidad	La sensibilidad programada en la central que disparará una alarma de un sensor de tipo inercial/shock.
Zona	Número de la zona en la central
Descripción	Introduzca texto que describa la entrada (máx. 16 caracteres). Este texto aparecerá en el navegador y el teclado.
Tipo	El tipo de zona (consulte *Tipos de zona* en la página 393).
Particiones	Sólo si la función de particiones (múltiples) está activada en el menú **Config. central > Config. sistema > Opciones.** Seleccione las particiones a las que ha sido asignada esta zona.
Atributos	Un icono en este campo indica que se han programado los atributos para esta zona (consulte *Zonas de entrada: atributos* abajo).

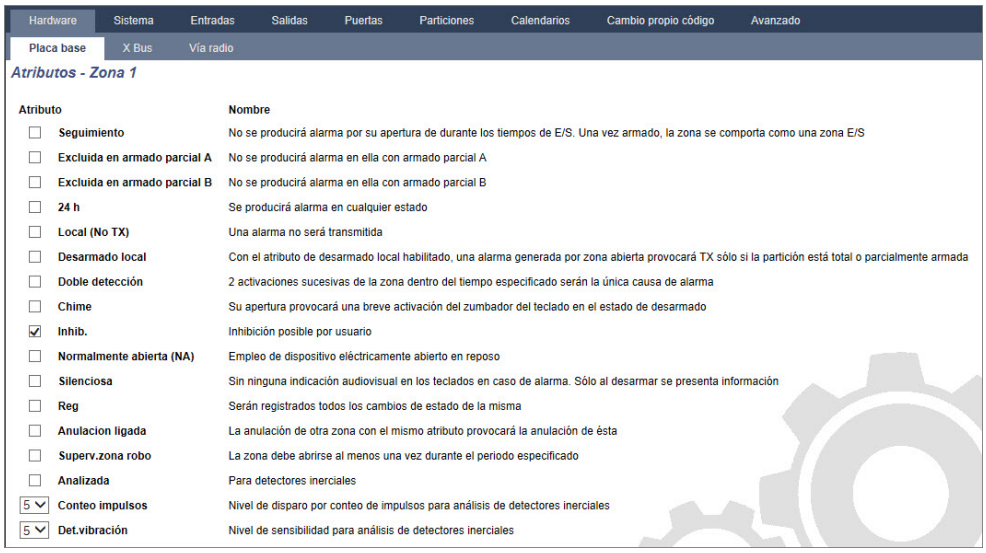
Zonas de entrada: atributos

Se puede asignar a cada zona de SPC un atributo que determine las propiedades de esa zona.

Para asignar un atributo a una zona:

1. Seleccione **Configuración> Hardware > Controlador > Atributos**.

   Se mostrará la siguiente página:

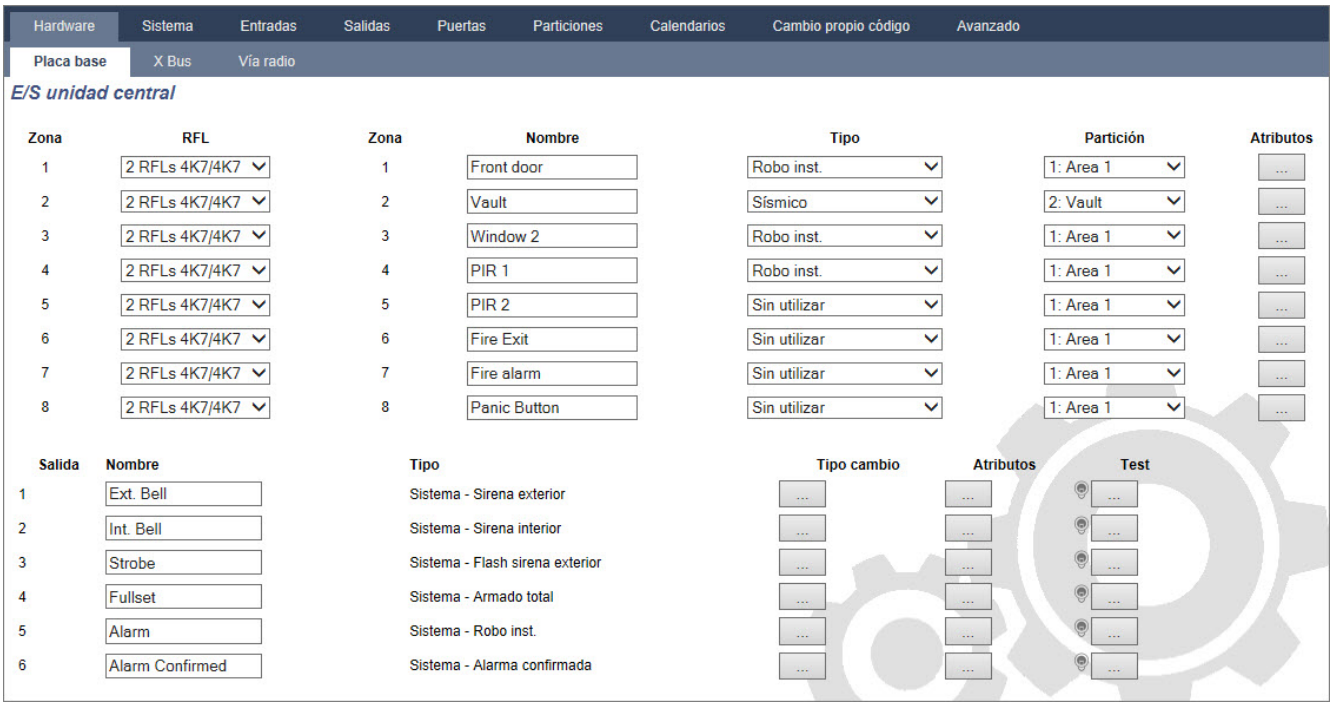


2. Marque la casilla junto al atributo preferido.

Los atributos de esta página dependerán del tipo de zona seleccionada. Para obtener una lista de los atributos asignables, consulte *Atributos aplicables a los tipos de zona* en la página 403.

17.9.1.2 Editar una salida

1. Seleccione **Configuración> Hardware > Controlador**.



2. Configure los campos tal como se describe en la siguiente tabla.

Tipo de salida	• **Salida del sistema:** Seleccione el tipo del menú desplegable. (Consulte *Tipos de salidas y puertos de salida* abajo.) • **Salida de partición:** Sólo si la función de **particiones (múltiples)** está activada en el menú **Config. central > Config. sistema > Opciones**. Seleccione una partición y el tipo de salida del sistema para esta partición. (Consulte *Tipos de salidas y puertos de salida* abajo.) • **Identificación de zona:** Seleccione qué zona se debe identificar. • **Puerta de mapeo:** Seleccione qué puerta de mapeo se debe identificar. • **Salida de puerta:** Seleccione el número de puerta y el tipo de salida para esa puerta. (Consulte *Tipos de salidas y puertos de salida* abajo.) • **Conmutador llave:** Seleccione el ID de nodo para el conmutador llave requerido y la posición de la llave requerida para mapear esta salida.
Descripción	Introduzca texto que describa la salida (máx. 16 caracteres). Este texto aparecerá en el navegador y el teclado.
Configuración de salidas	• **Modo:** Seleccione el modo operativo. Seguimiento continuo del tipo de salida. El pulso se activa y desactiva cuando el tipo de salida está activo. Genera momentáneamente un pulso cuando se activa el tipo de salida. • **Redisparo:** Marque la casilla para volver a disparar salidas momentáneas. • **Hora de activación:** Introduzca la hora de activación que se aplica a las salidas momentáneas y pulsadas. • **Hora de desactivación:** Introduzca la hora de activación que se aplica a las salidas pulsadas. • **Invertir:** Marque esta casilla para invertir la salida física. • **Registrar:** Marque esta casilla para registrar los cambios del estado de salida en el registro de incidencias. • **Calendario:** Seleccione, en caso de ser necesario, el calendario deseado. Consulte *Calendarios* en la página 289.

Consulte también

Calendarios en la página 289

Tipos de salidas y puertos de salida

Cada tipo de salida puede asignarse a uno de los seis puertos de salida físicos del controlador SPC o a una salida en uno de los módulos de expansión conectados. Los tipos de salida que no están asignados a salidas físicas funcionan como indicadores de incidencias en el sistema y pueden registrarse y/o informarse a las estaciones centrales en caso de ser necesario.

Los puertos de salida en los módulos de expansión son todas salidas de tipo relé unipolar (NA, COM, NC). Por lo tanto, es posible que los dispositivos de salida requieran fuentes de alimentación externas para activarse si están cableados a las salidas de módulos de expansión.

La activación de un tipo de salida concreto depende del tipo de zona (consulte *Tipos de zona* en la página 393) o de condición de la alerta que provoca la activación. Si se definen varias particiones en el sistema, las salidas en el SPC se agrupan en salidas del sistema y salidas de partición; las salidas del sistema se activan para indicar una incidencia que afecta a todo el sistema (como un fallo en la red de CA), mientras que las salidas de partición indican incidencias detectadas en una o más de las

particiones definidas en el sistema. Cada partición tiene su propio conjunto de salidas de partición. Si la partición es común para otras particiones, entonces las salidas indicarán el estado de todas las particiones en común, incluyendo el estado propio. Por ejemplo, si la partición 1 es común para las particiones 2 y 3, y Sirena Exterior está Si la sirena está activa, entonces la salida de sirena exterior de la Partición 1 también está activa.

Algunos tipos de salidas solo pueden indicar incidencias que afectan a todo el sistema (no específicas de particiones). Consulte la tabla a continuación para obtener más información.

Tipo de salida	Descripción
Sirena exterior	Este tipo de salida se utiliza para activar la sirena exterior del sistema y está activa cuando hay una sirena exterior activa. Por defecto, la salida está asignada a la primera salida de la placa del controlador (EXT+, EXT-). **Nota:** Se activa automáticamente una sirena exterior cuando una zona que está programada como zona de alarma dispara una alarma en modo Armado total o Armado parcial.
Flash exterior	Este tipo de salida se utiliza para activar el flash de la sirena exterior del sistema y está activa cuando hay un flash de partición activo. Por defecto, la salida está asignada a la salida de relé de flash (Salida 3) de la placa del controlador (NA, COM, NC). **Nota:** Se activa automáticamente una salida de flash exterior cuando una zona que está programada como zona de alarma dispara una alarma en modo Armado total o Armado parcial. El flash de sirena exterior se activa en una condición 'Fallo al armar' si el flash en la opción 'Fallo al armar' está marcada en las opciones del sistema.
Sirena interior	Este tipo de salida se utiliza para activar la sirena interior y está activa cuando hay una sirena interior activa. Por defecto, la salida está asignada a la segunda salida de la placa del controlador (INT+, INT-). **Nota:** Se activa automáticamente una sirena interior cuando una zona que está programada como zona de alarma dispara una alarma en modo Armado total o Armado parcial. La sirena interior se activa en una condición «Fallo al armar» si en las opciones del sistema está seleccionada la opción «Fallo al armar».
Alarma	Esta salida se activa tras la activación de una zona de alarma en el sistema o desde cualquier partición definida en el sistema.
Alarma confirmada	Esta salida se activa cuando se ha confirmado una alarma. Una alarma se confirma cuando se activan 2 zonas independientes en el sistema (o dentro de la misma partición) dentro de un período de tiempo específico.
Pánico*	Esta salida se activa tras la activación de tipos de zona de alarma de pánico desde cualquier partición. También se genera una salida de alarma de pánico si se produce una incidencia de coacción o si se habilita la opción de pánico para el teclado.
Atraco	Esta salida se activa cuando una zona programada como de tipo atraco dispara una alarma desde cualquier partición.
Incendio	Esta salida se activa tras la activación de una zona de incendio en el sistema (o desde cualquier partición).

Tipo de salida	Descripción
Tamper	Esta salida se activa cuando se detecta una condición de tamper desde cualquier parte del sistema. Para un sistema de Grado 3, si se pierde la comunicación hacia un dispositivo X-BUS durante más de 100 segundos, se genera un tamper y las incidencias informadas de SIA y CIR enviarán un tamper.
Alarma médica	Esta salida se activa cuando se activa una zona de alarma médica.
Fallo	Esta salida se activa cuando se detecta un fallo técnico.
Técnico	Esta salida se activa con actividad de una zona técnica.
Fallo red CA*	Esta salida se activa cuando se interrumpe la red de CA.
Fallo de batería*	Esta salida se activa cuando hay un problema con la batería de respaldo. Si el voltaje de la batería es inferior a 11 V, se activa esta salida. La opción 'Restaurar' para este fallo solo se presenta cuando el nivel de tensión asciende hasta por encima de 11,8 V.
Armado parcial A	Esta salida se activa si el sistema o cualquier partición definida en el sistema está en modo Armado parcial A.
Armado parcial B	Esta salida se activa si el sistema o cualquier partición definida en el sistema está en modo Armado parcial B.
Armado total	Esta salida se activa si el sistema está en modo Armado total.
Fallo al armar	Esta salida se activa si no se pudo armar el sistema o cualquier partición definida en el sistema. Se borra cuando se restaura la alarma.
Entrada/salida	Esta salida se activa si se ha activado una zona de entrada/salida, es decir, si se está ejecutando un temporizador de entrada o salida de una partición o del sistema.
Enclavamiento	Esta salida se activa según lo definido en la configuración de salida de enclavamiento del sistema (consulte *Configurar enclavamiento y autoarmado de salidas del sistema* en la página 232). Esta salida puede utilizarse para resetear los sensores de enclavamiento al igual que los sensores de humo o inerciales.
Salida incendio	Esta salida se activa si se activa alguna de las zonas de salida de emergencia.
Chime	Esta salida se activa momentáneamente cuando se activa el atributo chime de cualquier zona del sistema.
Humo	Esta salida se enciende momentáneamente (3 segundos) cuando un usuario desarma el sistema; puede utilizarse para restablecer detectores de humo. La salida también se activará cuando se restaure la zona. Cuando se utiliza la zona para restaurar detectores de humo bloqueados, la primera vez que se introduzca el código no se activarán las salidas de humo, sino que se silenciarán las sirenas; la siguiente vez que se introduzca el código, si la zona de incendio está en estado abierto, la salida de humo se activará momentáneamente. Este proceso se puede repetir hasta que se cierre la zona de incendio.
Test de paseo*	Esta salida se activa momentáneamente cuando se realiza un test de intrusión y se activa una zona. Esta salida se puede utilizar, por ejemplo, para activar tests funcionales de detectores conectados (si está disponible).

Tipo de salida	Descripción
Armado automático	Esta salida se activa cuando se activa la función de armado automático en el sistema.
Coacción de usuario	Esta salida se activa si se ha activado el estado de coacción de usuario (si se introdujo un código PIN + 1 en el teclado).
PIR enmascarado	Esta salida se activa si hay zonas PIR enmascaradas en el sistema. Genera una salida de fallo en la luz LED del teclado. Esta salida se bloquea y permanecerá activa hasta que sea restablecida por un usuario de nivel 2. Se registra el enmascaramiento PIR por defecto. La cantidad de entradas del registro no supera 8 entre los períodos de armado.
Zona omitida	Esta salida se activa si hay zonas inhibidas, aisladas o zonas de test de intrusión en el sistema.
Comunicación	Esta salida se activa si hay un fallo de comunicación con la estación central.
Test hombre caído	Esta salida se activa en un dispositivo vía radio de 'hombre caído', el cual se activa cuando se realiza el test de 'hombre caído'.
Desarmado	Esta salida se activa si el sistema está en modo Desarmado.
Aborto de alarmas	Esta salida se activa si se aborta una alarma, es decir, cuando se introduce un código de usuario válido a través del teclado luego de una alarma confirmada o no confirmada. Se utiliza, por ejemplo, con marcadores externos (SIA, CID, FF).
Test sísmico	Esta salida se utiliza para activar una prueba manual o automática en una zona sísmica. Los sensores sísmicos tienen un vibrador pequeño que se fijará a la misma pared que el sensor y estará cableado a una salida en la central o uno de sus módulos de expansión. Durante la prueba, la central espera hasta 30 segundos para que la zona sísmica se abra. Si esto no sucede, el test falla. Si se abre dentro de los 30 segundos, la central espera a que la zona se cierre dentro de un período de 10 segundos. Si esto no sucede, el test falla. Luego, la central espera otros 2 segundos antes de informar el resultado del test. El resultado del test, ya sea manual o automático, se almacena en el registro de incidencias del sistema.
Alarma local	Esta salida activa una alarma de intrusión local.
Salida RF	Esta salida se activa cuando se pulsa un botón de una APR o dispositivo de mando vía radio.
Fallo línea TX 1	Esta salida se activa cuando hay un fallo en la línea del módem principal.
Fallo TX 1	Esta salida se activa cuando falla el módem principal.
Fallo línea TX 2	Esta salida se activa cuando hay un fallo en la línea del módem secundario.
Fallo TX 2	Esta salida se activa cuando falla el módem secundario.
Batería baja	Esta salida se activa cuando la batería está baja.
Estado de entrada	Esta salida se activa si se implementa un procedimiento de entrada 'Todo OK' y no se genera una alarma, es decir, cuando se pulsa el botón 'Todo OK' dentro del período de tiempo configurado tras haber introducido el código de usuario.

Tipo de salida	Descripción
Estado de aviso	Esta salida se activa si se implementa un procedimiento de entrada 'Todo OK' y se genera una alarma silenciosa, es decir, cuando no se pulsa el botón 'Todo OK' dentro del período de tiempo configurado tras haber introducido el código de usuario.
Listo para armar	Esta salida se activa cuando una partición está lista para el armado.
Config. ACK	Esta salida señala el estado de armado. La salida alterna durante 3 segundos para indicar que el armado ha fallado. La salida permanece activa durante 3 segundos si el armado se ha realizado correctamente.
Arm. total hecho	Esta salida se activa durante 3 segundos para indicar que el sistema se ha armado completamente.
Blockschloss 1	Se utiliza para dispositivos Blockschloss normales. Cuando todas las zonas de una partición están cerradas, y no hay errores pendientes, la salida «Blockschloss 1» se activa. Si la cerradura del Blockschloss está cerrada, se activa una entrada de «Llave A/D», se arma la partición relevante y se activa la salida Config. ACK durante 3 segundos para indicar que el armado se ha realizado satisfactoriamente. «Blockschloss 1» no está desactivado. Si el Blockschloss está desbloqueado, el dispositivo Blockschloss desactiva la entrada de Llave A/D dejándola en estado desarmado (cerrado), y la partición queda desarmada. A continuación, «Blockschloss 1» se desactiva.
Blockschloss 2	Se utiliza para dispositivos de tipo Blockschloss: Bosch Blockschloss, Sigmalock Plus, E4.03. Cuando todas las zonas de una partición están cerradas, y no hay errores pendientes, la salida «Blockschloss 2» se activa. Si la cerradura del Blockschloss está cerrada, se activa una entrada de «Llave A/D», se arma la partición relevante y se activa la salida Config. ACK durante 3 segundos para indicar que el armado se ha realizado satisfactoriamente. A continuación, «Blockschloss 2» se desactiva. Si el Blockschloss está desbloqueado, la zona de Llave A/D pasa a quedar desarmada (cerrada) y la partición queda desarmada. «Blockschloss 2» está activado (si la partición está lista para el armado).
Elemento bloqueo	Se activa si el elemento de bloqueo está en la posición «bloqueada».
Elemento desbloqueo	Se activa si el elemento de bloqueo está en la posición «desbloqueada».
Código tamper	Se activa si hay un código tamper en la partición. Se desactiva cuando se restaura el estado.
Problema	Se activa si hay alguna zona con problemas.
Link Ethernet	Se activa si hay algún fallo en el link de Ethernet.
Fallo red	Se activa si hay algún fallo de comunicación de EDP.
Reset cristal	Sirve para conectar la alimentación para el módulo de interfaz de rotura de cristal y para desconectarla a fin de reiniciar el dispositivo. La salida se reinicia si un usuario introduce su código, la zona no está en estado cerrado y las campanas están desactivadas.

Tipo de salida	Descripción
Atraco confirmado	Se activa en los siguientes casos para cumplir con PD6662: • se producen dos activaciones de zona de atraco con una diferencia de más de dos minutos entre sí • se produce la activación de una zona de atraco y una zona de pánico con una diferencia de más de dos minutos entre sí • Si se produce la activación de una zona de atraco y una zona de tamper o una zona de pánico y una zona de tamper dentro del período de dos minutos.
Modo técnico completo	Se activa si hay un técnico in situ y el sistema se encuentra en modo técnico completo.

**Este tipo de salida sólo puede indicar incidencias que afectan a todo el sistema (no específicas de particiones).*

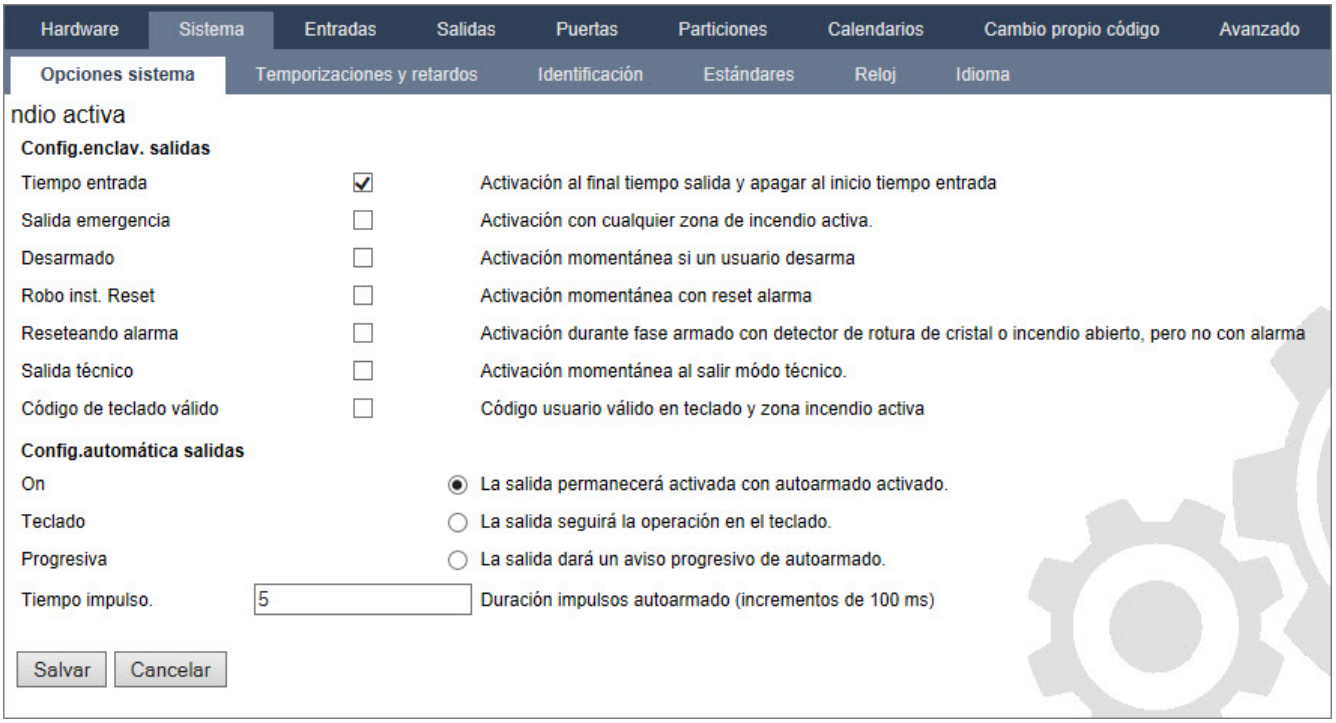
Consulte también

Configurar enclavamiento y autoarmado de salidas del sistema abajo

17.9.1.3 Configurar enclavamiento y autoarmado de salidas del sistema

1. Debajo de **Política**, haga clic en el botón **Editar** para la opción **Configuración de salida** en **Opciones del sistema**.

   Aparecerá la siguiente página:



2. Seleccione la condición bajo la cual se activará la salida con enclavamiento:

Tiempo entrada	La salida se activa al final del tiempo salida y se desactiva al inicio del tiempo entrada.
Salida incendio	La salida se activa si cualquier zona de salida de incendio está activa.
Desarmado	La salida se activa si el usuario desarma el sistema momentáneamente.
Reinicio de alarma	La salida se activa si se resetea la alarma momentáneamente.
Resetear alarma	La salida se activa durante la fase de armado si se detecta una rotura de cristal o humo y la alarma no está activa.
Salida de modo técnico	La salida se activa cuando el técnico sale del modo técnico momentáneamente.
Código de teclado válido	La salida se activa cuando se introduce un código de usuario válido en el teclado y la zona de incendio está activa.

3. Seleccione el comportamiento de la salida.

ON	La salida permanecerá activada si el armado automático está activo.
Teclado	La salida se regirá por las indicaciones en el teclado.
Progresiva	La salida dará un aviso progresivo de armado automático.
Tiempo de pulso	Seleccione cuánto permanecerá activa la salida de armado automático cuando sea seleccionada.

17.9.1.4 Config. X10 - Ajustes

La página de configuración X10 le permite configurar el funcionamiento de X10 en la central.

1. Seleccione **Configuración > Salidas > X-10**.

   Se mostrará la siguiente página:

2. Marque la casilla **Habilitar** para habilitar el funcionamiento de X-10 en la central.
3. Active la casilla **Registro** para habilitar el registro de todas las incidencias X-10 en la central.
4. Haga clic en **Salvar**.
5. Haga clic en la pestaña alfabética (A-P) para programar los disparos del dispositivo X-10.

   Se presentará una lista de disparadores de dispositivos programables (1-16) para ese carácter alfabético:

Número de unidad	Este es el número (1-16) asignado al dispositivo.
Activo	Este campo indica si el dispositivo está activo o no.
Descripción	Este campo muestra la descripción que se utiliza para ayudar a identificar el dispositivo: por ejemplo, luces escaleras (16 caracteres máx.).
Tecla de activación	Este campo indica si la activación del dispositivo X-10 puede alternarse al introducir un código desde el teclado.

Para editar un dispositivo X-10:

1. Haga clic en **Editar**.

   Se mostrará la siguiente página:

2. Para obtener más información sobre la programación, consulte *Disparadores* en la página 295.

17.9.2 X-BUS

Esta sección abarca:

17.9.2.1 Módulos de expansión

1. Seleccione **Configuración> Hardware > X-Bus > Módulos expansión**.

   Se mostrará la siguiente página:

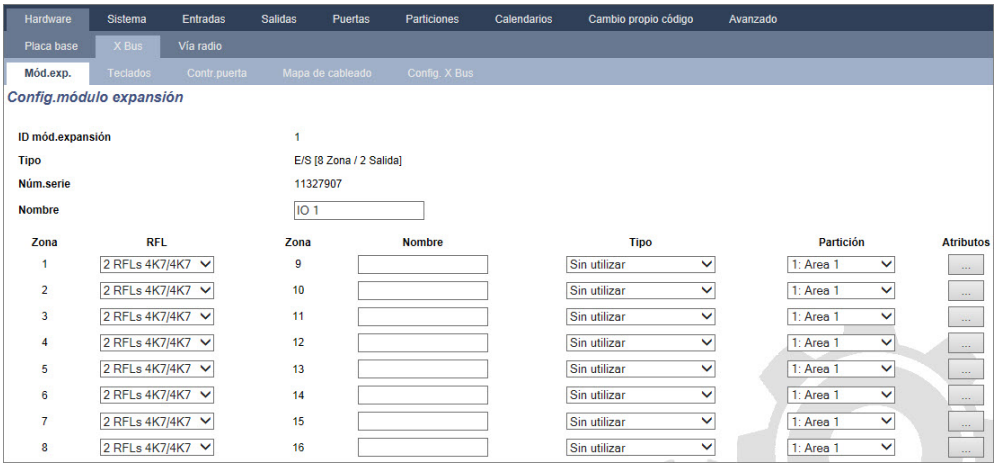
ID	Nombre	Estado	Tipo	Núm.serie	Firmware	Lector	Vía radio	F.A.
1	IO 1	En linea	E/S [8 Zona / 2 Salida]	11327907	1.11 [07AUG13]	Inexistente	Inexistente	Type 1 - V4
2	AEX 2	En linea	Audio [4 Zona]	1434900	1.03 [13MAR13]	Inexistente	Inexistente	Inexistente
3	AEX 3	En linea	Audio [4 Zona / 1 Salida]	37070907	1.03 [13MAR13]	Inexistente	Inexistente	Inexistente
4	WIR 4	En linea	Vía radio	489907	1.11 [07AUG13]	Inexistente	SiWay - V5	Inexistente
5	IOA 5	En linea	E/S analizada [8 Zona / 2 Salida]	165074801	2.00 [09Apr14]	Inexistente	Inexistente	Inexistente
6	IO 6	En linea	E/S [8 Salida]	443907	1.11 [07AUG13]	Inexistente	Inexistente	Inexistente
7	KSW 7	En linea	Llave desarmado [1 Salida]	226593801	1.01 [11NOV10]	Inexistente	Inexistente	Inexistente
8	IND 8	En linea	Indicador [1 Zona]	223387801	1.03 [13MAR13]	EM4100	Inexistente	Inexistente

Para nombrar e identificar:

En una configuración en lazo, cada módulo de expansión está numerado de forma consecutiva desde el primero (módulo de expansión conectado a 1A 1B en el controlador) al último (módulo de expansión conectado a 2A 2B en el controlador).

Ejemplo para SPC63xx: Los módulos de expansión, cuando están enumerados de 1 a 63, son zonas asignadas (en grupos de 8) en identidades subsiguientes de 1 a 512 (el número más alto en la identificación de zonas es 512). Por lo tanto, todo módulo de expansión con nombre o identificado por un número mayor que 63 no tiene zonas asignadas.

2. Haga clic en alguno de los parámetros de identificación del módulo de expansión para que aparezca la página **Configuración de módulo de expansión**.



3. Configure los siguientes campos:

Descripción	Para que aparezca en las luces LED del dispositivo.
Límite de volumen	**Módulo de expansión de audio únicamente** Volumen del altavoz para el módulo de expansión de audio y los satélites (WAC 11). Están todos cableados en paralelo. Tenga en cuenta que el altavoz del WAC 11 tiene un potenciómetro para un ajuste fino del volumen. El rango es de 0 (mín.) a 7 (máx.) o puede estar deshabilitado.

Canal auxiliar	**Módulo de expansión de audio únicamente:** Esta opción debe estar habilitada si los satélites (WAC 11) están conectados a este módulo de expansión. **Nota:** Esta opción, en caso de estar habilitada, enciende los micrófonos satélites. Los altavoces satélites están siempre habilitados, independientemente de la configuración.
RFL	Seleccione la RFL correcta (por defecto: PN 4K7). Esta configuración debería coincidir con el cableado real de la entrada del controlador o módulo de expansión. Consulte *Cableado del sistema* en la página 81.
(Zona) Descripción	Brinde una descripción de la zona asignada.
Tipo de zona	Seleccione el tipo de zona. Consulte *Atributos de zona* en la página 399.
Particiones	Seleccione la partición.
Atributos	Asigne los atributos según corresponda. Consulte *Tipos de zona* en la página 393.
Salidas/Salidas de fuente de alimentación (visibles SOLO para fuente de alimentación inteligente SPCP355.300)	
Salida	La salida numerada. El valor en paréntesis se corresponde con la salida física en la placa de la fuente de alimentación.
Descripción	Proporcione una descripción de la salida.
Cambiar tipo	Cambie el tipo de salida según sea necesario.
Atributos	Asigne atributos a la salida.
Test	Pruebe la salida.
Supervisión salida	Seleccione qué salidas se supervisarán. **Nota:** Antes de habilitar esta opción, deben aplicarse la resistencia en paralelo, el diodo y la carga requerida. El SPCP355.300 debe realizar una calibración antes de que se inicie la supervisión. Consulte *Salidas supervisadas* en la página 64 para obtener más información.
Sólo batería principal	Marque esta casilla si no hay ninguna batería secundaria conectada a la fuente de alimentación.

Cuando se añadan o retiren módulos de expansión, acceda a **Configuración > Hardware > X-BUS > Mapa de cableado y configuración**.

Haga clic en **Reconfigurar** para implementar los cambios.

Cuando hace clic en **Continuar reconfiguración**, se reconfigura el X-BUS completo. Si el módulo de expansión está fuera de línea y pulsa el botón Reconfigurar, el módulo de expansión desaparecerá sin que se notifique al usuario.

Reconfigurar el X-BUS

1. Seleccione **Configuración > Hardware > X-BUS > Mapa de cableado y configuración**.
2. Haga clic en **Reconfigurar**.

Aparecerá la página Aviso(s) – Mapa de cableado del X Bus:

3. Haga clic en **Continuar reconfiguración**.

   Se reconfigurará el X-BUS.

   Si el módulo de expansión está fuera de línea y pulsa el botón Reconfigurar, el módulo de expansión desaparecerá sin que se notifique al usuario.

Consulte también

Cableado del sistema en la página 81

Atributos de zona en la página 399

Tipos de zona en la página 393

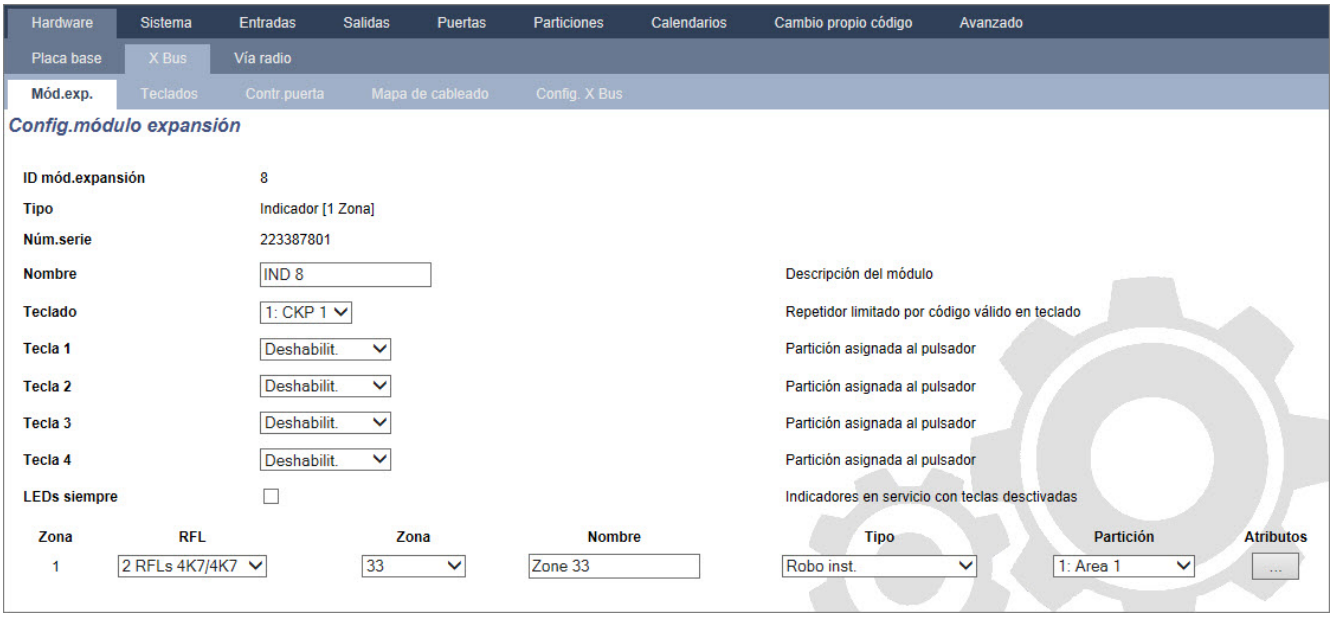
Configuración de un módulo de expansión de indicador

Hay dos modos de configuración posibles para el módulo de expansión de indicador:

- Modo enlazado
- Modo flexible

1. Seleccione **Configuración> Hardware > X-Bus > Módulos expansión**.
2. Haga clic en uno de los parámetros que identifican al indicador.

   Se mostrará la siguiente página para la configuración **Modo enlazado**.



Modo enlazado

1. Introduzca una descripción.
2. Seleccione si el módulo indicador debe estar limitado a un código válido introducido en un teclado.
3. Seleccione las particiones que se deben controlar con las 4 teclas de función.
4. Configure la entrada.

Modo flexible

1. Haga clic en el botón **Modo flexible**.
2. Configure los campos tal como se describe en la siguiente tabla.

Teclas de función	
Partición	Seleccione la partición que se debe controlar con la tecla de función.
Función	Seleccione la función que debe realizar esta tecla en esta partición.
Partición	Seleccione una partición si el módulo indicador está localizado en una partición segura.
Indicación visual	
Indicador	Hay 8 indicadores/luces LED a la derecha y 8 indicadores/luces LED a la izquierda.
Función	La función indicada por esta luz LED.
Función ACT (habilitada)	Seleccione el color y el estado para cada indicador si la función seleccionada está ACT.
Función DES (deshabilitada)	Seleccione el color y el estado para cada indicador si la función seleccionada está DES.
Cambiar función	Haga clic en este botón para cambiar la función de este indicador. La función puede habilitarse o utilizarse para un sistema, partición, zona o conmutador llave.
Indicaciones audibles	
Alarmas	Seleccione si las alarmas deben ser audibles.
Entrada/salida	Seleccione si la entrada/salida debe ser audible.
Pulsación de tecla	Seleccione si la pulsación de teclas debe ser audible.
Desactivación	
Calendario	Seleccione si el módulo de expansión de indicador debe estar limitado por calendario.
Puerta de mapeo	Seleccione si el módulo indicador debe estar limitado por una puerta de mapeo.
Conmutador llave	Seleccione si el módulo indicador debe estar limitado por un conmutador llave.
Teclado	Seleccione si el módulo indicador debe estar limitado a un código PIN válido introducido en un teclado. (consulte advertencia arriba)

Lector de tarjetas	Seleccione si el módulo indicador no debe activarse hasta que se utilice una tarjeta/mando vía radio válido en el lector de tarjetas incorporado.

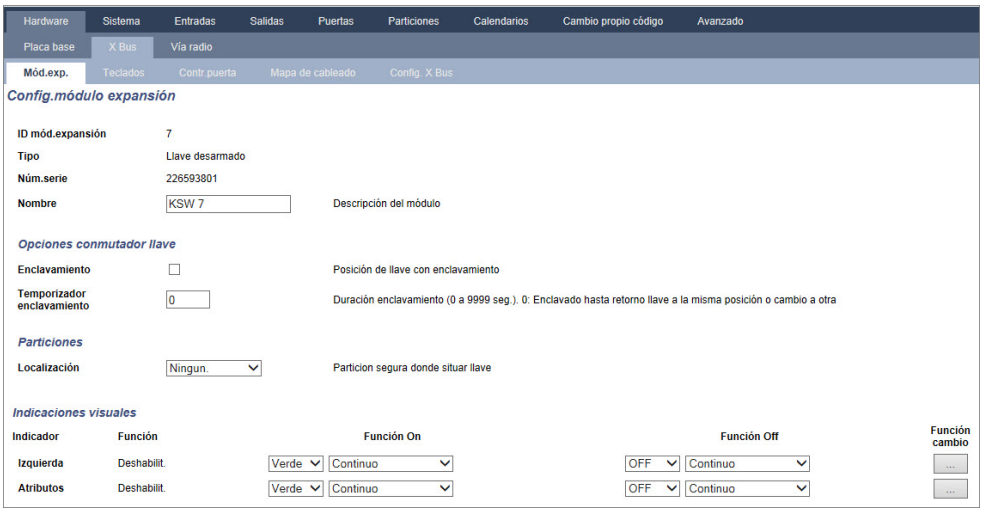
3. Configure la entrada.

ADVERTENCIA: Su sistema no cumplirá las normas EN si habilita una tecla de función para armar el sistema sin que se requiera un código PIN válido.

Configurar un módulo de expansión de conmutador llave

1. Seleccione **Configuración > X-Bus > Módulos expansión**.
2. Haga clic en uno de los parámetros que identifican al conmutador llave.

   Aparece el siguiente cuadro de diálogo.



3. Configure los campos tal como se describe en las siguientes tablas.

Descripción	Introduzca una descripción para el módulo de expansión de conmutador llave.
Opciones de llave	
Enclavamiento	Seleccione si la posición de llave debe tener enclavamiento.
Temporizador de enclavamiento	Introduzca la duración del enclavamiento en segundos (0 a 9999). '0' indica que el enclavamiento finalizará cuando se gire la llave.
Particiones	
Localización	Seleccione la partición en la que se encuentra el conmutador llave.
Indicaciones visuales	
Indicador/Luz LED	Hay 1 indicador/luz LED a la derecha y 1 indicador/luz LED a la izquierda.
Función	La función de este indicador/luz LED.

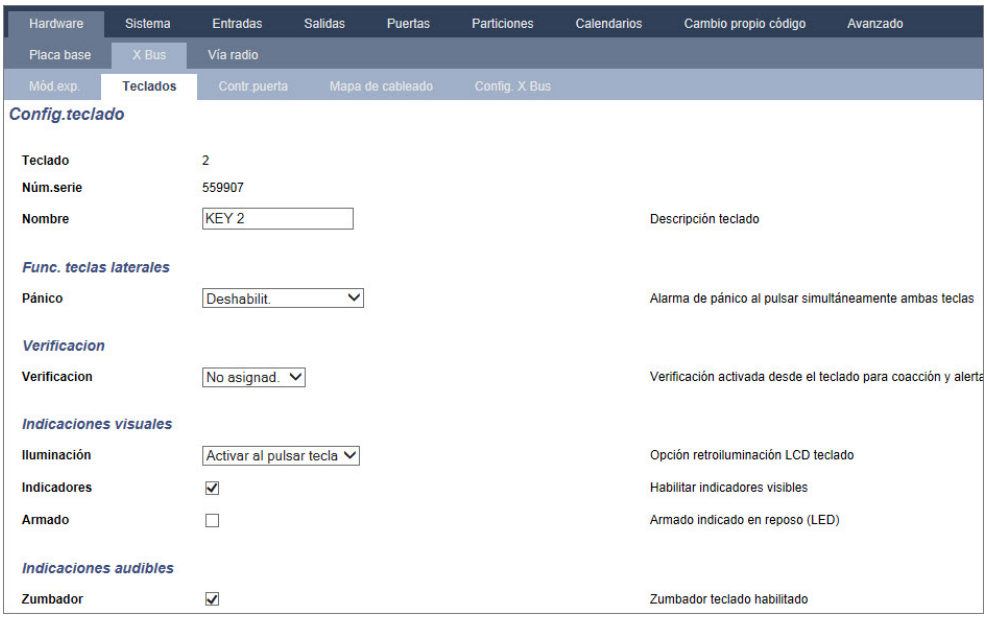
Función ACT (habilitada)	Seleccione el color y el estado para cada indicador si la función seleccionada está ACT.
Función DES (deshabilitada)	Seleccione el color y el estado para cada indicador si la función seleccionada está DES.
Cambiar función	Haga clic en este botón para cambiar la función de este indicador. La función puede habilitarse o utilizarse para un sistema, partición, zona o conmutador llave.
Desactivación	
Calendario	Seleccione si el módulo de conmutador llave debe estar limitado por calendario.
Puerta de mapeo	Seleccione si el módulo de conmutador llave debe estar limitado por una puerta de mapeo.
Salida	
Salida X	Configure y describa las salidas para el conmutador llave. Consulte *Editar una salida* en la página 226 para obtener más detalles.
Funciones del conmutador llave	
Posiciones Centro, Derecha e Izquierda	Seleccione la **Función** que realizará este conmutador llave y la **Partición** relevante. Las funciones de los conmutadores llave son: • Ninguno • Desarmado • Armado parcial A • Armado parcial B • Armado total • Alternar desarmado/armado total • Alternar desarmado/armado parc. A • Alternar desarmado/armado parc. B • Todo OK • Autorización de armado • Anulación ligada

ADVERTENCIA: Su sistema no cumplirá con las normas EN si habilita una tecla de conmutador llave para armar el sistema sin que se requiera un código PIN válido.

17.9.2.2 Teclados

Editar un teclado estándar

1. Seleccione **Configuración > Hardware > X-Bus > Teclados**.
2. Haga clic en uno de los parámetros que identifican al teclado estándar.



3. Configure los campos tal como se describe en la siguiente tabla.

Descripción	Introduzca una descripción única para identificar el teclado.
Teclas de función (en estado de reposo)	
Pánico	Seleccione Habilitar, Deshabilitar o Habilitado silencioso. En caso de estar habilitada, la alarma de pánico se activa al pulsar simultáneamente ambas teclas.
Verificación	Si asigna una zona de verificación al teclado, cuando se dispara una alarma de pánico por pulsar simultáneamente las dos teclas o por introducir un código de coacción, se activan las incidencias de audio y vídeo.
Indicaciones visuales	
Backlight	Seleccione cuándo se enciende la retroiluminación del teclado. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Indicadores	Habilite o deshabilite los LED en el teclado.
Estado armado	Seleccione esta opción si el estado de armado debe indicarse en reposo.
Indicaciones audibles	
Zumbador	Habilite o deshabilite el zumbador en el teclado.
Zumbador armado parcial	Habilite o deshabilite el zumbador de armado parcial durante el tiempo de salida.
Pulsación tecla	Seleccione si se debe activar el volumen del altavoz para las pulsaciones de teclas.
Desactivación	
Calendario	Seleccione si el teclado debe estar limitado por calendario. Consulte *Calendarios* en la página 289.

Puerta de mapeo	Seleccione si el teclado debe estar limitado por una puerta de mapeo.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador llave.
Entrada con dispositivo PACE	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay un dispositivo PACE configurado en el teclado.
Particiones	
Localización	Seleccione la partición segura donde está ubicado el teclado.
Particiones	Seleccione las particiones que pueden ser controladas por el teclado.
Opciones	
Retardo armado total	Seleccione para configurar un armado con retardo en todos los teclados. Se ignora la ubicación del teclado y todas las particiones realizarán una cuenta regresiva del tiempo de salida total.

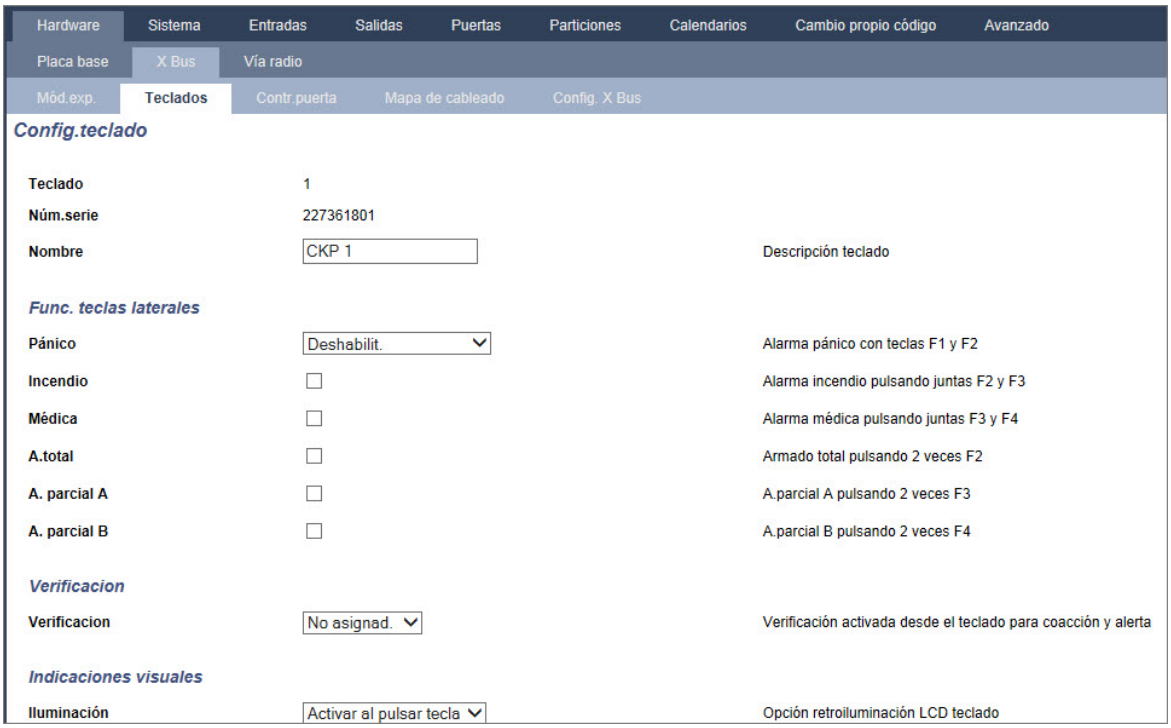
AVISO: Una partición debe estar asignada a un teclado solo si el teclado está dentro de la partición asignada y si la ruta de entrada/salida está definida. Si se asigna una partición, cuando esa partición en particular se arme o desarme, se utilizarán los temporizadores de entrada y salida (en caso de estar configurados). También estarán disponibles otras funciones relacionadas con las rutas de entrada/salida. Si no hay una partición asignada, la partición se armará o desarmará inmediatamente y las otras funciones de entrada/salida no estarán disponibles.

Consulte también

Calendarios en la página 289

Editar un teclado Comfort

1. Seleccione **Configuración > Hardware > X-Bus > Teclados**.
2. Haga clic en uno de los parámetros que identifican al teclado Comfort.



3. Configure los campos tal como se describe en la siguiente tabla.

Descripción	Introduzca una descripción única para identificar el teclado.
Teclas de función (en estado de reposo)	
Pánico	Seleccione Habilitar, Deshabilitar o Habilitado silencioso. En caso de estar habilitada, la alarma de pánico se activa al pulsar simultáneamente F1 y F2.
Incendio	Habilite esta opción para que la alarma de incendio se active al pulsar simultáneamente F2 y F3.
Alarma médica	Habilite esta opción para que la alarma médica se active al pulsar simultáneamente F3 y F4.
Armado total	Habilite esta opción para que el armado total se active al pulsar F2 dos veces.
Armado parcial A	Habilite esta opción para que el armado parcial A se active al pulsar F3 dos veces.
Armado parcial B	Habilite esta opción para que el armado parcial B se active al pulsar F4 dos veces.
Indicaciones visuales	
Backlight	Seleccione cuándo se enciende la retroiluminación del teclado. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Intensidad de retroiluminación	Seleccione la intensidad de la retroiluminación. Rango de 1 a 8 (alto).
Indicadores	Habilite o deshabilite los LED en el teclado.

Estado armado	Habilite esta opción si el estado de armado debe indicarse en reposo. (LED)
Marca	Seleccione esta opción si el logo debe estar visible en reposo.
Reloj analógico	Seleccione la posición del reloj en caso de estar visible en reposo. Las opciones son: Alineado a la izquierda, Centrado, Alineado a la derecha o Deshabilitado.
Teclas de emergencia	Habilite esta opción si las teclas de función de Pánico, Incendio o Emergencia médica deben aparecer indicadas en la pantalla LCD.
Armado directo	Habilite esta opción si las teclas de función de Armado total/Armado parcial deben aparecer indicadas en la pantalla LCD.
Icono de humano	Habilite esta opción si se debe indicar la puerta de mapeo.
Indicaciones audibles	
Alarmas	Seleccione el volumen del altavoz para las indicaciones de alarma o deshabilite el sonido.
Entrada/salida	El rango es de 0 a 7 (volumen máx.)
Chime	Seleccione el volumen del altavoz para las indicaciones de entrada y salida o deshabilite el sonido.
Pulsación tecla	El rango es de 0 a 7 (volumen máx.)
Mensajes hablados	Seleccione el volumen del altavoz para el chime o deshabilite el sonido.
Zumbador armado parcial	El rango es de 0 a 7 (volumen máx.)
Modo silencioso	Habilite esta opción para deshabilitar el zumbador durante la entrada y la salida cuando el teclado está en una partición armada. **NOTA:** El zumbador del teclado sólo será audible para entrada/salida/armado/desarmado si la partición es la misma en la que se encuentra el teclado o si el teclado está realizando la operación.
Desactivación	
Calendario	Seleccione si el teclado debe estar limitado por calendario. Consulte *Calendarios* en la página 289.
Puerta de mapeo	Seleccione si el teclado debe estar limitado por una puerta de mapeo.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador llave.
Entrada con dispositivo PACE	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay un dispositivo PACE configurado en el teclado.
Particiones	

Localización	Seleccione la partición segura donde está ubicado el teclado.
Particiones	Seleccione las particiones que pueden ser controladas por el teclado.
Opciones	
Retardo armado total	Seleccione para configurar un armado con retardo en todos los teclados. Se ignora la ubicación del teclado y todas las particiones realizarán una cuenta regresiva del tiempo de salida total.
Nivel de acceso en teclado	Seleccione el nivel de acceso en teclado (1 a 3). Nivel 1: Todas las funciones Nivel 2: Sólo armado, desarmado y restauración Nivel 3: Sólo ver

AVISO: Una partición debe estar asignada a un teclado solo si el teclado está dentro de la partición asignada y si la ruta de entrada/salida está definida. Si se asigna una partición, cuando esa partición en particular se arme o desarme, se utilizarán los temporizadores de entrada y salida (en caso de estar configurados). También estarán disponibles otras funciones relacionadas con las rutas de entrada/salida. Si no hay una partición asignada, la partición se armará o desarmará inmediatamente y las otras funciones de entrada/salida no estarán disponibles.

17.9.2.3 Controladores de puertas

Editar un controlador de puerta

1. Seleccione **Configuración > Hardware > X-BUS > Controladores de puerta**.
2. Haga clic en uno de los datos marcados en azul (por ejemplo: número de serie).

3. Configure los campos tal como se describe en la siguiente tabla.

Para nombrar e identificar:

En una configuración en lazo, cada módulo de expansión está numerado de forma consecutiva desde el primero (módulo de expansión conectado a 1A 1B en el controlador) al último (módulo de expansión conectado a 2A 2B en el controlador).

Ejemplo para SPC63xx: Los módulos de expansión, cuando están enumerados de 1 a 63, son zonas asignadas (en grupos de 8) en identidades subsiguientes de 1 a 512 (el número más alto en la identificación de zonas es 512). Por lo tanto, todo módulo de expansión con nombre o identificado por un número mayor que 63 no tiene zonas asignadas.

ID mód. expansión	El ID del controlador de puerta configurado con los interruptores rotativos.
Tipo	Tipo de controlador de puerta.
Núm.serie	Número de serie del controlador de puerta.
Descripción	Descripción del controlador de puerta.
E/S puerta 1 E/S puerta 2	• Si una puerta está asignada a la E/S de puerta, seleccione el número de puerta correspondiente. Si las dos entradas y salidas son configurables, seleccione **Zonas/Salidas**. • Si se selecciona un número de puerta para la E/S de puerta, puede cambiar los ajustes de puerta haciendo clic en el botón Editar. Esto es como navegar hasta **Ajustes > Puertas**. • Si la opción **Zonas/Opciones** está seleccionada, puede configurar las dos zonas y la salida haciendo clic en el botón Editar.
Perfil 1	Para lectores con LED verde y rojo.
Perfil 2	Para lectores VANDERBILT con LED amarillo (AR618X).
Perfil 3	El Perfil 3 se utiliza con lectores HID que envían un código PIN a la central como una lectura de tarjeta con un código de lugar predefinido (0).
Perfil 4	El Perfil 4 se utiliza con lectores HID que envían un código PIN a la central como una lectura de tarjeta con un código de lugar predefinido (255).
Perfil 5	Seleccionar para activar los lectores Sesam. También es recomendable seleccionar la opción «Anulación LEDs Lector» para proporcionar información sobre el proceso de configuración.

Editar zonas/salidas para E/S de puerta

1. Seleccione la zona/salida para la E/S de puerta.
2. Haga clic en el botón **Editar**.
3. Las 2 entradas y la salida que pertenecen a la E/S de esta puerta pueden configurarse como entradas y salidas de puertas normales. Consulte *Editar una puerta* en la página 283.
4. Para poder utilizar las entradas, deben estar asignadas a un número de zona.

17.9.2.4 Config. cabl.

Para ver una lista de los módulos de expansión y teclados en el orden en que han sido configurados en el sistema SPC:

- Seleccione **Configuración > Hardware > X-BUS > Mapa de cableado y configuración**.

  Se mostrará la siguiente página:

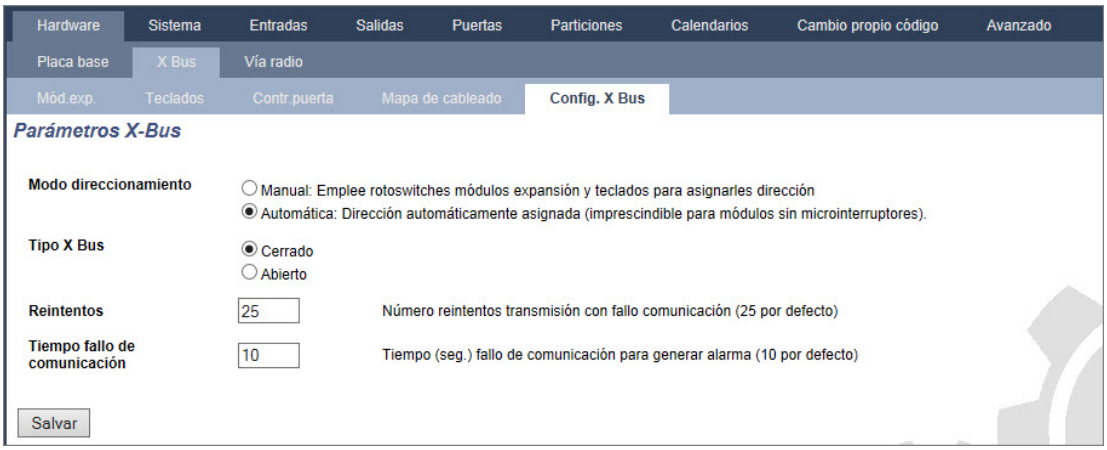
Para obtener más información sobre la interfaz X-BUS, consulte *Cableado de la interfaz X-BUS* en la página 81.

17.9.2.5 Ajustes

Para configurar las conexiones X-BUS:

1. Seleccione **Configuración > Hardware > X-BUS > Config. X-BUS**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

Modo direccionamiento	Seleccione si los módulos de expansión/teclados están direccionados manual o automáticamente en el X-BUS.
Tipo de X Bus	Seleccione una configuración en lazo o en punta.
Reintentos	El número de veces que el sistema intenta retransmitir datos en la interfaz X-BUS antes de generar un fallo de comunicación. (1–99: por defecto, 25)
Temporizador de comunicación	El período de tiempo antes del registro de un fallo de comunicación.

17.9.3 Vía radio

La detección con sensores vía radio (868 MHz) en la central PSC se realiza mediante módulos receptores vía radio que pueden venir montados de fábrica en el teclado o el controlador, o instalando un módulo de expansión vía radio.

1. Seleccione **Configuración > Hardware > Vía radio > Vía radio**.

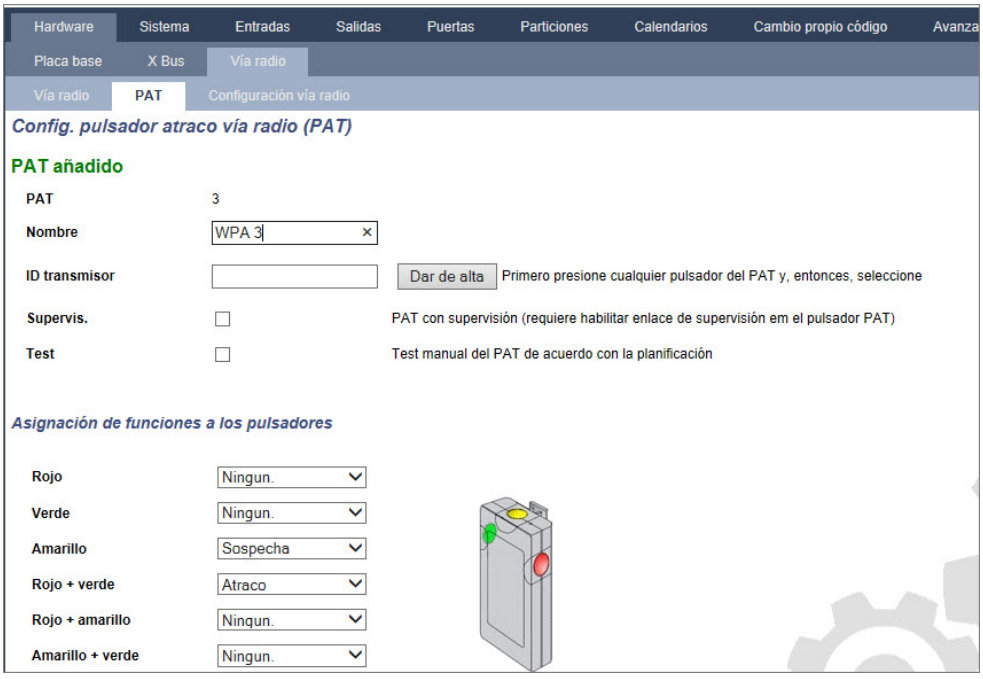
2. Consulte la tabla a continuación para obtener más información.

Sensor	El número del sensor registrado en el sistema (1 = primero; 2 = segundo; etc.).
ID	Un número de identidad único para ese sensor.
Tipo	El tipo de sensor vía radio detectado (contacto magnético, inercial/shock, etc.).
Zona	La zona a la cual ha sido dado de alta el sensor.
Batería	El estado de la batería conectada al sensor (si aplica).
Supervisar	El estado de la operación de supervisión (OK = señal de supervisión recibida; Sin supervisión = sin operación de supervisión).
Señal	La intensidad de la señal recibida desde el detector (01=baja, 09=alta). **Nota:** Aunque no es posible dar de alta un dispositivo con una intensidad de señal inferior a 3, los dispositivos cuya señal cae por debajo de 3 después de su registro no se anulan.

Acciones ejecutables

Registro	Haga clic para ver el Registro de sensor vía radio. Consulte *Registro - Sensor vía radio X* abajo.
Dar de alta	Haga clic para abrir la lista de dispositivos vía radio sin estar dados de alta.

1. Seleccione **Configuración > Hardware > Vía radio > APR**.
2. Se muestran la identidad de cada APR registrada y el estado.



17.9.3.1 Registro - Sensor vía radio X

Para ver un registro rápido de las incidencias para un sensor vía radio:

1. Haga clic en el botón **Registro**.
2. Consulte la tabla a continuación para obtener más información.

Fecha/Hora	La fecha y la hora de la incidencia registrada.
Receptor	La ubicación del receptor vía radio, es decir, el módulo vía radio montado en el teclado, controlador o módulo de expansión vía radio.
Señal	La intensidad de la señal recibida desde el detector (01=baja, 09=alta).
Estado	El estado físico del detector.
Batería	El estado de la batería conectada al sensor (OK, Fallo).

3. Cree un archivo de texto del registro haciendo clic en **Archivo de texto**.

17.9.3.2 Configuración de APR

AVISO: La configuración de una APR y la página de estado se muestran solo si cuenta con un módulo vía radio en la central o si alguno de los módulos de expansión y la central tiene licencia para el tipo de módulo utilizado.

No se asignó una APR a un usuario. Generalmente, varias personas comparten una APR (por ejemplo, guardias de seguridad que trabajan en turnos) o, alternativamente, las APR pueden estar ancladas de forma permanente a una superficie, como debajo de un escritorio o detrás de una caja registradora.

Se permite un máximo de 128 APR por central.

Para configurar una APR desde el navegador:

- Seleccione el modo técnico completo y luego seleccione las siguientes opciones **Configuración > Hardware > Vía radio > APR**.

Los siguientes elementos se deben verificar o configurar desde esta página:

- **Estado batería**

  La central recibe el estado de la batería desde la APR en cada imagen. El estado de la batería puede ser OK o Baja.

  El control de la batería requiere una APR con la revisión E-PC138612 o posterior de la placa.

- **Estado de supervisión**

  El estado de supervisión puede ser:

  – Fallo
  La central no ha recibido un mensaje de supervisión de la APR en el período configurado en la página Configuración vía radio.

  – Deshabilitado
  La supervisión no está configurada.

  – ACEPTAR
  La supervisión se está transmitiendo normalmente.

- **Estado del test**

  El estado del test puede ser:

  – Vencido
  La APR no ha sido comprobada en el período configurado en la página Configuración vía radio.

  – Deshabilitado
  La supervisión no está configurada.

  – ACEPTAR
  El test APR es correcto.

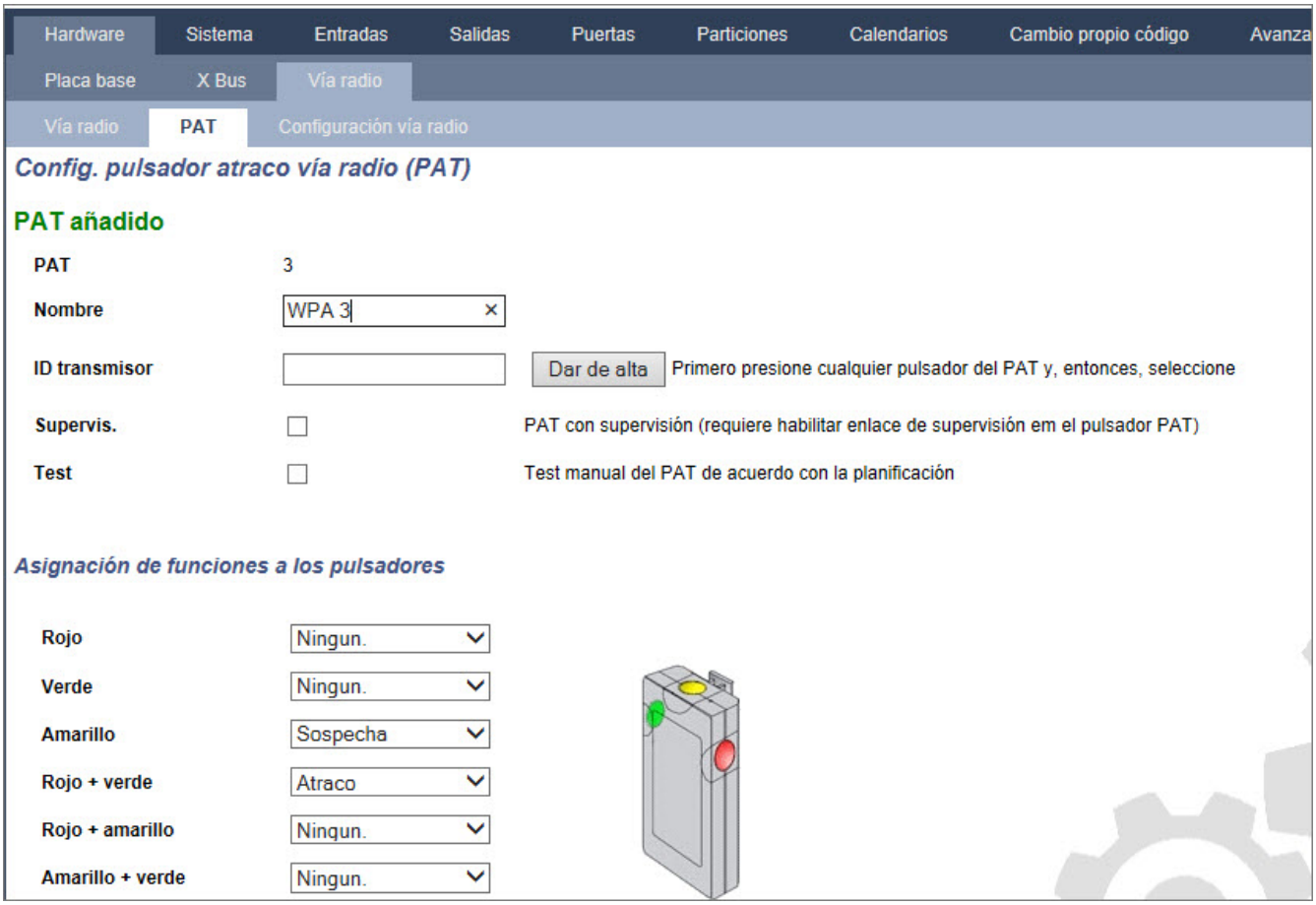
1. Haga clic en el botón **Editar** para editar la configuración de la APR.
2. Haga clic en el botón **Eliminar** para eliminar una APR del sistema.

Añadir una APR

Para añadir una APR al sistema:

1. Haga clic en el botón **Añadir** en la página de estado y de configuración de la APR principal.

   Se abrirá la página **Configurar APR** para la nueva APR.



2. Configure la APR con los siguientes detalles:

Descripción/Nombre	Introduzca una descripción o nombre para identificar la APR.
ID de transmisor	El ID de transmisor está impreso en la carcasa del APR y puede introducirlo manualmente aquí. También puede identificar el ID de forma remota al presionar cualquier botón de la APR y hacer clic en el botón **Alta**. La central introduce automáticamente este ID en el campo siempre que no haya otra APR definida.
Supervisar	Puede configurar la APR para que envíe señales de supervisión periódicas. La supervisión está habilitada en la APR mediante un puente. La función de supervisión también debe estar habilitada en la central para la APR específica para que pueda llevarse a cabo correctamente. Si la central no recibe la señal de supervisión, emite una alarma que aparece en el teclado y queda registrada. Si no se habilita la supervisión, la APR envía un mensaje de supervisión cada 24 horas para transmitir el estado de la batería de la APR a la central. Este mensaje también se envía de forma aleatoria para reducir las probabilidades de cruce con otras APR. Marque la casilla **Supervisar** si se habilitó la supervisión para esa APR específica.
Test	Marque la casilla **Test** si se requiere un test de APR periódico. El período de tiempo para los tests periódicos se configura en la página **Cambiar configuración vía radio** (consulte la página *Cambiar la configuración vía radio* en la página siguiente).
Asignación de botones	Use esta sección para asignar funciones a las combinaciones de botones. Las funciones disponibles son Pánico, Pánico silencioso, Atraco, Sospecha, Salida RF usuario y Alarma médica. Puede seleccionar más de una combinación para la misma función. La configuración por defecto para una instalación financiera es: • Amarillo - Sospecha • Rojo + Verde - Atraco Para instalaciones comerciales o domésticas, la configuración por defecto es: • Rojo + Verde - Pánico **Nota:** Si una combinación de botones no tiene asignada ninguna función, aún es posible usar esta combinación mediante un disparador. Consulte *Disparadores* en la página 295.

3. Haga clic en el botón **Salvar** para salvar la configuración.

Consulte también

Cambiar la configuración vía radio en la página siguiente

Cambiar la configuración vía radio en la página siguiente

Disparadores en la página 295

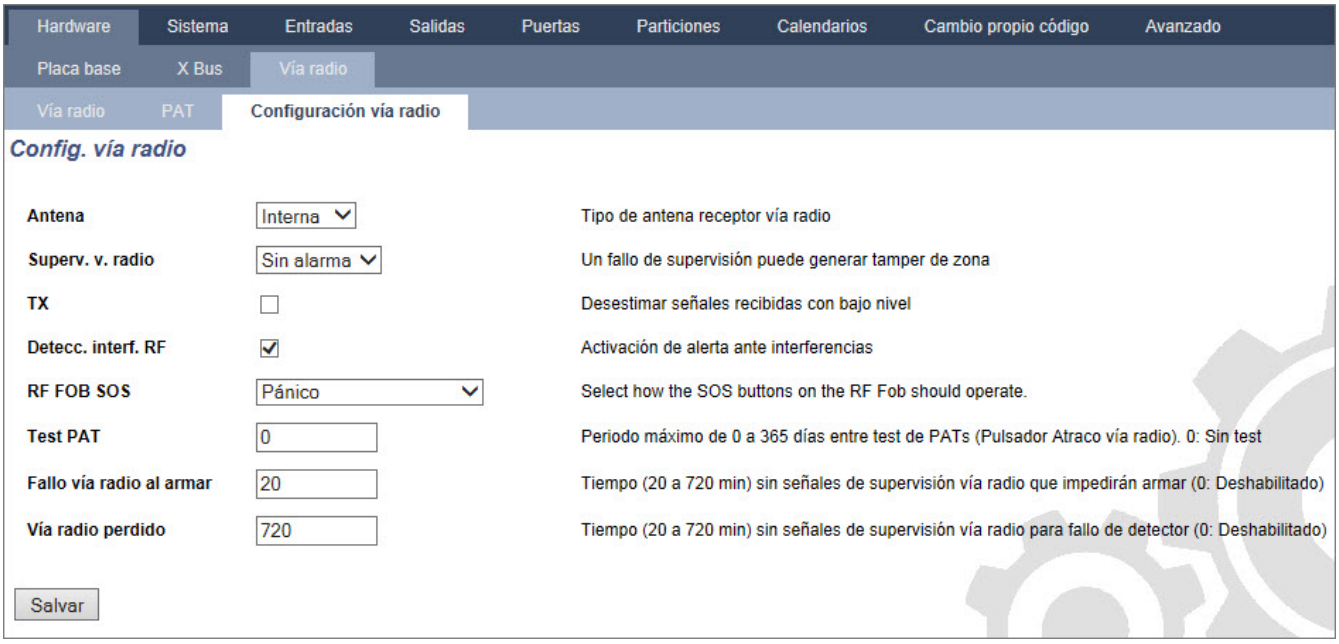
Editar una APR

Para editar una APR, haga clic en el botón **Editar** en la página de estado y de configuración de la APR principal.

La página **Editar** es similar a la página **Añadir** con la excepción de que no incluye el botón **Alta** para introducir el ID de la APR de forma automática.

17.9.3.3 Cambiar la configuración vía radio

1. Seleccione **Configuración > Hardware > Vía radio > Configuración vía radio**.



2. Consulte la tabla a continuación para obtener más información.

Antena	Seleccione el tipo de antena conectada al módulo vía radio (interno o externo) del menú desplegable. El tipo de antena requerido para el módulo vía radio depende del tipo de módulo vía radio que se utilice.
Supervisión	Seleccione en caso de que un sensor vía radio informado como perdido registre una condición de tamper en la central de SigNET. Se informa que falta un sensor vía radio cuando no se ha recibido ninguna señal de supervisión de ese receptor durante un período superior al programado en el temporizador **Sensor vía radio faltante**. Consulte *Temporizaciones* en la página 266.
Filtro	Marque para filtrar las señales de RF de baja intensidad.
Detección de interferencia RF	Marque para activar una alerta en caso de que se detecte interferencia RF.
Test PAT	Seleccione cómo deben operar los botones de SOS en el mando vía radio de RF: • Inhibir • Enable (habilitar) • Habilitado silencioso • Alarma médica usuario • Alarma de atraco usuario • Salida RF
Cronograma de test de APR	Introduzca el período máximo (en días) entre los test de APR.
Tiempo de impedimento de armado	Introduzca el tiempo en minutos tras el cual, si un sensor no envía informes, se debe impedir el armado para una partición donde está la zona vía radio. Esta configuración solamente se aplica para las siguientes zonas de intrusión. • Alarma • Entrada/salida • Robo fin salida • Pánico • Atraco • Tamper • Superv.llave • Sísmico • Todo OK • Autorización de armado • Elemento bloqueo

Tiempo de pérdida de dispositivo	Introduzca la cantidad de minutos tras la cual el dispositivo vía radio (sensor o APR) debe informarse como perdido.

17.9.4 Cambiar la configuración del sistema

Esta sección abarca:

17.9.4.1 Opciones

1. Seleccione **Configuración > Sistema > Opciones del sistema**.
2. Configure los campos tal como se describe en la siguiente tabla.

Opciones del sistema

Las opciones que se muestran varían según el grado de seguridad del sistema.

Restricciones	Opciones del sistema	Descripción
Configuración general		
	Particiones	Seleccione esta opción para habilitar múltiples particiones en el sistema. **Nota:** Esta opción solo se muestra para las instalaciones de tipo Doméstica e Industrial.
	Reposición código	Sólo grado 3: Un usuario sin atribución de restaurar una alarma puede hacerlo con esta función. Para resetear una alarma, se requiere un código de 6 dígitos. El usuario debe llamar al instalador para generar un código de restauración con el que el usuario restaurará la alarma.
	Tamper fuera de línea	Habilite esto para las zonas de módulos de expansión fuera de línea para generar un tamper de zona.
	Reset alarma mando	Si esta opción está habilitada, el mando vía radio se habilita para restaurar las alertas al pulsar la tecla Desarmar.
Web únicamente	LED del módulo de expansión de audio	En caso de estar habilitada esta opción, el módulo de expansión de audio no encenderá la luz LED cuando el micrófono esté activo.
	Informe en modo técnico	Si esta opción está habilitada, la central siempre notificará las activaciones de alarmas y las alarmas de pánico.
	Salidas en modo técnico	Si se selecciona esta opción, las siguientes opciones no estarán desactivadas en el modo Técnico total: • Salidas de controlador • Salidas de módulo de expansión • Luces LED de indicador • Luces LED de conmutador de llave
	Alarma con fallo TX	Con «fallo TX» se activarán las sirenas.

Restricciones	Opciones del sistema	Descripción
	Redisparo coacción	Si esta opción está habilitada, las alarma de coacción volverá a dispararse.
	Redisparo pánico	Si esta opción está habilitada, las alarma de pánico volverá a dispararse.
	Anular perfil de lector	Si esta opción está habilitada, la central controlará el comportamiento de los LED de los lectores.
	Silencio con verificación audio	Si esta opción está habilitada, las sirenas internas y externas (sistema y partición), los zumbadores del teclado y los mensajes del teclado Comfort quedarán silenciados durante la verificación de audio.
	Modo salida watchdog	Habilita la salida 6 de la placa del controlador SPC para su uso con fines de supervisión. Se pueden seleccionar los siguientes modos de funcionamiento de la salida watchdog: • Inhibir — La salida 6 está disponible como salida para fines generales. • Habilitada — La salida 6 está normalmente desactivada, pero se activa cuando se produce un fallo de watchdog. • Intermitente — La salida 6 parpadea a intervalos de 100 ms. • Habilit. invertido — La salida 6 está normalmente activada, pero se desactiva cuando se produce un fallo de watchdog. Las siguientes opciones combinan la opción Habilitada con la transmisión del fallo de hardware en caso de producirse un fallo importante de microprocesador. Si se produce un fallo de este tipo, se envía una incidencia SIA a la CRA1. **Nota:** La CRA debe configurarse para utilizar SIA y SIA Extendido 1 o 2. Este método de transmisión no admite CID ni FF. • Habilitada + transmisión (10 s) — La incidencia de fallo se envía a la CRA1 10 segundos después de detectarse el fallo. Esta opción debe utilizarse para cumplir con VdS 2252. • Habilitada + transmisión (60 s) — La incidencia de fallo se envía a la CRA1 60 segundos después de detectarse el fallo. La incidencia SIA informada es HF y SIA Extendido transmite **Fallo hardware**. **Nota:** Los fallos de hardware no se transmiten si el Técnico ha accedido al sistema. Para obtener más información sobre las CRA, consulte *Central de recepción de alarmas (CRA)* en la página 333.
	SPCP355	Se habilita la alimentación de VdS. En las instalaciones VdS, esta opción se selecciona automáticamente.
	Sirena por fallo al armar (FTS)	Habilite esta opción para activar la sirena interna si el sistema falla al armar.
	Flash por fallo al armar (FTS)	Habilite esta opción para activar el flash si el sistema falla al armar.

Restricciones	Opciones del sistema	Descripción
⏻	Ocultar anulación	Si esta opción está habilitada, los mensajes de anulación ya no se mostrarán en el teclado.
	Capacidad de la batería	Capacidad total de todas las baterías, sólo para la central (3 a 100 Ah). Debe introducir este valor en el campo **Corriente máxima** para ver el tiempo de batería restante en el teclado en caso de fallo de la red de CA. Esto se indica en el menú ESTADO > BATERÍA > DURACIÓN BATERÍA.
	Corriente máxima	Consumo total de corriente de las baterías (30 a 20.000 mA) ante un fallo en la red de CA. Debe introducir este valor en el campo **Capacidad de la batería** para ver el tiempo de batería restante en el teclado en caso de fallo de la red de CA. Esto se indica en el menú ESTADO > BATERÍA > DURACIÓN BATERÍA.
Armado parcial		
	Renombre Armado parcial A	Introduzca el nombre nuevo para el modo ARMADO PARCIAL A (por ejemplo: modo nocturno).
	Renombre armado parcial B	Introduzca el nombre nuevo para el modo ARMADO PARCIAL B (por ejemplo: Piso 1).
Alarma		
	Sirena primero	Habilite esta opción para activar las sirenas correspondientes en caso de una alarma sin confirmar. Cuando esta opción está deshabilitada, las sirenas correspondientes solo se activarán cuando se confirme una alarma o si se reactiva el detector que causó la alarma sin confirmar.
	Redisparo sirena	Habilite esta opción para disparar nuevamente las sirenas en caso de que se detecte una segunda activación de zona (una vez que el tiempo de la sirena haya pasado). Si no se habilita esta opción, las sirenas exteriores se dispararán solo una vez.
⏻ Web únicamente	Impedir armado tras alerta	Si esta opción está habilitada, un usuario no puede armar una partición si hay una alerta de sistema o partición presente en el sistema. **Nota:** Esta opción solo está disponible cuando la región seleccionada en **Normas > Región** es Suiza o el **Grado de seguridad** seleccionado es 'Libre'.
	Reset tras desarmado	Habilite esta opción para que las alertas se borren automáticamente después de 30 segundos en modo Desarmado. **Nota:** Para cumplir con la norma PD6662, se debe deshabilitar esta opción.

Restricciones	Opciones del sistema	Descripción
	Antienmascaramiento con armado	Seleccione el tipo de incidencia informada resultante de la detección de antienmascaramiento cuando la central está armada. Las opciones son Deshabilitar, Tamper, Problema o Alarma. Puede configurar esta opción cuando la central está en modo 'Libre'. En el modo Grado 2 o 3, el tipo de incidencia informada será conforme a los estándares de la región seleccionada: • Irlanda - Alarma • Resto de regiones - Alarma
	Antienmascaramiento con desarmado	Seleccione el tipo de incidencia informada resultante de la detección de antienmascaramiento cuando la central está desarmada. Las opciones son Deshabilitar, Tamper, Problema o Alarma. Puede configurar esta opción cuando la central está en modo 'Libre'. En el modo Grado 2 o 3, el tipo de incidencia informada será conforme a los estándares de la región seleccionada: • Irlanda - Deshabilitada • Resto de regiones - Tamper
	Desarmado fuera de limites RFL	Seleccione el tipo de incidencia notificada resultante de la detección de Fuera del límite RFL cuando la central está desarmada. Las opciones son: Deshabilitar, Tamper y Problema. Puede configurar esta opción cuando la central está en modo 'Libre'. En el modo Grado 2 o 3, el tipo de incidencia informada será conforme a los estándares de la región seleccionada: • Alemania VdS - Tamper • Resto de regiones - Problema
	Armado fuera de límites RFL	Seleccione el tipo de incidencia notificada resultante de la detección de Fuera del límite RFL cuando la central está armada. Las opciones son: Deshabilitar, Tamper y Problema. Puede configurar esta opción cuando la central está en modo 'Libre'. En el modo Grado 2 o 3, el tipo de incidencia informada será conforme a los estándares de la región seleccionada: • Alemania VdS - Tamper • Resto de regiones - Problema
	Zona inestable desarmado	Seleccione el tipo de incidencia notificada resultante de la detección de zona inestable cuando la central está desarmada. Las opciones son: Deshabilitar, Tamper y Problema. Una zona es inestable si no se puede obtener una muestra simple en un plazo de 10 segundos. Puede configurar esta opción cuando la central está en modo 'Libre'. En el modo Grado 2 o 3, el tipo de incidencia informada será conforme a los estándares de la región seleccionada: • Alemania VdS - Tamper • Resto de regiones - Problema

Restricciones	Opciones del sistema	Descripción
⏻	Zona inestable armado	Seleccione el tipo de incidencia notificada resultante de la detección de zona inestable cuando la central está armada. Las opciones son: Deshabilitar, Tamper y Problema. Una zona es inestable si no se puede obtener una muestra simple en un plazo de 10 segundos. Puede configurar esta opción cuando la central está en modo 'Libre'. En el modo Grado 2 o 3, el tipo de incidencia informada será conforme a los estándares de la región seleccionada: • Alemania VdS - Tamper • Resto de regiones - Problema
	Final de línea (RESIST. FL)	Seleccione los RFL de terminación que se aplicarán o bien a todas las zonas del sistema o a las nuevas zonas que se añadan al mismo. Seleccione un valor para habilitar la característica adecuada. Para aplicar un nuevo ajuste de RFL a todas las zonas existentes, marque la casilla Actualizar todas las zonas. Si modifica el valor de RFL pero no marca esta casilla, el nuevo ajuste solo se aplicará a las zonas añadidas después de modificar el valor.
⏻	Tolerancia RFL	Si esta opción está habilitada, se utilizan bandas anchas de RFL.
	Sospecha audible	Si esta opción está habilitada, las alertas de sospecha APR tienen indicadores audibles y visuales en los teclados (modo financiero únicamente).
	Test sísmico al armar	Si esta opción está habilitada, todos los sensores sísmicos de cualquier partición que se arme serán comprobados antes de que la partición o el sistema se arme (modo financiero únicamente).
⏻	Restauración automática	Habilite esta función para restaurar automáticamente las alertas en el sistema. Es decir, cuando la zona abierta que disparó una alarma se cierra, no se requiere una restauración manual en el teclado/navegador. Si esta opción está deshabilitada, evita que el usuario restaure las alarmas al resetear la entrada que disparó la alerta.
⏻	Alarma al salir	**Habilitado:** Si se activa una zona de no entrada/salida durante la cuenta atrás del temporizador de salida, se generará una alarma local sonando las campanas. **Deshabilitado:** Si se activa una zona de no entrada/salida durante la cuenta atrás del temporizador de salida, no se generará una alarma. **Nota:** Esta opción solo se muestra cuando está seleccionado el **Modo libre**, pues la habilitación no está conforme con la norma EN50131. Cuando usted elige la **región** de Suiza o Bélgica en **Configuración requisitos estándar**, esta opción se habilita automáticamente pero no está visible en **Opciones**.

Restricciones	Opciones del sistema	Descripción
	Alarma en entrada	**Habilitado:** Si se activa una zona de no entrada/salida durante la cuenta atrás del temporizador de entrada, se generará una alarma local sonando las campanas. **Deshabilitado:** Si se activa una zona de no entrada/salida durante la cuenta atrás del temporizador de entrada, no se generará una alarma. **Nota:** Esta opción solo se muestra cuando está seleccionado el **Modo libre**, pues la habilitación no está conforme con la norma EN50131. Cuando usted elige la **región** de Suiza en **Configuración requisitos estándar**, esta opción se habilita automáticamente pero no está visible en **Opciones**.

Restricciones	Opciones del sistema	Descripción
Confirmación		

Restricciones	Opciones del sistema	Descripción
⏻	Confirmación	La variable Confirmación determina cuándo se debe considerar que una alarma está confirmada. • BS8243: Impone el cumplimiento de los requisitos de la Policía británica y se trata de una obligación específica para las instalaciones comerciales británicas. Este requisito estipula que una alarma sólo se considerará confirmada si cumple las siguiente condición: Que después de activarse una alarma de zona inicial, y antes de que caduque el tiempo de confirmación de alarma, se active una segunda alarma de zona. El tiempo de confirmación de alarma debe ser de entre 30 y 60 minutos. (Consulte *Temporizaciones* en la página 266). Si no se activa una segunda alarma en zona dentro del tiempo de confirmación de alarma, la primera alarma de zona se inhibirá. La opción de confirmación BS8243 estará configurada automáticamente cuando la opción **Normas > Región** esté ajustada en Reino Unido. • Garda: Impone las directrices para alarmas confirmadas requeridas por la Garda (Policía) irlandesa. El requisito estipula que se considerará que una alarma está confirmada tan pronto como se activa una segunda alarma en el sistema dentro del período de armado de la primera alarma. La opción de confirmación Garda estará configurada automáticamente cuando la opción **Normas > Región** esté ajustada en Irlanda. • EN-50131-9 Impone el cumplimiento de la norma EN-50131-9 y de la «Orden INT/316/2011, de 1 de febrero, sobre el funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada» en España. Este requisito estipula que una alarma sólo se considerará confirmada si cumple las siguientes condiciones: - 3 activaciones de zona en 30 minutos (por defecto), dos de las cuales podrán proceder del mismo dispositivo si las activaciones son de diferentes tipos, p. ej.: alarma/tamper. - 1 activación de alarma seguida de un fallo del ATS[1] en un plazo de 30 minutos (por defecto). - Fallo del ATS seguido de una situación de tamper o de alarma en un plazo de 30 minutos (por defecto). Si caducan los 30 minutos y la zona se restablece a su estado físico normal, las alertas de la zona se restaurarán si un usuario de nivel 2 puede hacerlo. En este caso, la zona aceptará una nueva situación de alerta que provocará una nueva activación. Como alternativa, si la zona no se ha restaurado a su estado físico normal, dicha zona se inhibirá, siempre y cuando tenga permiso para ello. Si vuelve a producirse una alerta (STA) después de un período de 30 minutos (por defecto), el temporizador de 30 minutos se reiniciará. La opción de confirmación EN50131-9 estará configurada automáticamente cuando la opción **Normas > Región** esté ajustada en España. • VDS

Restricciones	Opciones del sistema	Descripción
		Esta opción impone el cumplimiento de la norma VdS.
Teclado		
ⓘ	Mostrar siempre el estado (MOSTRAR ESTADO)	Si esta opción está habilitada, el estado de armado del sistema (armado total/armado parcial/desarmado) se mostrará de forma permanente en la línea inferior de la pantalla del teclado. Si esta opción esta desmarcada, el estado de armado desaparecerá del teclado después de 7 segundos.
	Mostrar zonas abiertas	Si esta opción está habilitada, las zonas abiertas se mostrarán en el teclado en modo Desarmado.
	Mostrar mensaje CRA	Si esta opción está habilitada, el mensaje de la CRA se mostrará durante 30 segundos tras el desarmado, si se ha informado la alarma confirmada.
	Línea 1 mensaje teclado	Línea 1 mensaje CRA (16 caracteres).
	Línea 2 mensaje teclado	Línea 2 mensaje CRA (16 caracteres).
	Mostrar cámaras	Si esta opción está habilitada, se mostrarán las cámaras fuera de línea en el teclado en modo Desarmado.
	Registrar accesos teclado	Habilite esta opción para registrar el acceso al teclado por parte de usuarios (intentos de inicio de sesión exitosos y fallidos).
	Idioma en reposo	Seleccione el idioma que se mostrará en reposo. • Idioma del sistema: el idioma en que se mostrarán los menús y textos de los teclados, la interfaz Web y el registro de incidencias. • Ultimo usado: se muestra el último idioma usado en estado de reposo.
	Usar menú simplificado	Habilite esta opción para usar los menús simplificados para armado/desarmado en teclados 'Comfort' y 'Compact' (para la configuración de una partición únicamente).
Código		
	Dígitos del PIN	Introduzca el número de dígitos para los códigos PIN de usuario (máx. 8 dígitos). Al aumentar el número de dígitos, se añadirá el número de ceros correspondiente delante del código PIN existente; por ejemplo, un código PIN de usuario existente 2134 (cuatro dígitos) cambia a 00002134 si la cantidad de dígitos del código PIN se establece en ocho. Si se reduce el número de dígitos de los códigos PIN, se eliminarán los primeros dígitos de los códigos PIN existentes; p. ej., un código PIN de usuario existente 00002134 (8 dígitos) pasará a ser 02134 si los dígitos del código PIN se reducen a 5. **Nota:** Esta opción no se puede cambiar si se ha establecido un modo de dígitos de código PIN con SPC Manager. Consulte *SPC Manager* en la página 347. **Nota:** Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.

Restricciones	Opciones del sistema	Descripción
	PACE y código PIN	Si esta opción está habilitada, se requiere PACE y código PIN.
	Coacción de usuario	Seleccione una de las siguientes opciones de coacción para activar esta función en el sistema. • PIN+1 (el sistema reserva el número de código PIN anterior y posterior al código PIN del usuario para código de coacción). • PIN+2 (el sistema reserva dos números de código PIN anteriores y posteriores al código PIN del usuario para código de coacción). La opción de coacción debe estar habilitada para usuarios individuales. Consulte la sección Añadir/Editar un usuario.
	Política del PIN	Haga clic en el botón **Editar** para seleccionar opciones para el uso de códigos PIN. • Cambios periódicos requeridos: impone cambios programados en el PIN del usuario. El período está definido en el campo **PIN válido** de **Temporizaciones**. Consulte *Temporizaciones* en la página 266. • Aviso si cambios requeridos: genera una alerta para el usuario si el PIN de usuario está a punto de expirar o ya ha expirado. El período de advertencia está definido en el campo **Aviso expiración PIN** de **Temporizaciones**. Consulte *Temporizaciones* en la página 266. • Usuario selecciona último dígito: permite al usuario seleccionar el último dígito de su PIN. Los dígitos anteriores son generados automáticamente por el sistema. • Usuario selecciona 2 últimos dígitos: permite al usuario seleccionar los dos últimos dígitos de su PIN. Los dígitos anteriores son generados automáticamente por el sistema. • Límite cambios: limita el número de cambios que se pueden hacer dentro de un período de PIN válido. Este valor está definido en el campo **Límite cambios de PIN** de **Temporizaciones**. Consulte *Temporizaciones* en la página 266. • Código generado: si esta opción está habilitada, el PIN es generado automáticamente por la central.
Puerta y lector		
	Resetear tarjetas	Si esta opción está habilitada, se realizará el reset diario a medianoche del estado de retorno de tarjetas de acceso.
	Ignorar código de lugar	Si esta opción está habilitada, el sistema de acceso ignorará los códigos de lugar. Al ignorar el código de lugar, solo añade el número de tarjeta e incrementa los usuarios de tarjetas en el sistema de 100 a 2.500.

Restricciones	Opciones del sistema	Descripción
	Formatos de tarjeta	Haga clic en el botón **Editar** para seleccionar los formatos de tarjeta que se permitirán en esta central. Para obtener más información sobre los lectores de tarjetas y formatos de tarjetas soportados actualmente, consulte *Lectores de tarjeta y formatos de tarjeta admitidos* en la página 404. **Nota:** Si se selecciona **Wiegand**, se habilitan todos los formatos de tarjeta Wiegand.
Web únicamente	Modo puerta en armado	Permite seleccionar si se requiere la identificación del usuario para desbloquear la puerta cuando la partición está armada. Las opciones son **Por defecto**, **Tarj. y código**, **Tarjeta o código**.
Web únicamente	Modo puerta en desarmado	Permite seleccionar si se requiere la identificación del usuario para desbloquear la puerta cuando la partición está desarmada. Las opciones son **Por defecto**, **Tarj. y código**, **Tarjeta o código**.
	Anular perfil de lector	Si esta opción está habilitada, las luces LED del lector indican la confirmación de armado y la solicitud de tarjeta y código PIN.
Técnico		
⏻	Restauración de técnico	(Sólo para Reino Unido): Si se habilita esta opción, el técnico deberá restaurar las alarmas confirmadas. Esta opción funciona junto con la función «Confirmación».
	Salida de modo técnico	Si esta función está habilitada, el técnico puede salir del modo técnico completo con alertas activas.
⏻	Permitir técnico	Habilite esta opción para asegurarse de que el técnico solo pueda acceder al sistema si el usuario lo permite. Si esta opción está deshabilitada, la opción del menú HABILITAR TÉCNICO no estará disponible en el teclado. **Nota:** Solo disponible si el **grado de seguridad** es 'Libre'. Para el Grado 2/3, el control del usuario del acceso técnico al sistema siempre está disponible.
⏻	Permitir fabricante	Habilite esta opción para asegurarse de que el técnico solo pueda acceder al sistema si el usuario lo permite. Si esta opción está deshabilitada, la opción del menú HABILITAR FABRICANTE no estará disponible en el teclado. **Nota:** Solo disponible si el **grado de seguridad** es 'Libre'. Para el Grado 2/3, el control del usuario del acceso técnico al sistema siempre está disponible si el tipo de usuario es 'Gerente'.
Envío SMS		

Restricciones	Opciones del sistema	Descripción
	Autentificación SMS	Seleccione una de las siguientes opciones: • Sólo código PIN: Se trata de un código de usuario válido. • Sólo identificación de llamada: Es un número de teléfono (que incluye el prefijo nacional de tres dígitos) configurado para el control de SMS por parte del usuario. El control de SMS solo estará disponible para la configuración por parte del usuario cuando esta opción esté seleccionada. • Código PIN e ID de llamada • Sólo PIN SMS. Es un código PIN válido configurado para el usuario diferente del código de acceso del mismo usuario. Los controles de SMS solo estarán disponibles para la configuración por parte del usuario cuando esta opción esté seleccionada. • Código PIN de SMS e ID de llamada.
Política		
Web únicamente	Política del sistema	Configure el inicio de sesión del técnico y el comportamiento de informes de tamper del sistema.
Web únicamente	Política de temporizaciones	Muestra la política de temporizaciones del sistema.
Web únicamente	Configuración de salidas	Haga clic en el botón **Editar** para configurar los ajustes de salida de enclavamiento y autoarmado (consulte *Configurar enclavamiento y autoarmado de salidas del sistema* en la página 232).
Web únicamente	Política de alertas del sistema	Esta opción de programación le permite restringir la capacidad del usuario y del técnico de restaurar, aislar e inhibir alertas. La forma en la que el sistema reacciona ante las alertas también puede ser programada.
Web únicamente	Política de alarma de zona	Seleccione las alarmas de zona en particular que el usuario y el técnico pueden restaurar, inhibir o aislar.
Web únicamente	Política de tamper de zona	Seleccione los tamper de zona en particular que el usuario y el técnico pueden restaurar, inhibir o aislar.
Web únicamente	Política de pantalla del teclado	Seleccione las incidencias que se deben mostrar en los teclados, tanto en modo armado como desarmado.
Web únicamente	Política de luz LED del teclado	Seleccione las luces LED que se deben mostrar en los teclados, tanto en modo armado como desarmado.

Restricciones	Opciones del sistema	Descripción
Web únicamente	Política general sistema	Seleccione las opciones para gestionar el control remoto del sistema y los ajustes de alarma y sirena: - Sin alarmas confirmadas con armado interno - Bloquear restauración remota - Bloquear aislamientos remotos - Bloquear inhibiciones remotas - Sin sirena exterior con armado interno - Retardar informe con entrada activada - Alarma confirmada cancela retardo
Web únicamente	Alertas sist.alarma confirmada	Seleccione qué alertas del sistema provocarán alarmas confirmadas cuando al menos una alarma está activa, y qué alarmas del sistema harán que la central pase a estado provisional.
Datos atraco		
Web únicamente	Clave atraco 1	Introduzca la primera clave de atraco que se enviará al CMS en una incidencia de información de atraco (HD).
Web únicamente	Clave atraco 2	Introduzca la segunda clave de atraco que se enviará al CMS en una incidencia de información de atraco (HD).
Web únicamente	Número de teléfono 1	Introduzca el primer número de teléfono que se enviará al CMS en una incidencia de información de atraco (HD).
Web únicamente	Número de teléfono 2	Introduzca el segundo número de teléfono que se enviará al CMS en una incidencia de información de atraco (HD).

Consulte también

Añadir/Editar una partición en la página 275

17.9.4.2 Temporizaciones

Esta página brinda un resumen de los valores por defecto de un temporizador identificado y la descripción.

Estos ajustes, que pueden variar dependiendo del grado de seguridad definido en el sistema, solo deben ser programados por un ingeniero instalador autorizado. Si se cambian los ajustes, el sistema SPC podría dejar de cumplir los estándares de seguridad. Si se revierte el grado de seguridad a EN 50131 Grado 2 o EN 50131 Grado 3, se sobreescribirán los cambios hechos en esta página.

1. Seleccione **Configuración > Sistema > Temporizadores del sistema**.

   Se mostrará la página **Temporizadores del sistema.**
2. Configure los campos tal como se describe en la siguiente tabla.

Temporizaciones

Designación de las funciones en el siguiente orden:

- Primera fila: web
- Segunda fila: teclado

Temporizador	Descripción	Default
Audible		
Sirenas interiores TIEMPO SIR. INT.	Tiempo durante el cual las sirenas interiores sonarán cuando se active la alarma. (0-999 minutos; 0 = nunca)	15 min.
Sirenas exteriores TIEMPO SIR. EXT.	Tiempo durante el cual las sirenas exteriores sonarán cuando se active la alarma. (0-999 minutos; 0 = nunca)	15 min.
Retardo sirena exterior RET.SIR.EXT.	Esto generará un retardo en la activación de la sirena exterior. (0-999 segundos)	0 seg.
Chime TEMP.CHIME	Cantidad de segundos durante la cual se activará una salida chime al abrirse una zona con atributo de chime. (1-10 segundos)	2 seg.
Confirmación		
Confirmar TIEMPO CONFIRM.	**Nota:** Esta opción está disponible únicamente para determinadas combinaciones de opción de **Grado** y **Confirmación**. (Consulte *Opciones* en la página 254 y *Estándares* en la página 271). Este temporizador se aplica a la función de confirmación de alarma y se define como el tiempo máximo entre las alarmas de dos zonas no solapadas que dispararán una alarma confirmada. (0-60 minutos)	30 min.
Atraco confirmado	**Nota:** Esta opción está disponible únicamente para determinadas combinaciones de opción de **Grado** y **Confirmación**. (Consulte *Opciones* en la página 254 y *Estándares* en la página 271). Este temporizador se aplica a la función de atraco confirmado y se define como el tiempo máximo entre las alarmas de dos zonas no solapadas que dispararán una alarma confirmada. (480-1200 minutos)	480 min.
Retardo marcación RETARDO MARCACIÓN	Cuando está programado, el retardo de marcación inicia un período de retardo predefinido antes de que el sistema se comunique con una central de recepción de alarmas (CRA). Esto está diseñado específicamente para reducir las respuestas innecesarias de las centrales de recepción de alarmas y la policía. En caso de que otra zona se active, se ignorará el período de retardo de marcación y la marcación se realizará de inmediato. (0-999 segundos)	30 seg.
Abortar alarma ABORTAR ALARMA	Tiempo tras alarma informada en el que se puede informar un mensaje de alarma abortada. (0-999 segundos)	30 seg.
Configuración		
Autorización de armado AUTORIZ. ARMADO	Período durante el cual es válida la autorización de armado. (10-250 segundos)	20 seg.

Temporizador	Descripción	Default
Fin de salida SALIDA FINAL	El tiempo de salida final es la cantidad de segundos que se retarda el armado tras cerrarse una zona con el atributo de salida final. (1-45 segundos)	7 seg.
Sirena con armado total SIR.ARM.TOTAL	Activa momentáneamente la alarma exterior para indicar una condición de armado total. (0-10 segundos)	0 seg.
Fallo al armar FALLO AL ARMAR	Cantidad de segundos que se muestra este fallo en los teclados (0: Hasta la introducción de un PIN válido). (0-999 segundos)	10 seg.
Flash con armado total FLAH.ARM.TOTAL	Activa momentáneamente el flash de la alarma exterior para indicar una condición de armado total. (0-10 segundos)	0 seg.
Alarma		
Doble detección DOBLE DETECCIÓN	El máximo retardo entre la activación de zonas con el atributo de doble detección que generará una alarma. (1-99 segundos)	10 seg.
Pruebas DIAS PRUEBAS	La cantidad de días durante los cuales una zona permanece a prueba antes de retornar automáticamente al funcionamiento normal. (1-99 días)	14 días
Intervalo de test sísmico AUTOTEST SÍSMICO	El período promedio entre los tests automáticos del sensor sísmico. (12-240 horas) **Nota:** Para habilitar el test automático, se debe habilitar el atributo de **Test de sensor automático** para una zona sísmica.	168 horas
Duración test sísmico DUR. TEST SISM.	Tiempo máximo (en segundos) que tarda el sensor sísmico en disparar una alarma en respuesta a una salida de 'test sísmico'. (3-120 segundos)	30 seg.
Retardo reposición automática	Tiempo que se retardará una restauración automática después de que el estado de una zona vuelva a ser normal. (0-9999 segundos)	0 seg.
Bloqueo post-alarma BLOQUEO POST-ALARMA	El tiempo después de una alarma antes de que el usuario pueda tener acceso. (1-120 minutos)	0 min.
Tiempo de acceso	El tiempo durante el cual un usuario con acceso con alarma puede acceder al sistema tras finalizar el tiempo de bloqueo. (10-240 minutos)	
Flash exterior TIEMPO FLASH	Tiempo durante el cual la salida flash estará activa cuando se active la alarma. (1-999 minutos; 0 = indefinidamente)	15 min.
Avisos		
Retardo red CA RETAR.FALLO C.A.	El tiempo después de detectarse un fallo en la red de CA y antes de que el sistema active un aviso. (0-60 minutos)	0 min.

Temporizador	Descripción	Default
Retardo interferencia RF	El tiempo después de detectarse el retardo de interferencia RF y antes de que el sistema active un aviso. (0-999 segundos)	0 min.
Técnico		
Acceso de técnico ACCESO DE TÉCNICO	El temporizador para el acceso del técnico comienza tan pronto como el usuario habilita el acceso del técnico. (0-999 minutos; 0 indica sin limitación de tiempo para el acceso al sistema)	0 min.
Salida modo técnico automática SAL.AUTO.M.TÉC.	Tiempo de inactividad tras el cual se cerrará automáticamente la sesión del técnico. (0-300 minutos)	0 min.
Teclado		
Tiempo espera teclado TIEMPO ESP. TECL.	La cantidad de segundos que un RKD esperará la introducción de teclas antes de salir del menú actual. (10-300 segundos)	30 seg.
Idioma teclado IDIOMA TECLADO	El tiempo que un teclado esperará en reposo antes de cambiar al idioma por defecto. (0 -9999 seg.; 0 = nunca)	10 seg.
Incendio		
Prealarma incendio PREALARMA INCENDIO	Número de segundos que se debe esperar antes de notificar una alarma de incendio para zonas con el atributo «Prealarma incendio» seleccionado. Consulte *Editar una zona* en la página 274. (1-999 segundos)	30 seg.
Reconocimiento de alarma de incendio RECONOCIMIENTO ALARMA INCENDIO	Tiempo adicional de espera antes de informar una alarma de incendio para las zonas con los atributos de «Prealarma incendio» y «Reconocimiento de incendio». Consulte *Editar una zona* en la página 274. (1-999 segundos)	120 seg.
Código		
PIN Válido PIN VÁLIDO	Período durante el cual el PIN es válido. (1-330 días)	30 días
Límite cambios de PIN LÍMITE CAMBIOS DE PIN	Cantidad de cambios dentro de un período válido. (1-50)	5
Aviso PIN AVISO EXP. PIN	Tiempo antes de caducar un PIN tras el cual se mostrará una advertencia. (1-14 días)	5 días
Configuración general		
Tiempo salida RF SALIDA RF	El tiempo que la salida RF permanecerá activa en el sistema. (0-999 segundos)	0 seg.

Temporizador	Descripción	Default
Límite tiempo sincronismo LÍMITE TIEMPO SINCRONISMO	Límite de tiempo dentro del cual no se llevará a cabo la sincronización. La sincronización de tiempo solo se produce si la hora del sistema y la hora de actualización están fuera de este límite. (0-300 segundos)	0 seg.
T. fallo link T. Fallo Link	Tiempo de espera para fallo de enlace Ethernet. (0 -250 seg.; 0 = deshabilitado)	0 seg.
Cámara fuera de línea CAM.NO EN LÍNEA	Tiempo hasta que la cámara pase a estar fuera de línea. (10-9999 segundos)	10 seg.
Supervisada SUPERVISADA (!)	Este atributo solo se aplica a servicios remotos. La cantidad de horas durante las cuales una zona debe abrirse si la zona está programada con el atributo **Frecuente**. (1-9999 horas)	336 h (2 semanas)
Silencio por coacción	Tiempo durante el cual una alarma de coacción continuará silenciada y no podrá restaurarse desde el teclado. (0-999 minutos)	0 min.
Silencio por atraco/pánico	Cantidad de minutos durante los cuales una alarma de atraco/pánico continuará silenciada y no podrá restaurarse desde el teclado. (0-999 minutos)	0 min.

Los tiempos por defecto dependen de la configuración del técnico. Los tiempos por defecto pueden o no ser permisibles, y dependen de la configuración establecida por el técnico.

Los rangos/ajuste válidos podrían depender del grado de seguridad especificado en **Configuración > Sistema > Estándares**.

17.9.4.3 Identificación

1. Seleccione **Configuración > Sistema > Identificación**.

   Se mostrará la siguiente página.

2. Configure los campos tal como se describe en la siguiente tabla.

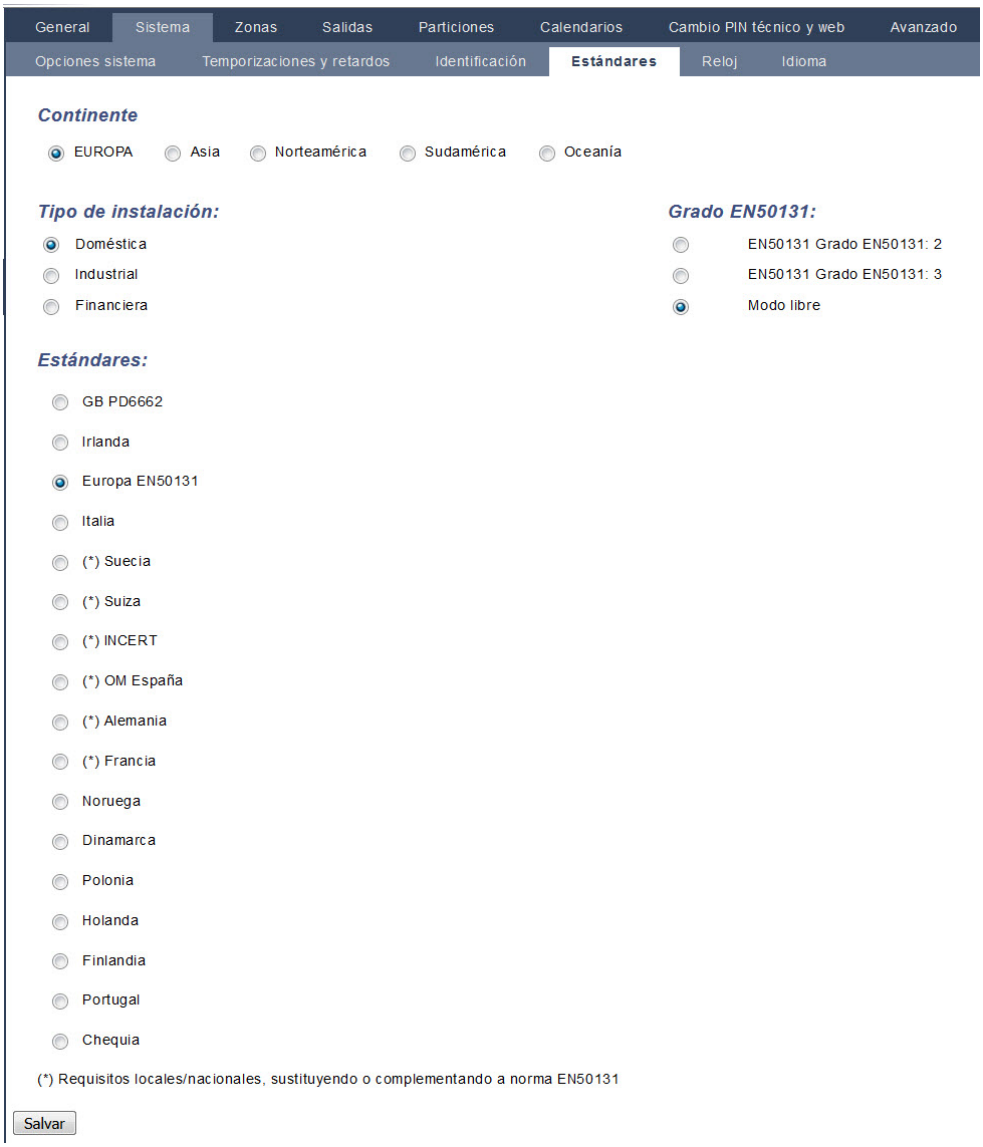
ID instalación	Introduzca un número exclusivo para cada instalación. Este número identifica la instalación (1-999999).
Nombre instalación	Introduzca el nombre de la instalación. Debe introducir el nombre de la instalación antes de que la instalación se salve en el sistema. La instalación puede verse desde el teclado.
Fecha de instalación	Seleccione la fecha en que se completó la instalación del menú desplegable.
Nombre instalador	Introduzca el nombre de la persona que instaló el sistema (para fines de soporte).
Teléfono del instalador	Introduzca el número de teléfono de contacto de la persona que instaló el sistema (para fines de soporte).
Detalles del instalador	Marque esta casilla para mostrar los detalles del instalador en el teclado conectado a la central cuando esté en reposo.
Bloqueo técnico	Marque esta casilla para requerir el uso del código PIN de bloqueo técnico para restaurar los valores por defecto de fábrica de la central.
Código PIN de bloqueo técnico	Introduzca el valor para el código PIN de bloqueo (4 dígitos).

17.9.4.4 Estándares

Todos los sistemas de alarma deben cumplir con los estándares de seguridad definidos. Cada estándar tiene requisitos de seguridad específicos que se aplican al mercado/país en el que se instala el sistema de alarma.

1. Seleccione **Configuración > Sistema > Estándares**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

Continente	Seleccione el emplazamiento apropiado para la instalación. Las opciones son: Europa, Asia, Norteamérica, Sudamérica u Oceanía.
Tipo de instalación	Seleccione el tipo de instalación. Las opciones son Doméstica, Industrial o Financiera.

	Para cambiar la región en su central, se recomienda encarecidamente restaurar la central y seleccionar una nueva región como parte del asistente de inicio. Seleccione la región de la instalaciones y los requisitos regionales con los que cumple.
Cumplimiento según la región	Algunas selecciones implementarán requisitos locales o nacionales, sustituyendo o complementando la norma EN50131. Las opciones en la sección **Grado** cambiarán en función de su selección en **Cumplimiento según la región**. Las opciones son: Reino Unido, Irlanda, Europa general (EN), Italia, Suecia, Suiza, Bélgica, España, Alemania (VdS), Francia, Noruega, Dinamarca, Polonia, Holanda, Finlandia, Portugal y la República Checa.
Grado	Seleccione el grado de seguridad que se aplica a la instalación. Las opciones en la sección **Grado** cambiarán en función de su selección en **Cumplimiento según la región**.

Grado libre

Si la opción de grado de seguridad es **Modo libre**, a la instalación no se le aplica ninguna restricción de seguridad aprobada a nivel regional. En su lugar, la configuración libre le permite al técnico personalizar la instalación al cambiar las opciones de la política de seguridad y al configurar opciones adicionales que no cumplen con la normativa de seguridad regional seleccionada.

Las opciones de configuración libre se indican en este documento mediante el siguiente símbolo:

Consulte *Opciones del sistema* en la página 254 para obtener más información sobre la configuración de políticas del sistema.

17.9.4.5 Reloj

Esta página le permite programar la fecha y hora en la central. El controlador incluye un **R**eloj de **T**iempo **R**eal (RTR) incorporado en la batería para conservar la información de hora y fecha en caso de fallo de la alimentación.

1. Seleccione **Configuración > Sistema > Reloj**.

   Se mostrará la siguiente página.

2. Seleccione **Hora** y **Fecha** del menú desplegable.
3. Configure los siguientes campos:

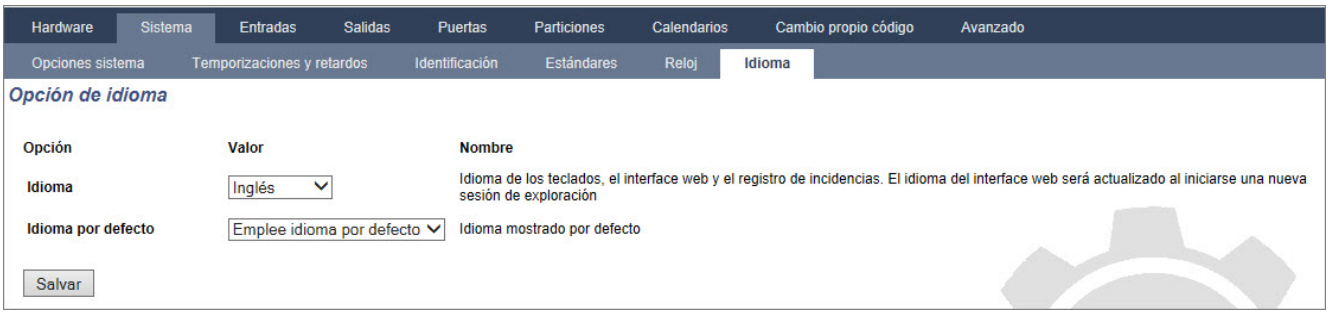
Cambio automático del horario de verano	Si esta opción está seleccionada, el sistema cambiará automáticamente al horario de verano.
Sincronización de la hora con la red de CA	Si esta opción está seleccionada, el RTR se sincroniza con la onda sinusoidal de la línea de alimentación.

La hora y la fecha seleccionadas aparecerán en el teclado, la interfaz web y el registro de incidencias.

17.9.4.6 Idioma

1. Seleccione **Configuración > Sistema > Idioma**.

   Aparecerá la siguiente página:



2. Para la opción **Idioma**, seleccione un idioma del menú desplegable.

   Esta opción determina el idioma del sistema en que se mostrarán los textos y menús de los teclados, la interfaz web y el registro de incidencias.

3. Para la opción **Idioma en reposo**, seleccione 'Usar idioma del sistema' o 'Último usado'.

   El Idioma en reposo determina el idioma que se muestra en los teclados cuando la central está en estado de reposo. Si se selecciona la opción 'Último usado', el idioma que se mostrará será el asociado al último inicio de sesión de usuario.

El idioma utilizado en los teclados y el navegador depende de la selección de idioma hecha para cada usuario. Por ejemplo, si el idioma del sistema está ajustado en francés, pero el idioma del usuario individual está ajustado en inglés, se utilizará el inglés tanto en los teclados como en el navegador para ese usuario, independientemente del idioma especificado para el sistema.

Consulte también

Opciones en la página 126

17.9.5 Configurar zonas, puertas y particiones

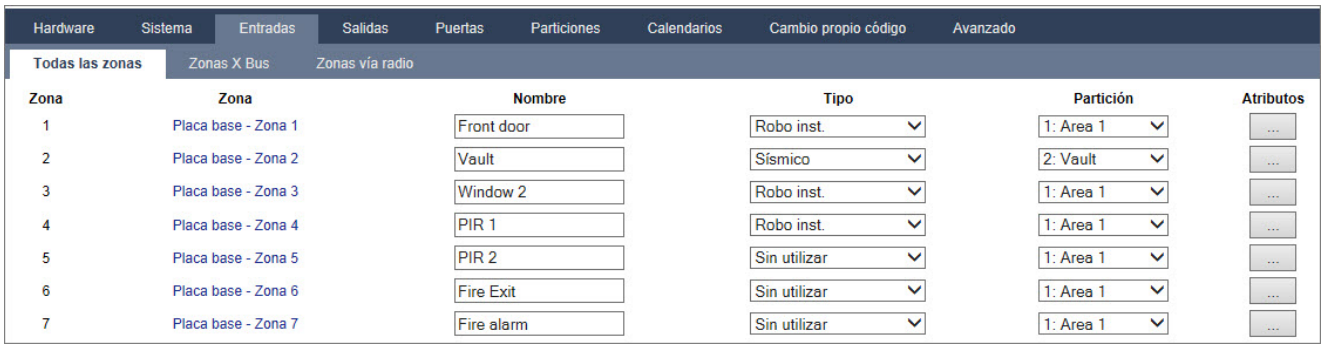
Esta sección abarca:

17.9.5.1 Editar una zona

Las acciones de Técnico y Usuario incluyen: Registrar, Aislar/Restaurar y Prueba/Salir de prueba para cada zona según lo permitan los grados de seguridad EN 50131 Grado 2 y EN 50131 Grado 3.

1. Seleccione **Configuración > Entradas > Todas las zonas**.

   Se mostrará la siguiente página.



Puede seleccionar **Configuración > Entradas > Zonas X-Bus** para configurar zonas cableadas únicamente, o bien **Configuración > Entradas > Zonas vía radio** para configurar zonas vía radio únicamente.

2. Configure los campos tal como se describe en la siguiente tabla.

Zona	El número se muestra para referencia y no puede programarse.
Descripción	Introduzca texto (máx. 16 caracteres) que sirva para identificar la zona.
Entrada	La entrada física se muestra como referencia y no se puede programar.
Tipo	Seleccione el tipo de zona del menú desplegable (consulte *Tipos de zona* en la página 393).
Particiones	Solo si la opción **Particiones** (múltiples) está activada. Seleccione una partición a la cual se asignará la zona del menú desplegable.
Calendario	Seleccione, en caso de ser necesario, el calendario deseado (consulte *Calendarios* en la página 289). Para los grados de seguridad 2/3, se puede asignar un calendario solo a las zonas de tipo Terminador de salida, Técnica, Llave armado, Anulación y Anulación X. Para el grado de seguridad Libre, se puede asociar cualquier tipo de zona al calendario.
Atributos	Marque la casilla que corresponda a la zona. Se presentarán solo los atributos que se aplican a ese tipo de zona (consulte *Atributos de zona* en la página 399).

17.9.5.2 Añadir/Editar una partición

Requisito previo

- Solo si la opción **Particiones** (múltiples) está activada.

1. Seleccione **Configuración > Particiones > Particiones**.

   Se mostrará la siguiente página:

2. Haga clic en **Editar** para editar una partición existente.
3. Haga clic en **Añadir** para añadir una partición nueva. Si el tipo de instalación es *Doméstica* o *Comercial*, se añade automáticamente una partición y se muestra la página **Editar configuración partición**.
   Tenga en cuenta que el tipo de partición para la partición nueva se configura automáticamente en Estándar.
   Si el tipo de instalación es *Financiera*, se mostrará la siguiente página, y la partición deberá añadirse manualmente.

4. Introduzca una descripción para la partición nueva y seleccione el tipo de partición de una de las siguientes opciones:

   - Estándar: adecuada para la mayoría de las particiones.

   - Cajero automático: brinda la configuración y funciones por defecto relevantes para cajeros automáticos.

   - Cámara acorazada: brinda la configuración y funciones por defecto relevantes para cajas fuertes.

   - Avanzado: brinda la configuración de todas las particiones (estándar, cajero automático y cámara acorazada).
5. Haga clic en el botón **Añadir** para añadir la partición.

- Configure los ajustes para cada tipo de instalación según las siguientes secciones.

Entrada/salida

Configure los siguientes ajustes de Entrada/Salida:

Tiempo entrada	El período de tiempo (en segundos) permitido para que el usuario DESARME la alarma tras abrir una zona de entrada/salida de un sistema armado. El tiempo de entrada se aplica a todas las zonas de entrada/salida de esa partición (por defecto: 45 segundos).

Tiempo de salida	El período de tiempo (en segundos) permitido para que el usuario salga de la partición protegida antes de que se complete el armado. La cuenta regresiva del tiempo de salida en el teclado comenzará cuando el zumbador suene para indicar al usuario que el sistema se armará cuando el contador de salida llegue a cero. El tiempo de salida se aplica a todas las zonas de entrada/salida de esa partición (por defecto: 45 segundos).
Sin t. de salida	Seleccione esta opción si no se requiere tiempo de salida y el armado se activa mediante la zona 'Plazo de salida' o Entrada/Salida' con atributo 'Salida final'. Consulte *Temporizaciones* en la página 266.
Entr. desar. mando vía radio	El mando vía radio solo desarmará la alarma cuando el temporizador de entrada esté en marcha. Función habilitada por defecto.
Acceso denegado con alarma	El acceso a la partición se deniega temporalmente durante el tiempo especificado en el temporizador de Bloqueo post-alarma.
Impedir armado	Si está habilitada esta opción, se impide el armado desde el teclado
Impedir desarmado	Si está habilitada esta opción, se impide el desarmado desde el teclado
Autorización de armado	Esta opción sirve para configurar el funcionamiento del cierre de bloqueo. Las opciones son: • Deshabilitado • Armado • Desarmado • Armado y Desarmado Si se encuentra seleccionada la opción Deshabilitado (por defecto), el sistema se armará y desarmará normalmente, sin cambios en el funcionamiento. Si se selecciona la opción Armado, se requerirá una señal de «Autorización de armado» para armar esta partición, y esta señal puede ser recibida de los teclados o de una entrada de zona (véase Armado autorizado del cierre de bloqueo). El usuario no puede armar el sistema desde el teclado. Cualquier partición que requiera autorización de armado aparecerá como bloqueada en el teclado Confort, y no aparecerá en el teclado estándar al armar. Si se selecciona la opción Desarmado, el usuario no podrá desarmar la partición desde los teclados, pero sí podrá utilizar el teclado para generar la señal de autorización de armado. Para las opciones de armado y desarmado, el usuario no podrá cambiar el estado de la partición en ningún momento desde el teclado. Se puede configurar un temporizador para autorización de armado. Consulte *Temporizaciones* en la página 266.

Opciones de armado parcial

Configure la operación de zonas determinadas para los modos Armado parcial A y Armado parcial B según lo detallado a continuación:

Armado parcial habilitado	Habilite el armado parcial para operación A y B según sea necesario.

Armado parcial con temporización:	Marque la casilla relevante (Armado parcial A o B) para aplicar el temporizador de salida al modo Armado parcial A o B.
Acceso a armado parcial:	Marque la casilla relevante para cambiar las zonas de acceso a zonas de tipo entrada/salida para la operación de Armado parcial A o B. Esta función es recomendable para una instalación doméstica en la que se coloca un sensor infrarrojo pasivo (PIR) en el pasillo. Si el usuario arma parcialmente el sistema por la noche y baja las escaleras durante la noche, podría activar involuntariamente el sensor PIR en el pasillo y disparar la alarma. Al configurar la opción de acceso de armado parcial, el zumbador sonará durante el período de tiempo de entrada cuando el sensor PIR esté activo para advertir al usuario que la alarma se activará si no realiza otra acción.
Armado parcial de entrada/salida:	Marque la casilla relevante para cambiar el comportamiento de las zonas de entrada/salida a zonas de alarma en modo Armado parcial A o B. Esta función es recomendable para una instalación doméstica cuando el sistema está configurado en modo Armado parcial. Si el usuario arma parcialmente el sistema por la noche, quizás desee que la alarma se active de inmediato si se abre la puerta delantera o trasera durante la noche.
Armado parcial local:	Marque la casilla relevante para restringir el informe de alarmas en modo Armado parcial a informes solo a nivel a local (sin informes remotos).
Sin sirenas	Si se marca esta opción, no habrá sirenas activadas para armado parcial A o B.

Particiones ligadas

Esta sección le permite enlazar particiones con fines de armado y desarmado:

Armado total	Armado total de esta partición cuando todas las particiones enlazadas están en Armado total.
Armado total todo	Armado total de todas las particiones cuanto esta partición está en Armado total.
Impedir armado total	Impedir el armado total de esta partición si todas las particiones enlazadas están en Armado total.
Impedir armado total todo	Impedir el armado total de las particiones enlazadas si esta partición no está en Armado total.
Desarmado	Desarmado de esta partición cuando todas las particiones enlazadas están en Desarmado.
Desarmado todo	Desarmado de todas las particiones cuando esta partición está en Desarmado.
Impedir desarmado	Impedir el desarmado de esta partición si alguna de las particiones enlazadas está en Armado total.
Impedir desarmado todo	Impedir el desarmado de las particiones enlazadas si esta partición está en Armado total.
Autorice armado	Se autoriza el armado para las particiones ligadas. Véase Armado autorizado del cierre de bloqueo.
Particiones ligadas	Haga clic en las particiones que desea enlazar a esta partición.

Schedule (planificación)

Configure la planificación con las siguientes opciones:

Calendario	Seleccione un calendario para controlar la planificación.
Desarmado	Seleccione esta opción si la partición debe desarmarse automáticamente según el horario especificado en el calendario seleccionado.
Armado total	Seleccione esta opción para el armado total de la partición según el horario especificado en el calendario seleccionado. La partición también se armará cuando haya transcurrido el tiempo de duración de desarmado o el intervalo de retardo (consulte *Armado/Desarmado* en la página 281). Si el período de duración de desarmado se superpone con el horario programado, la partición utilizará la configuración del calendario.
Bloqueo tiempo	Seleccione esta opción para bloquear el tiempo de la partición según el calendario seleccionado. (Partición de tipo Cámara acorazada solo en modo Financiero)
Temp.acc.cám.acorz.	Introduzca la cantidad de minutos (0 a 120) para activar este temporizador al final del período de desarmado con bloqueo de tiempo. Si esta partición no está desarmada una vez que este temporizador caduca, no se podrá desarmar la partición hasta el comienzo del siguiente período de desarmado con bloqueo de tiempo. (Partición de tipo Cámara acorazada solo en modo Financiero)

Generación de informes

Las opciones de configuración de informes se aplican a las particiones estándar en instalaciones comerciales y financieras únicamente y solo son relevantes si se ha seleccionado un calendario. (Consulte *Schedule (planificación)* en la página precedente.)

Esta configuración permite que se envíe un informe al centro de control o al personal nominado si la central se arma o desarma fuera de los períodos de tiempo programados en el calendario.

Armado prematuro	Permite que se envíe un informe si la central se arma manualmente antes de un armado programado y antes del período de tiempo (en minutos) introducido en el campo Temporizador.
Armado tardío	Permite que se envíe un informe si la central se arma manualmente después de un armado programado y después del período de tiempo (en minutos) introducido en el campo Temporizador.
Desarmado prematuro	Permite que se envíe un informe si la central se desarma manualmente antes de un desarmado programado y antes del período de tiempo (en minutos) introducido en el campo Temporizador.
Desarmado tardío	Permite que se envíe un informe si la central se desarma manualmente antes de un desarmado programado y antes del período de tiempo (en minutos) introducido en el campo Temporizador.

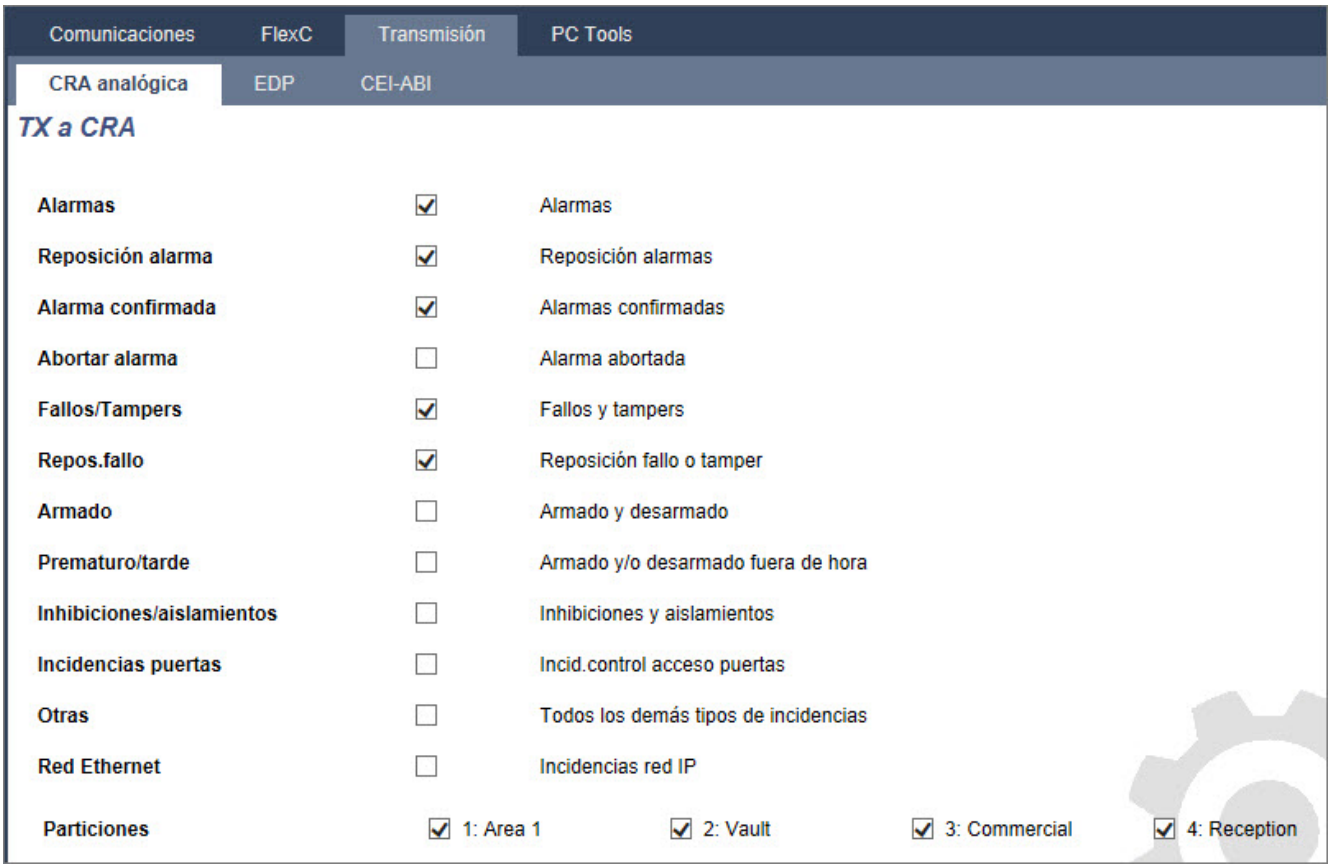
El envío de informes se realiza mediante el SMS, o bien a la CRA mediante SIA y Contact ID. Las incidencias también se guardan en el registro del sistema.

Solo se informarán las incidencias configuradas para informes tardíos o tempranos de la partición.

También se debe habilitar el informe de incidencias para una CRA o el SMS, según se describe en las secciones a continuación.

Habilitación de informes de armado/desarmado inusual para una CRA

Para configurar los informes de incidencias para que una CRA configurada se comunique mediante SIA o CID, seleccione **Comunicaciones > Informes > CRA analógica > Editar >Filtro** para mostrar la página Filtro de incidencias para una CRA.

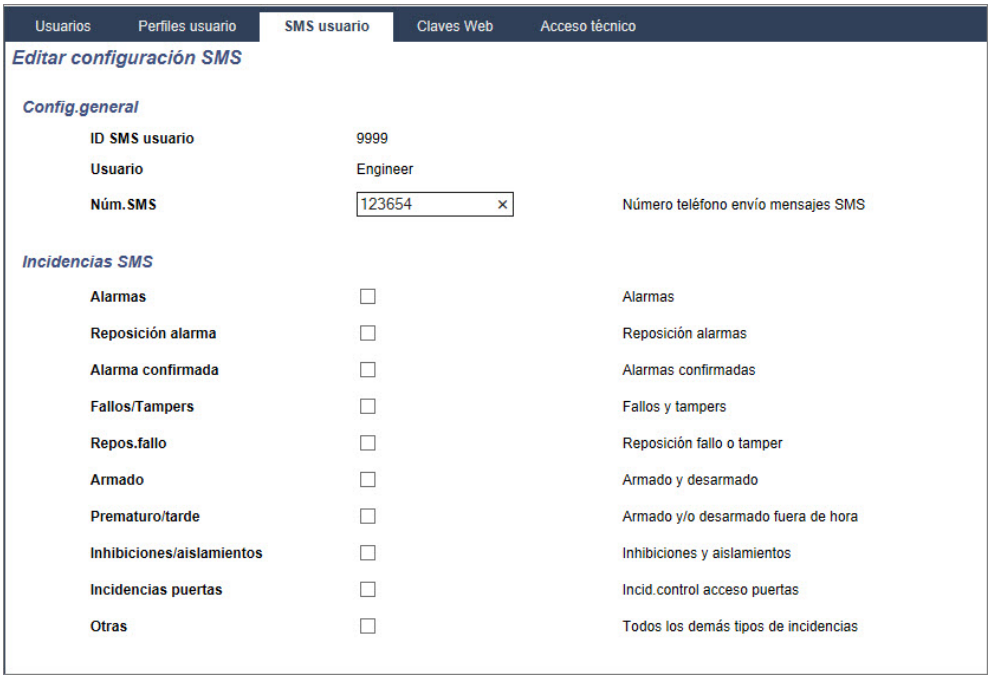


Se habilita el parámetro **Temprano/Tardío** para informar todo armado o desarmado que difiera del programa.

Habilitación de informes de armado/desarmado inusual para el SMS

Las incidencias del SMS pueden configurarse en las páginas de configuración de técnico y de usuario.

Para la configuración de técnico, seleccione **Usuarios > SMS de usuarios > SMS de técnico > Editar**.



Habilite Prematuro/tarde para transmitir cualquier armado o desarmado que difiera de la planificación.

Armado/Desarmado

Los siguientes parámetros (con la excepción del parámetro Interbloqueo) son solo relevantes en los siguientes casos:

- cuando hay un calendario seleccionado (consulte *Schedule (planificación)* en la página 278), o
- cuando la opción **Duración desarmado** está habilitada (tiene un valor superior a cero), o
- cuando se cumplen ambas condiciones expresadas anteriormente.

Advertencia armado automático	Introduzca la cantidad de minutos que se mostrará una advertencia antes del armado automático. (0-30) Tenga en cuenta que la central se arma a un horario programado o en el horario definido por el parámetro de retardo de desarmado. Aparecerá la primera advertencia en el horario configurado antes del horario programado. Existen otras advertencias que se disparan un minuto antes del horario de armado.
Cancelación armado automático	Le permite al usuario cancelar el armado automático al introducir un código en el teclado.
Retardo armado automático	Le permite al usuario retardar el armado automático al introducir un código en el teclado.
Conmutador llave	Permite el retardo del armado automático desde el módulo de expansión de conmutador de llave.
Intervalo de retardo	Introduzca la cantidad de minutos para retardar el armado automático. (1-300)
Contador de retardo	Introduzca la cantidad de veces que se puede retardar el armado automático. (0-99: 0 = ilimitado)
Retardo de desarmado	Introduzca la cantidad de minutos para retardar el desarmado. (0 = sin retardo)
Grupo de interbloqueos	Seleccione un grupo de interbloqueos para asignar a esta partición. El interbloqueo permite que únicamente se desarme una partición dentro del grupo a la vez. Generalmente se utiliza en particiones de cajeros automáticos.
Duración desarmado	Si la partición supera este tiempo desarmada, se armará automáticamente. (Rango 0–120 min.: 0 = no activa).
Código PIN doble	Si esta opción está habilitada, se requieren dos PIN para armar o desarmar la partición con el teclado. Ambos códigos PIN deben pertenecer a los usuarios que tienen la atribución de usuario requerida para la operación (Armado o Desarmado). Si no se introduce el segundo código PIN dentro de los 30 segundos, o si este es incorrecto, no se podrá armar o desarmar la partición.
Modo de armado forzado	Opciones de partición para operación de armado forzado (normal o bloqueado).
Restaurac. aut. en arm. forzado	Marque esta opción para restaurar automáticamente zonas cerradas durante el armado forzado. Con esta opción seleccionada, si hay una alerta activa o si se debe restaurar una zona, se restaurará de forma automática.

Asistencia para trabajo fuera de horario

Un ejemplo del uso de los parámetros de armado y desarmado es en situaciones de trabajo fuera de horario en las que el calendario se ha configurado para el armado automático de las instalaciones a un horario particular, pero el personal debe trabajar hasta tarde y se debe retardar el armado automático.

Cada retardo se determina por el período de tiempo configurado en el parámetro **Intervalo de retardo**, y el parámetro **Contador de retardo** determina la cantidad de veces que se puede retardar. Para usar esta función, el usuario necesita el valor correcto en **Retardo armado automático**.

Existen tres formas de retardar la función:

1. Introduciendo el código PIN en el teclado.
   RETARDO es una opción de menú en el teclado estándar. Los botones en la parte superior del teclado Comfort se usan para la función de retardo
2. Mediante el conmutador llave.
   Si se gira la llave a la derecha, el armado del sistema se retarda durante el tiempo que esté configurado, siempre y cuando no se haya sobrepasado la cantidad máxima de veces que se puede retardar el armado (**Contador de retardo**). Si se gira la llave hacia la izquierda, se establece un retardo de tres minutos (no configurable). Esto puede realizarse independientemente de la cantidad de veces que se retarde la función.
3. Mediante el uso de un mando vía radio, una APR o un botón que activa una acción de **Retardo autoarmado**.

Desarmado temporal

Para permitir que el sistema se desarme temporalmente en un período de tiempo especificado en el calendario, se deben configurar los siguientes tres parámetros:

1. **Calendario**
   Se debe configurar y seleccionar un calendario para esta partición.
2. **Bloqueo tiempo**
   Se debe marcar esta casilla para que se pueda desarmar la partición únicamente cuando lo permita el calendario configurado.
3. **Duración desarmado**
   El valor de este parámetro debe ser superior a cero para establecer un límite superior respecto del horario en el que se desarmará la partición.

Todo OK

Se requiere introducir «Todo OK»	Si está seleccionada, el usuario debe confirmar la entrada «Todo OK» o se generará una alarma silenciosa. Consulte *Editar una zona* en la página 274 para obtener más información sobre cómo configurar una entrada de zona «Todo OK».
Temporización «Todo OK»	Período de tiempo (en segundos) dentro del cual debe confirmarse la entrada 'Todo OK' antes de que se dispare una alarma. (Rango: 1–999 segundos)
Incidencia «Todo OK»	Seleccione el tipo de incidencia que se enviará cuando caduque el temporizador de «Todo OK». Las opciones son Pánico (silencioso), Pánico y Coacción.

Salida RF

Tiempo salida RF	Introduzca la cantidad de segundos que permanecerá activa la salida RF. «0 segundos» habilitará o deshabilitará la salida.

Ruta de salida en caso de incendio

Ruta salida incendio	Seleccione las puertas que se abrirán cuando se dispare una alarma de incendio en esta partición. Esta opción no se muestra en modo doméstico.

Disparadores de partición

La sección Disparadores solo se muestra si los disparadores se han definido previamente. (Consulte *Disparadores* en la página 295.)

Haga clic en el botón **Editar** para añadir, editar o borrar las condiciones de los disparadores para esta partición. Aparecerá la siguiente página:

Configure el disparador para la partición con los siguientes parámetros:

Disparador	Seleccione un disparador del menú desplegable.
Activación	Este disparador puede activarse desde la opción positiva o negativa de la señal de activación.
Acción	Esta es la acción que se lleva a cabo cuando se activa el disparador. Las opciones son: • Desarmado • Armado parcial A • Armado parcial B • Armado total • Retardo autoarmado Esta acción retardará el armado de la alarma cuando el temporizador de autoarmado esté en marcha. El disparador solo añadirá tiempo si no se ha superado el Límite de retardo y cada activación del disparador retardará el armado en función del tiempo definido en el Intervalo de retardo (consulte *Armado/Desarmado* en la página 281). • Restauración alarmas Esta acción borrará todas las alarmas en la zona configurada.

Aviso: No se pueden configurar los disparadores desde un teclado.

Consulte también

Disparadores en la página 295

17.9.5.3 Editar una puerta

1. Seleccione **Configuración > Puertas**.

   Se muestra una lista de puertas configuradas.

2. Haga clic en el botón **Editar**.
3. Configure los campos tal como se describe en las siguientes tablas.

Entradas de puerta

Cada puerta tiene 2 entradas con funcionalidad definida previamente. Se pueden configurar estas dos entradas, el sensor de posición de puerta y el interruptor de liberación de puerta.

Nombre	Descripción
Zona	La entrada del sensor de posición de puerta también se puede utilizar para la parte de intrusión. Si se utiliza la entrada del sensor de posición de puerta para la parte de intrusión, se debe seleccionar el número de zona a la cual está asignada. Si se utiliza la entrada del sensor de posición de puerta para la parte de acceso, se debe seleccionar la opción «SIN ASIGNAR». Si se asigna el sensor de posición de puerta a una zona de intrusión, puede configurarse como una zona normal, pero con funcionalidad limitada (por ejemplo: no se pueden seleccionar todos los tipos de zonas). Si una partición o el sistema está configurado con un lector de tarjetas, la entrada del sensor de posición de puerta debe estar asignada a un número de zona y a la partición o el sistema que se debe armar.
Descripción (Web únicamente)	Descripción de la zona a la cual está asignado el sensor de posición de puerta.
Tipo de zona (Web únicamente)	Tipo de zona de la zona a la cual está asignado el sensor de posición de puerta (no todos los tipos de zonas están disponibles).
Atributos de zona (Web únicamente)	Se pueden modificar los atributos para la zona a la cual está asignado el sensor de posición de puerta.
Particiones (Web únicamente)	La partición a la cual están asignados la zona y el lector de tarjeta. (Si se utiliza el lector de tarjetas para el armado y desarmado, esta partición se armará/desarmará).
Posición de puerta (web) RFL posic.puerta (teclados)	La resistencia utilizada con el sensor de posición de puerta. Seleccione el valor o la combinación de resistencia utilizada.
DPS normalmente abierto	Seleccione si el interruptor de liberación de puerta debe ser una entrada normalmente abierta o normalmente cerrada.
Liberar puerta (web) RFL LIBER.PUERTA (teclados)	La resistencia utilizada con el interruptor de liberación de puerta. Seleccione el valor o la combinación de resistencia utilizada.

Nombre	Descripción
DRS normalmente abierto	Seleccione si el interruptor de liberación de puerta es una entrada abierta normalmente o no.
Sin DRS (Web únicamente)	Seleccione esta opción para ignorar DRS. Si se utiliza un DC2 en la puerta, se DEBE seleccionar esta opción. Si no se selecciona, la puerta se abrirá.
Localización lector (Entrada/salida) (Web únicamente)	Seleccione la ubicación de los lectores de entrada y salida.
Formatos de lector (web) INFORMACIÓN DEL LECTOR (teclados)	Se muestra el formato de la última tarjeta utilizada con cada lector configurado.

Cada número de zona libre puede ser asignado a las zonas, pero la asignación no es fija. Si se asigna el número 9 a una zona, dicha zona y un módulo de expansión de entrada con la dirección ‘1’ se conectan al X-Bus (que está utilizando los números de zona 9–16). La zona asignada desde el controlador de dos puertas se trasladará al siguiente número de zona libre. La configuración se adaptará en consecuencia.

Atributos de puerta

Si no hay ningún atributo activado, se puede usar una tarjeta válida.

Atributo	Descripción
Nulo	La tarjeta se bloquea temporalmente.
Grupo de puertas	Se utiliza cuando se asignan diversas puertas a la misma partición y/o se requiere funcionalidad de anti-retorno, custodia o interbloqueo.
Tarjeta y PIN	Se requiere tarjeta y código PIN para entrar.
Solo código PIN	Se requiere código PIN. No se aceptará ninguna tarjeta.
Código PIN o tarjeta	Se requiere código PIN o tarjeta para entrar.
Código PIN para salir	Se requiere código PIN en lector de salida. Se requiere puerta con lector de entrada y salida.
PIN para desarmar	Se requiere PIN para armar y desarmar la partición vinculada. Antes de introducir el código PIN, se debe presentar la tarjeta.

Atributo	Descripción
Desarmado desde exterior (navegador)	Cuando se presente la tarjeta en el lector de entrada, la partición/área se desarmará.
Desarmado desde interior (navegador)	Cuando se presente la tarjeta en el lector de salida, la partición/área se desarmará.
Anular alarma	Se permite el acceso si la partición está armada y la puerta es un tipo de zona de entrada o con alarma.
Armado total desde exterior (navegador)	Cuando se presente dos veces la tarjeta en el lector de entrada, la partición/área se armará totalmente.
Armado total desde interior	Cuando se presente dos veces la tarjeta en el lector de salida, la partición/área se armará totalmente.
Armado total forzado	Si el usuario cuenta con los derechos necesarios, puede forzar el armado desde el lector de entrada.
Emergencia	La puerta bloqueada se abre si se detecta una alarma de incendio dentro de la partición asignada.
Otra emergencia	Una alarma de incendio en cualquier otra partición desbloqueará la puerta.
Acompañante	La función de Visita obliga a los titulares de tarjetas con este privilegio a acompañar a otros titulares de tarjetas por puertas específicas. Si esta función está asignada a una puerta, se debe presentar primero una tarjeta con derecho de Visita para permitir abrir la puerta a otros titulares de tarjeta sin este derecho. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con derecho de Visita; se puede configurar individualmente para cada puerta.
Evitar retorno*	Se debe reforzar la funcionalidad anti-retorno en la puerta. Todas las puertas deben tener lectores de entrada y salida, y deben estar asignadas a un grupo de puertas. En este modo, los titulares de tarjeta deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta válido presentó su tarjeta de acceso para entrar a un grupo de puertas y no presentó la tarjeta para salir, el titular está incumplimiento las normas de anti-retorno. La próxima vez que el titular de tarjeta intente acceder al mismo grupo de puertas, se disparará una alarma de anti-retorno estricta y el titular no tendrá autorización para entrar al grupo de puertas.
Retorno laxo*	Los incumplimientos de las normas anti-retorno solo se registran. Todas las puertas deben tener lectores de entrada y salida, y deben estar asignadas a un grupo de puertas. En este modo, los titulares de tarjeta deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta válido presentó su tarjeta de acceso para entrar a un grupo de puertas y no presentó la tarjeta para salir, el titular está incumplimiento las normas de anti-retorno. La próxima vez que el titular de tarjeta intente acceder al mismo grupo de puertas, se disparará una alarma de anti-retorno laxa. Sin embargo, el titular de la tarjeta seguirá teniendo autorización para entrar al grupo de puertas.

Atributo	Descripción
Custodia*	La función Custodia le permite al titular de la tarjeta con derecho de Custodia (el custodia) conceder a otros titulares de tarjetas (que no son custodia) acceso a la sala. El usuario Custodia debe ser el primero en entrar en la sala. Los usuarios que no son custodia solo pueden ingresar si el custodia está en la sala. El custodia no podrá salir hasta que todos los usuarios que no son custodia hayan salido de la sala.
Sirena puerta	La sirena integrada en la placa del controlador de puerta suena cuando se activan las alarmas de puerta.
Ignorar forzado	La apertura forzada de la puerta no se procesa.
Interrelacionada* (navegador)	Solo se permitirá la apertura de una sola puerta de la partición a la vez. Requiere Grupo de puertas.
Prefijo de armado	Autorización con prefijo de clave (A, B, * o #) para armar el sistema

* Requiere Grupo de puertas

Temporizadores de puerta

Temporizador	Mín.	Máx.	Descripción
Acceso autorizado	1 s	255 s	El período de tiempo durante el cual la cerradura permanecerá abierta tras la autorización de acceso.
Acceso denegado	1 s	255 s	Período de tiempo tras la cual el controlador estará listo para leer la siguiente incidencia tras una incidencia no válida.
Puerta abierta	1 s	255 s	Período de tiempo dentro del cual la puerta debe estar cerrada para evitar una alarma de «puerta abierta tiempo excesivo».
Puerta dejada abierta	1 min	180 min	Período de tiempo dentro del cual la puerta debe estar cerrada para evitar una alarma de «puerta dejada abierta».
Extendido	1 s	255 s	Tiempo adicional tras la autorización de acceso a una tarjeta con un atributo de tiempo extendido.
Acompañante	1 s	30 s	Período de tiempo después de presentar una tarjeta con atributo de Visita dentro del cual un usuario sin atributo de Visita puede acceder por la puerta.

Calendario de puertas

Puerta bloqueada	Seleccione el calendario que debe bloquear la puerta durante el período configurado. No se aceptará el uso de tarjeta o código PIN durante este período de tiempo.
Puerta bloqueada	Seleccione el calendario que debe desbloquear la puerta. La puerta se desbloqueará durante el período de tiempo configurado.

Disparadores de puertas

Trigger (activador)	Descripción
Activación desbloqueo momentáneo puerta	Si la activación asignada está activada, la puerta se desbloqueará durante un período definido y, a continuación, se volverá a bloquear.

Trigger (activador)	Descripción
Disparador que bloqueará la puerta	Si se activa el disparador asignado, la puerta se bloqueará. No se aceptará el uso de tarjeta o código PIN.
Disparador que desbloqueará la puerta	Si se activa el disparador asignado, la puerta se desbloqueará. No será necesario utilizar tarjeta/código PIN para abrir la puerta.
Disparador que restablecerá el estado de la puerta a normal	Si se activa el disparador asignado, la puerta regresará a su estado de funcionamiento normal. Esto es para deshacer el bloqueo/desbloqueo de la puerta. Será necesario utilizar tarjeta/código PIN para abrir la puerta.

Interbloqueo de puertas

El interbloqueo de puertas es una función que evita que las puertas restantes del grupo se abran si una de las puertas del grupo está abierta.

A continuación, se muestra un ejemplo de cómo se utiliza esta función:

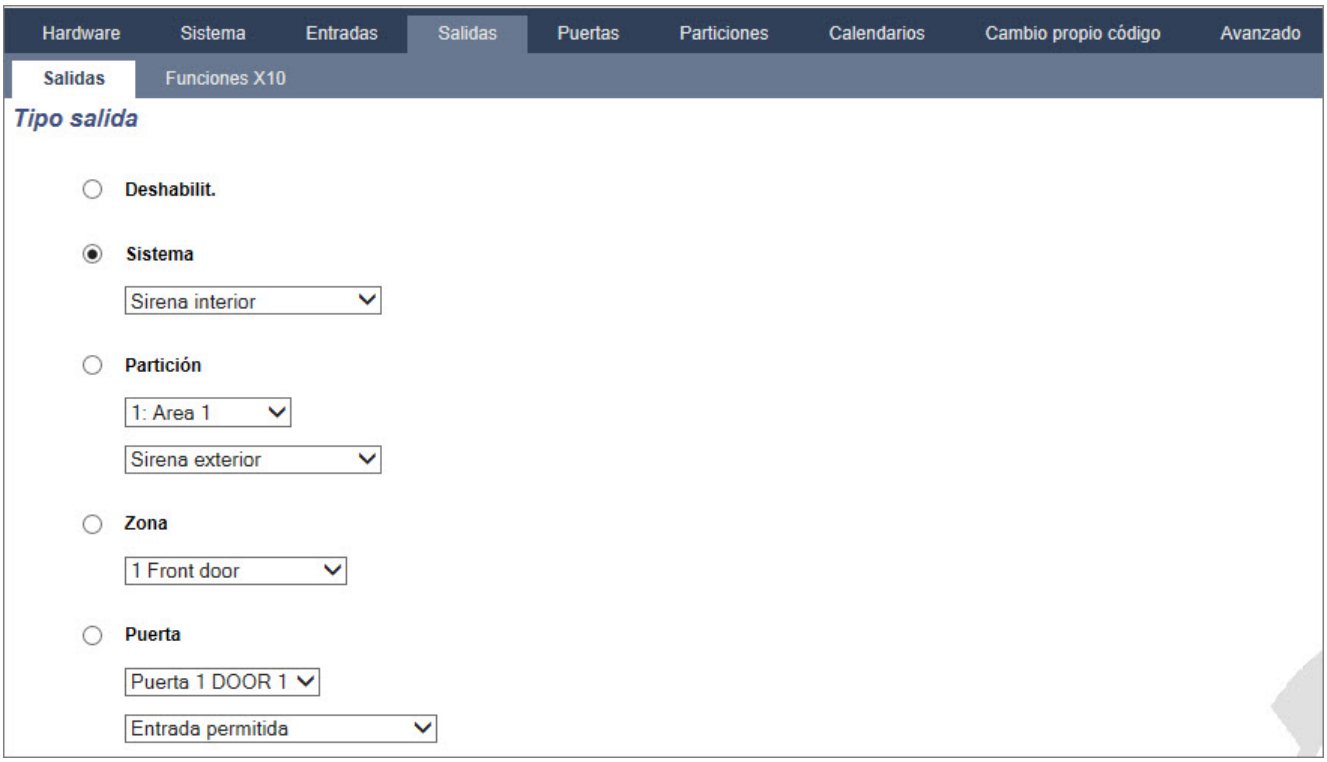
- En los sistemas de entrada de dos puertas utilizados en algunos bancos y otros edificios. Generalmente, se utilizan botones pulsadores o lectores de tarjetas para poder entrar, y las luces LED roja y verde muestran si se puede abrir la puerta o no.
- En particiones técnicas de cajeros automáticos que conectan las puertas de los cajeros automáticos. Generalmente se interbloquean todas las puertas de los cajeros automáticos, además de la puerta que permite el acceso a la partición.

Para crear un bloqueo de puertas:

1. Cree un grupo de puertas. Consulte *Editar una puerta* en la página 283.
2. Configure el atributo **Interbloqueo** para todas las puertas requeridas del grupo. Consulte *Editar una puerta* en la página 283.
3. Configure el funcionamiento de interbloqueo de puerta para una salida de puerta. Esta salida se activa para todas las puertas del grupo de interbloqueo cuando se abre una puerta del grupo, incluyendo la misma puerta abierta.
   Esta salida podría conectarse, por ejemplo, a una luz LED roja u otra luz para indicar que no se pudo abrir la puerta, y si se invierte podría conectarse a una luz LED verde u otro tipo de luz.

Para configurar una salida para interbloqueo de puerta.

1. En modo técnico completo, seleccione **Configuración > Hardware > X-BUS > Módulos expansión**.
2. En la página **Configuración de módulos de expansión**, haga clic en el botón **Cambiar tipo** para la salida que corresponda.
3. Seleccione **Puerta** como tipo de salida.
4. Seleccione la puerta que corresponda e **Interbloqueo** como tipo de salida.



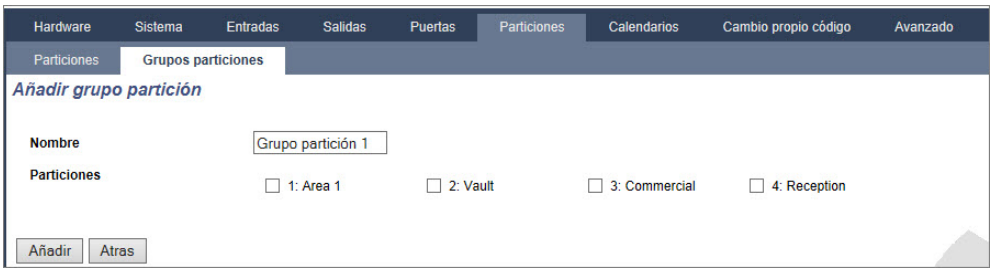
17.9.5.4 Añadir un grupo de particiones

Puede utilizar grupos de particiones para configurar diversas particiones. De esta forma, no es necesario configurar partición por partición.

Requisito previo

- Solo si la opción Particiones (múltiples) está activa.

1. Seleccione **Configuración > Particiones > Grupos de particiones**.



2. Haga clic en el botón **Añadir**.
3. Introduzca una descripción para el grupo.
4. Seleccione las particiones que asignará a este grupo.
5. Haga clic en **Añadir**.

AVISO: Para utilizar los grupos de particiones para el teclado Comfort, active todas las particiones en el campo **Particiones**, en **Configuración > Hardware > X-BUS > Teclados > Tipo: Teclado Comfort**.

17.9.6 Calendarios

Los calendarios sirven para programar el control basado en tiempos para realizar múltiples operaciones en la central, como se indica a continuación:

- Armado y/o desarmado automático de particiones
- El armado y/o desarmado automático de otras operaciones de la central, incluyendo disparadores, habilitación de usuarios, zonas, salidas físicas, etc.

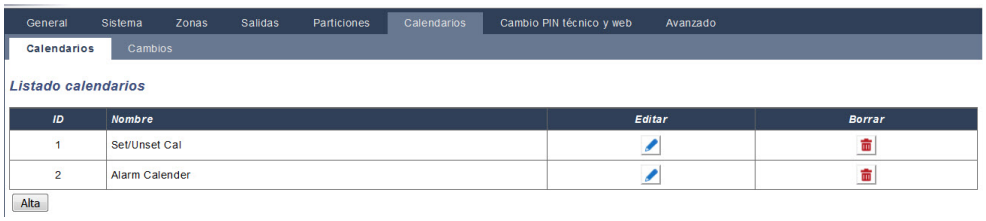
En cualquier momento, cualquier programación dentro del calendario puede estar «activa» si se cumplen sus condiciones temporales.

Cada semana del año tiene asignado un número ordinal. Según los días de cada mes, un año puede tener 52 o 53 semanas. La implementación del calendario de SPC cumple con el estándar internacional ISO 8601.

Configuración de calendarios

- Seleccione **Configuración > Calendarios**.

  Se muestra una lista de calendarios configurados:



Acciones ejecutables

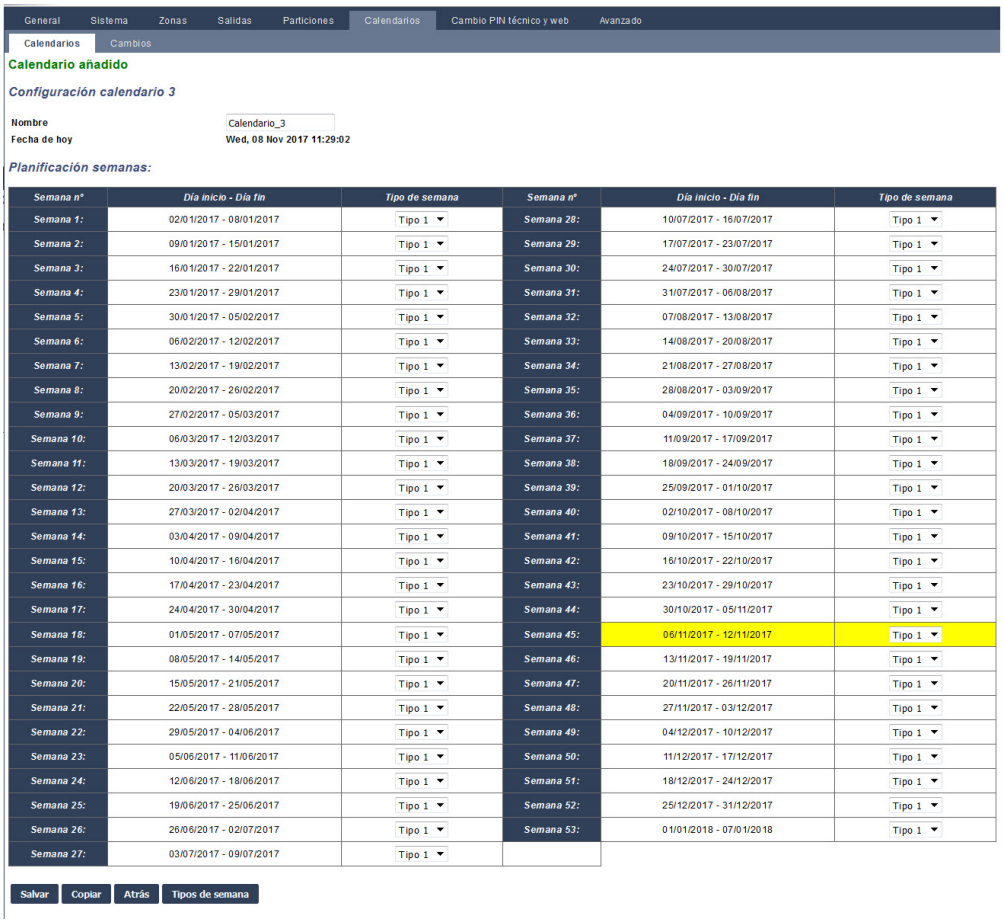
Agregar	Añadir un nuevo calendario.
Excepciones	Configurar una programación para circunstancias excepcionales fuera de las programaciones semanales normales.
Editar/Ver	Permite editar o ver el calendario seleccionado.
Borrar	Se borra el calendario seleccionado. El calendario no se puede borrar si está asignado actualmente a un elemento de configuración del SPC, es decir, zona, partición, perfil de usuario, salida, disparador, puerta o componente de X-Bus. Se muestra un mensaje indicando el elemento asignado.

Los calendarios globales creados mediante SPC Manager no se pueden borrar, como puede verse más arriba en el Calendario 3.

17.9.6.1 Añadir/Editar un calendario

1. Seleccione **Configuración > Calendarios > Añadir**.

   Se mostrará la siguiente página:



Semana nº	Día inicio - Día fin	Tipo de semana	Semana nº	Día inicio - Día fin	Tipo de semana
Semana 1:	02/01/2017 - 08/01/2017	Tipo 1	Semana 28:	10/07/2017 - 16/07/2017	Tipo 1
Semana 2:	09/01/2017 - 15/01/2017	Tipo 1	Semana 29:	17/07/2017 - 23/07/2017	Tipo 1
Semana 3:	16/01/2017 - 22/01/2017	Tipo 1	Semana 30:	24/07/2017 - 30/07/2017	Tipo 1
Semana 4:	23/01/2017 - 29/01/2017	Tipo 1	Semana 31:	31/07/2017 - 06/08/2017	Tipo 1
Semana 5:	30/01/2017 - 05/02/2017	Tipo 1	Semana 32:	07/08/2017 - 13/08/2017	Tipo 1
Semana 6:	06/02/2017 - 12/02/2017	Tipo 1	Semana 33:	14/08/2017 - 20/08/2017	Tipo 1
Semana 7:	13/02/2017 - 19/02/2017	Tipo 1	Semana 34:	21/08/2017 - 27/08/2017	Tipo 1
Semana 8:	20/02/2017 - 26/02/2017	Tipo 1	Semana 35:	28/08/2017 - 03/09/2017	Tipo 1
Semana 9:	27/02/2017 - 05/03/2017	Tipo 1	Semana 36:	04/09/2017 - 10/09/2017	Tipo 1
Semana 10:	06/03/2017 - 12/03/2017	Tipo 1	Semana 37:	11/09/2017 - 17/09/2017	Tipo 1
Semana 11:	13/03/2017 - 19/03/2017	Tipo 1	Semana 38:	18/09/2017 - 24/09/2017	Tipo 1
Semana 12:	20/03/2017 - 26/03/2017	Tipo 1	Semana 39:	25/09/2017 - 01/10/2017	Tipo 1
Semana 13:	27/03/2017 - 02/04/2017	Tipo 1	Semana 40:	02/10/2017 - 08/10/2017	Tipo 1
Semana 14:	03/04/2017 - 09/04/2017	Tipo 1	Semana 41:	09/10/2017 - 15/10/2017	Tipo 1
Semana 15:	10/04/2017 - 16/04/2017	Tipo 1	Semana 42:	16/10/2017 - 22/10/2017	Tipo 1
Semana 16:	17/04/2017 - 23/04/2017	Tipo 1	Semana 43:	23/10/2017 - 29/10/2017	Tipo 1
Semana 17:	24/04/2017 - 30/04/2017	Tipo 1	Semana 44:	30/10/2017 - 05/11/2017	Tipo 1
Semana 18:	01/05/2017 - 07/05/2017	Tipo 1	Semana 45:	06/11/2017 - 12/11/2017	Tipo 1
Semana 19:	08/05/2017 - 14/05/2017	Tipo 1	Semana 46:	13/11/2017 - 19/11/2017	Tipo 1
Semana 20:	15/05/2017 - 21/05/2017	Tipo 1	Semana 47:	20/11/2017 - 26/11/2017	Tipo 1
Semana 21:	22/05/2017 - 28/05/2017	Tipo 1	Semana 48:	27/11/2017 - 03/12/2017	Tipo 1
Semana 22:	29/05/2017 - 04/06/2017	Tipo 1	Semana 49:	04/12/2017 - 10/12/2017	Tipo 1
Semana 23:	05/06/2017 - 11/06/2017	Tipo 1	Semana 50:	11/12/2017 - 17/12/2017	Tipo 1
Semana 24:	12/06/2017 - 18/06/2017	Tipo 1	Semana 51:	18/12/2017 - 24/12/2017	Tipo 1
Semana 25:	19/06/2017 - 25/06/2017	Tipo 1	Semana 52:	25/12/2017 - 31/12/2017	Tipo 1
Semana 26:	26/06/2017 - 02/07/2017	Tipo 1	Semana 53:	01/01/2018 - 07/01/2018	Tipo 1
Semana 27:	03/07/2017 - 09/07/2017	Tipo 1			

2. Indique una **Descripción** para el calendario (máx. 16 caracteres).

Copiar un calendario

Para realizar una copia de este calendario, haga clic en el botón **Replicar**.

Se crea un nuevo calendario con la misma configuración que el calendario original. Puede proporcionar una nueva descripción para el nuevo calendario y editar su configuración según sea necesario.

Tipos de semana

Los calendarios se configuran asignando un tipo de semana opcional por cada semana natural. Se puede definir un máximo de tres tipos de semana para cada calendario. No es necesario que todas las semanas tengan un Tipo de semana (por ejemplo, el tipo de semana puede ser 'Ninguno'). El sistema permite un máximo de 64 configuraciones de calendario.

Para configurar un tipo de semana

1. Haga clic en **Tipos de semana**.
2. Introduzca las horas deseadas para armado/desarmado o para disparadores. Utilice las directrices sobre tiempo para Armado/desarmado automático de particiones (consulte *Armado/desarmado automático de particiones* en la página 293), o para Armado/desarmado automático de otras operaciones en la central (consulte *Armado/desarmado automático de otras operaciones en la central* en la página 293).

   Se pueden configurar hasta tres tipos de semana.
3. Haga clic en **Salvar** y, a continuación, en **Atrás**.

4. Seleccione el tipo de semana deseado en el menú desplegable para cada una de las semanas programadas deseadas en el calendario.
5. Haga clic en **Salvar**.
6. Haga clic en **Atrás**.

Consulte también

Armado/desarmado automático de particiones en la página opuesta

Armado/desarmado automático de otras operaciones en la central en la página opuesta

Excepciones

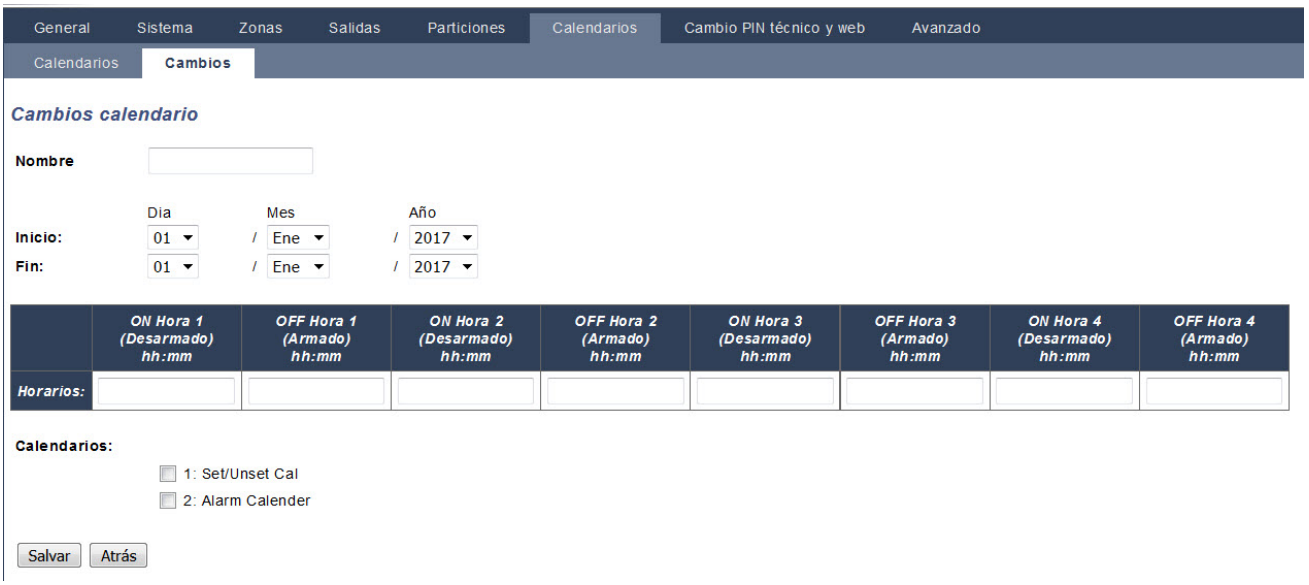
Las excepciones, o días especiales, sirven para configurar programaciones automáticas para circunstancias excepcionales fuera de las programaciones semanales normales definidas en los calendarios. Las excepciones se definen con una fecha de inicio y otra de fin (día/mes/año), y hasta cuatro períodos de tiempo de activación/desactivación para diferentes operaciones de la central, incluyendo el armado/desarmado automático de particiones, o la conexión/desconexión de fuentes o salidas. Se pueden configurar un máximo de 64 excepciones en el sistema.

Las excepciones son entidades genéricas que se pueden asignar a uno o varios calendarios. Cuando se asigna una excepción a un calendario, la configuración de la excepción anula cualquier configuración para dicho período de inicio y fin incluidas ambas fechas.

Configuración de días especiales

1. Seleccione **Configuración > Calendarios > Días excepcionales > Añadir**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

Descripción	Introduzca un nombre para la excepción (máx. 16 caracteres).
Fecha inicio / Fecha fin	Seleccione la fecha de inicio y de fin.
En hora / Fuera de hora	Seleccione las horas deseadas para armado/desarmado o para disparadores. Utilice las directrices sobre tiempo para Armado/desarmado automático de particiones (consulte *Armado/desarmado automático de particiones* abajo), o para Armado/desarmado automático de otras operaciones en la central (consulte *Armado/desarmado automático de otras operaciones en la central* abajo).
Calendarios	Seleccione el calendario deseado para que tenga efecto.

AVISO: Los días excepcionales globales creados de forma remota mediante la herramienta SPC Manager no se pueden editar ni eliminar.

17.9.6.2 Armado/desarmado automático de particiones

Puede configurar el calendario para el armado o desarmado automático de las particiones.

Para cualquier día de la semana, la configuración puede tener un máximo de 4 horarios de armado y 4 de desarmado. Los horarios configurados utilizan el reloj de 24 horas (hh:mm). Si la hora es 24, los minutos deben ser 00, pues la medianoche es 24:00. Se puede definir una hora de armado sin desarmado y viceversa. Los horarios configurados le indican el armado o desarmado a la partición (siempre que se cumplan todas las condiciones). Los horarios introducidos no se consideran una duración de tiempo, sino un punto en el tiempo para que se genere tal acción (armado/desarmado). Si el controlador está encendido o se restablece, se conserva el estado de armado/desarmado y se mantienen los horarios de armado y desarmado subsiguientes de conformidad con la configuración.

17.9.6.3 Armado/desarmado automático de otras operaciones en la central

Las operaciones en la central, incluyendo fuentes, habilitación de usuarios, zonas o salidas físicas se pueden armar o desarmar automáticamente mediante las configuraciones de estado Activado/Desactivado, Verdadero/Falso o Activo/Inactivo.

Los estados Activado/Desactivado, Verdadero/Falso o Activo/Inactivo se pueden asignar a una salida que se active o desactive efectivamente para cualquier día de la semana. Las configuraciones de estado cuentan con un máximo de cuatro horas de Armado y cuatro de Desarmado. Los horarios configurados utilizan el reloj de 24 horas (hh:mm). Si la hora es 24, los minutos deben ser 00, pues la medianoche es 24:00. Cada configuración consta de un par de ajustes para estados Activado/Desactivado, Verdadero/Falso o Activo/Inactivo. Cualquier ajuste sin su configuración respectiva correspondiente será ignorado.

17.9.7 Cambiar código PIN propio

Para cambiar un código PIN, consulte *Cambio de código de técnico y de clave web* en la página 223.

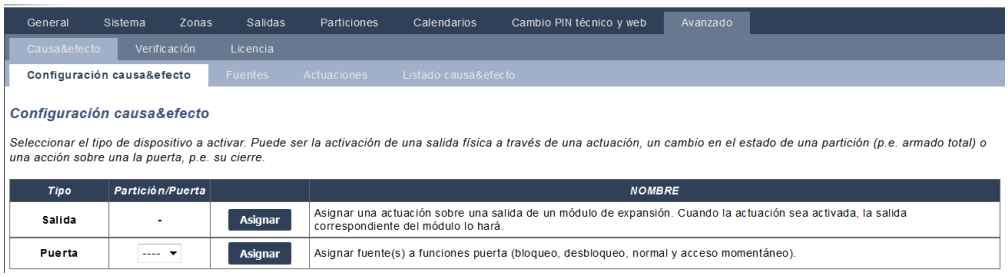
17.9.8 Configuración de ajustes avanzados

Esta sección abarca:

17.9.8.1 Causa y efecto

1. Seleccione **Configuración > Avanzada > Causa y efecto**.

   Se mostrará la siguiente página.



2. Haga clic en un botón Asignar para realizar una de las siguientes acciones:
   - **Salida:** Asigna una puerta de mapeo (salida virtual) para activar una salida física. Seleccione esta opción para mostrar la página **Puerta de mapeo - Lista**. Para obtener más información consulte *Actuaciones* abajo.
   - **Partición:** Asigna un disparador (entrada virtual) para activar la acción de una partición. Escoja una **Partición** del menú desplegable antes de hacer clic en el botón **Asignar**. Para obtener más información consulte *Disparadores* en la página opuesta.
   - **Puerta:** Asigna un disparador (entrada virtual) para activar la acción de una puerta. Escoja una **Puerta** del menú desplegable antes de hacer clic en el botón **Asignar**.

Para mostrar la lista de disparadores y acciones configuradas, seleccione **Configuración > Avanzada > Causa y efecto > Lista de causa y efecto**.

La página **Lista de causa y efecto** mostrará solo las causas y efectos en funcionamiento. Por ejemplo, si una puerta de mapeo no está asignada a un disparador o una tecla de activación, no aparecerá en la lista.

ADVERTENCIA: Su sistema no cumplirá las normas EN si habilita un disparador para armar el sistema sin que se requiera un código PIN válido.

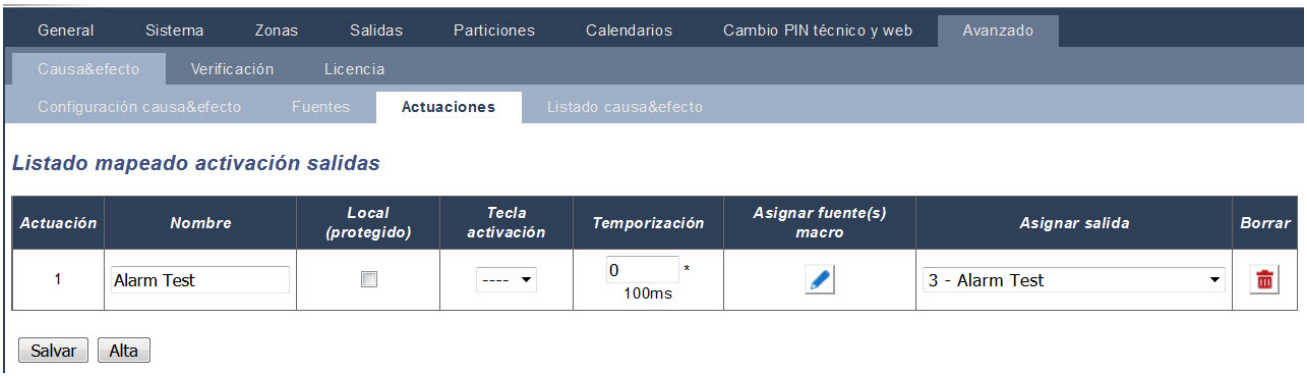
17.9.8.2 Actuaciones

Se utilizan disparadores con puertas de mapeo, las cuales son salidas virtuales definidas por el usuario que pueden mapearse a una salida física. Puede haber un máximo de 512 salidas de sistema.

Para una salida continua, cuando el disparador es un código de usuario válido, ambos estados deben ser iguales, ya sean positivos o negativos.

1. Seleccione **Configuración > Avanzada > Causa y efecto > Puertas de mapeo**.

   Aparecerá la siguiente página.



2. Introduzca una **descripción** para la puerta. Esto es importante, ya que no se muestra el número de puerta de mapeo, solo la descripción, en la página de usuario **Salidas** para habilitar y deshabilitar las puertas.
3. Marque la casilla **Local** si no desea que los usuarios habiliten y deshabiliten esta puerta, incluso si tienen el derecho para hacerlo. Las puertas locales no son visibles de forma remota.
4. Seleccione la **Tecla de activación** deseada.
   Una tecla de activación es una almohadilla (#) seguida de un único dígito que se pulsa en el teclado. Si se configura un atajo y este se pulsa en el teclado, se solicita al usuario que active o desactive la salida.

Un atajo puede activar muchas salidas, tanto X-10 como puertas de mapeo.

5. Añada un **Temporizador** para la puerta. El tiempo utilizado es una décima de un segundo.
6. Haga clic en el botón **Disparadores** para configurar disparadores para la activación y desactivación de la salida. En ambos casos, se debe definir un límite positivo o negativo en el disparador. Consulte *Disparadores* abajo para obtener más información sobre la configuración de los disparadores.
7. Seleccione una salida del menú desplegable.
8. Haga clic en **Añadir** para añadir una puerta nueva o en **Salvar** para salvar la nueva configuración de una puerta existente.

Consulte también

Disparadores abajo

17.9.8.3 Disparadores

Un disparador es un estado del sistema (por ejemplo: cierre de zona/temporizador/incidencia del sistema [alarma], etc.) que puede utilizarse como entrada para Causas y efectos. Los disparadores pueden ser asignados de forma lógica en conjunto con los operadores lógicos y/o para crear salidas de usuario. El sistema admite un máximo de 1024 macros por todo su sistema de Causa & Efecto.

1. Seleccione **Configuración > Avanzada > Disparadores**.

   Se mostrará la siguiente página.

2. Configure los campos tal como se describe en la siguiente tabla.

Trigger (activador)	Número generado por el sistema para el nuevo disparador. El disparador solo estará habilitado si se configura uno de los dos pasos opciones (limitación de tiempo/calendario)
Descripción	Introduzca una descripción del disparador.
Calendario	Seleccione un calendario, si corresponde. Si hay un calendario seleccionado, la macro sólo funcionará durante este periodo de tiempo. Consulte *Calendarios* en la página 289.
Límite de horario	Seleccione un período de tiempo entre 00:00 a 24:00 durante el cual el disparador estará habilitado. El tiempo de inicio es inclusivo y el tiempo de finalización es exclusivo. **Nota:** Este parámetro retarda la transición de un disparador de ACT a DES únicamente; de DES a ACT es inmediato.
Temporizador	Introduzca la cantidad de segundos durante la cual las condiciones del disparador deben ser ciertas antes de que se active.
Funcionamiento del disparador	• **Todas** Todas las condiciones del disparador deben estar activadas para que el sistema active el disparador. • **Cualquiera** Cualquier condición que está activa habilita el sistema para activar el disparador.

Acciones ejecutables

Agregar	Añadir condiciones para el disparador. Haga clic en este botón para añadir una o más condiciones para el activador seleccionado. Consulte *Condiciones del disparador* en la página opuesta.
Excepciones	Configure programaciones de armado para circunstancias excepcionales fuera de las programaciones semanales normales.
Editar/Ver	Permite editar o ver el calendario seleccionado.
Borrar	Se borra el calendario seleccionado. No se puede borrar el calendario si está actualmente asignado a un elemento de configuración de SPC, es decir: partición, área, perfil de usuario, salida, disparador, puerta o componente X-BUS. Se muestra un mensaje indicando el elemento asignado.

Condiciones del disparador

La siguiente tabla muestra las condiciones del disparador y los estados, salidas, incidencias o comunicaciones asociadas.

Condición del disparador	Estados, salidas, incidencias o comunicaciones
Zona	El disparador está ACT si se cumplen las siguientes condiciones (p. ej., se realiza una operación AND lógica): El disparador está ACT si la zona configurada está en uno de los siguientes estados: **Abierta**, **Cerrada**, **Cortocircuito** o **Desconectada**.
Puerta	El disparador está ACT si cualquiera de las siguientes opciones de puerta está configurada: **Acceso autorizado**, **Acceso denegado**, **Salida autorizada**, **Salida denegada**, **Puerta abierta tiempo excesivo**, **Puerta dejada abierta**, **Puerta forzada**, **Puerta normal**, **Puerta bloqueada**, **Puerta desbloqueada**.
Salida	El disparador está ACT si la salida del sistema se encuentra en el estado configurado, el cual puede ser **ACT** o **DES**: **Salida del sistema**, **Puerta de mapeo**, **Salida de partición**.
Sistema	El disparador está ACT para la incidencia del sistema y el ID escogidos. Los ID son: **Reinicio sistema**, **Sobrecarga**, **Acceso de técnico**, **Acceso de fabricante**, **Fallo cable X-BUS**, **Fallos X-BUS**. **Tiempo del disparador**: El disparador se activa a la hora específica introducida en el cuadro proporcionado, en formato hh:mm.
Operador	**Mando vía radio**: Esta condición se puede configurar para un usuario en particular o para cualquier usuario. Con esta configuración, si el usuario configurado (o cualquier usuario) pulsa la tecla '*' en el mando vía radio, provocará un pulso instantáneo ACT/DES/ACT. Esto sólo es aplicable a mandos vía radio que hayan sido registrados con el sistema. **Alarma de pánico mando vía radio**: Esta condición se puede configurar para un usuario en particular o para cualquier usuario. Con esta configuración, si el usuario configurado (o cualquier usuario) pulsa la tecla '*' en el pulsador de pánico vía radio, provocará un pulso instantáneo ACT/DES/ACT. Esto sólo es aplicable a pulsadores de pánico vía radio que hayan sido registrados con el sistema. **Código PIN de teclado**: Esta condición se puede configurar para un usuario en particular o para cualquier usuario. Con esta configuración, si el usuario configurado (o cualquier usuario) introduce un PIN válido o presenta una tarjeta configurada, provocará un impulso instantáneo OFF/ON/OFF. **Tarjeta de acceso**: El disparador se activa cuando el usuario seleccionado inicia sesión con una tarjeta de acceso. **Acceso web**: El disparador se activa cuando el usuario seleccionado inicia sesión a través del navegador. **APR**: El disparador se activa si se pulsa un botón o una combinación de botones. Es posible asignar una condición de disparador para todas las APR o solo una APR específica. Cuando se define una condición de disparador de APR, puede asignarse a una puerta de mapeo para muchos fines, incluyendo el armado del sistema, el encendido de luces o la apertura de una puerta. **Acceso de teclado**: El disparador se activa cuando un usuario inicia sesión en el teclado seleccionado.

Condición del disparador	Estados, salidas, incidencias o comunicaciones
Perfil	**Código PIN de teclado:** Si un usuario con el perfil de usuario configurado introduce un código PIN válido o presenta un PACE configurado, provocará un pulso instantáneo ACT/DES/ACT. **Tarjeta de acceso**: El disparador se activa cuando un usuario con el perfil de usuario configurado inicia sesión con una tarjeta de acceso. **Acceso web**: El disparador se activa cuando un usuario con el perfil de usuario configurado inicia sesión a través del navegador.
Módulo de expansión	**Conmutador llave**: El disparador se puede configurar para una posición de llave específica en el conmutador llave. **Indicador**: El disparador se puede configurar para una tecla de función específica.
Comunicación	**ATP FlexC**: El disparador se activa por la configuración de ATS y ATP seleccionada. **ATS FlexC**: El disparador se activa por la configuración de ATS seleccionada.

ADVERTENCIA: Su sistema no cumplirá las normas EN si habilita un disparador para armar el sistema sin que se requiera un código PIN válido.

17.9.8.4 Verificación de audio/vídeo

Para configurar una verificación de audio/vídeo en un sistema SPC:

1. Instale y configure los módulos de expansión de audio.
2. Instale y configure las cámaras de vídeo.
3. Instale y configure el equipo de audio.
4. Configure las zonas de verificación.
5. Pruebe la reproducción de audio de las zonas de verificación.
6. Asigne zonas de verificación a zonas físicas.
7. Configure ajustes de verificación.
8. Vea imágenes desde las zonas de verificación en el navegador web.

AVISO: Es posible deshabilitar los teclados y el control de accesos durante varios minutos mientras se envía un archivo de audio a la central, según el tamaño del archivo.

Configurar vídeo

Visión general

Se utilizan cámaras para la verificación de vídeo. La central SPC admite un máximo de cuatro cámaras. Solo se admiten cámaras IP y la central debe tener un puerto Ethernet.

AVISO: No se deben compartir cámaras con otras aplicaciones de CCTV.

Las cámaras solo pueden configurarse con el navegador web. No se admite configuración con el teclado.

La central admite dos resoluciones de cámara:

- 320X240
  Se recomienda esta configuración si desea ver imágenes en el navegador.
- 640X480 (con algunas restricciones).

Se admiten las siguientes cámaras además de otras cámaras genéricas:

- Vanderbilt CCIC1410 (cámara IP VGA a color 1/4")
- Vanderbilt CFMC1315 (cámara domo a color para interiores 1/3" 1,3 MP)

Por defecto, hay una cadena de comandos disponible para tener acceso directamente a los detalles de la configuración de las cámaras antes mencionadas. Otras cámaras IP genéricas requieren que se introduzca manualmente la cadena de comandos.

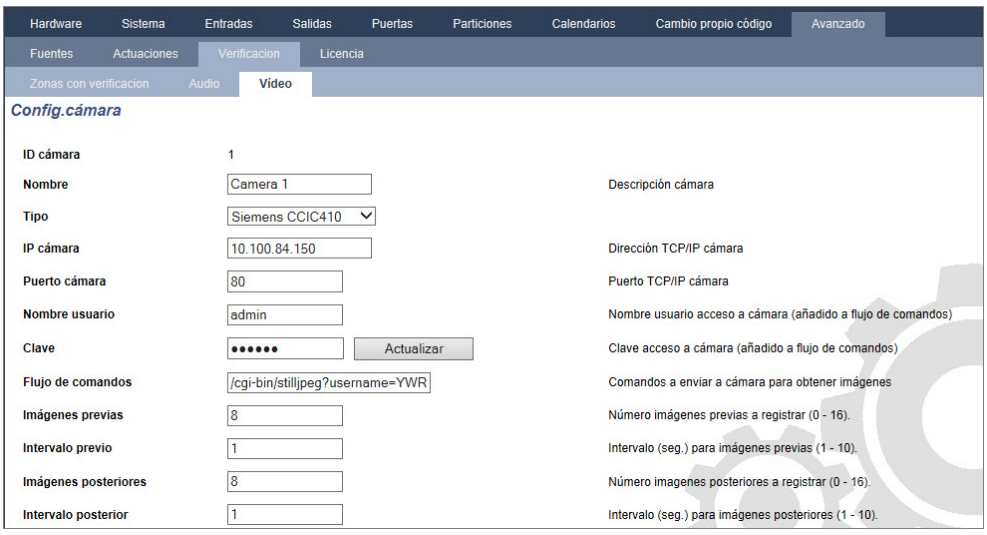
Agregar cámara

1. Seleccione **Configuración > Avanzada > Verificación > Vídeo**.

   Se muestra una lista de las cámaras configuradas anteriormente y el estado en línea o fuera de línea. Una cámara está en línea si se obtuvo imagen de la cámara dentro de los últimos 10 segundos.

2. Haga clic en el botón **Añadir** para añadir una cámara nueva o en el botón **Editar** para editar una cámara existente.

   Aparecerá la siguiente página.



3. Configure la cámara con los siguientes parámetros:

ID de cámara	ID de cámara generado por el sistema.
Descripción	Introduzca una descripción para identificar esta cámara.

Tipo	Seleccione uno de los siguientes tipos de cámara: • Genérico • Vanderbilt CCIC1410 • Vanderbilt CFMC1315
Cámara IP	Introduzca la dirección IP de la cámara.
Puerto de la cámara	Introduzca el puerto TCP desde el cual la cámara escucha. Por defecto es 80. **Aviso:** La cámara CCIC1410 solo se puede utilizar a través del puerto 80.
Nombre de usuario	Solo cámaras Vanderbilt CCIC1410 y CFMC1315. Introduzca un nombre de usuario de inicio de sesión en la cámara que se añadirá a la cadena de comandos que figura abajo cuando se haga clic en el botón **Actualizar cadena de comandos**.
Clave	Solo cámaras Vanderbilt CCIC1410 y CFMC1315. Introduzca una clave de inicio de sesión en la cámara que se añadirá a la cadena de comandos que figura abajo cuando se haga clic en el botón **Actualizar cadena de comandos**.
Cadena de comandos	Introduzca la cadena de comandos que se enviará al servidor HTTP de la cámara para poder obtener imágenes. Esta cadena debe incluir el nombre de usuario y la contraseña de la cámara. Consulte la documentación de la cámara para saber cuál es la cadena específica requerida para el tipo de cámara seleccionado. La cadena de comandos por defecto para una cámara Vanderbilt CCIC1410 o CFMC1315 sin clave es «/cgi-bin/stilljpeg».
Imágenes previas a la incidencia	Introduzca la cantidad de imágenes previas a la incidencia que se registrarán (0-16). Por defecto es 8.
Intervalo previo a la incidencia	Introduzca el intervalo de tiempo, en segundos, entre las imágenes previas a la incidencia (1-10). Por defecto es 1 segundo.
Imágenes posteriores a la incidencia	Introduzca la cantidad de imágenes posteriores a la incidencia que se registrarán (0-16). Por defecto es 8.
Intervalo posterior a la incidencia	Introduzca el intervalo de tiempo, en segundos, entre las imágenes posteriores a la incidencia (1-10). Por defecto es 1 segundo.

Configurar zonas de verificación

Para crear una zona de verificación

1. Vaya a **Configuración > Avanzada > Verificación > Zonas de verificación**.

   Se muestra una lista de los zonas de verificación existentes.

2. Haga clic en el botón **Añadir**.
3. Introduzca una **Descripción** para la zona.
4. Seleccione un módulo de expansión de **Audio** del menú desplegable.
5. Seleccione un **Vídeo** del menú desplegable.
6. Haga clic en el botón **Salvar**.
7. Asigne esta zona de verificación a una zona física en el sistema SPC. (Consulte *Editar una zona* en la página 274.)

Consulte también

Editar una zona en la página 274

Configurar ajustes de verificación

Aviso: Los siguientes ajustes son aplicables a todas las zonas de verificación (consulte *Configurar zonas de verificación* en la página precedente).

1. Seleccione **Configuración > Avanzada > Verificación > Audio**.

   Aparecerá la siguiente página.

2. Configure los siguientes ajustes.

Registro incid. previas	Introduzca la duración requerida en segundos (0-120) de la grabación de audio previo a la incidencia. Por defecto es 10.
Registro incidenc.poster.	Introduzca la duración requerida en segundos (0-120) de la grabación de audio posterior a la incidencia. Por defecto es 30.

Ver imágenes de vídeo

Las imágenes de vídeo de las cámaras configuradas pueden verse en un navegador web en modo técnico normal o completo. Esta funcionalidad también está disponible para los usuarios que tengan el derecho de Visualización de vídeo en su perfil. (Consulte *Añadir/Editar un usuario* en la página 209). Para esta funcionalidad, también debe estar habilitado el derecho de acceso web.

El derecho de Visualización de vídeo también puede configurarse en el teclado (configuración 'Vídeo en navegador').

Para ver imágenes, vaya a **SPC General > Vídeo**. Consulte *Ver vídeo* en la página 190.

Consulte también

Añadir/Editar un usuario en la página 209

Configurar vídeo en la página 298

17.9.8.5 Actualizar las licencias de SPC

La función **Opciones de licencia** proporciona un mecanismo para que el usuario actualice o añada una funcionalidad al sistema SPC, por ejemplo, para migraciones donde los periféricos instalados que no cuenten con licencia para SPC tengan que ser admitidos por un controlador SPC.

1. Seleccione **Configuración > Avanzada > Licencia**.

2. Contáctese con el equipo de asistencia técnica con la funcionalidad solicitada y mencione la clave de licencia actual según se indica.

   Si la solicitud es aprobada, se emitirá una nueva clave de licencia.

3. Introduzca la nueva clave en el campo que corresponde.

17.10 Configurar comunicaciones

Esta sección abarca:

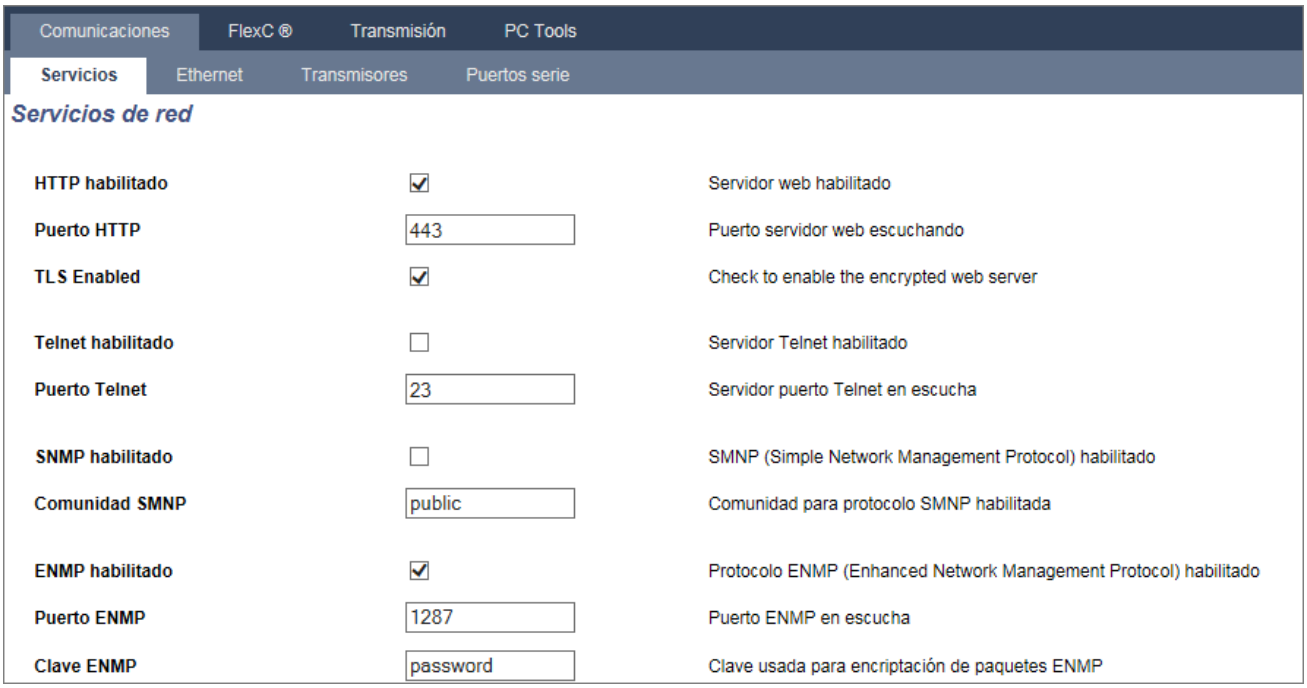
17.10.1 Configuración de comunicaciones

Esta sección abarca:

17.10.1.1 Configurar los servicios de red de la central

1. Seleccione **Comunicaciones > Comunicaciones > Servicios**.

   Se mostrará la siguiente página.


Comunicaciones
FlexC ®
Transmisión
PC Tools
Servicios
Ethernet
Transmisores
Puertos serie
Servicios de red
HTTP habilitado
Servidor web habilitado
Puerto HTTP
443
Puerto servidor web escuchando
TLS Enabled
Check to enable the encrypted web server
Telnet habilitado
Servidor Telnet habilitado
Puerto Telnet
23
Servidor puerto Telnet en escucha
SNMP habilitado
SMNP (Simple Network Management Protocol) habilitado
Comunidad SMNP
public
Comunidad para protocolo SMNP habilitada
ENMP habilitado
Protocolo ENMP (Enhanced Network Management Protocol) habilitado
Puerto ENMP
1287
Puerto ENMP en escucha
Clave ENMP
password
Clave usada para encriptación de paquetes ENMP

2. Configure los campos tal como se describe en la siguiente tabla.

HTTP habilitado	Marque esta casilla para habilitar el servidor web integrado en la central.
Puerto HTTP	Introduzca el número de puerto en el que el servidor del portal está «escuchando». El valor por defecto es 443.
TLS habilitado	Marque esta casilla para habilitar el funcionamiento de cifrado en el servidor web integrado. Por defecto, está habilitado. Con TLS habilitado, sólo se puede acceder a las páginas web utilizando el prefijo «https://» antes de escribir la dirección IP.
Telnet habilitado	Marque esta casilla para habilitar el servidor Telnet. (Por defecto: Habilitado) **Nota:** Usar Telnet sin un conocimiento integral puede dañar la configuración del controlador. Debe utilizarse si el usuario tiene el conocimiento suficiente o si está recibiendo capacitación de una persona con conocimientos suficientes.
Puerto Telnet	Introduzca el número de puerto Telnet.
SNMP habilitado	Marque esta casilla para habilitar el Protocolo Sencillo de Administración de Redes (SNMP). (Por defecto: Deshabilitado)
Comunidad SNMP	Introduzca el ID de comunidad para el protocolo SNMP. (Por defecto: Público)
ENMP habilitado	Marque esta casilla para habilitar el Protocolo de Gestión de Red Mejorado (ENMP). (Por defecto: Habilitado en modo técnico completo)
Puerto de ENMP	Introduzca el número de puerto ENMP (por defecto: 1287).
Clave de ENMP	Introduzca la clave para el protocolo ENMP.
Cambio ENMP habilitado	Marque esta casilla para habilitar los cambios de red con el protocolo de ENMP.

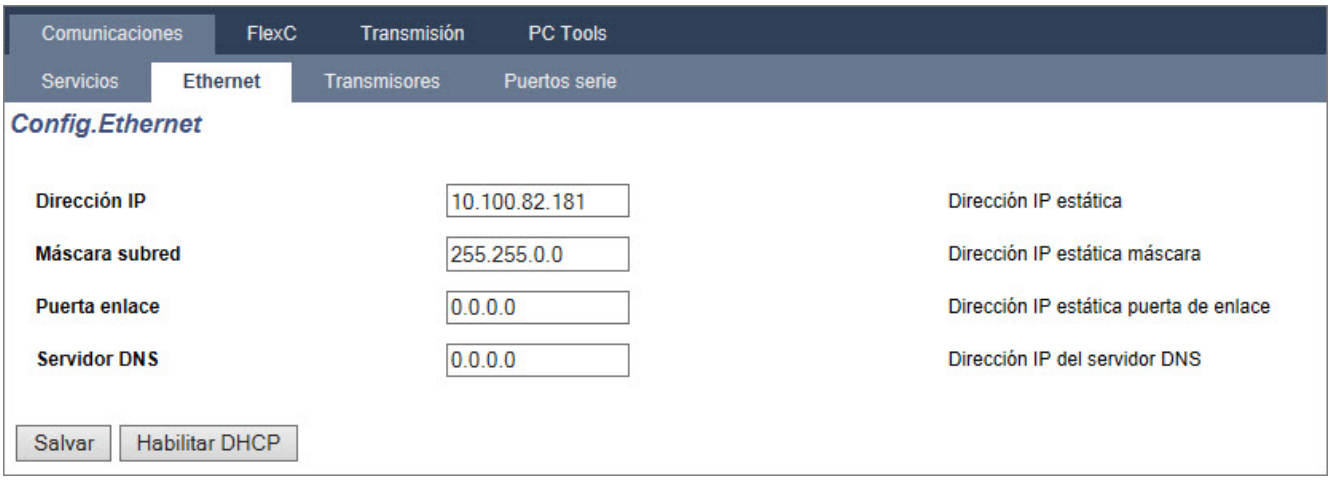
17.10.1.2 Ethernet

IP

Puede configurar el puerto Ethernet en el controlador desde la interfaz del navegador y del teclado. Se puede establecer una conexión Ethernet con el controlador SPC usando una conexión directa o una LAN.

1. Seleccione **Comunicaciones > Comunicaciones > Ethernet**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

Dirección IP	Introduzca la dirección IP de la central.
Red IP	Introduzca la máscara de subred que define el tipo de estructura de dirección de red implementada en la red de área local (LAN).
Dirección IP de puerta de enlace	Introduzca la dirección IP de la puerta de enlace, si existe una. Esta es la dirección por la que se enviarán paquetes IP cuando se acceda a direcciones IP externas en Internet.
Habilitar DHCP	Haga clic en este botón para habilitar la asignación de direcciones dinámicas en la central.
Servidor DNS	Introduzca la dirección IP del servidor DNS.

17.10.1.3 Configurar módems

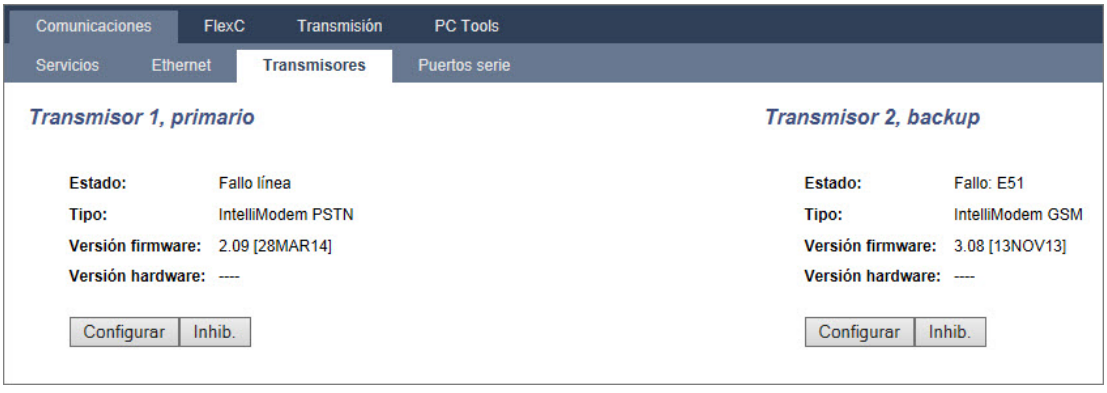
La central SPC proporciona dos conectores de interfaz de módem incorporados (principal y de respaldo) que le permiten instalar módulos GSM o RTB en el sistema.

Tras restablecer los valores por defecto de fábrica, durante el proceso de configuración inicial del sistema con el teclado, la central detecta si hay un módem principal o de respaldo y, en caso de ser así, muestra el tipo de módem y lo habilita automáticamente con la configuración por defecto. No se permite otro tipo de configuración en esta etapa.

Para programar el módem:

Nota: Se debe instalar e identificar un módem. (Consulte la sección *Instalación de módulos enchufables* en la página 96).

1. Seleccione **Comunicaciones > Comunicaciones > Módems**.



2. Haga clic en **Habilitar**.
3. Haga clic en **Configurar**.
   - Si instaló un módem GSM, aparecerá la página de configuración Módem GSM. Para obtener más información, consulte *Módem GSM* en la página opuesta.
   - Si instaló un módem RTB, aparecerá la página de configuración Módem RTB. Para obtener más información, consulte *Módem RTB* en la página 309.

La detección y la configuración de SMS no está disponible a menos que se configuren y habiliten módems.

Test de SMS

Una vez que está habilitada la función SIM para un módem, se debe realizar un test al número de destinatario deseado con un mensaje.

1. Introduzca el número de teléfono móvil (incluyendo el prefijo de 3 dígitos del país) en el campo numérico y un mensaje de texto corto en el recuadro del mensaje.
2. Haga clic en **Enviar SMS** y verifique la recepción del mensaje en el teléfono móvil.

El test de SMS se realiza únicamente con el fin de determinar si la función de SMS funciona correctamente. Se debe utilizar un mensaje de texto corto con caracteres alfanuméricos (A-Z) para comprobar esta función.

El SMS funciona utilizando un protocolo estándar que se utiliza en teléfonos con SMS. Tenga en cuenta que algunos operadores RTB no ofrecen el servicio de SMS a través de RTB. Para que los SMS funcionen a través de RTB, han de cumplirse los siguientes criterios:

- El ID de quien llama debe estar habilitado en la línea telefónica.
- La línea telefónica debe ser directa, no a través de PABX u otro equipo de comunicación.
- Tenga en cuenta también que la mayoría de los proveedores de servicios solo permite los SMS a un teléfono registrado en el mismo país (esto se debe a cuestiones de facturación).

Función de SMS

El controlador SPC permite la mensajería (SMS) remota en sistemas que tengan un módem instalado. Una vez que el módem está instalado, se necesita la siguiente configuración para los SMS:

- Módem compatible con SMS.
- Autenticación SMS.
- Control de SMS por parte del técnico.
- Control de SMS por parte del usuario.

Según la configuración, las funciones incluirán estas capacidades de SMS:

- Notificación de incidencias.
- Comandos remotos (los usuarios pueden tener asignados comandos remotos selectos).

Opciones del sistema de SMS

Una vez que el módem está instalado y la función de SMS habilitada, el sistema SPC debe aplicar la autenticación SMS para operaciones de SMS.

1. Seleccione **Configuración > Sistema > Opciones del sistema**.
2. Seleccione la opción deseada del menú desplegable **Autenticación SMS**:
   - **Solo código PIN:** Es un código de usuario válido. Consulte *Crear usuarios del sistema* en la página 119.
   - **Solo ID de llamada:** Es un número de teléfono (incluyendo el prefijo de 3 dígitos del país) configurado para el control de SMS por parte del usuario. El control de SMS estará disponible para la configuración por parte del usuario solo cuando esta opción está seleccionada.
   - **Código PIN e ID de llamada**
   - **Solo código PIN de SMS:** Es un código PIN válido configurado para el usuario diferente del código de acceso del mismo usuario. Los controles de SMS estarán disponibles para la configuración por parte del usuario solo cuando esta opción está seleccionada.
   - **Código PIN de SMS e ID de llamada**

Comandos de SMS

Consulte *Comandos de SMS* en la página 218 para obtener más información.

Módem GSM

Requisito previo

- Debe haber un módem GSM instalado y funcionando correctamente.

1. Seleccione **Comunicaciones > Comunicaciones > Módems**.
2. Haga clic en **Configurar**.
3. Configure los siguientes campos.

Configuración de módem GSM

País	Seleccione el país en que está instalado el sistema SPC.
PIN de la SIM	Introduzca el código PIN para la tarjeta SIM instalada en el módulo GSM.
Tecnología vía radio	**Solo GSM** Seleccione el tipo de señal que desea que utilice el módem: • **Solo 2G** Esta opción habilita la conexión a redes 2G únicamente. • **Solo 3G (por defecto)** Esta opción habilita la conexión a redes 3G únicamente. • **Buscar primero 2G** Esta opción fuerza al módem a conectarse a redes 2G disponibles. Si no hay una red 2G disponible, el módem se conecta a una red 3G. • **Buscar primero 3G** Esta opción fuerza al módem a conectarse a redes 3G disponibles. Si no hay una red 3G disponible, el módem se conecta a una red 2G.

Reconocimiento operador	**Tarjetas SIM multired únicamente** Habilite esta opción para que el módem busque todas las redes disponibles y que se conecte a la señal de mayor intensidad disponible.
Permitir roaming	Seleccione esta opción para habilitar el roaming con GSM. **Advertencia:** Si esta opción está habilitada, el módem puede conectarse a una red en un país diferente. **Nota:** Cambiar este ajuste reinicia el módem. **Nota:** Soportado en módems GSM v3.08 o más reciente.
USSD	**Tarjeta SIM prepaga únicamente** Introduzca el código que puede utilizar el módem para consultar a la red el saldo de crédito de la tarjeta SIM. Este código depende de la red. Consulte con su proveedor de servicios.
Llamadas entrantes	**Nota:** Vanderbilt recomienda que no se habiliten estas opciones para los sistemas actuales. El módem puede programarse para responder llamadas según las siguientes condiciones: • **No responder llamadas entrantes:** El módem nunca responde las llamadas entrantes. • **Responder llamadas entrantes:** El módem responde las llamadas entrantes. • **Responder solo con acceso técnico permitido:** El módem solo responde la llamada cuando se permite el acceso técnico al sistema.
Supervisión línea	• **Deshabilitado** • **Enable (habilitar)** • **Armado total** Habilite esta opción para controlar el nivel de señal del módulo GMS conectado al módem. La opción **Armado total** solo permite esta función cuando el sistema está en Armado total. **Nota:** Configuración de confirmación EN 50131-9 Para que la confirmación según EN50131-9 funcione correctamente, la supervisión de línea debe estar habilitada. (Consulte *Opciones* en la página 254.)
Temporizador de supervisión	Introduzca el período de tiempo en segundos durante el cual el nivel de señal debe caer a Bajo antes de que el sistema SPC registre un fallo. Rango de 0 a 9999 segundos.
Tiempo para fallo del módem	Introduzca el tiempo de retardo en segundos antes de que el sistema SPC envíe una alerta. Rango de 0 a 9999 segundos.
SMS habilitado	Marque esta casilla para habilitar la transmisión y la recepción de mensajes SMS y el control de comandos.

SMS automatizado	• **Deshabilitado** • **1 hora** • **24 horas** • **48 horas** • **7 días** • **30 días** Seleccione la temporización para los mensajes SMS automatizados.
Núm.SMS automatizado	Introduzca el número de SMS para recibir mensajes SMS automatizados. Solo un dispositivo puede recibir estos mensajes.
Fecha/hora inicio	Introduzca la fecha y la hora de inicio en la que el sistema enviará los mensajes SMS automatizados.
Configuración de datos móviles	
Punto de acceso (APN)	Introduzca la información del punto de acceso para habilitar las comunicaciones IP. Esta información dependerá del proveedor de servicios.
Punto de acceso Nombre de usuario	Introduzca la información del punto de acceso para habilitar las comunicaciones IP. Esta información dependerá del proveedor de servicios.
Clave del punto de acceso	Introduzca la información del punto de acceso para habilitar las comunicaciones IP. Esta información dependerá del proveedor de servicios.
Configuración de conexión de acceso telefónico a Internet	
Habilitar conexión de acceso telefónico a Internet	Seleccione esta opción para habilitar el módem y que se conecte a Internet a través de una conexión de acceso telefónico
Número de teléfono	Introduzca el número de teléfono para la conexión de acceso telefónico.
Nombre de usuario	Introduzca el nombre de usuario de la conexión de acceso telefónico.
Clave	Introduzca la clave de la conexión de acceso telefónico.

Haga clic en el botón **Test SMS** para enviar un mensaje corto de texto con el fin de probar el sistema.

El test de SMS se realiza únicamente con el fin de determinar si la función de SMS funciona correctamente. Se debe utilizar un mensaje de texto corto con caracteres alfanuméricos (A-Z) para comprobar esta función.

Módem RTB

1. Seleccione **Comunicaciones > Comunicaciones > Módems**.
2. Haga clic en **Configurar**.
3. Configure los campos tal como se describe en la siguiente tabla.

Configuración de módem RTB

País	Seleccione el país en que está instalado el SPC.

Llamadas entrantes	El módem puede programarse para responder llamadas según las siguientes condiciones: • **No responder llamadas entrantes:** El módem nunca responde las llamadas entrantes. • **Responder después de 'x' tonos** Seleccione la cantidad de tonos (1 a 8) tras los cuales el módem responderá la llamada entrante. • **Responder si, tras una llamada no atendida con un único tono, se recibe una nueva (modo contestador)** Si la persona que realiza la llamada llama al módem, cuelga después de escuchar un único tono e, inmediatamente después, vuelve a llamar al módem. El sistema SPC sabe que debe responder la llamada automáticamente dadas estas condiciones. • **Responder solo con acceso técnico permitido:** El módem solo responde la llamada cuando se permite el acceso técnico al sistema.
Prefijo	Introduzca el número que se necesita para acceder a una línea (p. ej., si está conectada a una PBX).
Supervisión línea	Habilite esta opción para controlar la tensión de la línea conectada al módem. Nota: Configuración de confirmación EN 50131-9 Para que la confirmación según EN50131-9 funcione correctamente, la supervisión de línea debe estar habilitada. (Consulte *Opciones* en la página 254.)
Temporizador de supervisión	Seleccione el período (en segundos) que el voltaje de línea debe parecer incorrecto antes de que el SPC considere que la línea presenta fallos.
Tiempo para fallo del módem	Retardo de tiempo para una alerta del sistema (0 a 9999 segundos). Por defecto es 60 segundos.
SMS habilitado	Marque esta casilla para habilitar la función de SMS en el sistema. **Nota:** El SMS funciona utilizando un protocolo estándar que se utiliza en teléfonos con SMS. Tenga en cuenta que algunos operadores RTB no ofrecen el servicio de SMS a través de RTB. Para que los SMS funcionen a través de RTB, han de cumplirse los siguientes criterios: El ID de quien llama debe estar habilitado en la línea telefónica. La línea telefónica debe ser directa, no a través de PABX u otro equipo de comunicación. Tenga en cuenta también que la mayoría de los proveedores de servicios solo permite los SMS a un teléfono registrado en el mismo país (esto se debe a cuestiones de facturación). **Nota:** Ya no se admite el SMS a través de RTB. Esta funcionalidad se mantiene en el producto para conservar la compatibilidad retroactiva.
Número de servidor de SMS	Solo para RTB. Este número muestra automáticamente el número por defecto para SMS en el país seleccionado. Introduzca un número de teléfono apropiado del proveedor de servicios SMS al que se pueda acceder desde la ubicación del usuario.
SMS automatizado	Seleccione la temporización para los mensajes SMS automatizados.
Núm.SMS automatizado	Introduzca el número de SMS para recibir mensajes SMS automatizados.
Configuración de conexión de acceso telefónico a Internet	

Habilitar conexión de acceso telefónico a Internet	Seleccione esta opción para habilitar el módem y que se conecte a Internet a través de una conexión de acceso telefónico.
Número de teléfono	Introduzca el número de teléfono para la conexión de acceso telefónico.
Nombre de usuario	Introduzca el nombre de usuario de la conexión de acceso telefónico.
Clave	Introduzca la clave de la conexión de acceso telefónico.

Haga clic en el botón **Test SMS** para enviar un mensaje corto de texto con el fin de probar el sistema.

El test de SMS se realiza únicamente con el fin de determinar si la función de SMS funciona correctamente. Se debe utilizar un mensaje de texto corto con caracteres alfanuméricos (A-Z) para comprobar esta función.

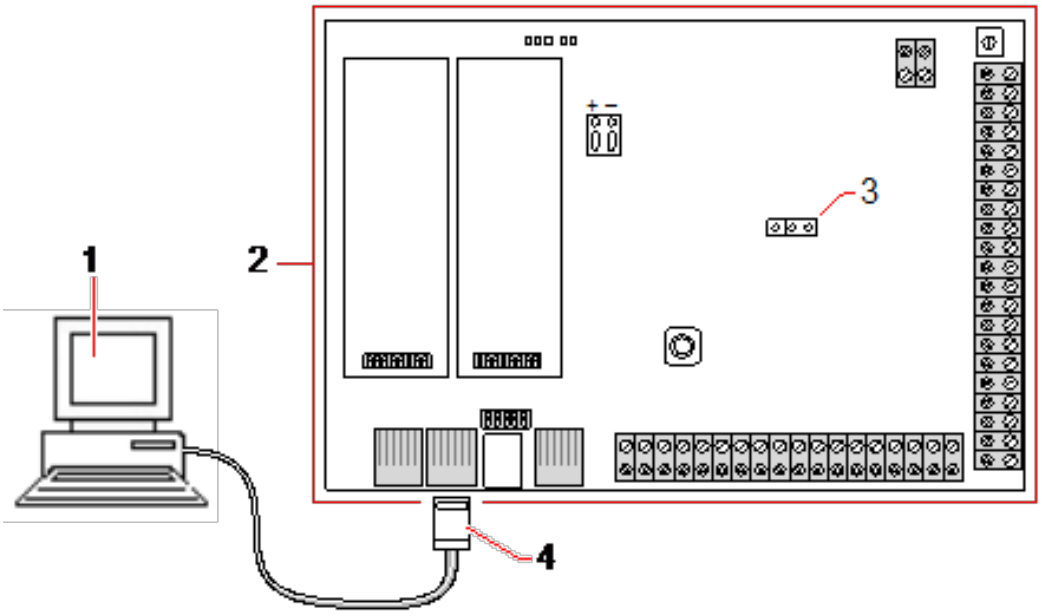
Cuando se utiliza la opción de mensaje SMS a través de una línea RTB, es necesario programar el número de teléfono del proveedor del servicio SMS que funciona en la partición en la que está instalado el SPC. El sistema SPC marca automáticamente este número para ponerse en contacto con el servidor de SMS siempre que la función SMS esté activada. DEBE habilitar la identidad de la línea de llamada en la línea RTB para que esta función se active. Cada país tendrá su propio proveedor de servicios SMS con un número de teléfono único.

Esta función no está habilitada en todos los países. Contáctese con su proveedor local para obtener más información (soporte de la función, proveedor de servicios recomendado).

17.10.1.4 Puertos serie

El controlador SPC ofrece 2 puertos serie (RS232) que proporcionan la siguiente funcionalidad:

- **X10:** El puerto serie 1 es una interfaz dedicada que admite el protocolo X10. Este protocolo permite el uso de los cables de alimentación existentes de un edificio para transmitir información de control a dispositivos X10, ofreciendo la posibilidad de activar y controlar estos dispositivos a través de la interfaz de programación del controlador SPC.
- **Registro de incidencias:** La interfaz del puerto serie 2 permite conectarse a un puerto serie en un PC o una impresora. Con esta conexión, un programa del terminal puede configurarse para recibir un registro de incidencias del sistema o incidencias de acceso del controlador SPC.
- **Información del sistema:** El puerto serie 2 también ofrece una interfaz a través del programa del terminal que permite la ejecución de un conjunto de comandos para obtener del controlador información específica del sistema. Esta función está disponible solo como una herramienta para fines informativos y de depuración, y solo deben utilizarla los instaladores con experiencia.

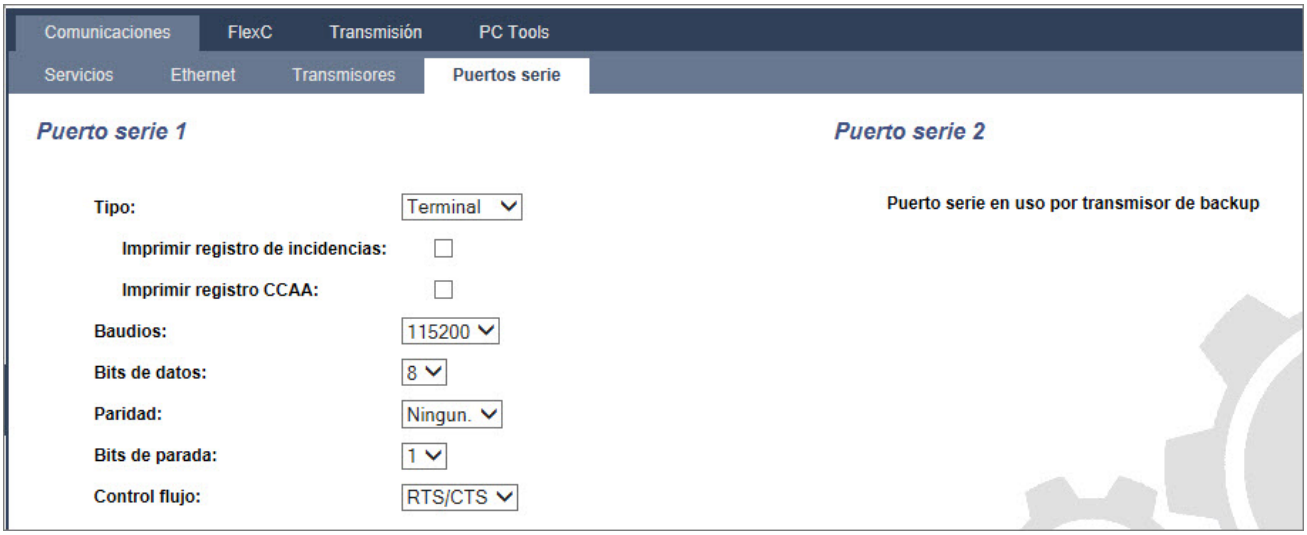


1	PC con puerto serie con HyperTerminal
2	Controlador SPC
3	JP9 
4	RS232

Para configurar los puertos serie:

- Seleccione **Comunicaciones > Comunicaciones> > Puertos serie**.

  Se mostrará la siguiente página:



La configuración que se muestra dependerá del tipo de conexión para la que se utilizan los puertos. La configuración se describe en las secciones a continuación.

17.10.2 FlexC®

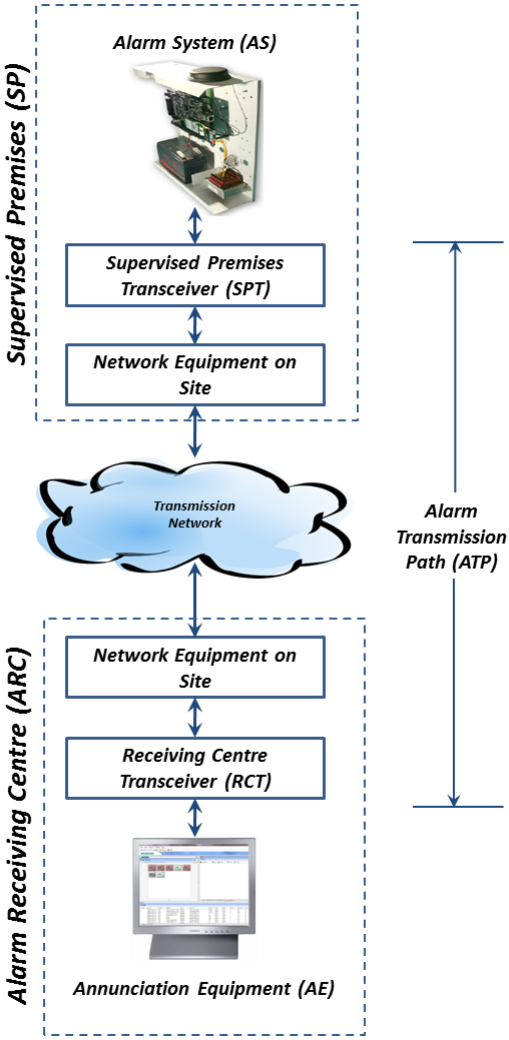
El protocolo de comunicaciones seguro flexible (FlexC) de SPC habilita las comunicaciones para un sistema de transmisión de alarmas (ATS) de ruta simple o múltiple basado en el protocolo de Internet (IP). Un ATS es un enlace de comunicaciones confiable entre un transceptor supervisado de la instalación (SPT, por ejemplo, Ethernet integrada en la central SPC) y un transceptor de central de recepción (RCT,

por ejemplo, SPC Com XT o SPC Connect, www.spcconnect.com). Un ATS FlexC está formada por una ruta de transmisión de alarma (ATP) primaria y por hasta nueve rutas de transmisión de alarmas (ATPs) de soporte. Habilita:

- La transferencia bidireccional de datos entre el SPT, por ejemplo, la central SPC a través de Ethernet, y el RCT, por ejemplo, el servidor SPC Com XT o el servidor SPC Connect, www.spcconnect.com.
- Control de comunicaciones de un ATS completo y ATP individuales.

Las centrales de intrusión SPC admiten FlexC a través de IP con cualquiera de las siguientes interfaces:

- Ethernet
- Módem GSM con GPRS habilitado
- Módem RTB



Consulte también

Configuración de ATP de inicio rápido para ATS EN50136 en la página siguiente

Configurar perfiles de incidencias en la página 328

Definición de excepción de incidencia en la página 329

Configurar perfiles de comandos en la página 331

Estado ATS y ATP de FlexC en la página 203

Configurar un ATS EN 50136-1 o un ATS personalizado en la página 316

17.10.2.1 Modo operativo

El sistema utiliza el método de almacenamiento y retransmisión cuando comunica las incidencias.

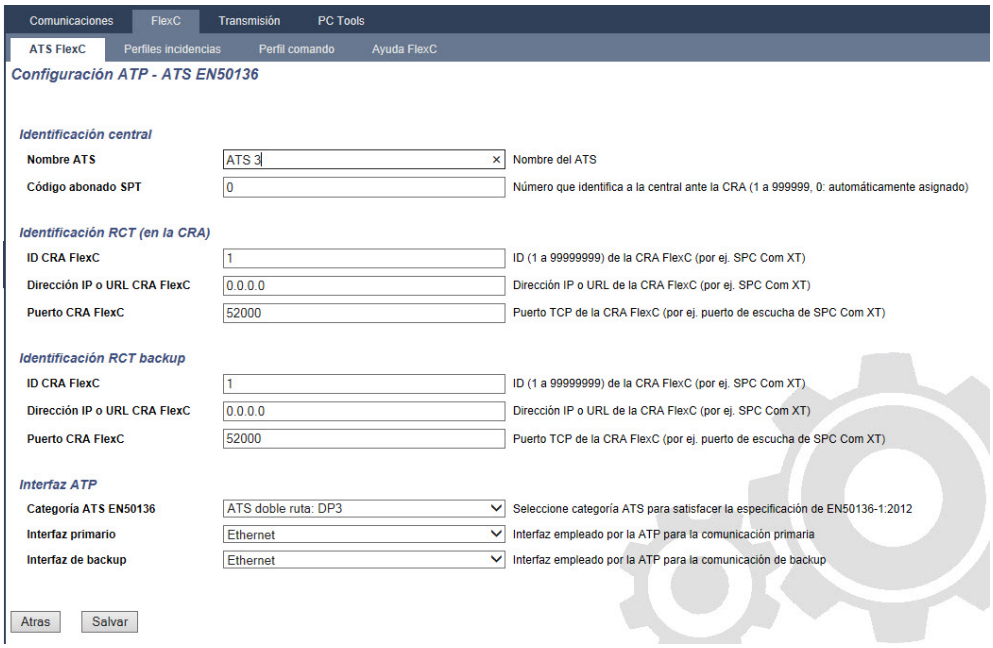
El sistema de alarma SPC envía las incidencias a SPC Com XT y requiere un reconocimiento desde SPC Com XT antes de que el sistema de alarma SPC considere que la incidencia se transmitió exitosamente. SPC Com XT solo envía un reconocimiento luego de que la incidencia se haya registrado exitosamente en la base de datos SQL. SPC Com XT luego transmite la incidencia las interfaces Sur-Gard y de cliente de SPC Com XT.

17.10.2.2 Configuración de ATP de inicio rápido para ATS EN50136

FlexC ofrece las siguientes funciones nuevas que le permiten implementar FlexC rápidamente:

- Página de configuración de inicio rápido para un **ATS ruta simple**, **ATS ruta doble** y **ATS ruta doble a servidor doble** de conformidad con la norma EN50136
- Perfil de incidencias por defecto
- Perfil de comandos por defecto (este no admite la verificación de audio y vídeo)
- **Nombre usuario de comandos FlexC** (FlexC) y **Clave de comandos** (FlexC) por defecto para controlar la central desde el RCT (por ejemplo: SPC Com XT)
- Cifrado automático sin clave

1. Para configurar rápidamente una conexión FlexC entre una central y un RCT (por ejemplo: SPC Com XT), vaya a **Comunicaciones > FlexC > ATS FlexC**.
2. Debajo de **Alta ATS EN50136-1**, seleccione una de las siguientes opciones para ver la **Configuración de ATP**:
   - **Alta ATS ruta simple** - ATP principal únicamente
   - **Alta ATS ruta doble** - ATP principal y de respaldo
   - **Alta ATS ruta doble a servidor doble** - ATP principal y de respaldo, servidores principal y de respaldo



3. Complete los campos en la página **Configuración de ATP - ATS EN50136** en la tabla a continuación. Como mínimo, debe completar el campo **URL de RCT** o **Dirección IP** para salvar los datos. Si no introduce un **Código de abonado SPT**, puede poner en marcha la central con el **ID de registro de ATS**, el cual se genera automáticamente cuando salva los datos. El operador del RCT también debe introducir este **ID de registro de ATS**, por ejemplo, en SPC Com XT.

4. Haga clic en **Salvar**. Se muestra la página **Configuración de ATS**, la cual indica el **ID de registro de ATS** y la ATP principal configurado o las ATP principal y de respaldo en la **Tabla de secuencia de incidencias**.
5. En la página **Configuración de ATS**, haga clic en **Salvar** para aceptar los ajustes por defecto, por ejemplo, el **Perfil de incidencias por defecto**, el **Perfil de comandos por defecto** (incluyendo el **Nombre usuario de comandos** FlexC y la **Contraseña de comandos**) FlexC, y el **cifrado automático** sin clave. Para cambiar la configuración, consulte *Configurar un ATS EN 50136-1 o un ATS personalizado* en la página siguiente.
6. Haga clic en **Atrás**. Se muestra el ATS en la tabla de **ATS configurado**.

Identificación de la central	
Nombre ATS	Introduzca el nombre del ATS. Si no introduce un valor, el nombre del ATS por defecto será ATS 1, ATS 2, etc.
Código de abonado SPT	El número que identifica de forma única la central ante el RCT. Introduzca 0 si no tiene el código de abonado SPT. En este caso, puede poner en marcha la central con el **ID de registro de ATS**. Para un ATS EN50136, el **ID de registro de ATS** se generará automáticamente cuando hace clic en **Salvar**. El RCT puede enviar el **código de abonado SPT** a la central cuando está disponible.
Identificación de RCT e Identificación de RCT de respaldo (doble ruta a doble servidor únicamente)	
ID de RCT	Introduzca el **ID de RCT** que identifica de forma única el RCT (por ejemplo, SPC Com XT) ante la central. Este valor debe coincidir con el valor introducido en la herramienta de gestor de configuración del servidor de SPC Com XT en el campo **ID de RCT del servidor** en la pestaña **Detalles del servidor**. Consulte *Manual de instalación y configuración SPC Com XT*.
Dirección IP o URL del RCT	Introduzca la **dirección IP** o **la URL** para la ubicación del RCT en el servidor (por ejemplo, servidor SPC Com XT).
Puerto TCP del RCT	Introduzca el puerto TCP para el RCT (por ejemplo, SPC Com XT). Esto debe coincidir con el número introducido en el campo **Puerto FlexC de servidor** en la herramienta de gestor de configuración del servidor de SPC Com XT.
Interfaz de ATP	
Categoría ATS EN50136	Seleccione la categoría ATS EN50136 (SP1-SP6, DP1-DP4). Para ver una descripción de las categorías, consulte *Tiempos categorías ATS* en la página 413.
Interfaz principal	Seleccione la **Interfaz principal** que se aplicará a la ruta de comunicaciones principal desde: • Ethernet • GPRS: Módem 1 • GPRS: Módem 2 • Internet por marcación: Módem 1 • Internet por marcación: Módem 2

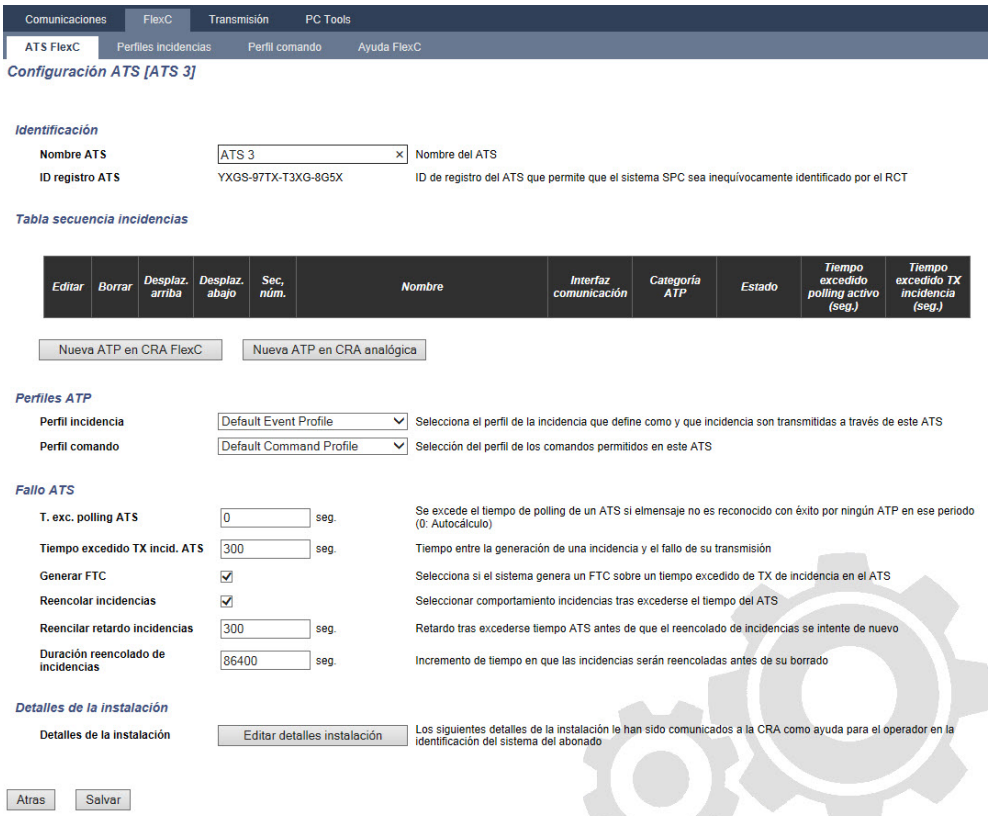
Interfaz de respaldo	Para un **ATS de ruta doble**, seleccione la **Interfaz de respaldo** que se utilizará para la ruta de comunicaciones de respaldo desde: • Ethernet • GPRS: Módem 1 • GPRS: Módem 2 • Internet por marcación: Módem 1 • Internet por marcación: Módem 2

17.10.2.3 Configurar un ATS EN 50136-1 o un ATS personalizado

Un ATS incluye una central de alarma, rutas de red y un RCT (por ejemplo, SPC Com XT). Combina una o más rutas de comunicación entre la central SPC y un RCT. Puede añadir hasta 10 ATP a un ATS.

AVISO: Para un ATS EN 50136-1, la secuencia de armado del ATS comienza con la configuración de una ATP para un ATS. Esto le ofrece una función de armado rápido. Consulte *Configuración de ATP de inicio rápido para ATS EN50136* en la página 314.

1. Para configurar un ATS, acceda a **Comunicaciones > FlexC > ATS FlexC**.
2. Escoja una de las siguientes opciones:
   - Añadir ATS ruta simple
   - Añadir ATS ruta doble
   - Añadir ATS ruta doble a servidor doble
   - Añadir ATS personalizado
3. Para un ATS EN 50136, primero debe configurar los ajustes en la página **Configuración de ATP - EN50136**. Consulte *Configuración de ATP de inicio rápido para ATS EN50136* en la página 314.
4. Se muestra la página **Configuración de ATS**. Un ATS EN 50136-1 mostrará una ATP principal o una ATP principal y de respaldo en la **Tabla secuencia incidencias**.



5. Introduzca el **Nombre del ATS** para identificar el ATS. Si no introduce un valor, el nombre del ATS por defecto será ATS 1, ATS 2, etc.
6. Para añadir 1 ATP principal y hasta 9 ATP de respaldo a un ATS, haga clic en **Añadir ATP a RCT FlexC** (consulte *Añadir ATP a RCT FlexC* en la página siguiente) o haga clic en **Añadir ATP a CRA analógica** (consulte *Añadir ATP a CRA analógica* en la página 323).
7. Seleccione un **Perfil incidencias** del menú desplegable. Para personalizar cómo se transmiten las incidencias en un ATS, consulte *Configurar perfiles de incidencias* en la página 328.
8. Seleccione un **Perfil de comandos** del menú desplegable. Para personalizar los comandos habilitados para que un RCT controle una central, consulte *Configurar perfiles de comandos* en la página 331.
9. Complete los campos **Fallos ATS** como se muestra en la tabla a continuación.

Tiempo de espera de polling de ATS	Este campo se calcula automáticamente al añadir los valores de la columna **Tiempo de espera de polling activo** en la Tabla de secuencia de incidencias, es decir, para todas las ATP en un ATS. Puede sobrescribir manualmente este campo. Por ejemplo, CAT 2 [Módem] tiene un valor de **Tiempo de espera de polling activo** de 24 horas y 10 minutos (87000 segundos). Para habilitar un tiempo de reacción más reducido, introduzca un valor inferior.
Tiempo de espera de incidencia de ATS	Se ha incrementado la cantidad de tiempo posterior a una incidencia y esto no se transmitió con éxito antes de que el ATS aborte. Por defecto: 300 segundos.
Generar FTC	Seleccione si el sistema genera un FTC al excederse el tiempo de espera del ATS.

Reencolar incidencias	Seleccione esta opción para reencolar las incidencias tras excederse el tiempo de espera del ATS.
Retardo reencolado incidencias	Retardo tras excederse el tiempo de espera del ATS antes de que se reintente la incidencia reencolada. Por defecto: 300 segundos.
Duración reencolado de incidencias	Cantidad de tiempo que la incidencia será reencolada antes de que sea borrada. Por defecto: 86400 segundos.

10. Haga clic en **Editar detalles de la instalación** para completar la configuración y que el operador del RCT identifique la central. Consulte *Editar detalles de instalación* en la página 325.
11. Haga clic en **Salvar** y **Atrás** para regresar a la página **Configuración de ATS**. Se muestra el nuevo ATS en la **Tabla de ATS configurado**.
12. Para múltiples ATP, puede utilizar las flechas ARRIBA y ABAJO en la **Tabla secuencia incidencias** para reordenar la secuencia de ATP.

AVISO: El ID de registro de ATS se genera automáticamente para el ATS. Identifica de forma única la central ante el RCT. Si no conoce el código de abonado SPT, puede poner en marcha la central con el ID de registro de ATS. El operador de CMS también debe introducir este ID de registro de ATS en el RCT (por ejemplo, SPC Com XT). Consulte *Manual de instalación y configuración SPC Com XT*.

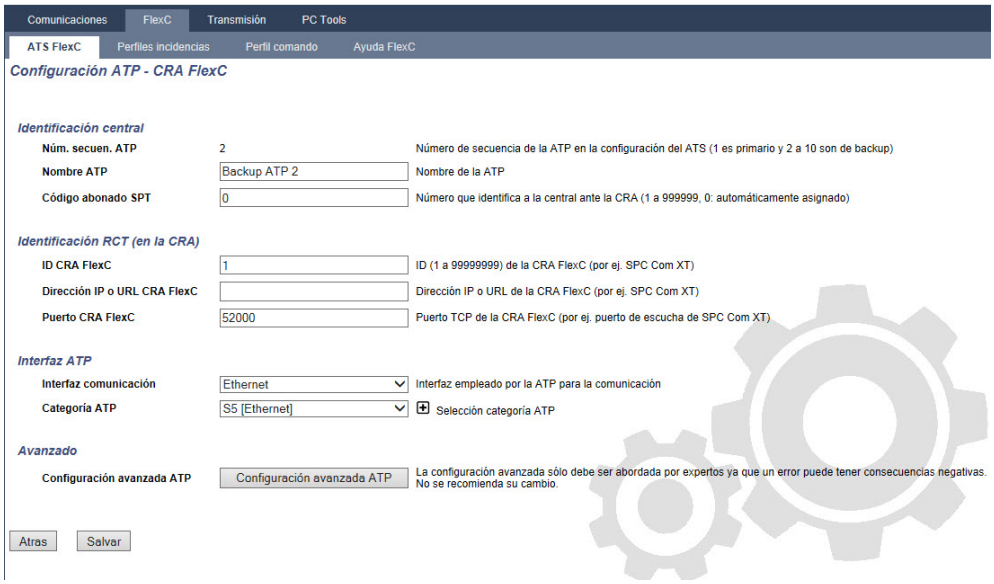
Consulte también

Tiempos categorías ATS en la página 413

Añadir ATP a RCT FlexC

La opción **Añadir ATP a RCT FlexC** le permite configurar una ATP entre la central PC y el RCT (por ejemplo, SPC Com XT). Puede configurar hasta 10 ATP por cada ATS.

1. Haga clic en el botón **Añadir ATP a RCT FlexC**.



2. Complete los campos de ATP tal como se describe en la siguiente tabla.

Identificación de la central

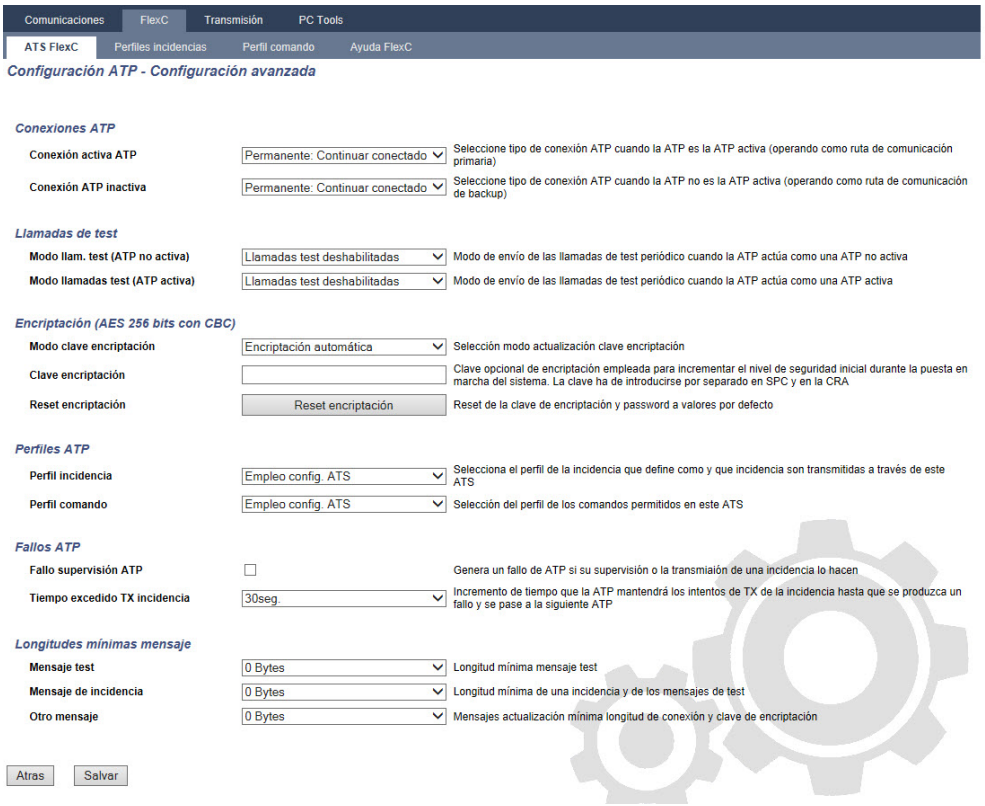
N.º secuencia ATP	Este campo muestra el número de secuencia de la ATP en la configuración del ATS. El número 1 es el principal, y los números 2 a 10 indican los de respaldo.
ID único de ATP	Cuando salva una ATP, el sistema le asigna un ID único a la ATP. Este es el ID único de la ATP por el que será identificada por el RCT.
Nombre de la ATP	Introduzca un nombre para la ATP.
Código de abonado SPT	Introduzca un número para identificar de forma única la central ante el RCT.
Identificación del RCT	
ID de RCT	Introduzca el número que identifica de forma única el RCT (por ejemplo, SPC Com XT) ante la central. Este número debe coincidir con el número introducido en el campo **ID de RCT de servidor** en la herramienta de gestor de configuración del servidor de SPC Com XT.
Dirección IP o URL del RCT	Introduzca la dirección IP o URL del RCT (por ejemplo, SPC Com XT).
Puerto TCP del RCT	Introduzca el puerto TCP desde el cual el RCT (por ejemplo, SPC Com XT) escucha. El predeterminado es 52000. Esto debe coincidir con el valor del campo **Puerto FlexC de servidor** en la herramienta de gestor de configuración del servidor. Consulte *Manual de instalación y configuración SPC Com XT*.
Interfaz de ATP	
Interfaz de comunicaciones	De la lista desplegable, seleccione la interfaz que utiliza la ATP para la comunicación. • Ethernet • GPRS: Módem 1 • GPRS: Módem 2 • Internet por marcación: Módem 1 • Internet por marcación: Módem 2
Categoría de ATP	Seleccione la categoría que se aplica a esta ATP. Para obtener información sobre las categorías de ATP, consulte *Tiempos categorías ATP* en la página 414.
Avanzado	
Configuración avanzada de ATP	No se recomienda que cambie la configuración avanzada. Los usuarios expertos deben realizar los cambios.

3. En caso de ser necesario, haga clic en **Configuración avanzada de ATP**, por ejemplo, si usa cifrado automático, puede introducir una clave en el campo **Clave de cifrado**. Consulte *Ajustes de la configuración avanzada de ATP* en la página siguiente.
4. Haga clic en **Salvar**.

Ajustes de la configuración avanzada de ATP

ADVERTENCIA: No se recomienda que cambie la **configuración avanzada de ATP**. Los usuarios expertos deben realizar los cambios.

1. Haga clic en el botón **Configuración avanzada de ATP**.



2. Configure los campos tal como se describe en la siguiente tabla.

Conexiones ATP	
Conexión ATP primaria	Seleccione el tipo de conexión ATP cuando la ATP funcione como la ruta de comunicación primaria. • Permanente: Siempre conectada • Temporal: Descolgada cada 1 segundo • Temporal: Descolgada cada 20 segundos • Temporal: Descolgada cada 80 segundos • Temporal: Descolgada cada 3 minutos • Temporal: Descolgada cada 10 minutos • Temporal: Descolgada cada 30 minutos

Conexión ATP no activa	Seleccione el tipo de conexión ATP cuando la ATP esté funcionando como ruta de comunicación de respaldo. • Permanente: Siempre conectada • Temporal: Descolgada cada 1 segundo • Temporal: Descolgada cada 20 segundos • Temporal: Descolgada cada 80 segundos • Temporal: Descolgada cada 3 minutos • Temporal: Descolgada cada 10 minutos • Temporal: Descolgada cada 30 minutos
Llamadas de test	
Modo de llamada de test (ATP no activa)	Seleccione el modo para enviar llamadas de test cuando la ATP es la ATP no activa. • Llamadas de test deshabilitadas • Llamadas de test cada 10 minutos • Llamadas de test cada 1 hora • Llamadas de test cada 4 horas • Llamadas de test cada 24 horas • Llamadas de test cada 48 horas • Llamadas de test cada 7 días • Llamadas de test cada 30 días
Modo de llamada de test (ATP activa)	Seleccione el modo para enviar llamadas de test cuando la ATP es la ATP activa. • Llamadas de test deshabilitadas • Llamadas de test cada 10 minutos • Llamadas de test cada 1 hora • Llamadas de test cada 4 horas • Llamadas de test cada 24 horas • Llamadas de test cada 48 horas • Llamadas de test cada 7 días • Llamadas de test cada 30 días
Cifrado (AES 256 bits con CBC)	
Modo de clave de cifrado	Seleccione cómo se actualiza el cifrado. • Cifrado automático • Cifrado automático con actualizaciones • Cifrado fijo **Nota:** El cifrado automático usa la clave predeterminada y la actualiza una vez. El cifrado automático con actualizaciones cambia la clave de cifrado cada 50.000 mensajes o una vez por semana, lo que suceda primero.

Contraseña de encriptado	La clave opcional utilizada para brindar mayor seguridad durante la puesta en marcha inicial de la ATP. Debe introducir la clave en el SPT o RCT de forma independiente.
Reset cifrado	Resetea la clave de cifrado y la clave a los valores por defecto.
Perfiles ATP	
Perfil de incidencias	Seleccione el perfil de incidencias que define cómo y qué incidencias se transmiten a través de este ATS. • Uso de configuración de ATS • Perfil de incidencias por defecto • Todas las incidencias
Perfil de comandos	Seleccione el Perfil de comandos que define los comandos permitidos en este ATS. • Uso de configuración de ATS • Perfil de comandos por defecto • Perfil de comandos personalizado
Fallos ATP	
Fallo supervisión ATP	Seleccione para generar un fallo ATP en caso de que falle la supervisión ATP o no se logre transmitir una incidencia en la ATP.
Tiempo de espera de incidencia	Cantidad de tiempo que la ATP seguirá intentando la transmisión de la incidencia hasta que se produzca un fallo y se pase a la siguiente ATP. • 30 segundos • 60 segundos • 90 segundos • 2 minutos • 3 minutos • 5 minutos • 10 minutos
Longitudes mínimas mensaje	
Mensaje polling	Longitud mínima mensaje polling. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes

Mensaje de incidencia	Longitud mínima de una incidencia y de un mensaje de llamada de test. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Otro mensaje	Longitud mínima de conexión y mensajes de clave de cifrado y actualización. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes

3. Haga clic en **Salvar**.

Añadir ATP a CRA analógica

Si se cae una conexión entre la central SPC y el RCT (por ejemplo, SPC Com XT), FlexC tiene la capacidad de conmutar a una conexión ATP de respaldo entre la central SPC y la CRA analógica. Puede configurar hasta 10 ATP por cada ATS.

1. Para configurar una ATP entre una central SPC y la CRA analógica, haga clic en el botón **Añadir ATP a CRA analógica**.
2. Complete los campos de ATP tal como se describe en la siguiente tabla.

Identificación de la central	
N.º secuencia ATP	Este campo muestra el número de secuencia de la ATP en la configuración del ATS. El número 1 es el principal, y los números 2 a 10 indican los de respaldo.
ID único de ATP	Este ID identifica de forma única la ATP ante el RCT.
Nombre de la ATP	Introduzca un nombre para la ATP.
Código de abonado SPT	Introduzca un número para identificar de forma única la central ante el RCT (1–999999).
Conexión CRA	
Número 1	Número de teléfono 1
Número 2	Número de teléfono 2
Selección de módem	Seleccione el módem que utilizará. • Módem 1 • Módem 2
Llamadas de test	

Modo de llamada de test (ATP no activa)	Seleccione el modo para enviar llamadas de test cuando la ATP está en modo no activa. Por defecto: 24 horas. • Llamadas de test deshabilitadas • Llamadas de test cada 10 minutos • Llamadas de test cada 1 hora • Llamadas de test cada 24 horas • Llamadas de test cada 48 horas • Llamadas de test cada 7 días • Llamadas de test cada 30 días
Modo de llamada de test (ATP activa)	Seleccione el modo para enviar llamadas de test cuando la ATP es una ATP activa. Por defecto: 24 horas. • Llamadas de test deshabilitadas • Llamadas de test cada 10 minutos • Llamadas de test cada 1 hora • Llamadas de test cada 24 horas • Llamadas de test cada 48 horas • Llamadas de test cada 7 días • Llamadas de test cada 30 días
Hora de la primera llamada de test	Hora de la primera llamada de test luego del reset o inicialización del ATS. • Enviar inmediatamente (por defecto) o bien • Seleccione un intervalo de media hora entre 00:00 y 23:30.
Protocolo de incidencia	
Protocol	Protocolo utilizado en la comunicación. • SIA • SIA extendido 1 • SIA extendido 2 • Contact ID
Perfil de incidencias	Seleccione el perfil de incidencias que define cómo y qué incidencias se transmiten a través de este ATS. • Uso de configuración de ATS • Perfil de incidencias por defecto • Perfil incidencias de portal por defecto • Todas las incidencias • Perfil de incidencias personalizado
Fallos ATP	
Fallo supervisión ATP	Seleccione para generar un fallo ATP en caso de que falle la supervisión ATP o no se logre transmitir una incidencia en la ATP.

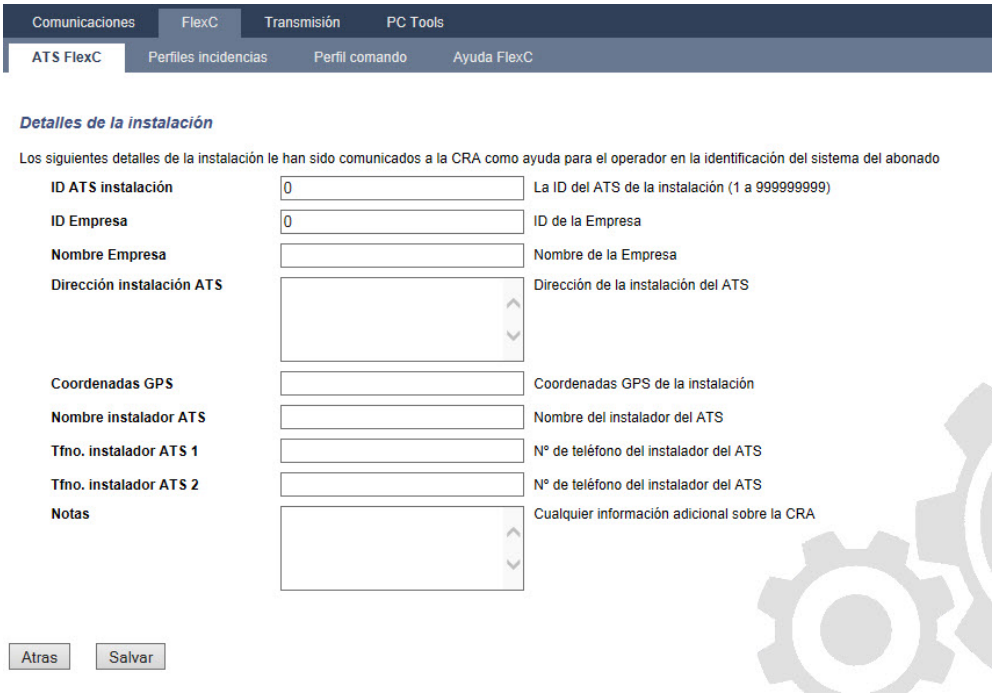
Tiempo de espera de incidencia	Cantidad de tiempo que la ATP seguirá intentando la transmisión de la incidencia hasta que se produzca un fallo y se pase a la siguiente ATP. Por defecto: 2 minutos. • 30 segundos • 60 segundos • 90 segundos • 2 minutos • 3 minutos • 5 minutos • 10 minutos

3. Haga clic en **Salvar**.

Editar detalles de instalación

Los detalles de la instalación se envían al RCT para ayudar al operador a identificar la central.

1. Haga clic en el botón **Editar detalles de instalación**.



2. Complete los campos en la siguiente tabla.

ID instalación ATS	El ID de la instalación de ATS (1 a 999999999).
ID empresa	Para uso futuro.
Nombre Empresa	Nombre de la empresa.
Dirección instalación ATS	La dirección de la instalación del ATS.
Coordenadas GPS	Las coordenadas GPS de la instalación.
Nombre instalador ATS	El nombre del instalador del ATS.
Número de teléfono 1 del instalador	El número de teléfono del instalador del ATS.
Número de teléfono 2 del instalador	El número de teléfono del instalador del ATS.
Notas	Información adicional para el RCT.

3. Haga clic en **Salvar**.

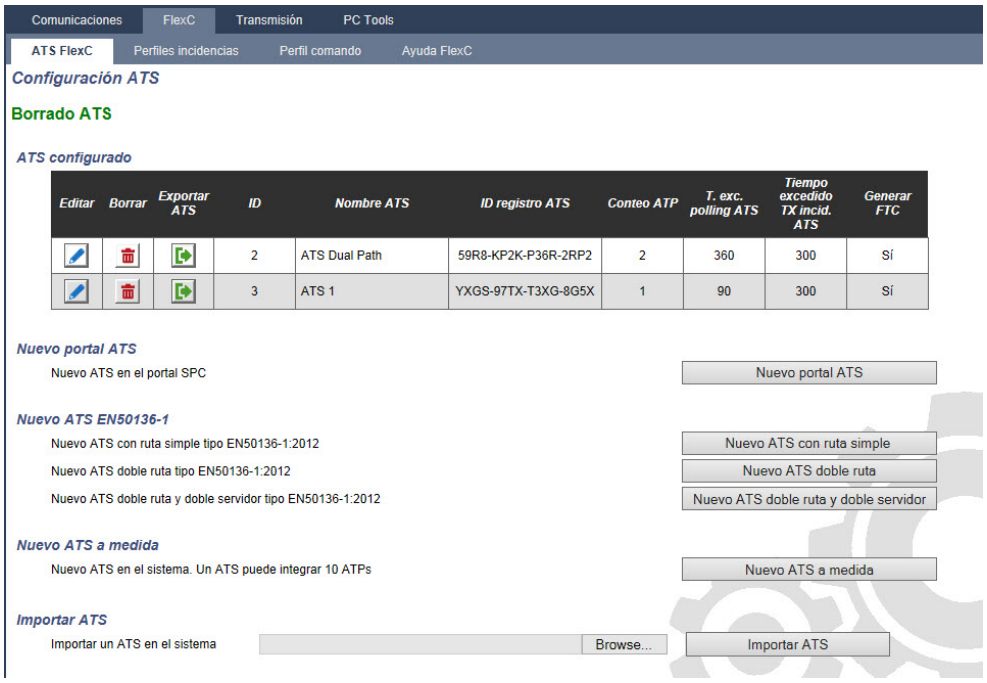
17.10.2.4 Configurar un ATS SPC Connect

La funcionalidad de ATS **Añadir SPC Connect** abre una ruta de comunicación entre la central (SPT) y el servidor **SPC Connect** (RCT), www.spcconnect.com. Usando el ID de registro de ATS SPC Connect generado, el usuario de la central puede registrar una cuenta de usuario y central en el sitio web de SPC Connect para acceder a la central de forma remota.

1. Para configurar un ATS SPC Connect, acceda a **Comunicaciones > FlexC > ATS FlexC**.
2. En la página **Configuración de ATS**, haga clic en **Añadir SPC Connect** para abrir una ruta de comunicación con el servidor SPC Connect.

   Se añade un ATS SPC Connect a la **Tabla secuencia incidencias** con los siguientes atributos:

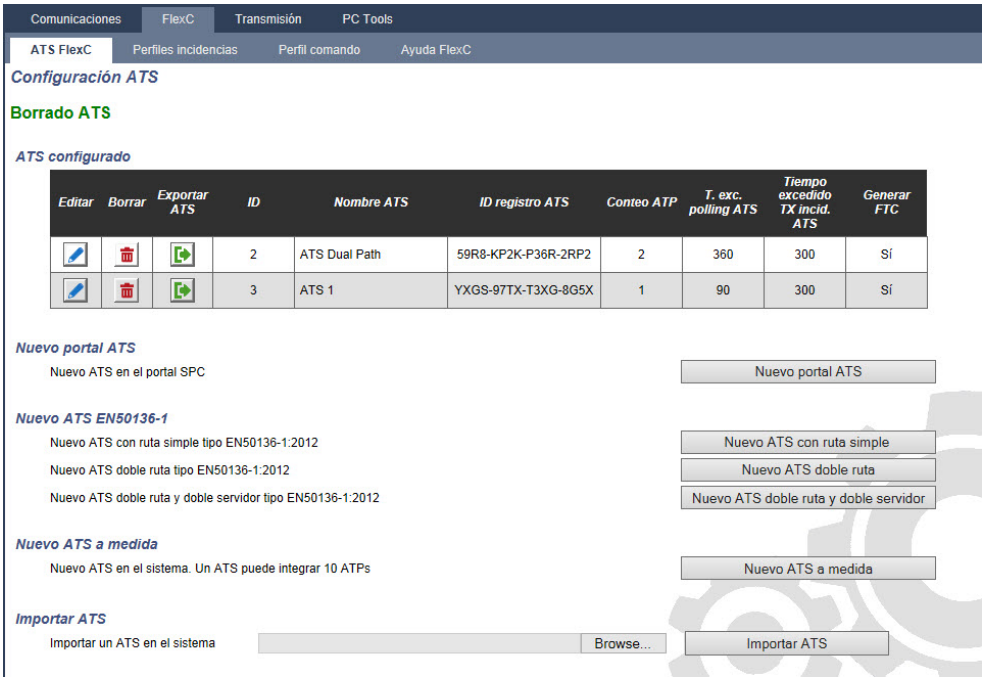
   - ID de registro de ATS SPC Connect
   - ATP por defecto por Ethernet. Para obtener información sobre los campos de ATP, consulte *Añadir ATP a RCT FlexC* en la página 318.
   - Perfil de incidencias por defecto para SPC Connect
   - Perfil de comandos por defecto para SPC Connect
   - La URL de RCT por defecto es www.spcconnect.com
   - El código de abonado SPT para la ATP se completa automáticamente.
   - Tome nota del **ID de registro de ATS** de SPC Connect y bríndeselo al cliente junto con *Guía de usuario del sistema SPC Connect*.



17.10.2.5 Exportar e importar un ATS

Los archivos de ATS tienen la extensión .cxml. Debe crear el ATS en el navegador SPC y exportarlo antes de importarlo al sistema.

1. Para exportar un ATS, acceda a **Comunicaciones > FlexC > ATS FlexC**.
2. En la tabla de **ATS configurados**, busque el ATS que exportará y haga clic en el botón **Exportar ATS** (flecha verde).



3. Salve el archivo con el nombre de archivo por defecto **export_flexc.cxml** o renombre el archivo.
4. Para ver el archivo, ábralo en el Bloc de notas.
5. Para importar un ATS al sistema, acceda a **Comunicaciones > FlexC > FlexC ATS**.
6. Desplácese hasta **Importar ATS**.

7. Haga clic en el botón **Buscar** y seleccione el ATS que importará (extensión de archivo .cxml).
8. Haga clic en **Importar ATS**.

   El ATS aparecerá en la tabla **ATS configurados** con el siguiente ID disponible.

Cuando exporta un ATS, el código de abonado SPT cambia a 0. Esto evita que se exporte el ATS y que luego se importe y se replique un ATS existente.

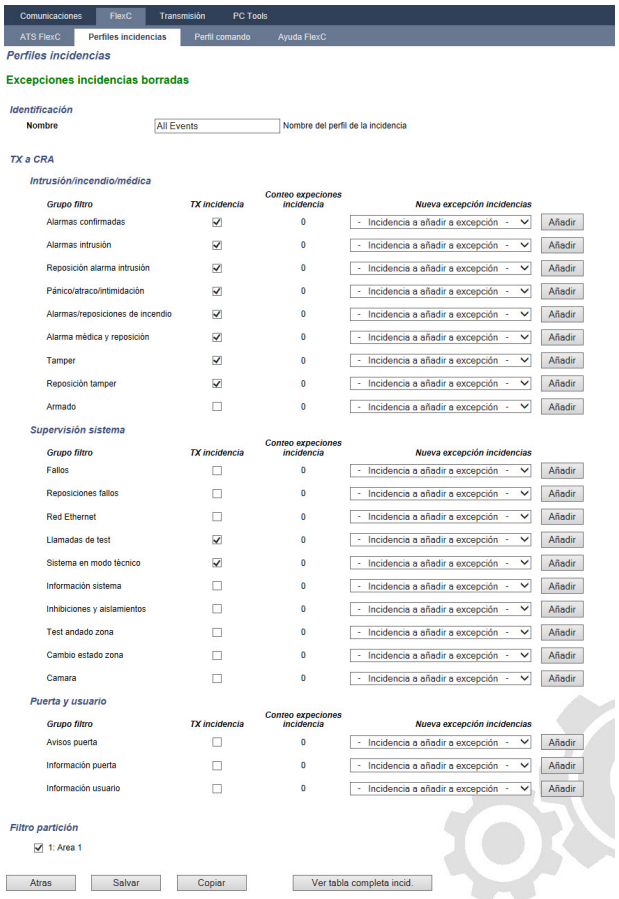
17.10.2.6 Configurar perfiles de incidencias

El perfil de incidencias define las incidencias que se transmiten en un ATS, el estado de informe para una incidencia y las excepciones. Las excepciones de incidencias le permiten cambiar los valores por defecto a valores personalizados. Para obtener más información, consulte *Definición de excepción de incidencia* en la página opuesta.

Para ver una lista de todas las incidencias, vaya a **Comunicaciones > FlexC > Perfiles de incidencias**. Haga clic en el icono **Editar** para el perfil de incidencias. Desplácese hasta el final de la página y haga clic en **Mostrar tabla de incidencias completa**.

Para crear rápidamente un nuevo perfil de incidencias, vaya a **Comunicaciones > FlexC > Perfiles de incidencias**. En la tabla **Perfiles de incidencias**, seleccione un perfil de incidencias y haga clic en el icono **Editar**. Desplácese hasta el final de la página y haga clic en **Replicar**. Ahora puede realizar los cambios que desea.

1. Para configurar perfiles de incidencias FlexC paso a paso, vaya a **Comunicaciones > FlexC > Perfiles de incidencias**.
2. Haga clic en **Añadir**. Se mostrará la página **Perfiles de incidencias**.



3. Introduzca un **nombre** para identificar el perfil de incidencias.

4. Seleccione los grupos de filtros de incidencias a informar para este perfil marcando las casillas **Informar incidencia**.
5. Para evitar que se informen determinadas incidencias o direcciones dentro de una incidencia, seleccione la incidencia de la lista desplegable **Añadir excepción de incidencia**.
6. Haga clic en **Añadir** para ver la página **Definición de excepción de incidencias**. Consulte *Definición de excepción de incidencia* abajo.
7. Haga clic en **Atrás** para regresar a la página **Perfiles de incidencias**.
8. Para aplicar un perfil de incidencias a una partición, seleccione la partición debajo de **Filtro de particiones**.
9. Haga clic en **Salvar** y **Atrás**. Se muestra el nuevo perfil en la tabla **Perfiles de incidencias**.

Puede ver una lista de todas las excepciones de incidencias para un perfil de incidencias debajo de **Excepciones de incidencias** en la página **Perfiles de incidencias**.

No puede borrar el **Perfil de incidencias por defecto**, el **Perfil de incidencias de portal por defecto** o un perfil de incidencias asignado a un ATS. Si intenta eliminar un perfil de incidencias que está en uso, aparecerá un error.

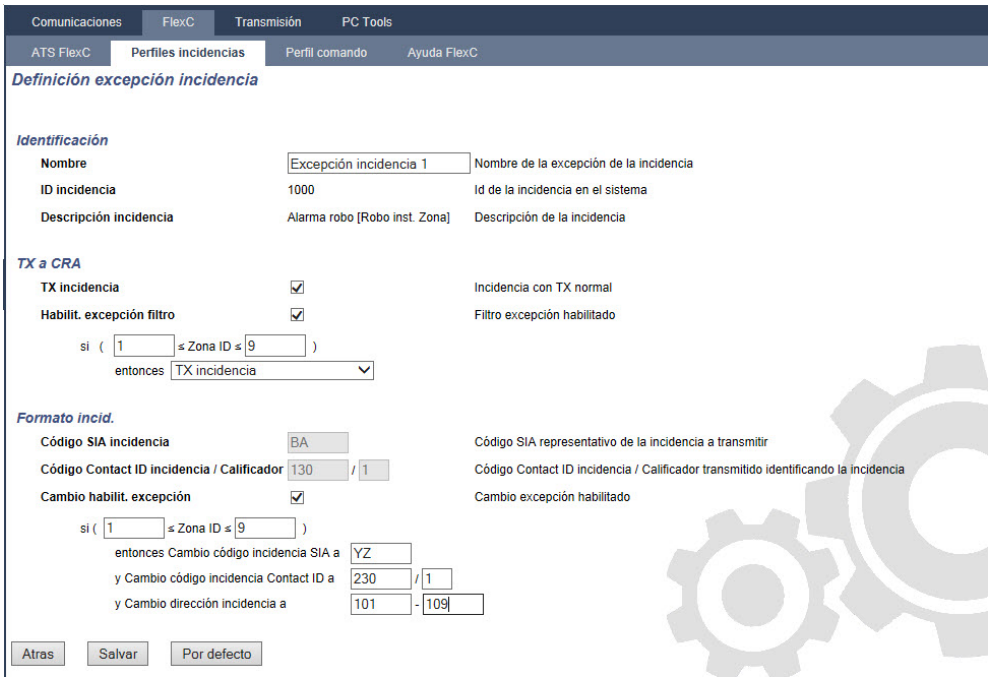
Definición de excepción de incidencia

Las excepciones de incidencias le permiten cambiar los siguientes ajustes para un rango de direcciones dentro de una incidencia:

- Informar incidencia
- Código SIA
- Código CID
- Dirección de incidencia (por ejemplo, ID de zona, ID de partición, ID de usuario)

Por ejemplo, en el grupo de filtros **Alarmas intrusión**, puede definir una excepción de incidencia para un rango de ID de zonas en la incidencia de alarma por robo (BA) como se indica a continuación:

- No informar incidencia de BA para los ID de zona 1 a 9
- Cambiar el código SIA de BA a YZ
- Cambiar el CID de 130/1 a 230/1
- Cambiar el ID de zona 1-9 a ID de zona 101-109



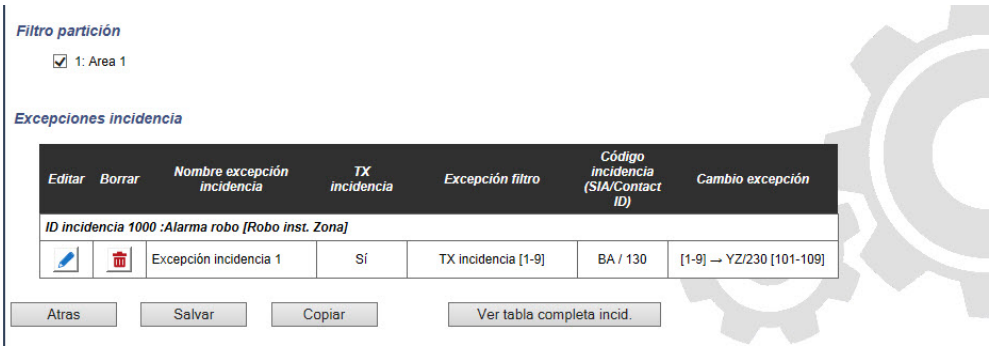
1. Para configurar una **Definición de excepción de incidencia**, complete los campos descritos en la tabla a continuación.

Identificación	
Nombre	Introduzca el nombre de la excepción de incidencia.
ID incidencia	ID de la incidencia en el sistema. Esto solo se muestra.
Descripción de incidencia	Descripción de la incidencia. Esto solo se muestra.
TX Incidencias	
Informar incidencia	Marque para informar la incidencia. Esto anula el valor de informe establecido para el grupo de filtros de eventos. Por ejemplo, si el grupo de filtros **Alarmas intrusión** está configurado para informar, puede excluir la incidencia de BA o deshabilitar este ajuste.
Habilitar excepción de filtro	Marque esta opción para excluir un rango de direcciones, por ejemplo, ID de zonas, del ajuste del campo **Informar incidencia**.
Si (0 ≤ *ID de zona* ≤ 9999) Entonces, informar incidencia/no informar incidencia	Introduzca el rango de direcciones que desea excluir del ajuste de **Informar incidencia**. Por ejemplo, si opta por informar el tipo de incidencia de BA, puede optar por no informar el *ID de zona 1 - 9* para esa incidencia. De forma alternativa, si opta por no informar el tipo de incidencia de BA, puede optar por informar el *ID de zona 1 - 9* para esa incidencia.
Formato de incidencia	
Código de incidencia SIA	Código de incidencia SIA por defecto que se transmite para representar la incidencia. Este campo solo se muestra.

Calificador/Código de incidencia Contact ID	Calificador/Código de incidencia Contact ID por defecto que se transmite para identificar la incidencia. Este campo solo se muestra.
Habilitar excepción de cambio	Marque para cambiar el código SIA, el CID/Calificador y la dirección de incidencia por defecto a valores personalizados, por ejemplo, para cambiar el *ID de zona 1 - 9* a *ID de zona 101 - 109*. Cuando esté habilitado, se mostrarán los campos a continuación.
Si (0 ≤ *ID de zona* ≤ 9999)	Introduzca el rango de direcciones que desea cambiar para una incidencia, por ejemplo, si desea cambiar el *ID de zona 1 - 9* a *ID de zona 101 - 109*, introduzca *1* y *9*. La cantidad de direcciones en el rango debe ser igual a la cantidad de direcciones definidas en el campo **Cambiar dirección de incidencia** a continuación.
entonces cambie el código de incidencia SIA a BA	Cambie el código SIA por defecto a un código SIA personalizado.
y cambie el calificador/código de incidencia Contact ID a	Cambie el calificador/código de incidencia Contact ID por defecto a un calificador/código de incidencia Contact ID personalizado.
y cambie la dirección de la incidencia a	Introduzca el nuevo rango de direcciones, por ejemplo, si desea cambiar el ID de *zona 1 - 9* a *ID de zona 101 - 109*, introduzca *101* y *109*.

2. Haga clic en **Salvar**.
3. Haga clic en **Atrás** para regresar a la página **Perfiles de incidencias**.

   Se mostrará el nombre de cada excepción en la tabla **Excepciones de incidencias** en la parte inferior de la página. La tabla a continuación muestra los ajustes para los campos **Informar incidencia**, **Filtrar excepción**, **Código de incidencia (SIA/CID)** y **Cambiar excepción** para la incidencia.



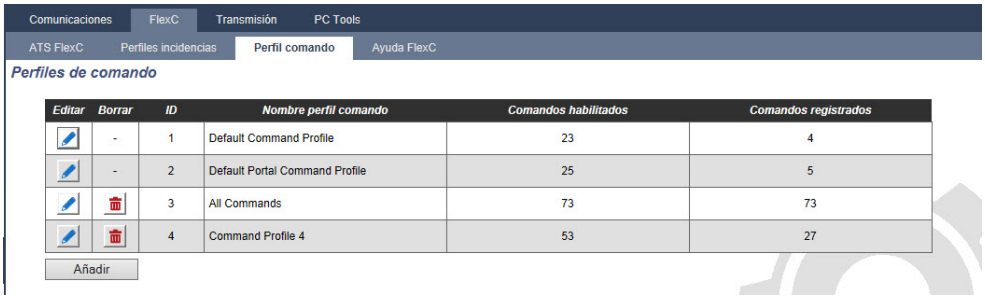
4. Haga clic en el icono **Editar** para realizar cambios o en el icono **Borrar** para eliminar una **Excepción de incidencia**.
5. Para aplicar un perfil de incidencias a una partición, seleccione la casilla de la partición.
6. Haga clic en **Salvar** para salvar el perfil de incidencias.
7. Haga clic en **Atrás** para ver el perfil en la tabla **Perfiles de incidencias**.

17.10.2.7 Configurar perfiles de comandos

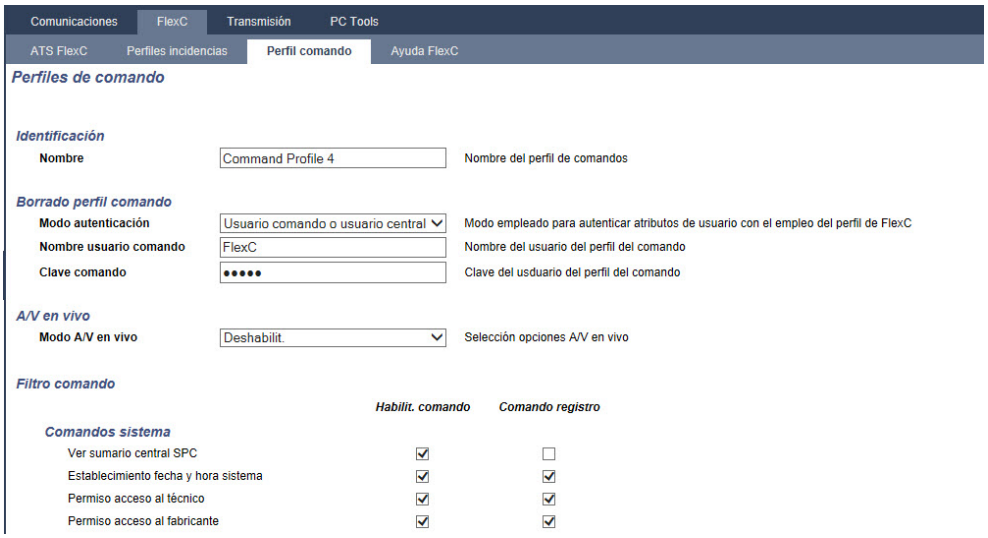
El perfil de comandos define los comandos permitidos en un ATS. Este perfil determina cómo un CMS puede controlar una central. El perfil de comandos por defecto no admite la verificación de vídeo.

AVISO: Para crear rápidamente un nuevo perfil de comandos, vaya a **Comunicaciones > FlexC > Perfiles de comandos**. En la tabla **Perfiles de comandos**, seleccione un perfil de comandos y haga clic en el botón de edición (lápiz azul). Desplácese hasta la parte inferior de la página y haga clic en **Replicar**. Ahora puede realizar los cambios que desea.

1. Para añadir un perfil de comandos paso a paso, vaya a **Comunicaciones > FlexC > Perfiles de comandos**.



2. Haga clic en **Añadir**.



3. Introduzca un **Nombre** para identificar el perfil de comandos.
4. Seleccione un **Modo de autenticación** (Usuario de comandos o Usuario de central, Usuario de comandos únicamente o Cualquier usuario de central) del menú desplegable.

AVISO: El **Nombre de usuario de comandos** por defecto habilita un usuario sin necesidad de configuración adicional que habilita el control rápido y sencillo de la central desde SPC Com XT. Habilita una gran cantidad de comandos. Por ejemplo, el usuario de comandos por defecto puede establecer todas las particiones o zonas de control. Para un control más estricto, por ejemplo, para permitir únicamente el armado de ciertas particiones, puede configurar un perfil de comandos personalizado con un conjunto de derechos definido. No puede borrar el **Perfil de comandos por defecto**, el **Perfil de comandos de portal por defecto** o un perfil de comandos asignado a un ATS.

5. Introduzca el nombre del usuario de perfil de comandos en el campo **Nombre de usuario de comandos**. Esto debe coincidir con el **Nombre de usuario de autenticación** en SPC Com XT.
6. Introduzca la clave del perfil de comandos en el campo **Clave de comandos**. Esto debe coincidir con el campo **Código PIN de usuario o clave** en SPC Com XT.

7. Seleccione el **Modo de transmisión en vivo** (Deshabilitado, Sólo tras alarma, Siempre disponible, Sistema en armado total) para determinar las opciones de privacidad de transmisión. **Siempre disponible** genera la mayor cantidad de datos.
8. Debajo de **Filtro comandos**, seleccione los comandos que habilitará. Para acceder a la lista completa de comandos, consulte *Comandos FlexC* en la página 410.
9. Seleccione los comandos que registrará.
10. Haga clic en **Salvar**.
11. Haga clic en **Atrás** para ver el perfil de comandos en la tabla **Perfiles de comandos**.
12. Para cambiar un perfil de comandos, haga clic en el botón **Editar** (icono de lápiz) junto al perfil de comandos.

17.10.3 Generación de informes

Esta sección abarca:

17.10.3.1 Central de recepción de alarmas (CRA)

La central SPC ofrece la posibilidad de comunicar información a una estación receptora remota cuando tiene lugar una incidencia de alarma específica.

Estas centrales de recepción de alarmas deben estar configuradas en la central para que pueda funcionar la comunicación remota.

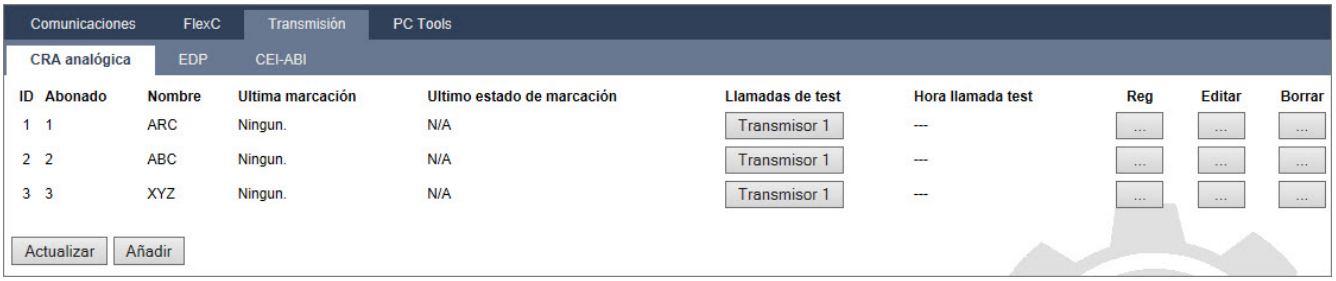
Añadir/Editar una CRA mediante el uso de SIA o CID

Requisito previo

- Un módem GSM o RTB instalado y funcionando correctamente.

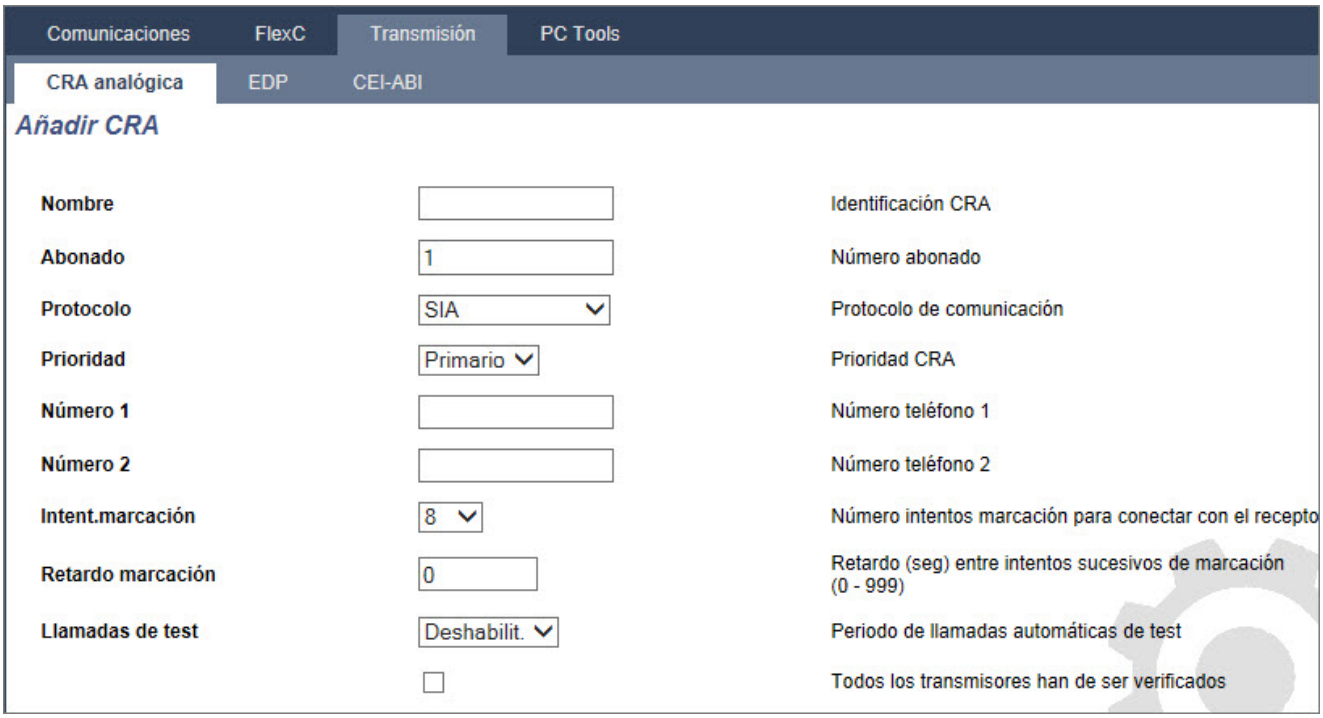
1. Seleccione **Comunicaciones > Informes > CRA analógica**.

   Se mostrará la siguiente página:



2. Haga clic en el botón **Módem1/2** para realizar una llamada de test a la CRA desde el módem 1 o el módem 2.
3. Haga clic en el botón **Registro** para recibir un archivo de registro. Se mostrará una página con los registros de todas las llamadas de test automáticas y manuales.
4. Para añadir o editar una CRA, haga clic en **Añadir**. – O BIEN –
   Haga clic en **Editar**.

   Se mostrará la siguiente página.


Comunicaciones
FlexC
Transmisión
PC Tools
CRA analógica
EDP
CEI-ABI
Añadir CRA
Nombre
Identificación CRA
Abonado
1
Número abonado
Protocolo
SIA
Protocolo de comunicación
Prioridad
Primario
Prioridad CRA
Número 1
Número teléfono 1
Número 2
Número teléfono 2
Intent.marcación
8
Número intentos marcación para conectar con el recepto
Retardo marcación
0
Retardo (seg) entre intentos sucesivos de marcación (0 - 999)
Llamadas de test
Deshabilit.
Periodo de llamadas automáticas de test
Todos los transmisores han de ser verificados

5. Configure los campos tal como se describe en la siguiente tabla.

Descripción	Introduzca la descripción de la central de recepción de alarmas remota.
Cód. abonado	Introduzca su número de abonado. Esta información debe estar disponible desde la estación de recepción y se utiliza para identificarlo cada vez que realiza una llamada a la CRA. Para un abonado de Contact ID, se permite un máximo de 6 caracteres.
Protocolo	Introduzca el protocolo de comunicación que pretende usar (SIA, SIA extendido, Contact ID, Formato rápido). **Nota:** El SPC admite el protocolo SIA extendido. Seleccione este protocolo para brindar descripciones textuales adicionales de las incidencias de SIA enviadas a la central de recepción de Alarmas.
Prioridad	Seleccione la prioridad para la CRA en términos de presentación de informes primarios o de respaldo.
Número 1	Introduzca el primer número que se debe marcar para contactar con la CRA. Este sistema siempre intentará contactar con la CRA marcando este número antes de intentar con otro.
Número 2	Introduzca el segundo número que se debe marcar para contactar con la CRA. El sistema sólo intentará contactar con la CRA mediante este número si el primer número de contacto no pudo establecer con éxito una llamada.
Intentos de marcación	Introduzca la cantidad de veces que el sistema intentará realizar una llamada al receptor. (por defecto, 8)
Retardo de marcación	Cantidad de segundos de retardo entre intentos fallidos de marcación (0-999).
Intervalo de marcación	Introduzca la cantidad de segundos de retardo entre intentos fallidos de marcación. (0-999)
Llamadas de test	Habilite una llamada de test al seleccionar un intervalo de tiempo. Esto enviará una llamada de test automática desde el módem 1 a la CRA principal.
Test todo	Marque esta casilla si también desea iniciar una llamada de test automática desde el módem 2 a la CRA de respaldo.

6. Haga clic en el botón **Añadir** para introducir estos detalles en el sistema.

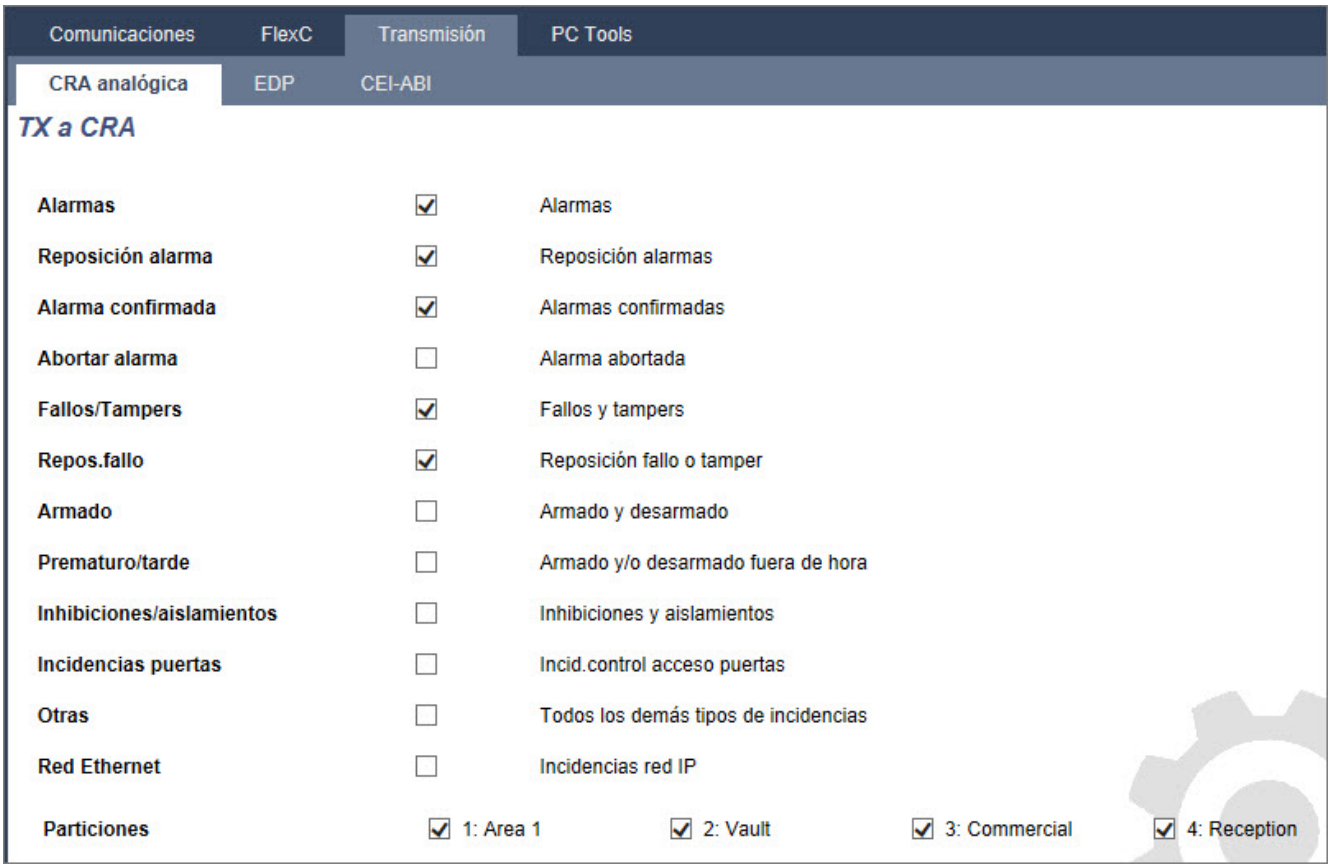
   Aparecerá una lista de abonados de CRA configurados en el navegador junto con la información del abonado, la descripción, el protocolo, el estado de marcación y la fecha y la hora de la última llamada a la CRA.

Editar un filtro de CRA mediante el uso de SIA o CID

Para configurar las incidencias en el SPC que activarán la llamada a la CRA:

1. Seleccione **Comunicaciones > Informes > CRA analógica > Editar > Filtro**.

   Se mostrará la siguiente página:



2. Configure los siguientes campos:

   Marque las casillas que correspondan si desea iniciar una llamada remota a la CRA para notificar de la incidencia en particular.

Alarmas	Se activan las alarmas.
Restauraciones de alarmas	Se restauran las alarmas del sistema.
Alarmas confirmadas	Alarmas confirmadas en múltiples zonas
Aborto de alarmas	Incidencias de abortos de alarmas. Se abortan las alarmas cuando se introduce un código de usuario válido en el teclado luego de una alarma confirmada o no confirmada,
Fallos	Se activan los fallos y los tampers.
Restauraciones de fallos	Se restauran las alarmas de fallo o tamper.
Ajustes	El sistema se arma o desarma.
Prem./tarde	Armado y desarmado no programado del sistema.
Inhibiciones	Se realizan operaciones de inhibición y de aislamiento en el sistema.
Incidencias de puerta	Se activan las incidencias de puerta. Solo funciona con el protocolo SIA.
Otros	Se detectan todos los otros tipos de incidencias en el sistema.

Red	Informar incidencias de polling arriba/abajo de red IP.
Particiones	Seleccione las particiones específicas a las que se aplican las incidencias mencionadas anteriormente.

Si se agrega un Centro de recepción de alarmas (CRA) para cada área definida en el sistema y se programa cada una para que informe a su propio receptor CRA independiente, el sistema puede asimilarse a uno de tipo múltiple ya que se asigna un alto grado de autonomía a cada área.

Editar un filtro de CRA mediante el uso de Formato rápido

Para configurar las incidencias en el SPC que activarán la llamada a la CRA cuando el protocolo seleccionado sea **Formato rápido**:

1. Seleccione **Comunicaciones > Informes > CRA analógica > Editar > Filtro**.

   Aparecerá una lista de ocho canales junto con las condiciones de alarma que pueden programarse para cada canal.
2. Seleccione las condiciones de alarma para cada canal según sea necesario. Para ver una descripción de cada una, consulte *Tipos de salidas y puertos de salida* en la página 227.
3. Desde el menú desplegable **Alcance**, seleccione **Sistema** o la partición específica a la que aplicará la configuración seleccionada.
4. Haga clic en el botón **Test** ubicado junto al primer canal para comprobar la activación de la alarma.

   El icono de bombilla de luz se encenderá.
5. Espere aproximadamente cinco segundos y vuelva a hacer clic en el botón **Test** para el mismo canal. Esto envía una restauración de canal a la CRA, y el icono de la bombilla de luz se apagará.
6. Continúe con el test de los otros canales.

17.10.3.2 Configuración EDP

IP

El sistema ofrece la posibilidad de transmitir información al servidor SPC Com de forma remota utilizando el protocolo propio de Vanderbilt, el Protocolo de Datagrama Mejorado (**E**nhanced **D**atagram **P**rotocol o EDP). Configurando correctamente el receptor EDP en el sistema, puede programarse para realizar llamadas de datos automáticamente al servidor SPC Com en una ubicación remota siempre que se produzcan incidencias como activaciones de alarmas, tampers o armados/desarmados. El técnico puede configurar el sistema para realizar llamadas a un servidor remoto a través de las siguientes rutas:

- **RTB** (Se requiere módem RTB)
- **GSM** (Se requiere módem GSM)
- **Internet** (Interfaz Ethernet)

Si usa la red RTB, asegúrese de que el módem RTB esté bien instalado y que funcione correctamente, y que haya una línea RTB conectada a los terminales A y B del módem RTB.

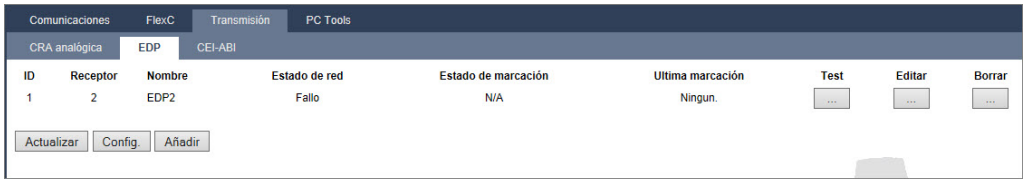
Si utiliza una red GSM, asegúrese de que el módulo GSM esté bien instalado y que funcione correctamente. Se puede realizar una conexión IP a través de Internet a un servidor con una dirección IP pública fija.

Si se requiere una conexión IP, asegúrese de que la interfaz Ethernet esté correctamente configurada (consulte *Interfaz Ethernet* en la página 183) y que el acceso a Internet esté habilitado en el router.

Agregar un receptor EDP

1. Seleccione **Comunicaciones > Informes > EDP**.

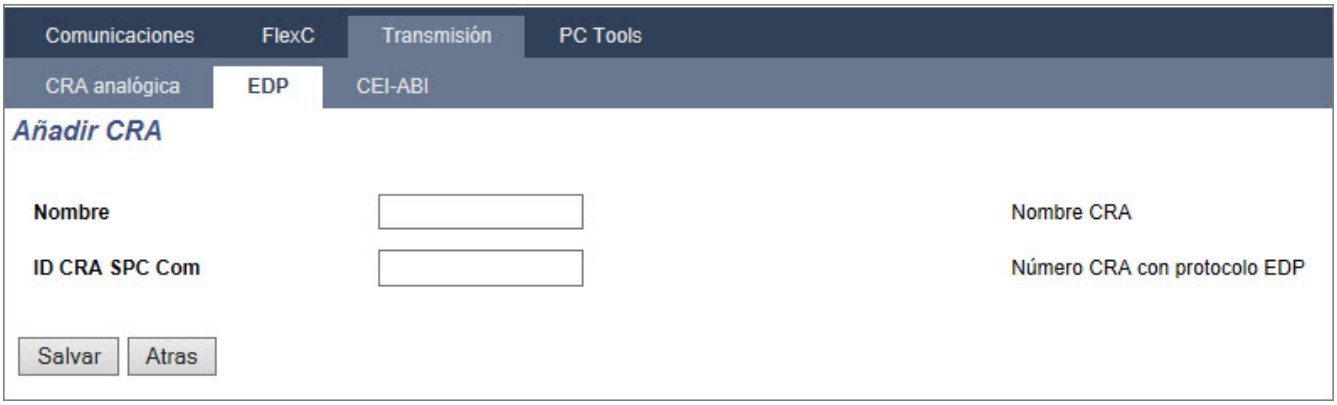
   Se mostrará la siguiente página:



Máx. Se pueden agregar ocho receptores al sistema SPC.

2. Haga clic en el botón **Añadir**.

   Se mostrará la siguiente página.



3. Consulte la tabla a continuación para obtener más información.

Descripción	Introduzca una descripción del receptor.
Núm.ID CRA	Introduzca un número único que utilizará el EDP para identificar al receptor.

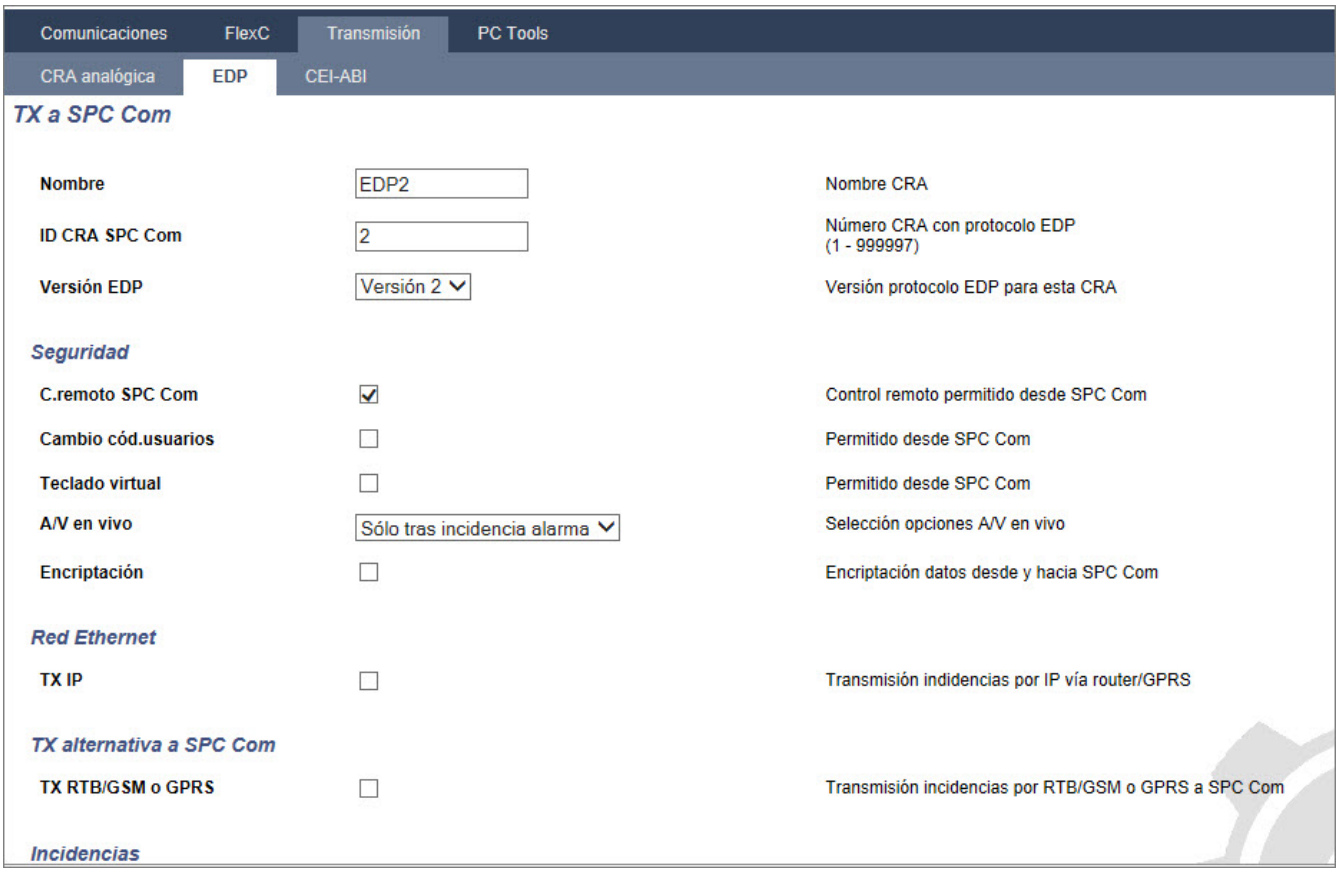
Consulte también

Editar la configuración del receptor EDP abajo

Editar la configuración del receptor EDP

1. Seleccione **Comunicaciones > Informes > EDP > Editar**.

   Se mostrará la siguiente página.


Comunicaciones
FlexC
Transmisión
PC Tools
CRA analógica
EDP
CEI-ABI
TX a SPC Com
Nombre
EDP2
Nombre CRA
ID CRA SPC Com
2
Número CRA con protocolo EDP (1 - 999997)
Versión EDP
Versión 2
Versión protocolo EDP para esta CRA
Seguridad
C.remoto SPC Com
Control remoto permitido desde SPC Com
Cambio cód.usuarios
Permitido desde SPC Com
Teclado virtual
Permitido desde SPC Com
A/V en vivo
Sólo tras incidencia alarma
Selección opciones A/V en vivo
Encriptación
Encriptación datos desde y hacia SPC Com
Red Ethernet
TX IP
Transmisión indidencias por IP vía router/GPRS
TX alternativa a SPC Com
TX RTB/GSM o GPRS
Transmisión incidencias por RTB/GSM o GPRS a SPC Com
Incidencias

2. Configure los campos tal como se describe en la siguiente tabla.

Descripción	Edite el nombre del receptor EDP si es necesario. Utilice 16 caracteres como máximo.
Núm.ID CRA	Edite el ID CRA SPC Com del EDP. El rango va del 1 al 999997 (999998 y 999999 están reservados para fines especiales).
Versión protocolo	Seleccione la versión del protocolo EDP que utilizará con este receptor EDP. Las opciones son Versión 1 o Versión 2. Si el receptor la admite, se recomienda la versión 2, ya que es un protocolo más seguro.
Compatible VdS 2471	(Estándar Vds solo) Si se selecciona esta opción, el receptor EDP impondrá los siguientes ajustes para ese receptor: • Intervalo test 8 s • Protocolo TCP impuesto • Los reintentos de TCP fallarán después de 10 s (9 s aprox.) • Los reintentos de incidencia EDP están ajustados en 1 independientemente del ajuste global de «Núm. máximo intentos» en «Configuración TX EDP». • Antes de 20 s a partir del fallo de red se generará un FTC.
Seguridad	
Habilitación comandos	Marque esta casilla para permitir que se acepten comandos desde el receptor.
Cambiar códigos PIN de usuario	Marque esta casilla para permitir el cambio de códigos PIN de usuario desde una ubicación remota. Esta función es aplicable solo si se habilitan los comandos desde el receptor.
Habilitar cifrado	Marque esta casilla para habilitar el cifrado de datos desde y hacia el receptor.
Clave de cifrado	Introduzca una clave hexadecimal (máx. 32 dígitos) que se utilizará para encriptar los datos. **Nota:** Se requerirá el uso de la misma clave para el receptor.
Teclado virtual	Habilita el acceso a la central con un teclado virtual, es decir, un módulo de software para PC que parece y funciona como un teclado SPC. Está disponible con el cliente SPC Com.
Transmisión en vivo / modo de transmisión	Especifica cuando está disponible la transmisión de audio y vídeo en vivo. Las opciones son Nunca, Siempre y Solo después de una alarma. La opción por defecto es 'Solo después de una alarma'. **Nota:** Esta configuración tiene obvias implicancias de privacidad y, por lo tanto, debe habilitarse únicamente cuando sea apropiado y conforme a las leyes y regulaciones locales.
Red (sólo aplicable a la conexión Ethernet)	
TX IP	Marque esta casilla para permitir que se informe de incidencias a través de la red.

Protocolo Ethernet	Seleccione el tipo de protocolo de red para el receptor. Las opciones son UDP y TCP. Si el receptor lo admite, se recomienda TCP.
Dirección ID CRA SPC Com	Introduzca la dirección IP del receptor.
Puerto IP del receptor	Introduzca el puerto IP desde el cual el receptor EDP escucha.
Siempre conectado	Si esta opción está habilitada, la central mantendrá una conexión permanente al receptor. Si está deshabilitada, la central solo se conectará al receptor tras una incidencia de alarma.
Central maestra	En caso de estar habilitada esta opción, la central será maestra de los mensajes de polling. Solo aplicable a conexiones UDP.
Intervalo test	Introduzca el número de segundos entre los tests.
Inicio test	Introduzca el número de tests que deben faltar antes de que se registre un fallo de conexión de red. Solo aplicable a conexiones UDP.
Generar fallo red	Si falla el test, se generará una alerta de fallo de red.
Conexión telefónica (sólo aplicable a la conexión de módem GPRS)	
Habilitación de acceso telefónico	Marque esta casilla para informar las incidencias a través de una conexión de acceso telefónico.
Tipo de llamada	Seleccione el tipo de llamada que se utilizará cuando esté habilitado el acceso telefónico. Seleccione GPRS.
Protocolo GPRS	Seleccione el protocolo de capa de transporte que se utilizará con la conexión GPRS. Las opciones son UDP o TCP. Solo aplicable si el tipo de llamada es GPRS.
Dirección GPRS	Introduzca la dirección IP del receptor EDP para las conexiones GPRS. Solo aplicable si el tipo de llamada es GPRS.
Puerto GPRS	Introduzca el puerto desde el cual el receptor EDP escucha para las conexiones GPRS. Las opciones son UDP o TCP. Solo aplicable si el tipo de llamada es GPRS. Por defecto es 50000.
Tiempo de espera para colgar de GPRS	Introduzca la cantidad de tiempo en segundos tras la cual la llamada GPRS debe colgar. (0 = mantener la conexión hasta que se active la conexión IP)
Conexión automática de GPRS	Marque esta casilla para realizar automáticamente una llamada GPRS al servidor si se produce un fallo en la red IP.
Acceso telefónico con fallo de red	Marque esta casilla para informar los fallos de red en una llamada de test mediante conexión telefónica.

Intervalo de TX alternativa a SPC Com 1*	Introduzca la cantidad de minutos entre llamadas de test mediante conexión telefónica cuando el enlace de la red está activo.
Intervalo de TX alternativa a SPC Com 2*	Introduzca la cantidad de minutos entre llamadas de test mediante conexión telefónica cuando el enlace de la red está inactivo.
Dirección de red*	Introduzca la dirección IP del receptor. Esto solo se requiere si la conexión al receptor EDP se realiza a través de una interfaz Ethernet. Si utiliza uno de los módems integrados, deje este campo en blanco.
Número de teléfono*	Introduzca el primer número de teléfono al que debe marcar el módem para contactarse con el receptor.
Número de teléfono 2*	Introduzca el segundo número de teléfono al que debe marcar el módem en caso de que no se pueda establecer una llamada al marcar el primer número.
Incidencias	
Receptora primaria	Marque esta casilla para indicar que este es el receptor principal. Si no está marcada, este es un receptor de respaldo.
Reencolar incidencias	Marque esta casilla si las incidencias que no pudieron ser informadas deben ser reencoladas para la transmisión.
Verificación	Marque esta casilla si se debe enviar la verificación de audio/vídeo a este receptor.
TX Incidencias	Haga clic en este botón para editar las incidencias de filtro que activarán una llamada de EDP. Consulte *Editar la configuración de filtros de incidencias* abajo.

* En esta versión, no se admite la marcación EDP a través de RTB.

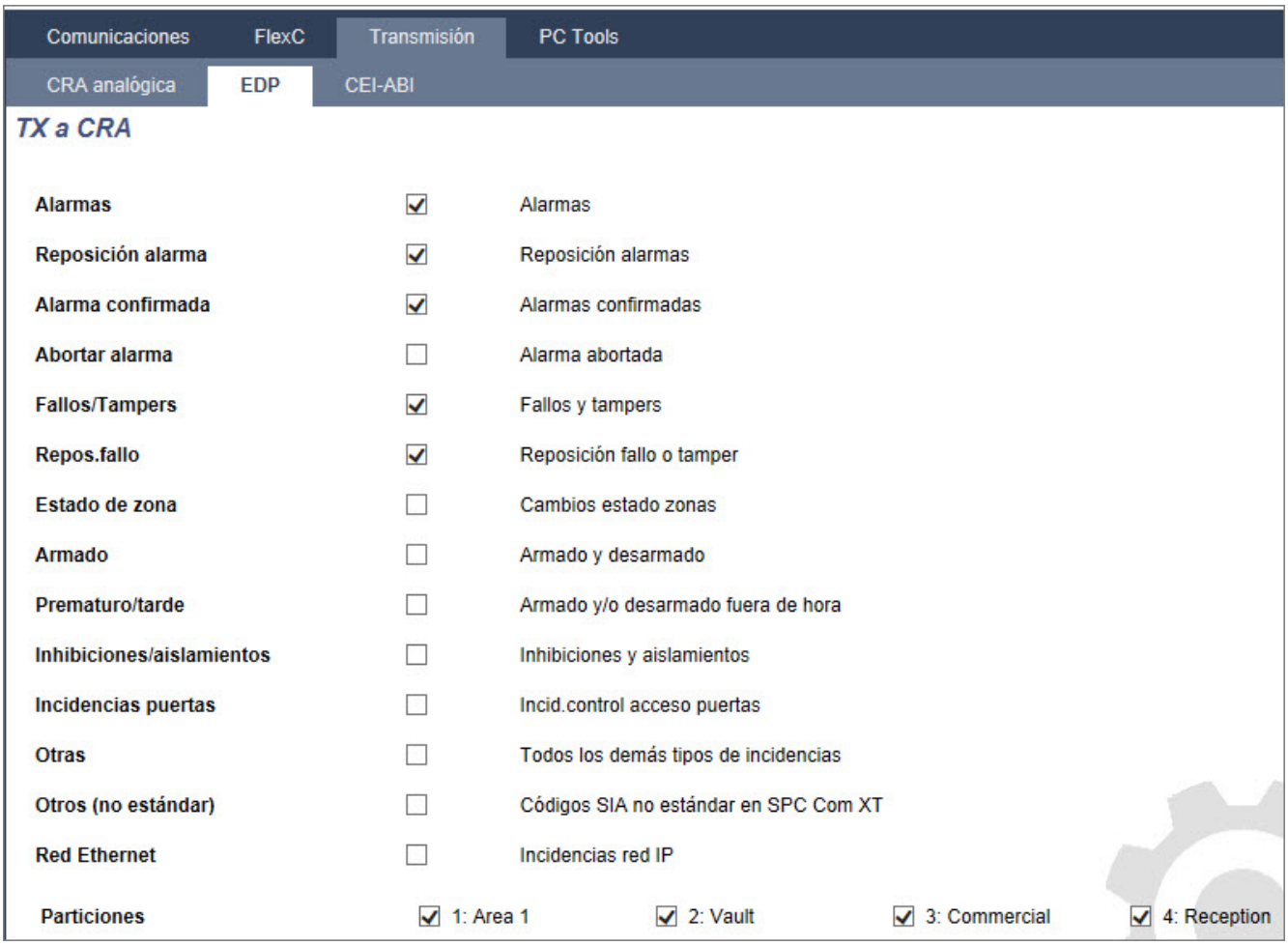
Consulte también

Configuración de SMS en la página 217

Editar la configuración de filtros de incidencias

1. Seleccione **Comunicaciones > Informes > EDP > Editar > Filtro**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

   Marque las casillas que correspondan si desea iniciar una llamada remota a un receptor EDP para notificar una incidencia en particular.

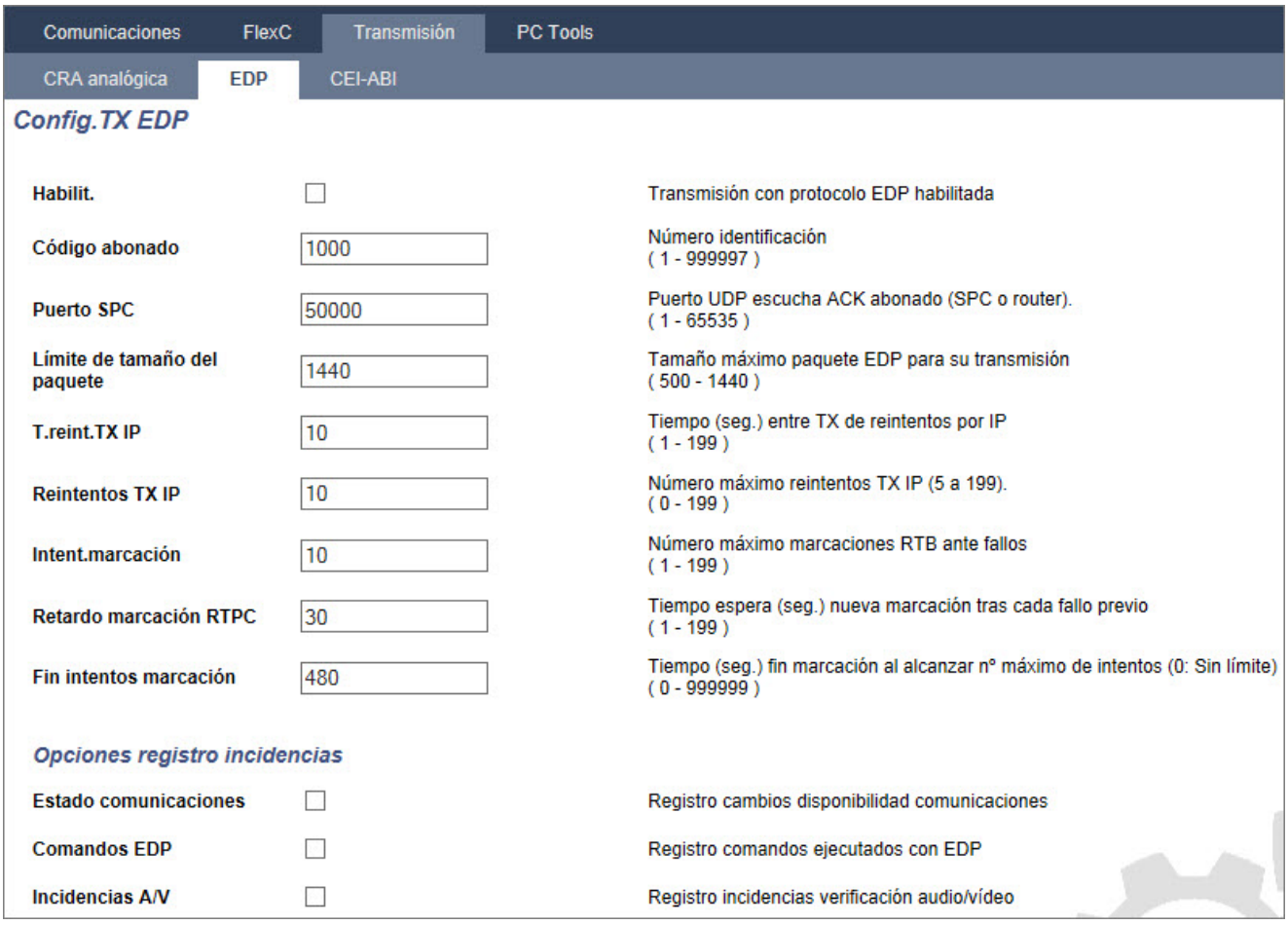
Alarmas	Se activan las alarmas.
Restauraciones de alarmas	Se restauran las alarmas del sistema.
Alarmas confirmadas	Alarmas confirmadas en múltiples zonas
Aborto de alarmas	Incidencias de abortos de alarmas. Se abortan las alarmas cuando se introduce un código de usuario válido en el teclado luego de una alarma confirmada o no confirmada,
Fallos	Se activan los fallos y los tampers.
Restauraciones de fallos	Se restauran las alarmas de fallo o tamper.
Estado de zona	Informa todos los cambios de estado de entrada de zona.
Ajustes	El sistema se arma o desarma.
Prem./tarde	Armado y desarmado no programado del sistema.

Inhibiciones	Se realizan operaciones de inhibición y de aislamiento en el sistema.
Incidencias de puerta	Se activan las incidencias de puerta. Solo funciona con el protocolo SIA.
Otros	Se detectan todos los otros tipos de incidencias en el sistema.
Otro (no estándar)	Códigos SIA no admitidos utilizados con SPC COM XT, incluyendo incidencias de cámara en línea/fuera de línea.
Red	Informar incidencias de polling arriba/abajo de red IP.
Particiones	Seleccione las particiones específicas a las que se aplican las incidencias mencionadas anteriormente.

Editar la configuración de EDP

1. Seleccione **Comunicaciones > Informes > EDP > Configuración**.

   Se mostrará la siguiente página.



2. Configure los campos tal como se describe en la siguiente tabla.

Enable (habilitar)	Marque esta casilla para habilitar el funcionamiento de EDP en el sistema.
ID de la central de EDP	Introduzca el identificador numérico que utiliza el receptor EDP para identificar la central de forma única.
Puerto IP	Seleccione el puerto IP para recibir los paquetes IP. Por defecto es 50000.
Límite de tamaño de paquete	Introduzca la cantidad máxima de bytes en un paquete de EDP para su transmisión.
Tiempo de espera de incidencia	Introduzca el período de tiempo de espera (en segundos) entre retransmisiones de incidencias no reconocidas.
Conteo de reintentos	Introduzca la cantidad máxima de retransmisiones de incidencias permitidas por el sistema.
Intentos de marcación	Introduzca la cantidad máxima de intentos de marcación fallidos aceptados por el sistema antes de que se bloquee el módem (para evitar que continúen los intentos de marcación). El período de bloqueo se define en la opción Bloqueo de marcación.
Retardo de marcación	Introduzca el período de tiempo (en segundos) que esperará el sistema antes de volver a marcar tras una falla de intento de marcación.
Bloqueo de marcación	Introduzca el período de tiempo (en segundos) que el sistema suspenderá la marcación cuando se alcance la cantidad máxima de intentos de marcación fallidos. Introduzca el valor ‘0’ para que los intentos de marcación sean continuos.

Opciones de registro de incidencias

Estado de comunicaciones	Registrar toda la disponibilidad de comunicaciones.
Comandos EDP	Registrar todos los comandos ejecutados a través de EDP.
Incidencias de A/V	Registrar cuando se envían al receptor incidencias de verificación de audio/vídeo.
Transmisión de A/V	Registrar el inicio de transmisiones de audio/vídeo en vivo.
Uso de teclado	Registrar cuando se activa el teclado remoto.

17.10.3.3 Configuración del protocolo CEI-ABI

1. Seleccione **Comunicaciones > Informes > CEI-ABI**.

   Se mostrará la siguiente página:

2. Configure los campos tal como se describe en la siguiente tabla.

Enable (habilitar)	Marque esta casilla para habilitar el soporte CEI-ABI.
Modo conexión	• Seleccione **Cliente** para conectar la central al receptor CEI-ABI. • Seleccione **Servidor** para habilitar a la central a escuchar conexiones.
Servidor IP	Si selecciona **Cliente** para el **Modo de conexión**, introduzca la dirección TCP/IP del receptor CEI-ABI.
Puerto servidor	Introduzca un puerto IP para el servidor.
Dirección física	Introduzca una dirección física para el CEI-ABI en la central.
Dirección lógica	Introduzca una dirección lógica para el CEI-ABI en la central.

17.10.4 Herramientas del PC

Esta sección abarca:

17.10.4.1 SPC Connect PRO

SPC Connect PRO es una aplicación de escritorio diseñada para brindar asistencia técnica para la instalación y el mantenimiento de los sistemas SPC. Si usa SPC Connect PRO, puede crear instalaciones y configurarlas antes de llegar al lugar. La herramienta puede utilizarse en conjunto con el servicio en la nube SPC Connect para conectarse de forma remota a sitios y brindar asistencia técnica.

1. Seleccione **Comunicaciones > Herramientas del PC > SPC Connect PRO**.
2. Configure los campos tal como se describe en la siguiente tabla y, luego, haga clic en **Salvar**.

SPC Connect PRO	Marque esta casilla para permitir que SPC Connect PRO se conecte a la central.
Ethernet	Marque esta casilla para permitir que SPC Connect PRO se conecte a través de Ethernet.
Puerto TCP	Introduzca el puerto TCP en el que la central escucha conexiones entrantes desde SPC Connect PRO.
USB	Marque esta casilla para permitir que SPC Connect PRO se conecte a través de USB.
Serie 1 (X10)	Marque esta casilla para permitir que SPC Connect PRO se conecte a través de un puerto serie 1 (X10).
Módem 1	Marque esta casilla para permitir que SPC Connect PRO se conecte a través del módem 1.

17.10.4.2 SPC Manager

La configuración del modo de SPC Manager determina el número de dígitos para códigos PIN de usuarios y, por lo tanto, el número de códigos PIN disponibles en un sistema global controlado por SPC Manager.

Modo41: código PIN de 4 dígitos que habilita a 1.000 de usuarios globales

Modo51: código PIN de 5 dígitos que habilita a 10.000 de usuarios globales

Modo61: código PIN de 6 dígitos que habilita a 100.000 de usuarios globales

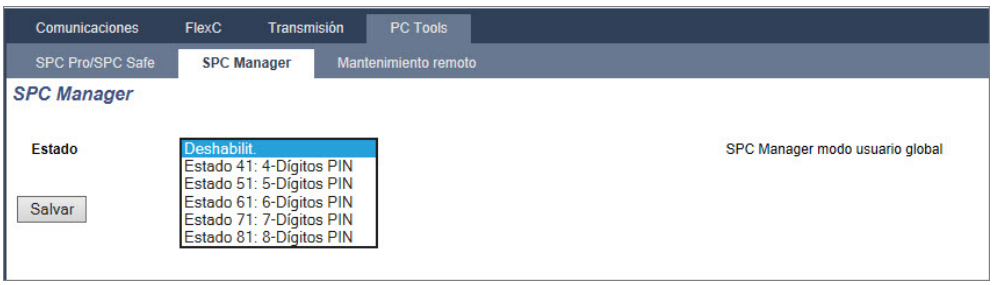
Modo71: código PIN de 7 dígitos que habilita a 1000,000 de usuarios globales

Modo81: código PIN de 8 dígitos que habilita a 10.000.000 de usuarios globales

Cuando se configura un modo de SPC Manager, se añaden ceros adicionales delante de los códigos PIN de usuario existentes de 4 o 5 dígitos, modificándose así el código PIN para su uso global. Por ejemplo, si se selecciona el **Modo71: PIN de 7 dígitos**, se añaden 3 ceros a los códigos PIN de 4 dígitos, y el PIN 2222 se convierte en 0002222.

Para configurar el modo SPC Manager:

1. Seleccione **Comunicaciones > Herramientas del PC > SPC Manager**.



2. Seleccione el modo de usuario global de SPC Manager en la lista desplegable.
3. Haga clic en el botón **Salvar**.

   El modo no se puede salvar si hay un conflicto entre un código PIN de usuario local existente y otro código PIN de usuario en el sistema global. En ese caso se muestra un mensaje de error de «Código PIN no válido».

4. Haga clic en el botón correspondiente para borrar el código PIN y salvar el nuevo modo, o cambie el código PIN por el nuevo código PIN generado aleatoriamente que se muestra y, a continuación, salve el nuevo modo.

AVISO: Los modos de SPC Manager no se pueden modificar si existen usuarios globales en el sistema.

17.11 Operaciones de archivos

Para realizar operaciones en los ficheros y en la configuración de la central:

- Seleccione **Archivo**.

  Aparecerán las siguientes pestañas:

Actualizado	Opciones para actualizar el firmware del controlador y los periféricos, así como el idioma en la central. Consulte *Operaciones de actualización de archivos* abajo.
Gestión fichero	Opciones para gestionar el archivo de configuración del sistema y cargar y descargar datos de usuarios desde y hacia la central. Consulte *Operaciones del Gestor de archivos* en la página 353.
Audio	Cargar un archivo de audio en el SPC. Haga clic en **Buscar** y luego haga clic en **Cargar** para añadir el archivo de audio al SPC. Después de la carga, haga clic en el botón **Test** para validar el archivo de audio.
Default	Se restaura el sistema SPC a la configuración por defecto de fábrica. **¡AVISO! La dirección IP para conectarse con la interfaz web se mantiene después de restaurar los valores por defecto de fábrica desde la página web.**
Reset	Se reinicia la central.
Política de textos	Esta pestaña resume la configuración para los ajustes de sus productos SPC en función de la **Región**, el **Grado** y el **Tipo** seleccionados.

17.11.1 Operaciones de actualización de archivos

Para actualizar el firmware y los idiomas en el sistema:

- Seleccione **Archivo > Actualizar**.

  Aparecerá la siguiente página:

Consulte también

Opciones en la página 254

17.11.1.1 Actualizar el firmware

AVISO: Para realizar operaciones de actualización de firmware, se necesita acceso de fabricante; cuando está habilitado, se pueden completar las actualizaciones de firmware tanto del controlador como de los periféricos. Consulte *Opciones* en la página 254.

El firmware para SPC está incluido en dos archivos por separado:

- Archivo de firmware del controlador
  Solamente contiene el firmware para las CPU del controlador. El nombre de archivo tiene la extensión *.fw.
- Archivo de firmware de periféricos
  Contiene el firmware para los nodos X-BUS, más los módems RTB y GSM. El nombre de archivo tiene la extensión *.pfw.

Los dos archivos se actualizan por separado.

AVISO: Se recomienda actualizar el firmware de todos los periféricos tras una nueva actualización del firmware del controlador.

Aviso: Puede actualizar el firmware con el teclado.

Firmware del controlador

Para actualizar el firmware del controlador en el sistema:

1. Seleccione la opción **Operaciones de actualización de central** en la pestaña **Fichero**.

   Aparecerá la siguiente página:

2. Seleccione el fichero de firmware para actualizar haciendo clic en el botón **Browse** (examinar) para elegir la opción adecuada, seleccionando a continuación el fichero de firmware necesario, y haciendo clic en el botón de **Actualizado** correspondiente.

   Se muestra una página de confirmación.

3. Haga clic en el botón **Confirmar** para aceptar la actualización a la nueva versión del firmware del controlador.

   Cuando se actualice el firmware del controlador, el sistema mostrará un mensaje para indicar que el sistema se está reseteando. Debe iniciar sesión en el sistema nuevamente para continuar la operación.

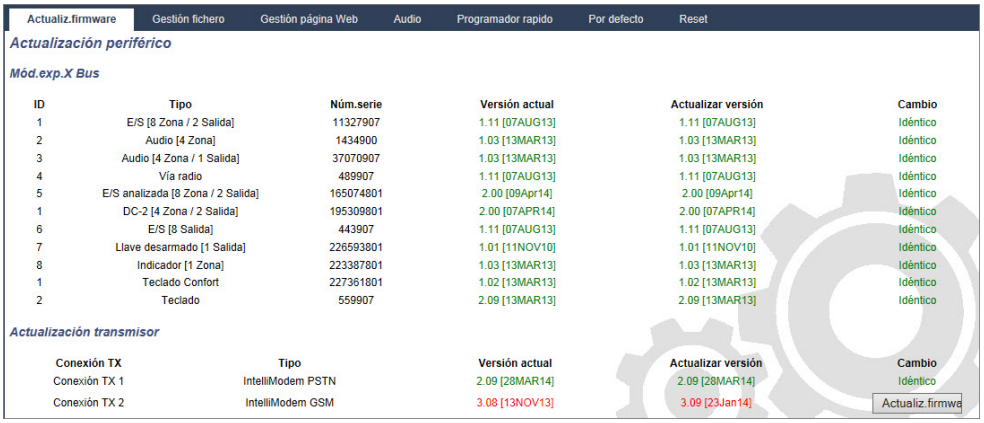
ADVERTENCIA: Si instala una versión anterior del firmware del controlador, el sistema restablecerá todos los ajustes a la configuración por defecto. Asimismo, cuando se instala una versión anterior de firmware, es importante instalar la versión anterior correspondiente del firmware de los periféricos; de lo contrario, las zonas podrían aparecer desconectadas, abiertas o cerradas.

ADVERTENCIA: Si se actualiza desde una versión de firmware anterior a la 3.3, tenga en cuenta lo siguiente:
- La clave web del técnico, si estaba configurada, se borra, por lo que debe volver a introducirse tras la actualización.
- Todos los usuarios existentes se asignarán a perfiles de usuario nuevos correspondientes a sus niveles de acceso de usuario previos. Si se sobrepasa el número máximo de perfiles de usuarios, no se asignará ningún perfil (consulte *Añadir/Editar perfiles de usuario* en la página 212). Revise toda la configuración de usuario tras actualizar el firmware.
- El ID de técnico por defecto cambia de 513 a 9999.

Actualización de firmware de periféricos

Actualice el firmware de los periféricos mediante el mismo procedimiento utilizado para actualizar el firmware del controlador.

El archivo de firmware de periféricos solo se almacena temporalmente en el sistema de archivos. Cuando se carga el archivo de firmware de un periférico nuevo, se muestran las versiones actual y nueva de cada periférico y del módem como se indica a continuación:



- Haga clic en el botón **Actualizar** para los periféricos que requieran actualización, o haga clic en el botón **Actualizar todo** para actualizar todos los periféricos.

  Si el firmware para el dispositivo periférico en el archivo .pfw es anterior al firmware existente de este dispositivo, encontrará el botón **Retroceso**.

Durante la actualización, la central comprueba si el firmware en el archivo del periférico admite las versiones de hardware específicas de los periféricos instalados y no permite la actualización de los periféricos no admitidos.

Si la versión del archivo pfw difiere de la versión del controlador, aparecerá un mensaje de advertencia.

Si el número de versión principal del firmware disponible para un dispositivo difiere del número de versión principal de un dispositivo existente, aparecerá un mensaje de advertencia.

Actualización de firmware de la fuente de alimentación inteligente SPCP355.300

Para actualizar la fuente de alimentación inteligente SPCP355.300, debe comprobar lo siguiente:

- La alimentación eléctrica debe estar conectada.

El firmware de la fuente de alimentación inteligente SPCP355.300 solo se puede actualizar a través del navegador.

El procedimiento de actualización puede tardar hasta 2 minutos. No realice ninguna otra acción en el navegador, y apague o reinicie el sistema para completar la actualización. Cuando el proceso se haya completado, aparecerá un mensaje.

Consulte también

Añadir/Editar perfiles de usuario en la página 212

17.11.1.2 Actualización de idiomas

Se puede cargar un fichero de idioma personalizado (*.clng) en la central.

AVISO: La central debe contar con licencia para usar idiomas personalizados, así como otros idiomas.

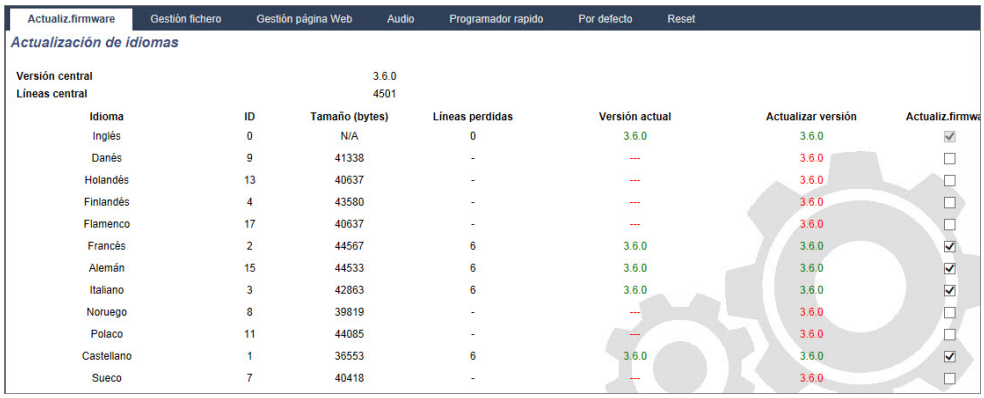
Para actualizar los idiomas en el sistema:

1. Seleccione **Archivo > Actualizar**.

   Se mostrará la página **Operaciones de actualización de central**:

2. Seleccione el fichero de idioma que desee actualizar haciendo clic en el botón **Browse** (examinar) para elegir la opción **Actualización de fichero de idioma**, seleccionando a continuación el fichero de idioma necesario, y haciendo clic en el botón de **Actualizado** correspondiente.

   Se muestra una lista de los idiomas disponibles en este fichero.



3. Marque la casilla situada junto al idioma que desee instalar.

Se puede instalar un máximo de 4 idiomas.

4. Haga clic en el botón **Actualización seleccionada**.

   Aparece la página **Confirmar actualización idioma**, donde se muestran los idiomas que se están instalando.

5. Haga clic en el botón **Confirmar**.

Se muestra un mensaje indicando si la actualización del idioma ha sido satisfactoria o si ha fallado.

Borrado de idiomas

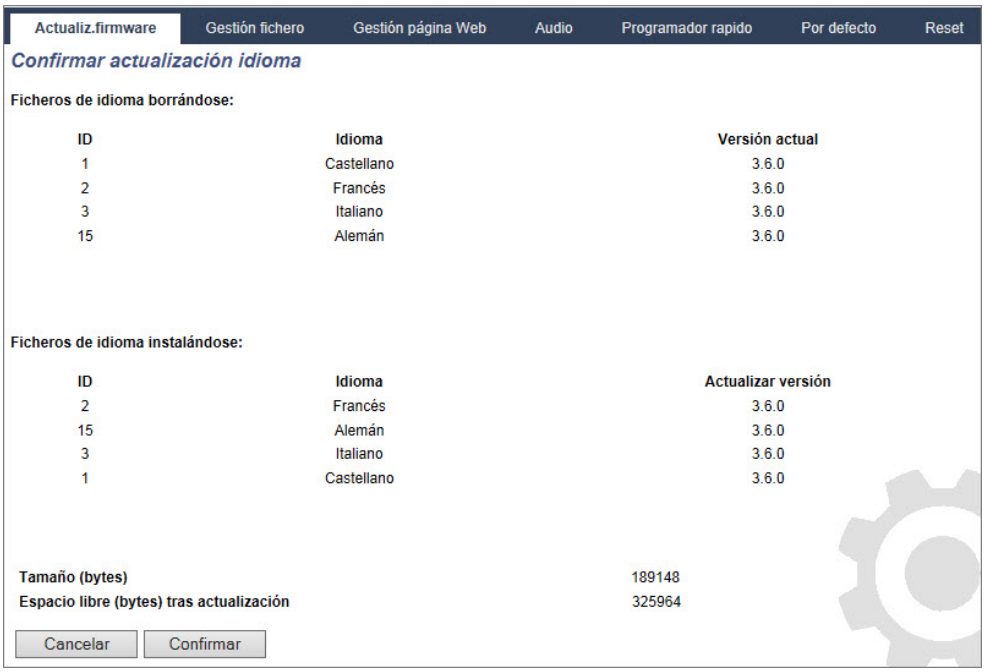
Para borrar idiomas del fichero de idioma:

1. Seleccione el fichero de idioma que desee actualizar haciendo clic en el botón **Browse** (examinar) para elegir la opción **Actualización de fichero de idioma**, seleccionando a continuación el fichero de idioma necesario, y haciendo clic en el botón de **Actualizado** correspondiente.

   Se muestra una lista de los idiomas disponibles en este fichero.

2. Desmarque las casillas para cada uno de los idiomas que desee borrar.
3. Haga clic en el botón **Actualización seleccionada**.

   Se muestra la página **Confirmar actualización idioma**. Cuando se borra un idioma, la central borra todos los idiomas y reinstala solo los idiomas requeridos.



4. Haga clic en el botón **Confirmar** para confirmar los idiomas que se borrarán.

Consulte *Idioma* en la página 274 para obtener más información sobre cómo seleccionar en el navegador los idiomas de la central para 'Sistema' y 'Reposo'.

Consulte *Opciones* en la página 126 para obtener más información sobre cómo seleccionar en el teclado los idiomas de la central para 'Sistema' y 'Reposo'.

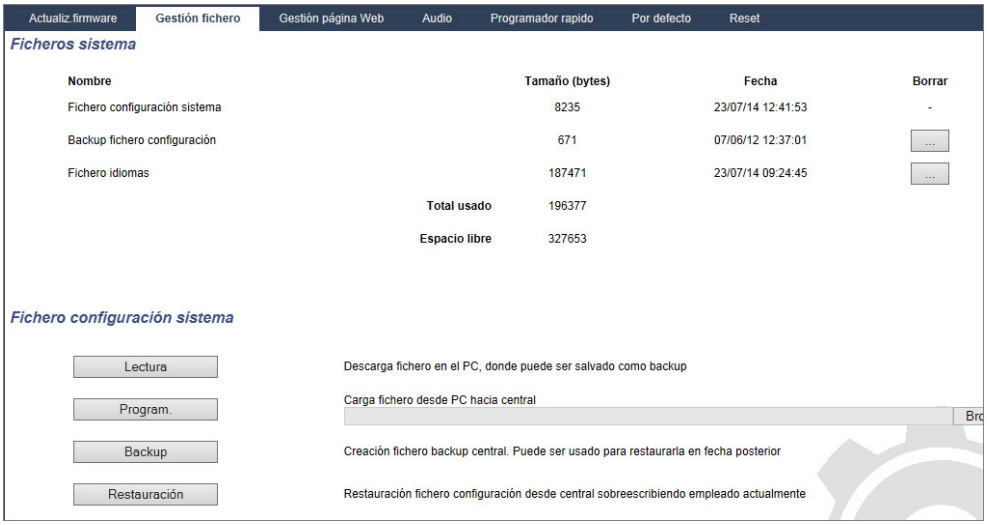
Consulte también

Idioma en la página 274

17.11.2 Operaciones del Gestor de archivos

- Seleccione **Archivo > Gestor de archivos**.

  Se abrirá una página que muestra los detalles de la configuración del sistema, el idioma y los archivos de rastreo.



Fichero de configuración del sistema

Para gestionar el fichero de configuración del sistema están disponibles las siguientes opciones:

Lectura	Descarga un archivo de configuración del controlador. **Nota:** Si aparece un mensaje de error luego de hacer clic en el botón Descargar, debe proceder como se indica a continuación: 1. Seleccione **Opciones de Internet** en el menú **Herramientas**. 2. Seleccione la pestaña **Avanzado**. 3. Seleccione la casilla **No salvar páginas cifradas en el disco**. 4. Haga clic en **Aplicar**. 5. Haga clic en **OK**. 6. Vuelva a hacer clic en **Descargar**. Cuando descarga un archivo de configuración, los ajustes de configuración se guardan en un archivo **.cfg**. Luego, puede cargar este archivo para otros controladores y evitar procedimientos de programación extensos.
Cargar	Carga un archivo de configuración al controlador.
Respaldo	Guarda una copia de respaldo de la configuración actual en una memoria flash.
Restaurar	Restaura una copia de respaldo de la configuración actual desde una memoria flash.

Datos de usuarios

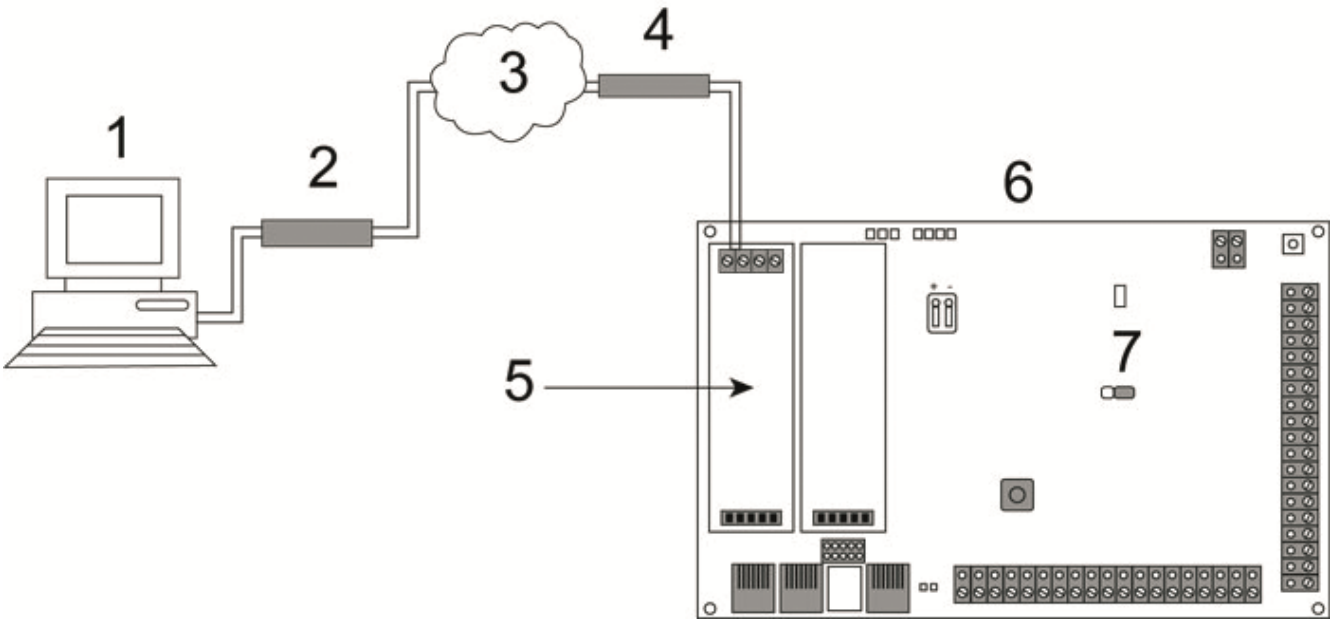
Para gestionar datos de usuarios, están disponibles las siguientes opciones:

Lectura	Haga clic en el botón **Descargar** para obtener los datos de usuarios desde la central. Aparecerá un cuadro de diálogo que le preguntará si desea salvar el archivo **users.csv**.
Cargar	Haga clic en el botón **Buscar** para **Cargar** datos de usuarios a la central. Debe ser un archivo con formato .csv.

18 Acceso al servidor web de forma remota

Este capítulo abarca:

18.1 Conexión RTB



Conexión RTB

1	PC remoto con navegador
2	Módem RTB
3	Red RTB
4	Línea telefónica
5	Módem RTB
6	Controlador SPC
7	JP9 SPC4xxx

Puede acceder al servidor web del controlador mediante una conexión remota a través de una línea telefónica RTB. Se debe conectar un módulo RTB y una línea RTB al controlador como se muestra anteriormente para ofrecer acceso remoto al controlador.

Del lado remoto de la conexión, el usuario debe contar con un módem RTB instalado en el PC con acceso a una línea RTB.

Para conectar de forma remota el controlador:

1. Instale un módem RTB en el controlador (consulte las instrucciones de instalación correspondientes).

2. Conecte la línea telefónica a los terminales de tornillo A/B del conector en la parte superior del módem.
3. Acceda a la programación en modo técnico desde el teclado y configure el módem (principal o de respaldo) para responder a una llamada entrante.
4. En el teclado, desplácese hasta **Modo técnico completo > Comandos > Módems**.
5. Seleccione los siguientes ajustes:

   - **Habilitar módem:** Configurado en habilitado

   - **Tipo:** Muestra el tipo de módem (RTB)

   - **Código del país:** Seleccione el código de país pertinente (Irlanda, Reino Unido, Europa)

   - **Modo de respuesta:** Seleccione la cantidad de tonos; esto le indica al módem que espere una cantidad determinada de tonos antes de responder una llamada entrante

   - **Tonos del módem:** Seleccione la cantidad de tonos que se debe esperar antes de responder la llamada (máx. 8 tonos)
6. Cree una conexión de acceso telefónico en el PC remoto con el número de teléfono de la línea telefónica conectada al módulo RTB del controlador. A continuación se muestran las instrucciones para hacer esto en el sistema operativo Windows XP.

En Windows XP:

1. Abra el Asistente para nueva conexión navegando hasta **Panel de control > Conexiones de red > Crear nueva conexión** (en la página **Tareas de red**).
2. En la página **Tipo de conexión de red**, seleccione **Conectarse a Internet**.
3. En la página **Preparando** , seleccione **Configurar mi conexión manualmente**.
4. En la página **Conexión a Internet**, seleccione **Conectar utilizando módem de acceso telefónico**.
5. En la página **Nombre de la conexión** introduzca el nombre de la conexión, por ejemplo: conexión remota SPC.
6. En la página **Número de teléfono para discar**, introduzca el número de teléfono de la línea RTB conectada al módem RTB.
7. En la página **Disponibilidad de la conexión**, elija si esta conexión estará disponible para todos los usuarios.
8. En la página **Información de cuenta de Internet**, introduzca los siguientes datos:

   - Nombre de usuario SPC

   - Clave: password (por defecto)

   - Confirmar clave: password

   Se mostrará la página **Completando el Asistente para nueva conexión**.
9. Haga clic en el botón **Finalizar** para salvar la conexión de acceso telefónico en el PC.

Se debe cambiar el código por defecto y se debe tomar nota según corresponda, ya que Vanderbilt no puede recuperar este código nuevo. En caso de perder el código, solo se podrán restablecer los valores por defecto de fábrica, de manera que se perderá la programación. La programación se puede restaurar si hay una copia de respaldo disponible.

Para activar esta conexión de acceso telefónico:

- Haga clic en el icono ubicado en la página **Panel de control > Conexiones de red**.

  El PC realizará una llamada de datos a la línea RTB conectada al módulo RTB del SPC.

El módulo RTB del SPC responde a la llamada de datos entrante después del número de tonos designado y establece un vínculo IP con el ordenador remoto.

El sistema SPC asigna automáticamente una dirección IP al PC remoto.

Para algunos sistemas operativos Windows, aparecerá un cuadro de diálogo sobre la certificación de Windows. Vanderbilt considera que es aceptable para continuar. Si tiene más dudas, póngase en contacto con el administrador de la red o con un técnico de Vanderbilt.

Para obtener esta dirección IP:

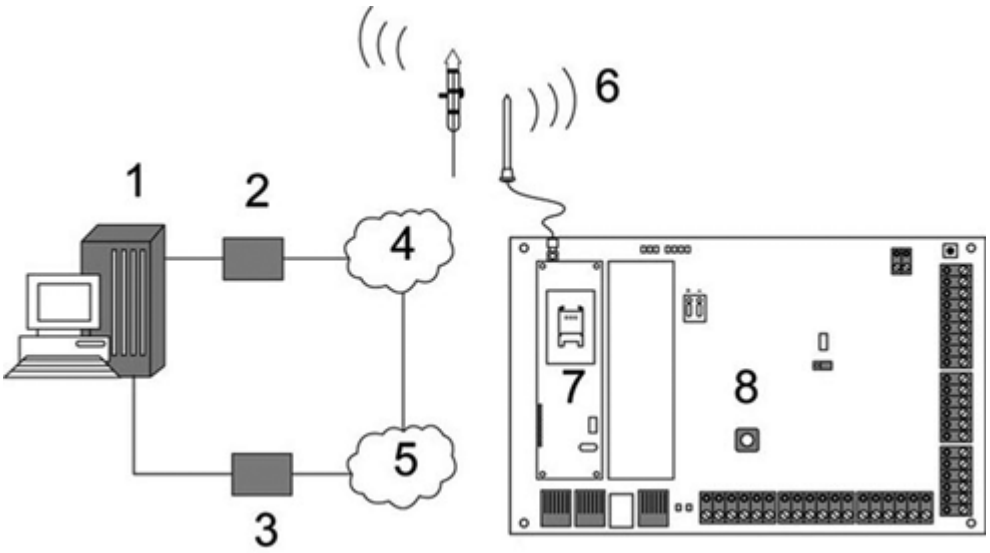
1. Haga clic con el botón derecho sobre el icono de acceso telefónico.
2. Haga clic en la pestaña **Detalles**.

   Se mostrará la dirección IP como la dirección IP del servidor.
3. Introduzca esta dirección IP en la barra de direcciones del navegador y haga clic.
4. Cuando se muestre el icono de conexión de acceso telefónico en la barra de tareas del PC, abra el navegador e introduzca la dirección IP del SPC.

   Se muestra la página Inicio de sesión del navegador.

Para configurar una conexión de acceso telefónico en otro sistema operativo, consulte el menú de ayuda de ese sistema operativo.

18.2 Conexión GSM



Conexión GSM

1	PC remoto con navegador
2	Módem GSM
3	Módem RTB
4	Red GSM
5	Red RTB

6	Antena exterior
7	Módem GSM
8	Controlador SPC

Puede acceder al servidor web del controlador mediante una conexión remota a través de la red GSM. Debe instalarse un módulo GSM (con tarjeta SIM) en el controlador como se muestra anteriormente para ofrecer acceso remoto al SPC. Se debe activar la opción de datos de la tarjeta SIM y se debe utilizar el número de datos.

En el lado remoto de la conexión, el usuario debe contar con un módem GSM o RTB instalado en un PC con navegador. Si el módem RTB está instalado, entonces debe estar conectado a una línea RTB funcional.

Para conectar de forma remota el controlador:

1. Instale un módem GSM en el controlar (consulte las instrucciones de instalación correspondientes).
2. Acceda a la programación en modo técnico completo desde el teclado y configure el módem (principal o de respaldo) para responder a una llamada entrante.
3. En el teclado, desplácese hasta el siguiente menú: TÉCNICO COMPLETO > COMUNICACIÓN > MÓDEMS, y seleccione los ajustes a continuación:

Habilitar módem	Configurar en TX habilitado.
Tipo	Se muestra el tipo de módem (GSM).
Código del país	Seleccione el código de país que corresponda.
Modo de respuesta	Seleccione la cantidad de tonos; esto le indica al módem que espere una cantidad determinada de tonos antes de responder una llamada entrante.
Tonos del módem	Seleccione la cantidad de tonos que se debe esperar antes de responder la llamada (8 tonos máx.).

En Windows XP:

1. Abra el **Asistente para nueva conexión** navegando hasta **Panel de control > Conexiones de red > Crear nueva conexión** (en la ventana **Tareas de red**).
2. En la ventana **Tipo de conexión de red**, seleccione **Conectarse a Internet**.
3. En la ventana **Preparando** , seleccione **Configurar mi conexión manualmente**.
4. En la ventana **Conexión a Internet**, seleccione **Conectar utilizando módem de acceso telefónico**.
5. En la ventana **Nombre de la conexión** introduzca el nombre de la conexión, por ejemplo: conexión remota SPC.
6. En la ventana **Número de teléfono para discar**, introduzca el número de teléfono de la línea GSM conectada al módem GSM.
7. En la ventana **Disponibilidad de la conexión**, elija si esta conexión estará disponible para todos los usuarios.
8. En la ventana **Información de cuenta de Internet**, introduzca los siguientes datos:

   - Nombre de usuario SPC

   - Clave: password

   - Confirmar clave: password

Se mostrará la página **Completando el Asistente para nueva conexión**.

9. Haga clic en el botón **Finalizar** para salvar la conexión de acceso telefónico en el PC.

Para activar esta conexión de acceso telefónico:

- Haga clic en el icono ubicado en la página **Panel de control > Conexiones de red**.

  El PC realizará una llamada de datos a la línea GSM conectada al módulo GSM del SPC.

  El módulo GSM del SPC responde a la llamada de datos entrante después del número de tonos designado y establece un vínculo IP con el ordenador remoto.

  El sistema SPC asigna automáticamente una dirección IP al PC remoto.

Para algunos sistemas operativos Windows, aparecerá un cuadro de diálogo sobre la certificación de Windows. Vanderbilt considera que es aceptable para continuar. Si tiene más dudas, póngase en contacto con el administrador de la red o con un técnico de Vanderbilt.

Para obtener esta dirección IP:

1. Haga clic con el botón derecho sobre el icono de acceso telefónico.
2. Haga clic en la pestaña **Detalles**.

   Se mostrará la dirección IP como la dirección IP del servidor.
3. Introduzca esta dirección IP en la barra de direcciones del navegador y haga clic.
4. Cuando se muestre el icono de conexión de acceso telefónico en la barra de tareas del PC, abra el navegador e introduzca la dirección IP del SPC.

   Se muestra la página Inicio de sesión del navegador.

Para configurar una conexión de acceso telefónico en otro sistema operativo, consulte el menú de ayuda de ese sistema operativo.

---

19 Funcionalidad de alarma de intrusión

El sistema SPC puede admitir 3 modos distintos de funcionamiento de alarma de intrusión —Financiero, Comercial o Doméstico—, y todos admiten varias particiones.

Cada partición puede admitir 4 modos de alarma diferentes. El modo Comercial y Financiero presentan más tipos de alarmas programables que el modo Doméstico. Los ajustes de tipo y nombre de zona por defecto para cada modo se listan en *Ajustes por defecto de modo doméstico, comercial y financiero* en la página 380.

19.1 Funcionamiento en modo financiero

El modo financiero es adecuado para instituciones bancarias y financieras que tienen áreas de seguridad especiales, como cámaras acorazadas y cajeros automáticos.

Cada partición definida en el sistema admite los modos de alarma que se detallan a continuación.

Modo de alarma	Descripción
Desarmado comun	La partición está desarmada, y solo las zonas de alarma clasificadas como 24 horas activarán la alarma.
ARMADO PARCIAL A	Este modo brinda protección del perímetro de un edificio, al tiempo que permite el movimiento libre por la salida y las particiones de acceso. Las zonas clasificadas como Excl.A.Parc.A continúan sin protección en este modo. Por defecto, no existe tiempo de salida (el sistema lo establece al instante al seleccionar este modo). Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial A.
ARMADO PARCIAL B	Este modo proporciona protección a todas las zonas, con excepción de aquellas clasificadas como Excl.A.Parc.B. Por defecto, no existe tiempo de salida (el sistema lo establece al instante al seleccionar este modo). Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial B.
ARMADO TOTAL	El área se arma por completo. La apertura de zonas de entrada/salida inicia el temporizador de entrada. Si la alarma no se ha desarmado antes de que termine el contador de entrada, la alarma se activa.

19.2 Funcionamiento en modo comercial

El modo comercial es adecuado para las instalaciones comerciales con múltiples particiones y una gran cantidad de zonas de alarma. Cada partición definida en el sistema admite los modos de alarma que se detallan a continuación.

Modo de alarma	Descripción
Desarmado comun	La partición está desarmada, y solo las zonas de alarma clasificadas como 24 horas activarán la alarma.

Modo de alarma	Descripción
ARMADO PARCIAL A	Este modo brinda protección del perímetro de un edificio, al tiempo que permite el movimiento libre por la salida y las particiones de acceso. Las zonas clasificadas como Excl.A.Parc.A continúan sin protección en este modo. Por defecto, no existe tiempo de salida (el sistema lo establece al instante al seleccionar este modo). Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial A.
ARMADO PARCIAL B	Este modo proporciona protección a todas las zonas, con excepción de aquellas clasificadas como Excl.A.Parc.B. Por defecto, no existe tiempo de salida (el sistema lo establece al instante al seleccionar este modo). Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial B.
ARMADO TOTAL	El área se arma por completo. La apertura de zonas de entrada/salida inicia el temporizador de entrada. Si la alarma no se ha desarmado antes de que termine el contador de entrada, la alarma se activa.

19.3 Funcionamiento en modo doméstico

El modo doméstico es adecuado para las instalaciones residenciales con una o más particiones y una cantidad pequeña a moderada de zonas de alarma. Cada partición definida en el sistema admite los modos de alarma que se detallan a continuación.

Modo de alarma	Descripción
Desarmado comun	La partición está desarmada, y solo las zonas de alarma clasificadas como 24 horas activarán la alarma.
ARMADO PARCIAL A	Este modo brinda protección del perímetro de un edificio, al tiempo que permite el movimiento libre por la salida y las particiones de acceso (por ejemplo, puerta delantera y pasillo). Las zonas clasificadas como Excl.A.Parc.A continúan sin protección en este modo. No existen tiempos de salida asociados a este modo y la protección se aplica al instante al seleccionar este modo.
ARMADO PARCIAL B	Este modo proporciona protección a todas las zonas, con excepción de aquellas clasificadas como Excl.A.Parc.B. Por defecto, no existe tiempo de salida (el sistema lo establece al instante al seleccionar este modo). Es posible aplicar un temporizador de salida a este modo habilitando la variable programada Armado parcial B.
ARMADO TOTAL	El área está armada por completo. La apertura de zonas de entrada/salida inicia el temporizador de entrada. Si la alarma no se desarma antes de que termine el temporizador de entrada, la alarma se activa.

19.4 Alarmas completas y locales

El tipo de alarmas generadas por el sistema SPC puede variar en función del tipo de zona que disparó la activación de la alarma. La gran mayoría de las alarmas requiere una indicación visual (flash) y audible (sirena) de una intrusión en las instalaciones o el edificio.

Por defecto, las tres primeras salidas físicas del controlador SPC están asignadas a la sirena exterior, la sirena interior y el flash de sirena exterior. Cuando están activadas, estas 3 salidas juntas advierten sobre

una condición de alarma a las personas ubicadas dentro del edificio o en las cercanías donde se produjo la intrusión.

Las alarmas completas y locales del SPC activan las siguientes salidas físicas:

- Salida del controlador 1: Sirena exterior
- Salida del controlador 2: Sirena interior
- Salida del controlador 3: Flash

Para obtener más información sobre cómo cablear las sirenas y el flash, consulte *Cableado del sistema* en la página 81.

La activación de una **Alarma completa** informa sobre la alarma a la CRA, si se ha configurado una en el sistema.

La activación de una **Alarma local** no intenta llamar a la CRA, aunque ya se haya configurado una.

La activación de una **Alarma silenciosa** no activa las salidas 1-3 (no hay indicaciones visuales ni acústicas de la alarma). Se informa de la incidencia de alarma a la CRA. Las alarmas silenciosas sólo se generan si se han abierto zonas de alarma con el atributo Silenciosa cuando el sistema está armado.

20 Ejemplos y escenarios del sistema

Este capítulo abarca:

20.1 Cuándo utilizar una partición común

Las particiones comunes representan una forma conveniente de configurar múltiples particiones dentro de una misma instalación. Un usuario asignado a una partición común tiene la posibilidad de ARMAR TODAS las particiones dentro de esa partición común (incluso aquellas particiones que no han sido asignadas a ese usuario). Sin embargo, los usuarios solo pueden DESARMAR las particiones que tienen asignadas.

Las particiones comunes deben utilizarse cuando se instala un único teclado en la ubicación de acceso principal y lo comparten todos los usuarios dentro del edificio (no se recomienda definir una partición común en un sistema con múltiples teclados en particiones distintas).

Ejemplo: 2 departamentos de una compañía (Cuentas y Ventas) comparten un punto de acceso común (puerta delantera)

En este caso, cree 3 particiones en el sistema (Partición común, Cuentas y Ventas). La partición común debe incluir el punto de acceso principal (puerta delantera). Asigne las zonas de Contabilidad a la partición 2 y las zonas de Ventas a la partición 3. Instale un teclado en la puerta delantera y asígnelo a las 3 particiones. Defina 2 usuarios (mínimo) en el sistema, uno para cada departamento, y asigne los usuarios a las respectivas particiones y la partición común.

Funcionamiento: Armado del sistema

El gerente de Cuentas se retira de la oficina a las 5:00 p. m. Cuando introduce su código en el teclado, la opción ARMADO TOTAL presenta los 3 submenús que se muestran a continuación:

- TODAS LAS PART.: arma todas las particiones asignadas a la partición común (Partición común, Contabilidad y Ventas) y cualquier partición adicional asignada al jefe de contabilidad; en este caso, no hay particiones adicionales. El temporizador de salida para la puerta delantera informa que el usuario se retiró del edificio.
- COMÚN: arma todas las particiones asignadas a la partición común (Partición común, Contabilidad y Ventas) e inicia el temporizador de salida de la puerta delantera.
- CONTABILIDAD: arma sólo la partición Contabilidad; la partición de Ventas sigue desarmada y aún se permite el acceso por la puerta delantera.

Cuando el último trabajador del departamento de Ventas se retira del edificio, cierra todas las puertas y las ventanas de la PARTICIÓN 3 e introduce su código en el teclado. Para la opción ARMADO TOTAL, se presentan los siguientes 3 submenús:

- TODAS LAS PART.: arma todas las particiones asignadas a la partición común (Partición común, Contabilidad y Ventas) y cualquier partición adicional asignada a los trabajadores de Ventas; en este caso, no hay particiones adicionales. El temporizador de salida para la puerta delantera informa que el usuario se retiró del edificio.
- COMÚN: arma todas las particiones asignadas a la partición común (Partición común, Contabilidad y Ventas) e inicia el temporizador de salida de la puerta delantera.
- VENTAS: arma TODAS las particiones asignadas a la partición común (Partición común, Contabilidad y Ventas); es así porque no hay otras subparticiones desarmadas en el sistema.

Funcionamiento: Desarmado del sistema

Cuando el gerente de Cuentas regresa a abrir el edificio e introduce su código en el teclado, la opción DESARMAR presenta los siguientes 3 submenús:

- TODAS LAS PART.: desarma todas las particiones asignadas a los empleados de Contabilidad (Partición común, Contabilidad) y cualquier partición adicional asignada a los empleados de Contabilidad. En este caso, no hay particiones adicionales.

  Nota: Un trabajador del departamento de Cuentas no puede DESARMAR la partición de Ventas.
- COMÚN: desarma SÓLO la partición común (Recepción). Esto permite desarmar la partición de la recepción mientras que quedan armados los departamentos de Cuentas y de Ventas.
- CONTABILIDAD: desarma la partición de Contabilidad y la partición común (Recepción). En este caso, la partición de Ventas sigue armada e igualmente se permite el acceso por la puerta delantera.

Uso de particiones comunes:

- Zona de llave armado

  Si la ruta de entrada/salida de la partición común está programada como zona de llave armado, cuando está activada, todas las particiones de la partición común están ARMADAS. Desactivar la zona de llave armado DESARMA todas las particiones de las particiones comunes.
- Teclados múltiples

  Si las particiones asignadas a la partición común tienen sus propios teclados para la entrada/salida, es importante que los horarios de salida asociados a esas particiones cuenten con el tiempo suficiente para que el usuario llegue a la salida de la partición común. Esto es en caso de que la partición que se esté armando sea la última partición sin armar en el sistema y, por lo tanto, eso disparará el armado de toda esa partición común.

Como norma, se recomienda que se utilicen particiones comunes en instalaciones que tiene solo un teclado ubicado en el punto de acceso común, es decir, el acceso de la puerta delantera a todo el edificio.

21 Sensores sísmicos

Los sensores de vibración, también llamados sensores sísmicos, se utilizan para detectar intentos de intrusión por medios mecánicos, tales como perforaciones a través de las paredes o cajas de seguridad.

Se admite el uso de sensores sísmicos solo si el tipo de instalación para la central es financiero.

Los sensores sísmicos se pueden probar de diversas formas. La forma más fácil de probar un sensor sísmico es golpeando una pared o una caja fuerte y ver si la zona se abre durante el test de intrusión. Este medio de comprobación está disponible con todos los tipos de sensores sísmicos.

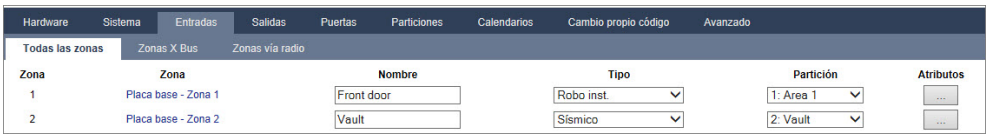
Si el sensor sísmico está instalado con un transmisor de test, estarán disponibles las siguientes opciones de comprobación:

- Test manual iniciado en el teclado (no admitido por el navegador).
- Test automático de forma periódica o cuando la central está configurada para ser usada con el teclado.

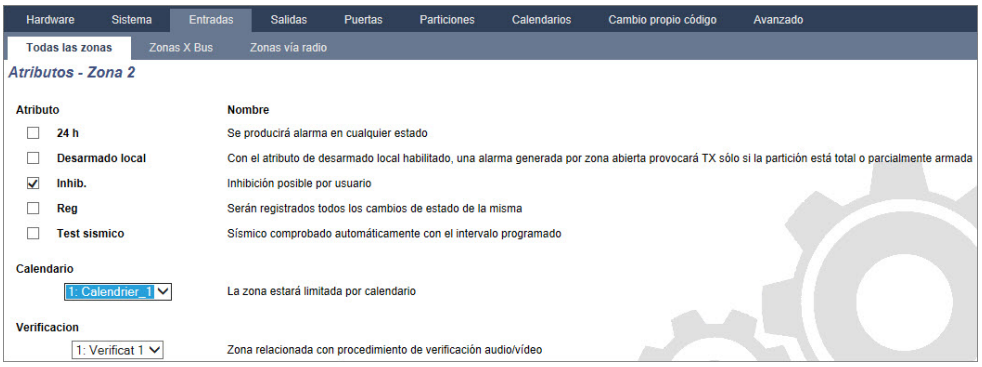
El transmisor de test es un vibrador de alta frecuencia colocado a una corta distancia del sensor ubicado en la misma pared. El transmisor de test está cableado a una salida en la central o el módulo de expansión.

Configuración de sensores sísmicos en la central

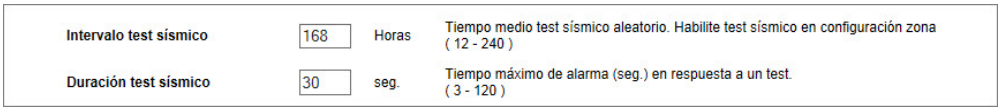
1. Configurar una zona sísmica. Los sensores sísmicos deben estar asignados a una zona. (Consulte *Editar una zona* en la página 274.)



2. Configure los atributos para la zona.



3. Habilite el test automático del sensor con el atributo **Test Sísmico**.
4. Seleccione un calendario para controlar la zona sísmica, si es necesario.
5. Asigne esta zona a una zona de verificación si se requiere una verificación de audio/vídeo.
6. Configure los temporizadores para especificar con qué frecuencia se comprobarán las zonas sísmicas (por defecto es 7 días) y la duración de los tests. (Se debe configurar el atributo de zona de test sísmico automático). (Consulte *Temporizaciones* en la página 266.)



7. Configure una salida para el test de una zona sísmica. (Consulte *Tipos de salidas y puertos de salida* en la página 157).
   La salida se puede asignar al sistema o a una partición si la central está configurada para utilizar

particiones, como suele ocurrir en los entornos financieros. La salida solo debería estar asignada al sistema si la central no utiliza particiones.

Mediante el teclado

1. Seleccione **MODO TÉCNICO COMPLETO > ZONAS > (seleccione la zona) > TIPO DE ZONA > SÍSMICA**.
2. Seleccione **MODO TÉCNICO COMPLETO > ZONAS > (seleccione la zona) > TIPO DE ZONA > TEST SÍSMICO AUTOMÁTICO**.

Consulte también

Temporizaciones en la página 266

Tipos de salidas y puertos de salida en la página 157

Editar una zona en la página 274

21.1 Test de sensor sísmico

Se debe configurar las zonas sísmicas para que estén disponibles los tests manuales y automáticos. El resultado del test, ya sea manual o automático, se almacena en el registro de incidencias del sistema.

Durante un test sísmico, se comprueba una o más zonas sísmicas. Cuando se comprueba una zona, el resto de las zonas de la misma partición quedan deshabilitadas temporalmente, ya que existe una sola salida de test sísmico por partición.

21.1.1 Proceso de test manual y automático

El test manual o automático funciona como se describe a continuación:

1. La central activa la salida de test sísmico para la partición que corresponda en la que se debe realizar el test sísmico de la zona.
2. Luego, la central espera a que se abran todas las zonas sísmicas del test y verifica que todos los sensores sísmicos de la partición entren en estado de alarma dentro del período de tiempo configurado para la **'Duración test sísmico'**. Se considera que las zonas que no se abrieron durante el período de tiempo máximo han fallado el test.
3. Cuando todas las zonas sísmicas de la partición están abiertas o se alcanzó el período máximo de duración del test sísmico (lo que suceda primero), la central deberá borrar la salida de test sísmico para esa partición.
4. Luego, la central espera un período de tiempo fijo para que se cierren todos los detectores sísmicos de la partición. Se considera que las zonas que no se cerraron han fallado el test.
5. Luego, la central espera otro período de tiempo antes de informar el resultado del test. El resultado del test, ya sea manual o automático, se almacena en el registro de incidencias del sistema.

La salida sísmica generalmente tiene un valor alto, y baja durante los tests (es decir, cuando está activa). Si esta señal no es adecuada para un sensor en particular, se puede configurar la salida física para que se invierta.

21.1.2 Test automático de sensores

Los sensores sísmicos se prueban de forma periódica o una vez que el sistema se configura con el teclado.

Tests automáticos periódicos

Los tests automáticos periódicos se realizan en todas las zonas sísmicas para las que los tests automáticos están habilitados.

Los tests automáticos son aleatorios dentro del período de comprobación configurado y se realizan de forma independiente para cada partición.

Todas las zonas sísmicas de la misma partición (para la que los tests automáticos están habilitados) se comprueban simultáneamente.

La opción de configuración **Intervalo de test sísmico** en el menú **Temporizadores del sistema** (consulte *Temporizaciones* en la página 266) determina el período de comprobación promedio para los tests automáticos de los sensores sísmicos. El valor predeterminado es de 168 horas (7 días) y los valores permitidos se encuentran dentro del rango de 12 a 240 horas.

El horario de comprobación es aleatorio dentro de un rango especificado +/- 15%. Por ejemplo, si el test está programado para realizarse cada 24 horas, es posible que se realice el test entre 20,4 y 27,6 horas del último test.

El test sísmico se realiza luego de un reinicio si están habilitados los tests automáticos. Si la central estaba en modo técnico completo antes del reinicio, el test se realiza únicamente una vez que la central no esté en modo técnico completo luego de un reinicio.

Si el test sísmico falla, se informará una incidencia de problema (código SIA «BT»). También hay una incidencia de restauración correspondiente (código SIA «BJ»).

Test automático al armar

La opción **Test sísmico durante el armado** puede configurarse en el menú **Opciones** (consulte *Opciones* en la página 254). Si está habilitada, se realizarán tests de todas las zonas sísmicas de todas las particiones que están configuradas antes de la secuencia de armado usual. Esto se aplica al funcionamiento de teclado únicamente.

Mientras se realiza el test, verá el mensaje 'TEST SÍSMICO AUTOMÁTICO' en el teclado. Si el test sísmico tiene éxito, el armado continúa como siempre.

Si todas las particiones, un grupo de particiones o una partición simple se seleccionan para el armado y el test sísmico falla, aparecerá el mensaje 'FALLO SÍSMICO'. Presionar **Regresar** muestra una lista de las zonas con fallos, y puede desplazarse hacia arriba o hacia abajo con las flechas.

Según la configuración **Inhibir** para las zonas sísmicas con fallos y su perfil de usuario, puede suceder lo siguiente:

- Si todas las zonas sísmicas que tuvieron fallos en el test tienen el atributo **Inhibir** configurado, y su perfil de usuario está configurado con el derecho de **Inhibir**:

1. Presione **Regresar** en cualquiera de las zonas con fallos.

   Se muestra el mensaje «¿ARM. FORZ. TODO?».

2. Presione **Regresar** nuevamente para inhibir todas las zonas sísmicas que tuvieron fallos en el test. (Alternativamente, regrese al menú anterior).

   El armado continúa como siempre.

- Si algunas de las zonas sísmicas que tuvieron fallos en el test tienen el atributo **Inhibir** configurado o su perfil de usuario no está configurado con el derecho de **Inhibir**, presione **Regresar**.

  Aparecerá el mensaje 'FALLO AL ARMAR' y no se armarán las particiones.

No existe test sísmico automático para particiones que tienen armado automático por cualquier motivo (por ejemplo, particiones activadas por calendario o disparador). Asimismo, no existe test sísmico automático cuando el sistema está configurado con SPC Com o el navegador. Sin embargo, existe un test sísmico automático cuando se utiliza el teclado virtual con SPC Com.

No se informa incidencia si falla el test sísmico durante el armado.

El temporizador de test automático periódico del sistema se reinicia luego de que se realiza un test posterior al armado.

21.1.3 Sensores de test manuales

Para comprobar manualmente los sensores, seleccione TEST > TEST SÍSMICO del menú TEST del teclado.

El técnico puede realizar un test sísmico manual en modo técnico completo, y también puede realizarlo un usuario de tipo Gerente o Estándar:

- Un técnico puede comprobar todos los sensores en las particiones configuradas en el sistema usando el teclado.
- Un usuario solo puede comprobar los sensores en las particiones que tiene asignadas y las que están asignadas al teclado que está usando.

Para realizar un test sísmico en modo técnico, seleccione TÉCNICO COMPLETO > TEST > TEST SÍSMICO.

Para realizar un test sísmico en modo usuario, seleccione MENÚS > TEST > TEST SÍSMICO.

Nota: Las instrucciones a continuación se aplican a los modos técnico y usuario, pero tenga en cuenta que el usuario solo tendrá algunas opciones disponibles.

Las siguientes opciones están disponibles en el menú TEST SÍSMICO:

- TEST TODAS PARTICIONES
  Comprueba las zonas sísmicas en todas las particiones disponibles en caso de que haya más de una partición que contenga zonas sísmicas.
- *'NOMBRE PARTICIÓN'*
  Los nombres de las particiones que contienen zonas sísmicas se listan de manera individual. Cuando se selecciona una partición específica, están disponibles las siguientes opciones:

  – TEST TODAS ZONAS
  Se comprueban todas las zonas sísmicas en esta partición si hay más de una zona sísmica.

  – *'NOMBRE ZONA'*
  Se listan los nombres de todas las zonas sísmicas, y estas se pueden seleccionar para su comprobación individual.

Mientras se está realizando el test, en el teclado se muestra el mensaje «TEST SÍSMICO».

Si el test falla, se muestra el mensaje «FALLO SÍSMICO». Si se pulsa la tecla «i» o «VER», se muestra una lista de las zonas con fallo por la que es posible desplazarse.

Si el test es satisfactorio, se muestra «SÍSMICO OK».

Se registran las entradas en el registro de incidencias con la siguiente información:

- Usuario que inició la prueba
- Resultado (OK o FALLO)
- Nombre y número de zona y partición

No se informaron incidencias para los test manuales.

22 Funcionamiento del cierre de bloqueo

La central de intrusión SPC admite el funcionamiento del cierre de bloqueo y del armado autorizado de un cierre de bloqueo.

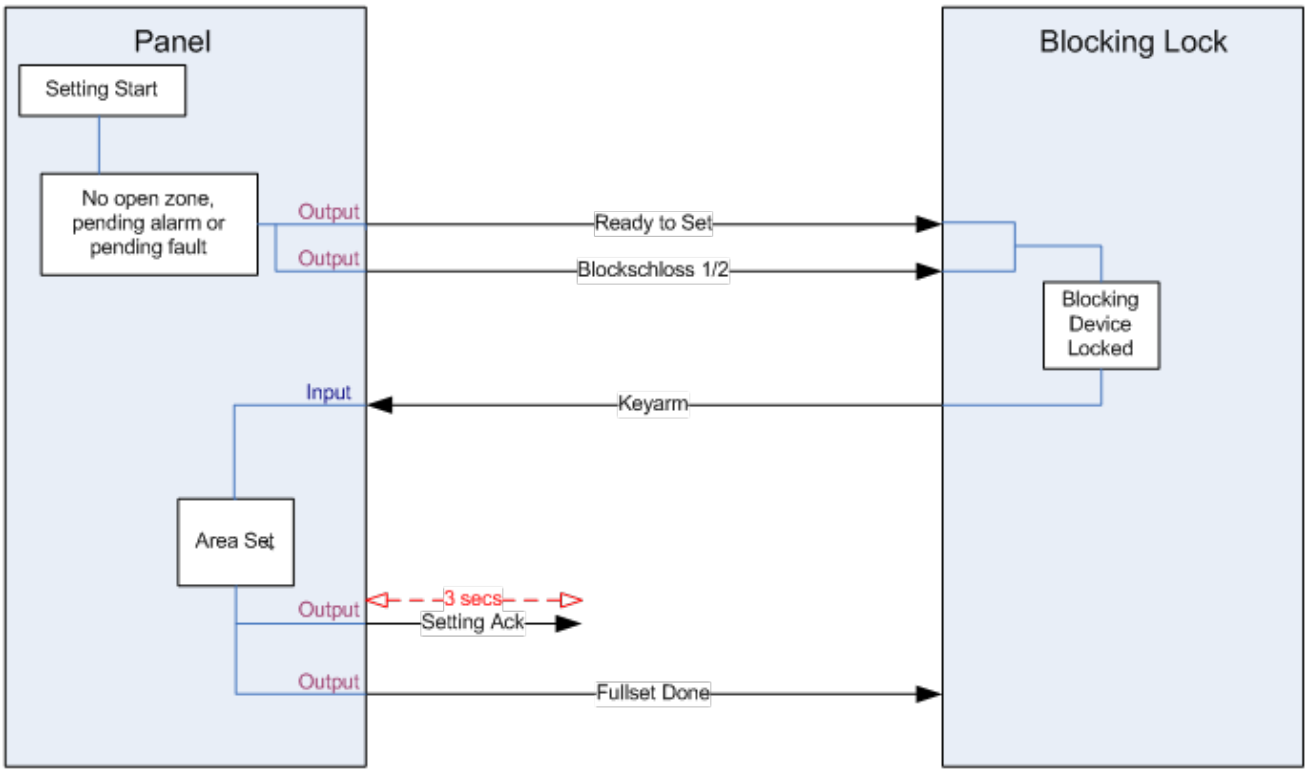
22.1 Cierre de bloqueo

El cierre de bloqueo es un cierre mecánico que se monta en una puerta además del cierre normal, y sirve para armar y desarmar el sistema de intrusión. El SPC admite tanto dispositivos de cierre de bloqueo normales (Blockschloss 1) como el dispositivo Bosch Blockschloss, Sigmalock Plus, E4.03 (Blockschloss 2).

Dependiendo del tipo de cierre de bloqueo, se necesita una señal para habilitar el cierre y la apertura, es decir, solo puede cerrarse el cierre de bloqueo y armarse el sistema si la señal Listo para armar está disponible desde la central. Esto se controla mediante un interruptor magnético.

El funcionamiento de un cierre de bloqueo es el siguiente:

1. Si no hay ninguna zona abierta, alarma pendiente o fallo pendiente en la partición, la partición está lista para armar y la señal de Listo para armar se envía desde la central.
2. Si el dispositivo de cierre de bloqueo se cierra, se activa la salida Blockschloss 1/2.
3. Tras el correspondiente cambio en el tipo de entrada de llave A/D, la partición correspondiente se arma.
4. La salida Config. ACK se activa durante 3 segundos para indicar que la partición se ha armado correctamente. La salida Blockschloss 1 se desactiva cuando el sistema está armado. Blockschloss 2 permanece activo cuando el sistema está armado.
5. Si el cierre de bloqueo se cierra, la entrada de llave A/D cambia a estado desarmado (cerrado).
6. Tras el cambio en el tipo de entrada de llave A/D, la partición se desarma. Blockschloss 1 se desactiva si la partición está lista para armar mientras Blockschloss 2 está activo si la partición está lista para armar.



Los requisitos de configuración para un cierre de bloqueo son los siguientes:

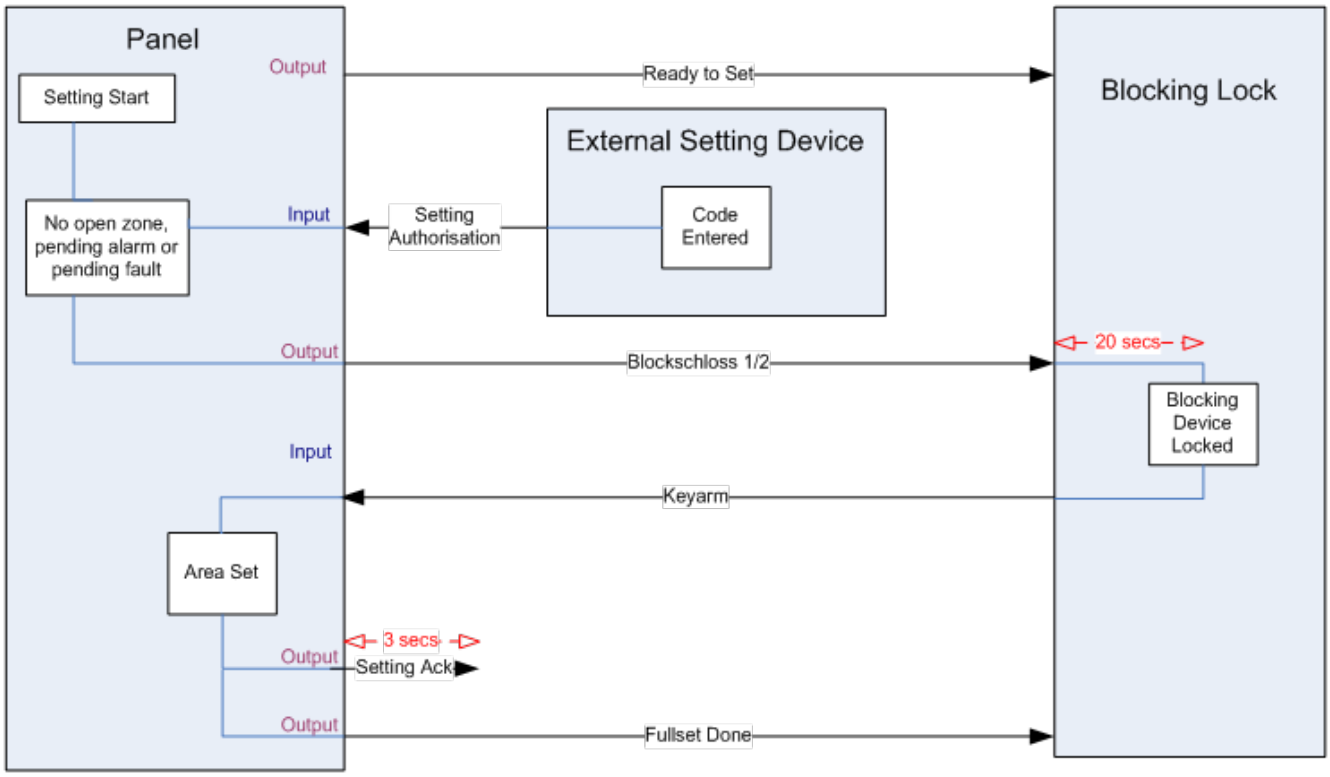
- Salidas:
  – Listo para armar
  – Armado recon.
  – Arm. total listo
  – Blockschloss 1/2
- Entradas
  – Llave armado

22.2 Armado autorizado del cierre de bloqueo

La funcionalidad de «Armado autorizado» amplía el procedimiento de armado y desarmado para un bloqueo de cierre con un segundo nivel de seguridad. Antes de que se pueda armar o desarmar el sistema, se debe introducir un código en un dispositivo de armado externo como una tarjeta o un lector de códigos con un controlador aparte. Este controlador se puede conectar a cualquier tipo de sistema de intrusión mediante entradas y salidas.

El método es el siguiente:

1. La central envía una señal al dispositivo de armado externo cuando es posible realizar el armado mediante un mensaje de Listo para armar.
2. Cuando se introduce el código, se activa la entrada de Autorización de armado y el Blockschloss 1/2.
3. El cierre de bloqueo abre una entrada de central (Llave A/D) que inicia el procedimiento de armado en la central.
4. El dispositivo de armado externo espera hasta 8 segundos a que se active, desde la central, la señal de salida de Arm. total hecho.
5. Si no se recibe esta señal, el armado falla y el dispositivo de armado externo vuelve a desarmar el sistema.



Los requisitos de configuración para el armado autorizado son los siguientes:

- Atributos de partición:

  – Autorización de armado

  Armado

  Armado y Desarmado (requerido para VdS)

  Desarmado
- Salidas:

  – Listo para armar

  – Armado recon.

  – Arm. total listo
- Entradas

  – Llave armado

22.3 Elemento de bloqueo

Para VdS es obligatorio impedir el acceso a una partición armada. Esto se realiza mediante un elemento de bloqueo montado en el marco de la puerta. El elemento de bloqueo consta de un pequeño perno de plástico que bloquea la puerta cuando está en estado ARMADO. La posición del perno se indica mediante las salidas **Elemento bloqueo - Bloqueo** o **Elemento bloqueo - Desbloqueo**. Esta señal se comprueba durante el proceso de armado. Si no se recibe la información de «bloqueado», el armado falla.

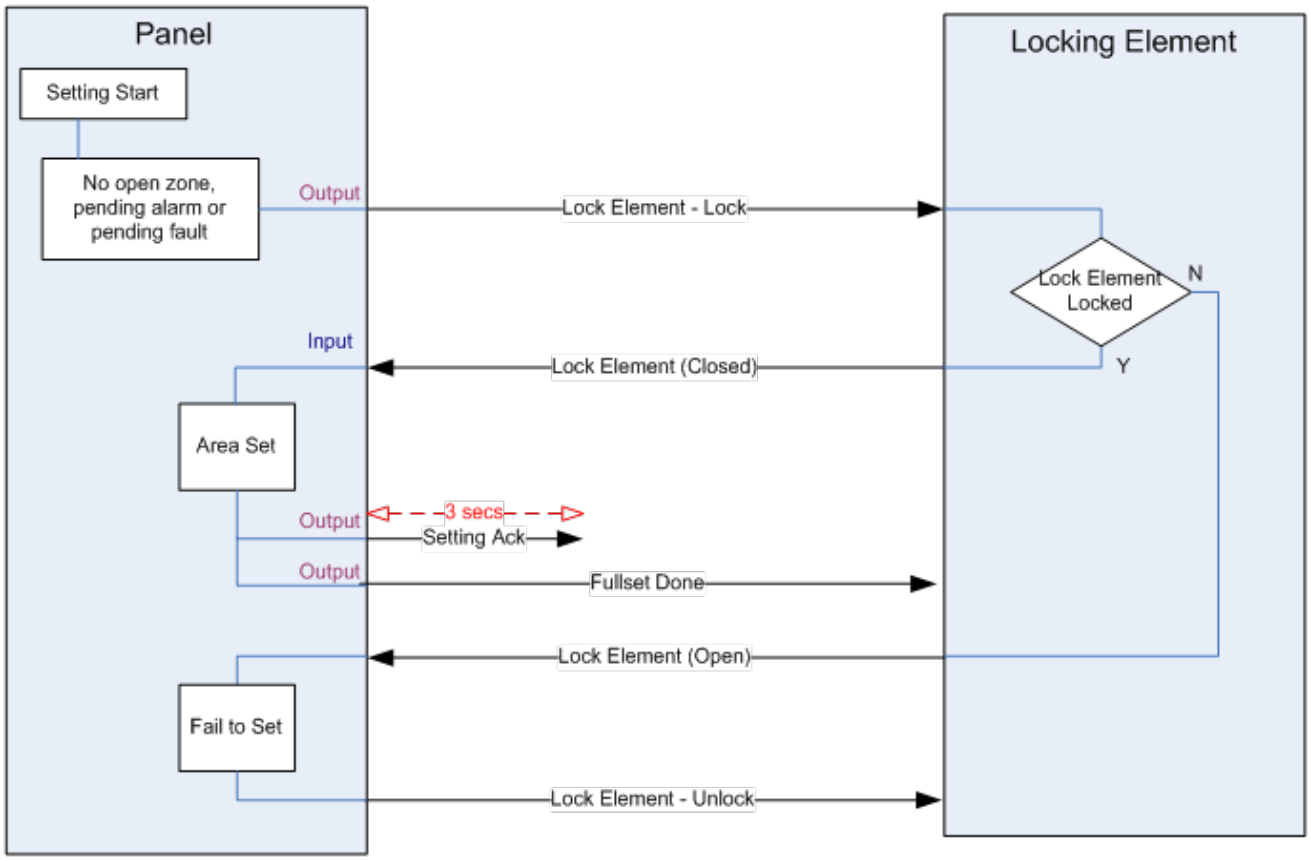
Si se coloca un elemento de bloqueo dentro de una partición, el temporizador de salida se restringirá a un mínimo de 4 segundos, de modo que el elemento de bloqueo se pueda activar. Cuando el temporizador de salida llega a los cuatro segundos, el elemento de bloqueo se activara durante tres segundos. Cuando caduca el temporizador de salida, la entrada **Elemento bloqueo** debe estar cerrada, y entonces se arma el sistema.

Si un elemento de bloqueo se abre durante un período de armado, se gestionará como una zona de alarma.

Si un elemento de bloqueo se cierra durante un proceso de desarmado, se considerará como saboteado, y se emitirá una alarma de tamper en la zona.

Si el elemento de bloqueo no consigue abrir después de que se envíe la señal de desbloqueo al dispositivo, se notificará un problema en esa zona para indicar que se ha producido un fallo mecánico.

Si la entrada **Elemento de bloqueo** (si está configurado) no está cerrada cuando caduca el temporizador de salida, el sistema no se armará y se emitirá una señal Fallo al armar. Se activará la salida **Elemento bloqueo – Desbloqueo**.



Los requisitos de configuración para el elemento de bloqueo son los siguientes:

- Salidas:
  – Elemento bloqueo - Bloqueo
  – Elemento bloqueo - Desbloqueo
- Entradas
  – Elemento bloqueo

23 Apéndice

El apéndice incluye:

23.1 Conexiones de cable de red

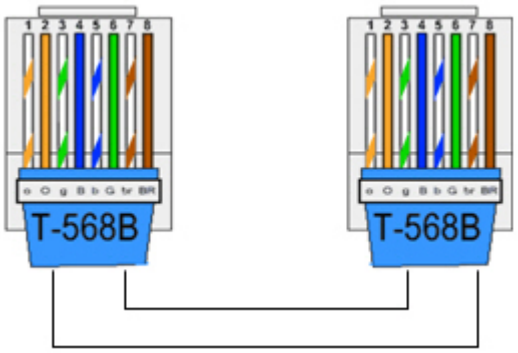
IP

Puede conectar un PC directamente a la interfaz Ethernet del controlador SPC o a través de una conexión LAN. Las tablas a continuación muestran las dos posibles configuraciones.

- Si el SPC está conectado a una red existente a través de un concentrador, conecte un cable directo desde el concentrador al SPC y otro desde el concentrador al PC.
- Si el controlador no está conectado a una red (es decir, si no se utiliza un concentrador o un interruptor), se deberá conectar un cable cruzado entre el controlador SPC y el PC.

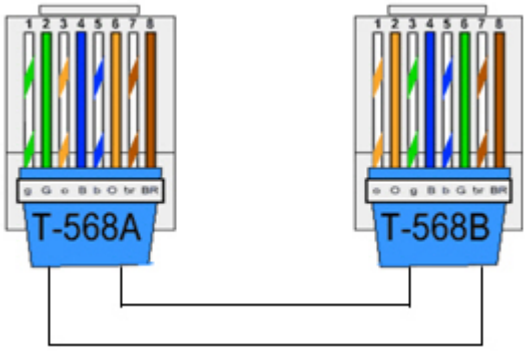
Utilice el cable directo para conectar el controlador SPC al PC a través de un concentrador.

CLAVIJA RJ45	CLAVIJA RJ45
1 (RX+)	1 (TX +)
2 (RX-)	2 (TX -)
3 (TX +)	3 (RX+)
6 (TX -)	6 (RX-)



Utilice el cable cruzado para conectar el controlador SPC directamente al PC.

CLAVIJA RJ45	CLAVIJA RJ45
1 (RX+)	3 (TX +)
2 (RX-)	6 (TX -)
3 (TX +)	1 (RX+)
6 (TX -)	2 (RX-)



23.2 Luces LED de estado del controlador

LED	Función
LED 1	Datos vía radio PARPADEANDO: El módulo vía radio está recibiendo datos vía radio APAGADO: No se están recibiendo datos vía radio
LED 2	Estado batería ENCENDIDO: El voltaje de la batería ha caído por debajo del nivel de descarga mínimo (10,9 V) APAGADO: Estado de la batería correcto
LED 3	Suministro de la red de CA ENCENDIDO: Fallo en la red de CA APAGADO: Red de CA correcta
LED 4	Estado X Bus ENCENDIDO: La configuración X-BUS es una configuración en lazo APAGADO: La configuración X-BUS es una configuración en punta PARPADEANDO: Detecta módulos de expansión de final de línea o roturas en el cableado.
LED 5	Fallo del sistema ENCENDIDO: Se detectó un fallo de hardware en la placa APAGADO: No se detectó fallo de hardware

LED	Función
LED 6	Escribiendo en la memoria flash ENCENDIDO: El sistema está escribiendo en la memoria flash APAGADO: El sistema no está escribiendo en la memoria flash
LED 7	Pulso PARPADEANDO: el sistema está funcionando con normalidad.

ENCENDIDO	APAGADO	PARPADEANTE

23.3 Suministrar alimentación a los módulos de expansión desde los terminales de alimentación auxiliar

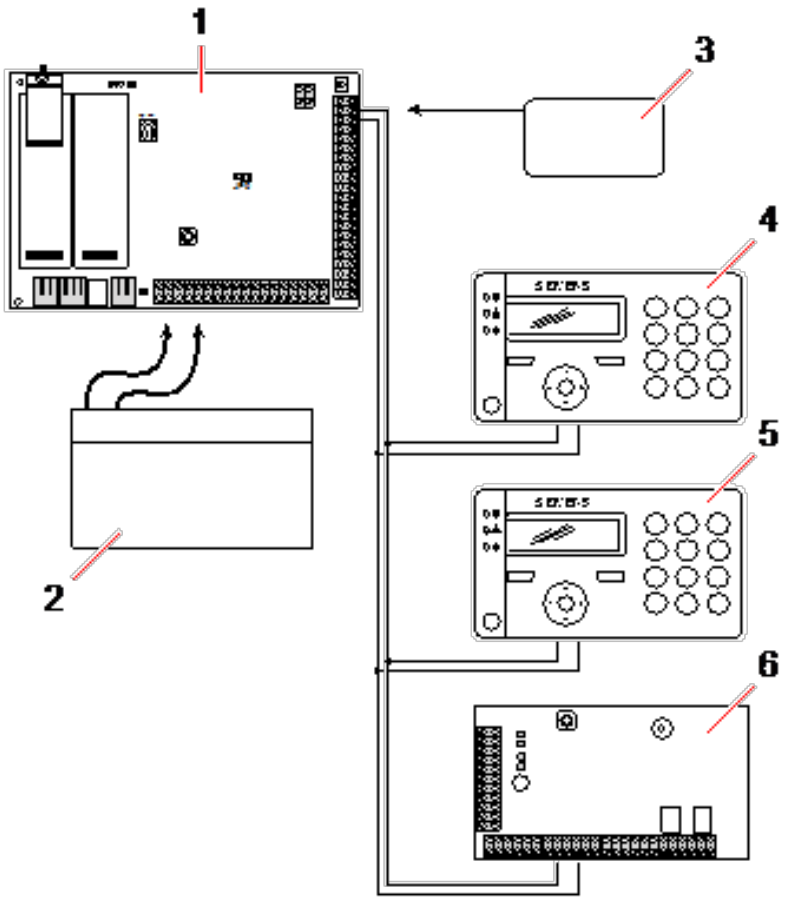
Para calcular el número de módulos de expansión y de teclados que pueden alimentarse con seguridad desde los terminales de alimentación auxiliares de 12 V CC, sume el consumo de corriente máximo total de todos los módulos de expansión y teclados que se deben alimentar, y determine si el total es inferior a la alimentación auxiliar especificada de 12 V CC.

Consulte los datos técnicos para obtener información sobre la corriente auxiliar específica y las instrucciones de instalación correspondientes o la hoja de datos sobre el consumo de corriente de los módulos, teclados y módulos de expansión.

Corriente del módulo de expansión 1 (mA) + Corriente del módulo de expansión 2 (mA) + ... < Alimentación auxiliar

Si las salidas electrónicas o de relé ya están alimentando dispositivos externos, la alimentación suministrada a estos dispositivos deberá restarse de la alimentación auxiliar de 12 V CC para determinar la cantidad de alimentación disponible desde los terminales de alimentación auxiliares (0 V, 12 V).

Si el amperaje máximo total de los módulos de expansión supera la alimentación auxiliar, debería utilizarse un módulo de expansión de fuente de alimentación para proporcionar una alimentación adicional.



Suministrar alimentación a los módulos de expansión desde los terminales de alimentación auxiliar

1	Controlador SPC
2	Batería
3	Terminales auxiliares de alimentación de 12 V
4	Teclado
5	Teclado
6	Módulo de expansión de E/S

23.4 Calcular los requisitos de alimentación de la batería

Es importante contar con el suministro eléctrico adecuado para todos los dispositivos en caso de que haya una falla en el suministro de la red de CA. Para garantizar contar con alimentación suficiente, siempre conecte la batería de respaldo y la fuente de alimentación correspondiente.

Las siguientes tablas indican, de forma aproximada, la corriente de carga máxima que puede extraerse de cada tipo de batería en los períodos de espera indicados.

Las cifras aproximadas, abajo indicadas, consideran que la placa del controlador SPC está funcionando con su carga máxima (todas las entradas cableadas tienen sus resistencias RFL colocadas) y que la alimentación que puede proporcionar la batería es de un 85% de su capacidad máxima.

$$\frac{0{,}85 \times \text{tamaño de batería (Ah)}}{\text{Tiempo (horas)}} - (\text{Icont} + \text{Ibell}) = \text{Imax}$$

Tamaño de la batería = capacidad, en Ah, dependiendo de la carcasa del SPC elegida

Tiempo = tiempo de reserva, en horas, dependiendo del grado de seguridad

Icont = corriente de reposo (en A) para el controlador SPC

Ibell = corriente de reposo (en A) para las sirenas exteriores e interiores adjuntas

Imax. = Corriente máxima que se puede extraer de la salida de alimentación auxiliar

Cantidad de corriente de la salida auxiliar utilizando una batería de 7 Ah (SPC422x/522x)

Comunic. / Tiempo en espera	NINGUNA (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	356	331	226	201
30 h	58	33	N/A	N/A

Cantidad de corriente de la salida auxiliar utilizando una batería de 17 Ah (SPC523x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	750	750	750	750
30 h	342	317	212	187

Cantidad de corriente de la salida auxiliar utilizando una batería de 7 Ah (SPC432x/532x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	326	301	196	171
30 h	28	N/A	N/A	N/A

Cantidad de corriente de la salida auxiliar utilizando una batería de 17 Ah (SPC533x/633x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	750	750	750	750
30 h	312	287	182	157

Cantidad de corriente de la salida auxiliar utilizando una batería de 24 Ah (SPC535x/635x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	1650	1625	1610	1585
24 h	650	625	610	585
30 h	450	425	410	385
60 h	50	25	10	N/A

Cantidad de corriente de la salida auxiliar utilizando dos baterías de 24 Ah (SPC535x/635x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	2205	2180	2165	2140
24 h	1650	1625	1610	1585
30 h	1250	1225	1210	1185
60 h	450	425	410	385

Cantidad de corriente de la salida auxiliar utilizando una batería de 27 Ah (SPC535x/635x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	1900	1875	1860	1835
24 h	775	750	735	710
30 h	550	525	510	485
60 h	100	75	60	35

Cantidad de corriente de la salida auxiliar utilizando dos baterías de 27 Ah (SPC535x/635x)

Comunic. / Tiempo en espera	Ninguna (mA)	RTB (mA)	GSM (mA)	RTB+GSM (mA)
12 h	2205	2180	2165	2140
24 h	1900	1875	1860	1835
30 h	1450	1425	1410	1385
60 h	550	525	510	485

Los valores listados como N/A indican que la batería seleccionada no tiene capacidad para alimentar la carga mínima únicamente desde el controlador SPC por el tiempo de espera indicado. Consulte *Calcular los requisitos de alimentación de la batería* en la página 378 para ver la carga máxima de los dispositivos y módulos.

Solo se debe utilizar baterías reguladas por válvula y selladas.

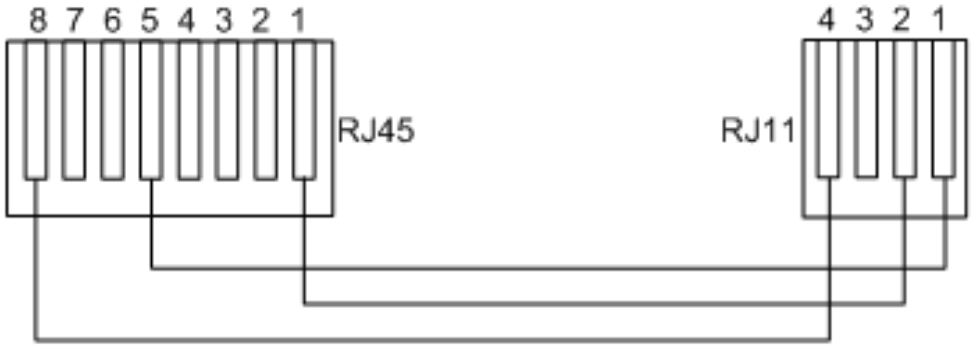
Para cumplir con las normas EN, la corriente suministrada debe estar respaldada por la batería por el tiempo en espera requerido.

23.5 Ajustes por defecto de modo doméstico, comercial y financiero

Esta tabla indica el nombre de zona y los tipos por defecto en el controlador para cada modo de funcionamiento. Todas las zonas de los módulos de expansión conectados se categorizan como no utilizadas hasta que el técnico de instalación las configura explícitamente.

Función	Modo doméstico	Modo comercial	Modo financiero
Nombres de zona			
Controlador - Zona 1	Puerta principal	Puerta principal	Puerta principal
Controlador - Zona 2	Salón	Ventana 1	Ventana 1
Controlador - Zona 3	Cocina	Ventana 2	Ventana 2
Controlador - Zona 4	Escalera delantera	PIR 1	PIR 1
Controlador - Zona 5	Escalera trasera	PIR 2	PIR 2
Controlador - Zona 6	Pasillo PIR	Salida incendio	Salida incendio
Controlador - Zona 7	PIR rellano	Alarma incendio	Alarma incendio
Controlador - Zona 8	Botón de emergencia	Botón de emergencia	Botón de emergencia
Tipos de zona			
Controlador - Zona 1	ENTRADA/SALIDA	ENTRADA/SALIDA	ENTRADA/SALIDA
Controlador - Zona 2	ALARMA	ALARMA	ALARMA
Controlador - Zona 3	ALARMA	ALARMA	ALARMA
Controlador - Zona 4	ALARMA	ALARMA	ALARMA
Controlador - Zona 5	ALARMA	ALARMA	ALARMA
Controlador - Zona 6	ALARMA	Salida incendio	ALARMA
Controlador - Zona 7	ALARMA	INCENDIO	ALARMA
Controlador - Zona 8	PÁNICO	PÁNICO	ALARMA

23.6 Cableado de la interfaz X10



Cableado X10 al controlador

Código	RJ45	RJ11
TX	8	4
Terminal de masa	5	1
RX	1	2

23.7 Códigos SIA

DESCRIPCIÓN	CÓDIGO
REPOSICIÓN RED CA	AR
PROBLEMA RED CA	AT
ALARMA ROBO	BA
ANULACIÓN ROBO	BB
CANCELACIÓN ROBO	BC
PROBLEMA SWINGER	BD
RESTAURACIÓN PROBLEMA SWINGER	BE
RESTAURACIÓN PROBLEMA ROBO	BJ
RESTAURACIÓN ROBO	BR
PROBLEMA ROBO	BT
ROBO DESANULADO	BU
ROBO VERIFICADO	BV
TEST ROBO	BX
CIERRE PENDIENTE	CD
CIERRE FORZADO	CF
CERRAR PARTICIÓN	CG
FALLO AL CERRAR	CI
TEMPRANO PARA ARMAR	CK
INFORME DE CIERRE	CE
CIERRE AUTOMÁTICO	CP
CIERRE REMOTO	CQ
CONMUTADOR LLAVE DE CIERRE	CS
TARDE PARA ABRIR	CT
ACCESO CERRADO	DC
ACCESO DENEGADO	DD
PUERTA FORZADA	DF
ACCES.AUTORIZADO	DG
RETORNO DE ACCESO DENEGADO	DI
PUERTA DEJADA ABIERTA	DN
ACCESO ABIERTO	DO

DESCRIPCIÓN	CÓDIGO
RESTAURACIÓN DE PUERTA	DR
SOLICITUD PARA SALIR	DX
ALARMA AL SALIR	EA
RESTAURACIÓN TAMPER MÓDULO EXPANSIÓN	EJ
MÓDULO DE EXPANSIÓN FALTANTE	EM
RESTAURACIÓN MÓDULO DE EXPANSIÓN FALTANTE	EN
RESTAURACIÓN MÓDULO EXPANSIÓN	ER
TAMPER DISPOSITIVO EXPANSIÓN	ES
PROBLEMA MÓDULO EXPANSIÓN	ET
ALARMA INCENDIO	FA
ANULACIÓN INCENDIO	FB
CANCELACIÓN INCENDIO	FC
RESTAURACIÓN PROBLEMA INCENDIO	FJ
RESTAURACIÓN INCENDIO	FR
PROBLEMA INCENDIO	FT
INCENDIO DESANULADO	FU
ALARMA ATRACO	HA
ANULACIÓN ATRACO	HB
RESTAURACIÓN PROBLEMA ATRACO	HJ
RESTAURACIÓN ATRACO	HR
PROBLEMA ATRACO	HT
ATRACO DESANULADO	HU
ATRACO CONFIRMADO	HV
CÓDIGO TAMPER USUARIO ¦WEB o ¦XBUS	JA
HORA CAMBIADA	JT
PROGRAMACIÓN LOCAL	Abajo izquierda
RESTAURACIÓN DE MÓDEM ¦ 1 o 2	LR
PROBLEMA DE MÓDEM ¦ 1 o 2	Arriba izquierda
PROGRAMACIÓN LOCAL FINALIZADA	LX
ALARMA MÉDICA	MA
ANULACIÓN ALARMA MÉDICA	MB

DESCRIPCIÓN	CÓDIGO
RESTAURACIÓN PROBLEMA ALARMA MÉDICA	MJ
RESTAURACIÓN ALARMA MÉDICA	MR
PROBLEMA ALARMA MÉDICA	MT
ALARMA MÉDICA DESANULADA	MU
PERÍMETRO ARMADO	NL
RESTAURACIÓN IP ENLACE RED	NR
RESTAURACIÓN GPRS ENLACE RED	NR
FALLO IP ENLACE RED	NT
FALLO GPRS ENLACE RED	NT
APERTURA AUTOMÁTICA	OA
PARTICIÓN ABIERTA	OG
APERTURA PREMATURA	OK
INFORME DE APERTURA	OP
CONMUTADOR LLAVE APERTURA	OS
TARDE PARA CERRAR	OT
APERTURA REMOTA	OQ
DESARMADO CON ALARMA	OR
ALARMA PÁNICO	PA
ANULACIÓN ALARMA PÁNICO	PB
RESTAURACIÓN PROBLEMA PÁNICO	PJ
RESTAURACIÓN PÁNICO	PR
PROBLEMA PÁNICO	PT
PÁNICO DESANULADO	PU
CIERRE RELÉ	RC
RESET REMOTO	RN
APERTURA RELÉ	RO
TEST AUTOMÁTICO	RP
ENCENDIDO	RR
ÉXITO PROGRAMACIÓN REMOTA	RS
PÉRDIDA DATOS	Arriba derecha
TEST MANUAL	RX

DESCRIPCIÓN	CÓDIGO
TAMPER	TA
ANULACIÓN TAMPER	TB
RESTAURACIÓN TAMPER	TR
TAMPER DESANULADO	TU
LLAMADA DE TEST	TX
ALARMA INDETERMINADA	UA
ANULACIÓN INDETERMINADO	UB
RESTAURACIÓN PROBLEMA INDETERMINADO	UJ
RESTAURACIÓN INDETERMINADO	UR
PROBLEMA INDETERMINADO	UT
INDETERMINADO DESANULADO	UU
FALLO SIRENA	YA
RESTAURACIÓN INTERFERENCIA RF	XH
RESTAURACIÓN TAMPER RF	XJ
LECTOR BLOQUEADO	RL
LECTOR DESBLOQUEADO	RG
TECLADO DESBLOQUEADO	KG
FALLO INTERFERENCIA RF	XQ
TAMPER RF	XS
FALLO COMUNICACIÓN	YC
FALLO CHEKCSUM	YF
RESTAURACIÓN SIRENA	YH
RESTAURACIÓN COMUNICACIÓN	YK
BATERÍA FALTANTE	YM
PROBLEMA FUENTE ALIMENTACIÓN	YP
RESTAURACIÓN FUENTE ALIMENTACIÓN	YQ
RESTAURACIÓN BATERÍA	YR
PROBLEMA COMUNICACIÓN	YS
PROBLEMA BATERÍA	YT
RESET WATCHDOG	YW
SERVICIO REQUERIDO	YX

DESCRIPCIÓN	CÓDIGO
SERVICIO COMPLETO	YZ
INCIDENCIAS SIA ESPECIALES	
CÓDIGO COACCIÓN	HA
RESTAURACIÓN COACCIÓN USUARIO	HR
ALARMA PÁNICO ENET	PA
RESTAURACIÓN PÁNICO ENET	PR
ALARMA PÁNICO USUARIO	PA
ALARMA INCENDIO ENET	FA
RESTAURACIÓN INCENDIO ENET	FR
ALARMA MÉDICA ENET	MA
RESTAURACIÓN ALARMA MÉDICA ENET	MR
PÁNICO HCD	PA
TILT HCD	MA
CLIP CINTURÓN HCD	HA
RESTAURACIÓN PÁNICO HCD	PR
RESTAURACIÓN TILT HCD	MR
RESTAURACIÓN CLIP CINTURÓN HCD	HR
PÁNICO RPA	PA
RESTAURACIÓN PÁNICO RPA	PR
ATRACO RPA	HA
RESTAURACIÓN ATRACO RPA	HR
CAMBIO CÓDIGO USUARIO	JV
CÓDIGO BORRADO	
CÓDIGOS SIA NO ESTÁNDAR PARA NOTIFICACIÓN DE ESTADO DE ZONA	
ZONA ABIERTA	ZO
ZONA CERRADA	ZC
CORTOCIRCUITO EN ZONA	ZX
DESCONEX. ZONA	ZD
ZONA ENMASCARADA	ZM
ZONA INTRUSIÓN	TP
INICIO TEST INTRUSIÓN	ZK

DESCRIPCIÓN	CÓDIGO
FIN TEST INTRUSIÓN	TC
ZONA BAT. BAJA	XT
REPOSICIÓN ZONA BAT. BAJA	XR
OTROS CÓDIGOS SIA NO ESTÁNDAR	
CÁMARA EN LÍNEA	CU
CAM.NO EN LÍNEA	CV
ALERTA CIERRE	SD
ALERTA REAPERTURA	SO
XBUS ALERTA CIERRE	NB
XBUS ALERTA REAPERTURA	NO
TARJETA DESCONOCIDA	AU
ACCESO USUARIO	JP
FIN ACCESO USUARIO	ZG
BAJO VOLTAJE	XD
RESTAURACIÓN DE BAJO VOLTAJE	XG
CARGA PROFUNDA	XK
BLOQUEADO	WW

23.8 Códigos CID

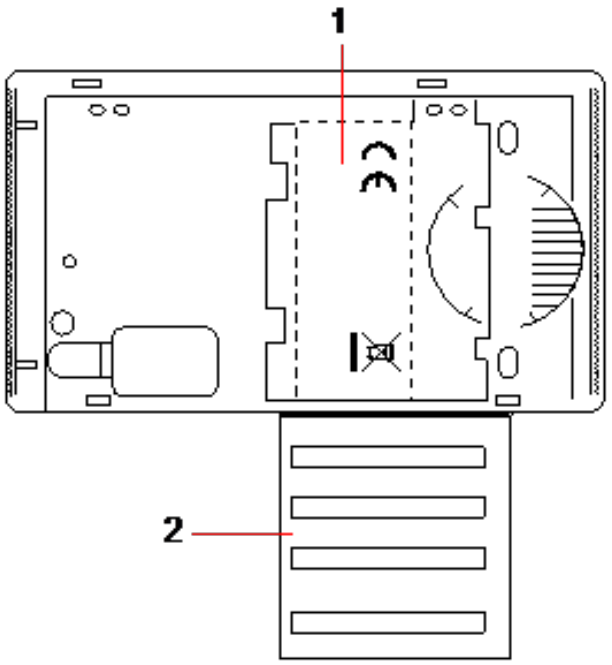
CÓDIGO	INCIDENCIA CID	DESCRIPCIÓN
100	MÉDICA	Alarma médica y de hombre caído y reposición
110	INCENDIO	
120	PÁNICO	
121	COACCIÓN	
129	ATRACO CONFIRMADO	Consulte *Requisitos de configuración para el cumplimento de la norma PD 6662:2010.* en la página 29.
130	ROBO	
134	ENTRADASALIDA	
137	TAMPER	Fallo y restauración de carcasa y tamper auxiliar.
139	VERIFICADA	Alarma confirmada.
144	SENSOR TAMPER	Fallo y restauración de tamper de la zona.
150	NO ROBO	

CÓDIGO	INCIDENCIA CID	DESCRIPCIÓN
300	PROBLEMA DEL SISTEMA	Fallo y restauración de la fuente de alimentación.
301	PÉRDIDA DE CA	Fallo y restauración de la red de CA de la fuente de alimentación.
302	BATERÍA BAJA	
305	RESET (restablecer)	Reinicio del sistema.
311	FALLO BATERÍA	Fallo y restauración de la batería de la fuente de alimentación.
312	SOBRECARGA DE LA FUENTE DE ALIMENTACIÓN	Fallo y restauración de fusible interno, externo y auxiliar de la fuente de alimentación.
320	SIRENA	Fallo y restauración de tamper de sirena.
330	PROBLEMA PERIFÉRICO DEL SISTEMA	Fallo y restauración de la fuente de alimentación.
333	FALLO EXP	Fallo y restauración de comunicación del nodo y cable X-BUS.
338	BAT. EXP	Fallo y restauración de batería del nodo X-BUS.
341	TAMPER EXP	Alarma y restauración de tamper de antena de RF y tamper X-BUS.
342	CA EXP	Fallo y restauración de la red de CA del nodo X-BUS.
344	INTERFERENCIA RF	Fallo y restauración de interferencia RF.
351	TELCO 1	Fallo y restauración de módem principal.
352	TELCO 2	Fallo y restauración de módem secundario.
376	PROBLEMA ATRACO	
380	PROBLEMA DE SENSOR	
401	ABIERTOCERRADO	Desarmado, post-alarma y armado total.
406	ABORTAR ALARMA	Cancelar alarma.
451	ABIERTOCERRADO PREMATURO	
452	ABIERTO/CERRADO TARDE	
453	FALLO AL ABRIR	Desarmado tarde.
454	FALLO AL CERRAR	Tarde para armar.
456	INCIDENCIA ARMADO PARCIAL	Armado parcial A y B.
461	TAMPERCÓDIGO	Tamper de código de usuario.
466	SERVICIO	Modo técnico habilitado y deshabilitado.
570	ANULACIÓN	Zona inhibida y desinhibida, zona aislada y no aislada.
601	TEST MANUAL	Test manual de módem.

CÓDIGO	INCIDENCIA CID	DESCRIPCIÓN
602	TEST AUTOMÁTICO	Test automático de módem.
607	TEST INTRUSIÓN	
613	ZONA INTRUSIÓN	
614	INCENDIO ZONA INTRUSIÓN	
615	PÁNICO ZONA INTRUSIÓN	
625	RESET DE HORA	Establecimiento de hora.

23.9 Información general de tipos de teclados

Tipo de teclado	Nº de modelo	Funcionalidad básica	Detección de proximidad	Audio
Teclado estándar	SPCK420	✓	-	-
Teclado con tarjeta	SPCK421	✓	✓	-
Teclado Confort	SPCK620	✓	-	-
Teclado confort con Audio/CR	SPCK623	✓	✓	✓



Etiqueta de teclado SPCK420/421

1	Etiqueta en el interior del teclado
2	Extraiga la etiqueta para obtener la información sobre el instalador. Rellene todos los datos relevantes una vez finalizada la instalación.

23.10 Combinaciones de código PIN de usuario

El sistema admite códigos PIN de 4, 5, 6, 7 y 8 dígitos para cada usuario (códigos PIN de usuario o de técnico). En la tabla a continuación, encontrará la cantidad máxima de combinaciones/variaciones lógicas para cada número de dígitos de código PIN.

Número de dígitos	Número de variaciones	Últimos códigos de usuario válidos
4	10.000	9999
5	100.000	99999
6	1.000.000	999999
7	10.000.000	9999999
8	100.000.000	99999999

La cantidad máxima de combinaciones/variaciones lógicas se calcula de la siguiente manera:

$10^{\text{N.° de dígitos}}$ = Número de variaciones (incluyendo código PIN de usuario o de técnico)

Nota: Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.

El código de técnico por defecto es 1111. Consulte *Código PIN de técnico* en la página 117 para obtener más detalles.

23.11 Códigos PIN de coacción

No se puede configurar un código PIN de usuario para el último PIN de usuario en una ubicación de códigos PIN para un número específico de dígitos de PIN. Para configurar un código de coacción con «PIN+1» o «PIN+2» es necesario que haya uno o dos códigos PIN adicionales disponibles después de un código PIN específico. Por ejemplo, para asignar códigos PIN de 4 dígitos, el número total de códigos PIN disponibles es de 10.000 (0 a 9999); en este caso, si el código de coacción se configura como 'PIN+1', el último código PIN de usuario al que se le puede asignar un código de coacción es el 9998. Si se utiliza la configuración «PIN+2», entonces el último código PIN de usuario al que se le puede asignar un código de coacción es el 9997.

Así pues, si la función de coacción está habilitada, no se permiten códigos de usuario consecutivos (por ejemplo: 2906, 2907), ya que introducir este código desde el teclado activaría una incidencia de coacción de usuario.

Una vez que se ha configurado el sistema para PIN +1 o PIN +2 en **Opciones del sistema** (consulte *Opciones* en la página 254) y se han habilitado usuarios específicos para coacción (consulte *Usuarios* en la página 209), no se debe cambiar a menos que se borren todos los usuarios y se reasignen nuevos códigos PIN de usuario.

23.12 Inhibiciones automáticas

El sistema admite inhibiciones automáticas en las siguientes instancias.

23.12.1 Zonas

Cuando se seleccionan GB y Comercial (consulte *Estándares* en la página 271), el sistema proporcionará la funcionalidad DD243. En este caso, el sistema inhibirá las zonas dadas estas condiciones:

- La zona de entrada no disparará una señal de alarma a la estación central y no puede ser parte de una alarma confirmada, por lo tanto, quedará inhibida efectivamente como lo requiere la

funcionalidad DD243.

- Si se dispara una zona y otra no dentro del período de tiempo de confirmación (por defecto, 30 minutos), pero la primera sigue activada, entonces, la primera zona quedará automáticamente inhibida y no se dispararán más alarmas desde esta zona durante el período establecido.

23.12.2 Códigos PIN de acceso

Para sistemas de Grado 2: Tras 10 intentos fallidos con un código PIN incorrecto, el teclado o navegador quedará deshabilitado durante 90 segundos. Tras otros 10 intentos con un código PIN incorrecto, el teclado o navegador quedará deshabilitado durante otros 90 segundos. Solo cuando se introduzca el código PIN correcto, el contador se restablecerá a cero y permitirá otros 10 intentos antes de deshabilitarse.

Para sistemas de Grado 3: Tras 10 intentos fallidos con un código PIN incorrecto, el teclado o navegador quedará deshabilitado durante 90 segundos. Tras cada intento subsiguiente con un código PIN incorrecto, el teclado o navegador quedará deshabilitado durante otros 90 segundos. Solo cuando se introduzca el código PIN correcto, el contador se restablecerá a cero y permitirá otros 10 intentos antes de deshabilitarse.

23.12.3 Acceso de técnico

Un técnico solo puede acceder al sistema si un usuario 'Gerente' lo autoriza (consulte Atributo 'Técnico' en *Derechos de usuario* en la página 213) y solo durante un período de tiempo específico (consulte 'Acceso técnico' en *Temporizaciones* en la página 266).

23.12.4 Cierre de sesión de usuario en teclado

Si no se pulsa ninguna tecla en el teclado durante un período de tiempo específico, (consulte 'Tiempo de espera de teclado' en *Temporizaciones* en la página 266), se cierra automáticamente la sesión del usuario.

23.13 Cableado de la red CA al controlador

Requisitos:

Se debe incorporar un dispositivo de desconexión aprobado de fácil acceso en el cableado de instalación del edificio. Este debe desconectar ambas fases al mismo tiempo. Los dispositivos aceptables son: conmutadores, disyuntores o dispositivos similares

- El dispositivo de desconexión debe estar al menos a 3 mm de distancia entre los contactos
- El tamaño mínimo de conductor utilizado para conectar la red de CA es de 1,5 mm cuadrados
- Los disyuntores deben tener una clasificación máxima de 16 A

El cable de red de CA está sujeto a un doblez de metal en forma de V en la placa base mediante una tira de amarre, de manera que el doblez de metal esté entre el cable y la tira de amarre. Asegúrese de que la tira de amarre esté sujeta al aislamiento complementario del cable de red de CA, es decir, la funda externa del cable de PVC. La tira de amarre debe estar ajustada de tal forma que, cuando se tire del cable, no se mueva de la tira de amarre.

Se debe conectar el conductor protector de conexión a tierra al bloque de terminales de manera que, si el cable de red de CA se deslizase del anclaje y ejerciese presión en los conductores, el conductor protector de conexión a tierra sea el último en soportar la presión.

El cable de red de CA debe estar aprobado y marcado HO5 VV-F o HO5 VVH2-F2.

La tira de amarre de plástico debe tener una clasificación de flamabilidad V-1.

23.14 Controlador de mantenimiento

Se debe realizar el mantenimiento del sistema de conformidad con el cronograma de mantenimiento vigente. Las únicas partes reemplazables del controlador son el fusible de red, la batería de tiempo en

espera y la batería de fecha y hora (montada en la placa).

Se recomienda que, durante el mantenimiento, se verifique lo siguiente:

- El registro de incidencias para verificar si hubo algún fallo en los tests de la batería de tiempo en espera desde el último mantenimiento; si se produjo un fallo en los tests de la batería de tiempo en espera, entonces, se debe controlar la batería de tiempo en espera.
- Se debe reemplazar la batería de tiempo en espera de conformidad con el cronograma de mantenimiento para garantizar que tenga la capacidad suficiente de mantener al equipo funcionando durante el período de tiempo definido en el diseño del sistema. Se debe inspeccionar físicamente la batería y determinar si tiene deformaciones de la carcasa o algún indicio de fuga. En caso de detectarse deformaciones o fugas, se debe reemplazar la batería de inmediato.

AVISO: La batería nueva debe tener la misma capacidad o una capacidad superior (hasta el máximo admitido por el sistema).

- Si el fusible principal se quema, entonces se debe controlar y buscar la causa en el sistema. Se debe reemplazar el fusible por otro de la misma capacidad. La etiqueta del sistema en la parte posterior de la carcasa indica la capacidad del fusible.
- La batería de litio de fecha y hora integrada en la placa se utiliza únicamente cuando el sistema no está conectado a la alimentación. En este estado, la batería tiene una vida útil de aproximadamente 5 años. Se debe inspeccionar la batería visualmente una vez al año y se debe desconectar la alimentación del sistema para garantizar que el sistema mantenga la fecha y la hora. Si el sistema no mantiene la fecha y la hora, se debe reemplazar la batería con una nueva de litio tipo CR1216.
- Se deben controlar todas las conexiones eléctricas para asegurarse de que el aislamiento esté en su lugar y que no haya riesgo de cortocircuito o de desconexión.
- También se recomienda que se controlen las notas de lanzamiento de actualización de firmware para determinar si existen actualizaciones adicionales que puedan mejorar la seguridad del sistema.
- Verifique que todos los acoples físicos estén intactos. Los acoples rotos deben ser reemplazados con las mismas partes.

23.15 Mantenimiento de la fuente de alimentación inteligente

Se debe realizar el mantenimiento del sistema de conformidad con el cronograma de mantenimiento vigente. Las únicas partes reemplazables de la fuente de alimentación inteligente son el fusible de red y la batería de tiempo en espera.

Se recomienda que, durante el mantenimiento, se verifique lo siguiente:

- El registro de incidencias del controlador para verificar si hubo algún fallo en los tests de la batería de tiempo en espera desde el último mantenimiento; si se produjo un fallo en los tests de la batería de tiempo en espera, entonces, se debe controlar la batería de tiempo en espera.
- Se debe reemplazar la batería de tiempo en espera de conformidad con el cronograma de mantenimiento para garantizar que tenga la capacidad suficiente de mantener al equipo funcionando durante el período de tiempo definido en el diseño del sistema. Se debe inspeccionar físicamente la batería y determinar si tiene deformaciones de la carcasa o algún indicio de fuga. En caso de detectarse deformaciones o fugas, se debe reemplazar la batería de inmediato.

AVISO: La batería nueva debe tener la misma capacidad o una capacidad superior (hasta el máximo admitido por el sistema).

- Verifique que las luces LED de la placa de control de la fuente de alimentación tengan el estado esperado. Consulte la documentación de la fuente de alimentación inteligente para obtener información sobre las luces LED.
- Si el fusible principal se quema, entonces se debe controlar y buscar la causa en el sistema. Se debe reemplazar el fusible por otro de la misma capacidad. La etiqueta del sistema en la parte posterior de la carcasa indica la capacidad del fusible.
- Se deben controlar todas las conexiones eléctricas para asegurarse de que el aislamiento esté en su lugar y que no haya riesgo de cortocircuito o de desconexión.
- También se recomienda que se controlen las notas de lanzamiento de actualización de firmware para determinar si existen actualizaciones adicionales que puedan mejorar la seguridad del sistema.
- Verifique que todos los acoples físicos estén intactos. Los acoples rotos deben ser reemplazados con las mismas partes.

23.16 Tipos de zona

Los tipos de zona del sistema SPC pueden programarse tanto desde el navegador como desde el teclado. La tabla siguiente incluye una breve descripción de cada tipo de zona disponible en el sistema SPC. Cada tipo de zona activa su propio tipo de salida (un indicador o marca interna) que luego puede registrarse o asignarse a una salida física para la activación de un dispositivo específico en caso de ser necesario.

Tipo de zona	Categoría de procesamiento	Descripción
ALARMA	Intrusión	Este tipo de zona es el tipo de zona por defecto y también el tipo de zona más utilizada para instalaciones estándar. A la activación de tamper, abierta o por desconexión en cualquier modo (excepto modo desarmado) provoca una alarma total inmediata. En el modo Desarmado, se registran las condiciones de tamper, se genera el mensaje de alerta TAMPER DE ZONA y se dispara la alarma local. En los modos ARMADO PARCIAL A, ARMADO PARCIAL B y ARMADO TOTAL, se registra toda la actividad.
ENTRADA/SALIDA	Intrusión	Esta zona debe estar asignada a todas las zonas en la ruta de entrada/salida (por ejemplo: una puerta delantera u otra área de acceso al edificio o instalaciones). Este tipo de zona cuenta con un retardo de tiempo de entrada y de salida. El temporizador de entrada controla este retardo. Cuando el sistema está completamente armado, este tipo de zona ofrece un retardo de salida lo que da tiempo para desalojar la partición. El temporizador de salida controla este retardo. En modo Armado parcial A, este tipo de zona es inactivo.
TERMINADOR DE SALIDA	Intrusión	Este tipo de zona se utiliza junto con un botón pulsador sobre una ruta de salida, y funciona como terminador de salida, es decir, el período de retardo de salida será indeterminado y no permitirá que se arme el sistema hasta que no se pulse el botón.

Tipo de zona	Categoría de procesamiento	Descripción
INCENDIO	Atraco	Las zonas de incendio son zonas que controlan los incendios durante 24 horas y la respuesta es independiente del modo operativo de la central. Cuando se abre una zona de incendio, se genera una alarma total y se activa el tipo de salida INCENDIO. Si el atributo 'Solo TX' está configurado, la activación solo se informará a la estación central y no se generará una alarma total.
Salida incendio	Atraco	Este es un tipo especial de zona de 24 horas que se utiliza con puertas de salida en caso de incendio que nunca deben abrirse. En modo Desarmado, si se activa esta zona se activará la salida Inc.X, provocando mensajes de alerta.
Línea	Fallo	Entrada de control de línea de telemetría. Se utiliza generalmente en conjunto con una salida de estado de línea telefónica desde un marcador digital externo o un sistema de comunicación de línea directa. Cuando se activa, dispara una alarma local en modo Desarmado y una alarma total en el resto de los modos.
ALARMA PÁNICO	Atraco	Este tipo de zona está activa las 24 horas y la alarma se activa a través del botón de pánico. Cuando se activa una zona de pánico, se informará la incidencia de pánico independientemente del modo de armado de la central. Si el atributo de registro está activado, se registrarán y se informarán todas las activaciones. Si el atributo SILENCIO está configurado, la alarma será silenciosa (la activación se informará a la CRA). De lo contrario, se generará una alarma total.
ALARMA ATRACO	Atraco	Este tipo de zona está activa las 24 horas y la alarma se activa a través de un botón. Cuando se activa una zona de atraco, se informará de una incidencia de atraco independientemente del modo de armado de la central. El atributo Silenciosa está ajustado por defecto; por lo tanto, la alarma será silenciosa. Si no está ajustado, se generará una alarma completa. Si el atributo de registro está activado, se registrará y se informará de todas las activaciones.
TAMPER	Tamper	Cuando se abre en modo Desarmado, se dispara una alarma local pero no se activa ninguna sirena exterior. Si el sistema está armado total, se genera una alarma total. Si el grado de seguridad del sistema es de Grado 3, se requerirá el código del técnico para restaurar la alarma.
TÉCNICA	Intrusión	La zona técnica controla una salida de zona técnica determinada. Cuando el estado de la zona técnica cambia, seguirá una salida de zona técnica. Es decir: • Si la zona técnica se abre, la zona técnica se activa. • Si la zona técnica se cierra, la zona técnica se desactiva. Si se asigna más de una zona técnica, la salida de la zona técnica permanecerá activada hasta que se cierren todas las zonas técnicas.

Tipo de zona	Categoría de procesamiento	Descripción
MÉDICA	Atraco	Este tipo de zona se utiliza junto con los interruptores de alarma médica cableados o de mando vía radio. La activación en cualquier modo: • Disparará una salida de comunicador digital de alarma médica (a menos que esté configurado el atributo local) • Disparará el zumbador de la central (a menos que esté configurado el atributo Silencio) • Mostrará el mensaje Alarma médica
LLAVE ARMADO	Intrusión	Este tipo de zona se utiliza normalmente junto con un mecanismo de bloqueo de teclas. Se puede configurar una llave armado para las siguientes **Opciones de configuración**: • **Armado total** • **Armado parcial A** • **Armado parcial B** Una zona de llave armado ARMARÁ el sistema/partición/áreas comunes de conformidad con las **Opciones de configuración seleccionadas** cuando esté ABIERTA y DESARMARÁ el sistema/partición/áreas comunes de conformidad con las **Opciones de configuración** cuando esté CERRADA. • Si la zona con el tipo de zona de llave armado está asignada en un sistema sin particiones, el funcionamiento de la llave armado ARMARÁ/DESARMARÁ el sistema. • Si la zona con el tipo de zona de llave armado está asignada a una partición, el funcionamiento de la llave armado ARMARÁ/DESARMARÁ el sistema. • Si la zona con el tipo de zona de llave armado está asignada a un área común, el funcionamiento de la llave armado ARMARÁ/DESARMARÁ todas las particiones del área común. • Si está configurado el atributo 'Solo abrir', el estado de armado del sistema/partición/áreas comunes cambiará cada vez que se abra el bloqueo de las teclas (es decir: Abrir una vez para ARMAR el sistema, Cerrar y abrir nuevamente para DESARMAR). • Si el atributo 'Habilitar armado total' está configurado, la activación de la zona solo generará el armado total del sistema. • Si el atributo 'Habilitar desarmado' está configurado, la activación de la zona solo generará el desarmado del sistema. La llave armado forzará el armado del sistema/partición e inhibirá las zonas abiertas o condiciones de fallos. **Nota: Su sistema no cumplirá las normas EN si usted activa este tipo de zona para armar el sistema y no introduce previamente un PIN válido.**

Tipo de zona	Categoría de procesamiento	Descripción
ANULACIÓN	Intrusión	Este tipo de zona solo está disponible en modo Comercial. Aunque el tipo de zona de alarma de anulación puede configurarse en modo Doméstico, no tiene efecto. Cuando se abre este tipo de zona, se inhiben todas las zonas que tienen el atributo de anulación configurado. Este funcionamiento se aplica tanto a los modos ARMADO como DESARMADO. En cuanto se cierra la zona de Anulación ligada, las zonas que tengan el atributo Anulación ligada activado dejarán de estar anuladas.
ANULACIÓN LIGADA	Intrusión	Este tipo de zona solo está disponible en modo Comercial. Una zona programada con el tipo de zona de anulación ligada inhibe la siguiente zona consecutiva en el sistema cuando se abre. Este funcionamiento se aplica tanto a los modos ARMADO como DESARMADO. Tan pronto como se cierra el tipo de zona de anulación ligada, se vuelve a desinhibir la zona siguiente.
FALLO DETECTOR	Fallo	Las zonas de fallo de detector son zonas de 24 horas aplicables a un dispositivo señalizador de atraco, por ejemplo un PIR. El tipo de zona de fallo genera una salida de fallo. Cuando se arma el sistema, se activa una salida de fallo. Tanto el LED del teclado como el zumbador se activan cuando se desarman.
SUPERV.LLAVE	Intrusión	Solo disponible en modo Comercial. Se utiliza para controlar el bloqueo de puerta. El sistema puede programarse para no armarse a meno que la puerta esté bloqueada.
SÍSMICA	Intrusión	Solo disponible si la central está en modo de funcionamiento Financiero. Los sensores de vibración, también llamados sensores sísmicos, se utilizan para detectar intentos de intrusión por medios mecánicos, tales como perforaciones a través de las paredes o cajas de seguridad.
TODO OK	Intrusión	Este tipo de zona permite que se implemente un procedimiento de entrada especial mediante un código de usuario y la entrada 'TODO OK'. Se genera una alarma silenciosa si no se pulsa el botón 'TODO OK' dentro de un período de tiempo configurable tras haber ingresado un código de usuario. (Consulte *Añadir/Editar una partición* en la página 275 para obtener más información sobre la configuración de 'Todo OK'). La opción 'TODO OK' utiliza dos salidas: estado de entrada (luz LED verde) y estado de advertencia (luz LED roja) para indicar el estado de la entrada mediante luces LED en el teclado.
SIN UTILIZAR	Intrusión	Permite que se deshabilite una zona sin que todas las zonas tengan resistencias final de línea. Se ignorarán todas las activaciones de la zona.

Tipo de zona	Categoría de procesamiento	Descripción
FALLO ATRACO	Fallo	Las zonas de fallo de atraco son zonas de 24 horas aplicables a un dispositivo señalizador de atraco, por ejemplo un PAT. El tipo de zona de fallo genera una salida de fallo. Cuando se arma el sistema, se activa una salida de fallo. Tanto el LED del teclado como el zumbador se activan cuando se desarman. Este tipo de zona enviará mensajes SIA, HT (Problema atraco) y HJ (Restauración problema atraco) y para el ID de contacto, se genera la incidencia de problema de sensor (380).
FALLO ADVERTENCIA	Fallo	Las zonas de fallo de advertencia son zonas de 24 horas aplicables a un dispositivo señalizador de advertencia, por ejemplo: una sirena interior o exterior. El tipo de zona de fallo genera una salida de fallo. Cuando se arma el sistema, se activa una salida de fallo. Tanto el LED del teclado como el zumbador se activan cuando se desarman. Este tipo de zona enviará mensajes SIA, YA (Fallo de sirena) y YH (Restauración de sirena) y para el ID de contacto, se genera la incidencia de problema de sensor (380). **Nota:** En un sistema de Grado 2, un fallo del cable generará un falló y no una alarma.
AUTORIZACIÓN DE ARMADO.	Intrusión	Aplicable al funcionamiento con Blockschloss. Este tipo de zona se utiliza para enviar una señal de autorización de armado a la central de que el Blockschloss está listo para armar. Se debe seleccionar la opción Armado para el atributo «Autorización de armado» para la partición.
ELEMENTO BLOQUEO	Intrusión	Si se utiliza un elemento de bloqueo (un perno) con un Blockschloss, este tipo de zona indica la posición del elemento de bloqueo a la central (bloqueado o no bloqueado). Este perno bloquea la puerta en estado armado. Esta señal se comprueba durante el proceso de armado. Si no se recibe la información de «bloqueado», el armado fallará.

Tipo de zona	Categoría de procesamiento	Descripción
ROTURA DE CRISTAL	Intrusión	La zona está conectada a una interfaz de rotura de cristal RI S 10 D-RS-LED en combinación con detectores de rotura de cristal GB2001. • Este tipo de zona está disponible en controladores y módulos de expansión. No está disponible como vía radio ni como un tipo de zona de puerta si el DC2 está configurado como una puerta. • Este tipo de zona informa del mismo modo que una zona de alarma a través de SIA e ID de contacto. • Los derechos para restaurar/inhibir/aislar una rotura de cristal son los mismos que los del tipo de zona de alarma. • Condición de encendido: dado que la alimentación es suministrada por la central, cualquier cambio de estado que se produzca en los 10 primeros segundos es ignorado para permitir que el dispositivo se asiente. • Condición de Reset: las señales procedentes de la interfaz de rotura de cristal se ignoran durante 3 segundos a partir del reinicio del dispositivo. • Salida del modo técnico: la salida de rotura de cristal se puede activar cuando se abandona el modo técnico, en cuyo caso las señales de este sensor se ignorarán temporalmente durante 3 segundos.
AGUA		Este tipo de zona sigue el mismo comportamiento que un tipo de zona técnica.
CALOR		Este tipo de zona sigue el mismo comportamiento que un tipo de zona técnica.
REFRIGERADOR		Este tipo de zona sigue el mismo comportamiento que un tipo de zona técnica.
GAS		Este tipo de zona sigue el mismo comportamiento que un tipo de zona técnica.
ROCIADOR		Este tipo de zona sigue el mismo comportamiento que un tipo de zona técnica.
CO		Este tipo de zona sigue el mismo comportamiento que un tipo de zona técnica.
ENTRADA/SALIDA 2		Este tipo de zona sigue el mismo comportamiento que un tipo de zona de Entrada/Salida con un temporizador de entrada por separado. Debido a esto pueden haber dos temporizadores de entrada a un edificio desde puntos distintos.

23.17 Atributos de zona

Los atributos de zona del sistema SPC determinan la forma en que funcionarán los tipos de zona programados.

Atributo de zona	Descripción
Seguimiento	Cuando el atributo 'Acceso' de una zona está configurado, al abrir esa zona no se generará una alarma en caso de que el temporizador de entrada o salida esté activo. Cuando el sistema está armado total, el atributo Acceso no está activo y la apertura de la zona disparará una alarma completa. El atributo 'Acceso' se utiliza para los sensores PIR ubicados cerca de una zona de entrada/salida. Le permite al usuario un libre movimiento dentro de la partición de acceso mientras que el temporizador de entrada o salida está en cuenta regresiva. El atributo de 'Acceso' solo es válido para los tipos de zona de alarma. Se activan todos los dispositivos conectados (sirenas: interior y exterior, zumbadores, flash). **Nota:** Una zona de alarma con atributo Acceso se puede cambiar automáticamente a zona de entrada/salida en modo Armado parcial si la opción Acceso a armado parcial está configurada.
Excluida en armado parcial A	Si el atributo 'Excluida en armado parcial A' está configurado en una zona, la apertura de esa zona no generará una alarma si la central está en modo Armado parcial A. El atributo 'Excluida en armado parcial A' es válido para el tipo de zona de alarma y zonas de entrada/salida únicamente. Se genera una alarma de armado TOTAL si se abre la zona con el atributo 'EXCLUIDA EN ARMADO PARCIAL A' mientras que el sistema está en modo ARMADO TOTAL o ARMADO PARCIAL B (sirenas interior y exterior, flash).
Excluida en armado parcial B	Si el atributo 'Excluida en armado parcial B' está configurado, la apertura de la zona no generará una alarma si la central está en modo Armado parcial B. El atributo 'Excluida en armado parcial B' es válido para el tipo de zona de Alarma y zonas de entrada/salida únicamente. Se genera una alarma de armado TOTAL si se abre la zona con el atributo 'EXCLUIDA EN ARMADO PARCIAL B' mientras que el sistema está en modo ARMADO TOTAL o ARMADO PARCIAL A (sirenas interior y exterior, flash).
24 h	Si una zona tiene asignado el atributo '24 horas', entonces está activa en todo momento y generará una alarma completa si se abre en cualquier modo. Este atributo solo puede asignado a un tipo de zona de ALARMA. Genera una alarma TOTAL en los modos DESARMADO, ARMADO Y ARMADO PARCIAL. **Nota:** El atributo de 24 horas anula la configuración de cualquiera de los otros atributos para una zona de alarma en particular.
Local	Si el atributo 'Local' está configurado, una alarma generada por una zona que se abre no generará el informe externo de esa incidencia. El atributo 'Local' es válido para los tipos de zona de alarma, entrada/salida, incendio, salida de incendio y médica.
Desarmado local	Cuando este atributo está configurado, una alarma generada por la apertura de la zona cuando el área está parcial o totalmente armada se informará de forma usual. Sin embargo, si la partición está desarmada, solo se producirá una alarma local, es decir: zumbador del teclado, flash de la luz LED y visualización de zona. Este atributo solo es aplicable a las zonas de alarma, incendio y sísmica.

Atributo de zona	Descripción
Doble detección	Utilice este atributo para resolver los problemas que presenten los detectores (es decir, algunos detectores pueden generar señales de activación falsas y, como consecuencia, pueden disparar, inadvertidamente, alarmas de activación en el sistema). Si se activa la misma zona de doble detección dos veces durante el período de doble detección, entonces, se disparará la alarma. El tiempo de doble detección se establece en segundos (consulte *Temporizaciones* en la página 266). Dos acciones de apertura durante ese período de tiempo generarán una alarma. Cuando el sistema está armado, se registran todas las zonas de doble detección abiertas.
Chime	Cuando el atributo 'Chime' está configurado para una zona, la apertura de la zona durante el modo Desarmado hará que los zumbadores internos se activen durante un período corto de tiempo (2 segundos aproximadamente). El atributo Chime es válido para los tipos de zona de alarma, entrada/salida y técnica.
Inhibir	Cuando el atributo 'Inhibir' está configurado, un usuario puede inhibir esta zona. La operación de inhibición deshabilitará dicho fallo o zona sólo durante un período de armado.
Normalmente abierta (NA)	Cuando se establece el atributo «Normalmente abierta», el sistema espera que un detector conectado sea un dispositivo Normalmente Abierto (p. ej.: un detector se considera activado siempre que los contactos en el dispositivo estén cerrados).
Silenciosa	Si el atributo 'Silenciosa' está configurado, entonces, no habrá indicaciones de audio o visuales de la alarma. La activación de la alarma se enviará a la estación receptora. Si el sistema está desarmado, aparecerá un mensaje de advertencia.
Registro	Si este atributo está armado, se registrarán todos los cambios de estado de zona.
Salida abierta	Si esta opción está configurada, se indicará la zona en caso de apertura durante el armado.
Supervisada	Este atributo solo se aplica a servicios remotos*. Si este atributo está configurado para una zona, la zona debe abrirse para fines de servicios remotos dentro del período de tiempo frecuente definido.
RFL	El atributo Resistencia final de línea (RFL) ofrece una cantidad de configuraciones de cableado de zona de entrada en el sistema.
Analizada	El atributo Analizada debe estar configurado para una zona si esa zona está cableada con un sensor inercial. Los valores de N.° de impulsos y Sensibilidad deben estar programados para cada sensor inercial en el sistema de conformidad con los resultados de la simple calibración del dispositivo.
Cantidad de pulsos	Cantidad de pulsos de nivel de alarma para sensores inerciales analizados.
Sensibilidad	Nivel de sensibilidad de alarma para sensores inerciales analizados
Fin de salida	El atributo Salida final puede ser solo asignado a un tipo de zona de entrada/salida. Utilice este atributo para anular el proceso estándar de cuenta regresiva del temporizador de salida cuando el sistema esté armado total. Cuando todas las rutas de entrada/salida de las instalaciones estén cerradas, se debe armar todo el sistema y cerrar la zona de entrada/salida final. En cuanto se cierre la puerta, el tiempo de Fin de salida empezará a avanzar para armar el sistema.

Atributo de zona	Descripción
Anulación ligada	Una zona con el atributo de inhibición quedará anulada cuando se abra la zona de tipo anulación. Esto permite agrupar la inhibición de zonas con la apertura del tipo de zona de anulación.
Sólo TX	Este atributo solo puede asignado a un tipo de zona de INCENDIO. Si este atributo está configurado, la activación de la zona de incendios solo informará la activación a la estación central. No se generarán alarmas en el sitio.
Con retorno	Este atributo solo se aplica al tipo de zona de LLAVE ARMADO. Si está configurado, el estado de armado del edificio cambiará con las aperturas únicamente.
Habilitar armado total	Este atributo solo se aplica al tipo de zona de LLAVE ARMADO. Si este atributo está configurado, la activación de la zona generará el ARMADO TOTAL del sistema/partición. Aplique este atributo si se espera que el usuario solo tenga la capacidad de aplicar el ARMADO TOTAL del sistema desde una zona de llave armado.
Habilitar desarmado	Este atributo solo se aplica al tipo de zona de LLAVE ARMADO. Si este atributo está configurado, la activación de la zona generará el desarmado del sistema/partición. Aplique este atributo si se espera que el usuario solo tenga la capacidad de aplicar el DESARMADO del sistema desde una zona de llave armado.
Informe de zona técnica	Habilita una zona cuando está abierta, independientemente del modo de envío de alarma a la CRA en FF, ID de contacto, SIA y SIA extendido. Cuando se seleccionan las particiones, solo se enviará la alarma a la CRA a la que la partición ha sido asignada. Esta será una alarma desconocida (UA) seguida del número de zona y el texto en caso de que la opción SIA extendido esté seleccionada. También enviará un SMS al usuario final y al técnico (si la opción está marcada) cuando se seleccione el filtro de alarma sin confirmar.
Visualización de zona técnica	Permite visualizar una zona de apertura en el teclado del sistema. También se debe activar la luz LED de alerta. Cuando se seleccionan las particiones, solo se mostrará en el teclado la partición de la zona seleccionada. Solo se puede mostrar la alerta en el teclado cuando la partición está en modo desarmado y no en modo Parcial A, Parcial B y Armado.
Alarma audible de zona técnica	Permite a una zona activada utilizar el zumbador. Éste funcionará igual que Pantalla zona técnica en los diferentes modos de configuración y en los sistemas con particiones.
Retardo de zona técnica	Permite que la zona tenga un retardo programable. El retardo varía de 0 a 9999 segundos y se aplicará a todas las zonas técnicas. El funcionamiento es el mismo que el del temporizador de retardo de red c.a., si la zona se cierra dentro del período de retardo, no se envían alarmas a la CRA, ni SMS al usuario y la salida técnica no se disparará. **Nota:** La salida técnica no se disparará hasta que haya transcurrido el tiempo del temporizador de retardo.
Informe de armado únicamente	Las aperturas solo se informan en modo armado.
Prealarma incendio	Si esta opción está habilitada y se dispara una alarma de incendio, se inicia el temporizador de prealarma incendio y se activan las sirenas de interior y los zumbadores. (Consulte *Temporizaciones* en la página 266.) Si la alarma no se cancela durante el período de tiempo designado, se confirma la alarma de incendio, se activan las sirenas de interior y de exterior y se envía una incidencia a la CRA.

Atributo de zona	Descripción
Reconocimiento alarma incendio	Si esta opción está habilitada, se activa el temporizador de reconocimiento de alarma de incendio el cual añade tiempo adicional a la duración del temporizador de prealarma de incendio hasta que se informe una alarma de incendio para esa zona. Consulte *Temporizaciones* en la página 266.
Prueba sísmica/Prueba de sensor automático	Se puede comprobar el tipo de zona sísmica de forma manual o automática. Este atributo permite que se habilite la comprobación automática. Consulte *Temporizaciones* en la página 266 para obtener más información sobre cómo configurar el temporizador que determina con qué frecuencia comprueba la central todas las zonas sísmicas que tienen habilitado este atributo. El valor predeterminado para el temporizador es 7 días.
Temporizado	El atributo «retraso» sirve para que las zonas de Llave armado retrasen el armado de una partición. El retardo viene a continuación del temporizador de salida para la partición a la que está asociada la llave armado.
Verificación	Seleccione la zona de verificación configurada par asignar esta zona al activador de verificación de audio/video.
Armado forzado	Si está habilitado, el dispositivo de llave armado puede armar el sistema inhibiendo todas las zonas abiertas.

23.18 Atributos aplicables a los tipos de zona

La siguiente tabla muestra qué atributos se aplican a cada tipo de zona:

Zone Type / Attribute	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock Supervision	Seismic **	All Okay	Hold-up Fault	Warning Fault	Setting Authorisation	Lock Element	Glass Break
Access	v																							v
Exclude A	v	v																					v	v
Exclude B	v	v																					v	v
24 Hour	v																	v						v
Local	v	v		v	v						v					v				v	v		v	v
Unset Local	v			v														v						v
Double Knock	v																							v
Chime	v	v								v												v		v
Inhibit	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v		v	v
Normal Open	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v		v	v	v	v	v	v
Silent	v						v	v																v
Log	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v
Shunt	v	v			v																			v
Frequent *	v	v	v							v		v		v	v									v
Analyzed	v	v			v																			
Pulse Count	v	v			v																			
Gross attack	v	v			v																			
Calendar	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v
Verification	v	v		v	v		v	v		v	v							v						v
Exit Open		v																						
Seismic Test																		v						
Timed												v												
Report Only				v																				
Open Only												v										v		
Final Exit		v																					v	
Fullset enable												v												
Unset enable												v												
Shunt	v	v			v																			v
Report (Tech)										v														
Display(Tech)										v														
Audible (Tech)										v														
Delay (Tech)										v														
Report When Set										v														
Fire Pre-alarm				v	v																			
Fire Recognition				v	v																			
Force set												v												

Solo disponible en modo Comercial.

** Sólo en combinación con servicios remotos.*

*** Solo disponible en modo Financiero*

23.19 Niveles y especificaciones de atenuación del ATS

Niveles del sistema de transmisión de alarma (ATS)

La siguiente tabla muestra los niveles del ATS requeridos para la central cuando la comunicación es entre:

- GSM y la central de recepción de alarmas (CRA)
- RTB y la central de recepción de alarmas (CRA)
- Software receptor de comunic. Ethernet a SPC
- Software receptor de comunic. GPRS a SPC

	CRA GSM	CRA RTB	Ethernet	GPRS
Nivel del ATS	ATS 2	ATS 2	STA 6	STA 5

Atenuación de RTB

Para un marcador automático de RTB, se debe utilizar un cable CW1308 Internal Telecom o equivalente para conectar el módem a la línea telefónica. El cable debe tener una longitud de entre 0,5 y 100 m.

Atenuación de Ethernet

Para Ethernet, se debe utilizar un cable Cat 5 con una longitud de entre 0,5 y 100 m.

Atenuación de GSM

La intensidad de campo de la señal GSM debe ser de al menos -95dB. Por debajo de este nivel, el módem indicará un fallo por baja señal en la central. Esto se trata de la misma forma que otros fallos en el sistema.

Monitoreo y control de RTB (SPCN110) y GSM (SPCN320)

Una falla en la interfaz entre el módem RTB y la central se detectará luego de 30 segundos, tras lo cual se producirá un fallo de ATS.

Una falla en la interfaz entre el módem GSM y la central se detectará luego de 30 segundos, tras lo cual se producirá un fallo de ATS.

23.20 Lectores de tarjeta y formatos de tarjeta admitidos

El sistema SPC admite los siguientes lectores de tarjeta y formatos de tarjeta:

Lector	Formatos de tarjeta
HD500-EM PR500-EM SP500-EM PM500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR

Lector	Formatos de tarjeta
AR6181-RX AR6182-RX	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HD500-Cotag PR500-Cotag SP500-Cotag PM500-Cotag HF500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-MX AR6182-MX	ABP5100-BL Mifare Classic 1K ABR5100-PR Mifare Classic 4K
iClass R10 iClass R15 iClass R30 iClass R40 iClassRK40	ABP5100-BL Por defecto, solo Mifare 32 bits

Lector	Formatos de tarjeta
MultiClass RP40 MultiClass RP15 MultiClass RPK40	ABP5100-BL Por defecto, solo Mifare 32 bits IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HID Prox Pro	Wiegand 26 bits EPX Wiegand 36 bits

Códigos locales y restricciones

Formato del lector	Código local disponible	Restricciones
EM4102	No	N.º tarjeta máx. 9999999999
COTAG	No	N.º tarjeta máx. 9999999999
Wiegand 26 bits	Sí	Código local máximo 255 N.º tarjeta máx. 65535
Wiegand 36 bits	Sí	Código local máximo 32767 N.º tarjeta máx. 524287
HID Corporate 1000	Sí	Código local máximo 4095 N.º tarjeta máx. 1048575
HID 37	No	N.º tarjeta máx. 34359738370
HID 37F	Sí	Código local máximo 65535 N.º tarjeta máx. 5242875
HID 37BCD	No	N.º tarjeta máx. 99999999
HID ICLASS MIFARE	No	N.º tarjeta máx. 4294967295
HID ICLASS DESFIRE	No	Número tarjeta encriptado N.º tarjeta máx. 72×10^{16}. Este número se debe dar de alta en la central
AR618 WIE BCD 52 BIT	No	N.º tarjeta máx. 4294967295
AR618 OMRON 80 BIT	No	N.º tarjeta máx. 9999999999999

23.21 Soporte de SPC para dispositivos E-Bus

El Gateway E-Bus SPC (SPCG310) es un módulo de expansión X-Bus que permite la comunicación entre un controlador SPC y dispositivos E-Bus Sintony. El direccionamiento con E-BUS Sintony permite duplicar direcciones para dispositivos E-Bus en diferentes secciones de E-BUS. Los dispositivos X-Bus requieren direcciones únicas. Para solucionar este conflicto, puede que sea necesario realizar un

redireccionamiento periférico del E-BUS. Para obtener más información, consulte *Modo direccionamiento* en la página 147.

AVISO: Vanderbilt recomienda leer el documento **Migración del sistema Sintony** antes de configurar dispositivos E-Bus.

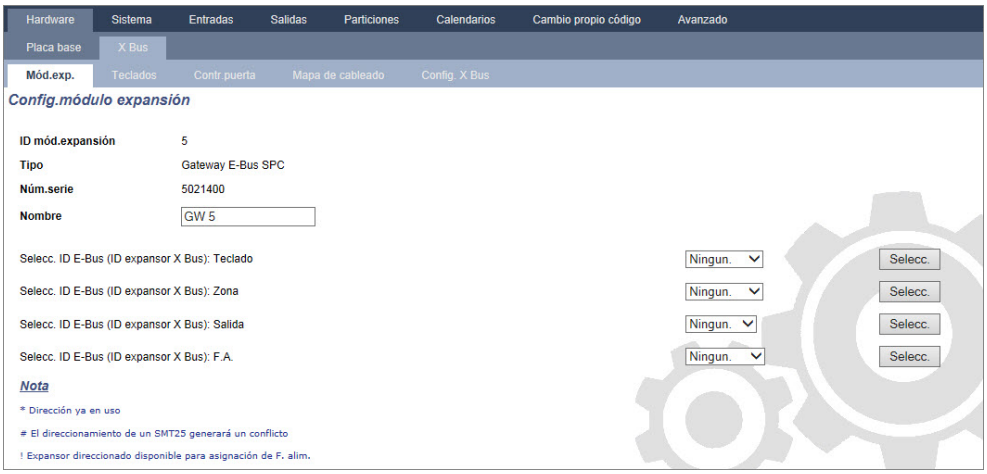
23.21.1 Configuración y direccionamiento de dispositivos E-Bus

Puede configurar y direccionar los siguientes dispositivos E-Bus Sintony para comunicarse con el controlador SPC:

- Teclados Sintony SAK41/SMK41, SAK51/SMK51 y SAK53/SMK53
- Transpondedores de entrada Sintony
- Transpondedores de salida Sintony
- Fuentes de alimentación Sintony: SAP 8, SAP 14, SAP 20 y SAP 25

1. En el navegador, vaya a **Configuración > X-BUS > Módulos expansión**.

   Se muestra una lista de **Módulos de expansión configurados**.
2. Seleccione un **Gateway E-Bus SPC**.
3. En la página **Configuración de módulo de expansión**, introduzca una **Descripción** para el **Gateway E-Bus SPC**. Para obtener más información sobre la configuración de módulos de expansión, consulte *Módulos de expansión* en la página 235.



4. Para direccionar un dispositivo E-Bus, seleccione un ID del menú desplegable correspondiente tal como se describe en la siguiente tabla. Un asterisco (*) por delante significa que ese ID ya se está utilizando. No se puede seleccionar este ID.
5. Haga clic en el botón **SELECC**.

   En la parte superior de la página, se muestra el mensaje `Direccionamiento en curso... Se requiere reconfiguración X BUS.`

   El Gateway E-Bus SPC emite un pitido repetidamente.
6. Dependiendo del dispositivo E-Bus, mantenga pulsado el botón de direccionamiento tal como se describe en la columna **Direccionamiento** en la siguiente tabla.

   El Gateway E-Bus SPC emite un pitido continuo para indicar que el ID ahora está asociado al dispositivo E-Bus.
7. Vaya a **Configuración > X-BUS > Módulos de expansión**.
8. Haga clic en el botón **Reconfigurar**.

Se mostrará el mensaje `Reconfiguración completa` en la parte superior de la página. Las entradas y salidas de E-Bus se muestran en la lista de **Módulos de expansión configurados**. Si un módulo de expansión de entrada tiene una fuente de alimentación asociada, el tipo de fuente de alimentación se muestra en la columna **F.alimentación**. Los teclados se muestran en la lista de **Teclados configurados**.

9. Para completar los pasos de direccionamiento manual para añadir los dispositivos de fuente de alimentación SAP 8, SAP 14 y SAP 20 a la lista de **Módulos de expansión configurados**, consulte *Direccionamiento de transpondedores para SAP 8, SAP 14 y SAP 20* abajo.
10. Si el X-BUS tiene conflictos de direccionamiento, se mostrará la advertencia `ID duplicado o no válido para IDx módulo de expansión`. Repita los pasos de direccionamiento indicados hasta que no quede ningún conflicto de direccionamiento.

Dispositivo E-BUS: menú desplegable	Descripción	Formato de ID	Direccionamiento
Teclado	IDs para asignar a teclados Sintony	ID de E-BUS (ID de X-BUS)	Mantenga pulsadas simultáneamente las teclas 1 y 3 hasta que el Gateway E-Bus SPC emita un pitido continuado.
Entrada	IDs para asignar a transpondedores de entrada Sintony	ID de E-BUS (ID de X-BUS)	Mantenga pulsado el botón de direccionamiento durante 5 segundos y suéltelo cuando suene un pitido continuado.
Salida	IDs para asignar a transpondedores de salida Sintony	ID de E-BUS (ID de X-BUS)	Mantenga pulsado el botón de direccionamiento durante 5 segundos y suéltelo cuando el Gateway E-Bus SPC emita un pitido continuado.
F.alimentación	IDs para asignar a dispositivos de fuente de alimentación Sintony SAP 8, SAP 14, SAP 20 y SAP 25	ID de E-BUS (ID de X-BUS de transpondedor asociado)	Mantenga pulsado el botón de direccionamiento hasta que el Gateway E-Bus SPC emita un pitido continuado.

Consulte también

Modo direccionamiento en la página 147

23.21.1.1 Direccionamiento de transpondedores para SAP 8, SAP 14 y SAP 20

Tras asignar un ID de PSU a un SAP 8, SAP 14 o SAP 20 (consulte *Configuración y direccionamiento de dispositivos E-Bus* en la página precedente), debe asignar un transpondedor de entrada a la PSU. De este modo se simula la comunicación con el controlador SPC a través de un módulo de expansión.

1. En la lista de **Módulos de expansión configurados**, seleccione el **Gateway E-Bus SPC**.

   Se muestra la página **Configuración de módulo de expansión**.
2. En la lista desplegable puede ver el ID de fuente de alimentación recientemente asignado.

   Un signo de exclamación (!) por delante señala el ID de fuente de alimentación que usted ha asignado al dispositivo. Esto indica que hay un transpondedor de entrada disponible para asignar a la fuente de alimentación.
3. Tome nota del número que aparece entre corchetes junto al ID de fuente de alimentación. Este número es el ID que usted debe asignar al transpondedor de entrada. Por ejemplo, si el ID de la fuente de alimentación es **ID 14 (27)**, debe seleccionar manualmente un transpondedor con el **ID 27** en la lista desplegable de **Entrada**.
4. En la lista desplegable de **Entrada**, seleccione el ID de transpondedor que aparece en corchetes junto al ID de la fuente de alimentación.
5. Haga clic en el botón **SELECC**.

6. Vaya a **Configuración > X-BUS > Módulos de expansión**.
7. Haga clic en **Reconfigurar**.

   El dispositivo de fuente de alimentación se muestra en la lista de **Módulos de expansión configurados**.

23.21.1.2 Direccionamiento de transpondedores para fuente de alimentación SAP 25

La fuente de alimentación Sintony SAP 25 tiene dos transpondedores internos. Cada transpondedor requiere un ID. Estos dos ID se asignan automáticamente cuando se completan los pasos de direccionamiento descritos en *Configuración y direccionamiento de dispositivos E-Bus* en la página 407. Se aplica la fórmula `2n – 1`, donde `n` es el valor del ID de la fuente de alimentación. Por ejemplo, si asigna el ID 10 a un SAP 25, a cada transpondedor se le asignarán los ID de X-BUS 19 y 20.

AVISO: En la lista desplegable de fuente de alimentación, un signo de almohadilla (#) por delante del ID de SAP 25 indica que el direccionamiento automático de los transpondedores entrará en conflicto con los transpondedores de entrada existentes. Para resolver este conflicto, deberá redireccionar uno de los dispositivos en conflicto.

23.22 Glosario FlexC

Sigla	Descripción EN50136-1	Ejemplo FlexC
AE	**Equipo de aviso** Equipamiento localizado en la CRA que asegura y presenta el estado de alarma o los cambios del estado de alarma de los sistemas en respuesta a la recepción de alarmas entrantes antes del envío de una confirmación. El AE (equipo de alarma) no es parte del ATS (sistema de transmisión de alarma).	Cliente de SPC Com XT
CRA	**Central de recepción de alarmas** Centro con atención 24H al que se reporta información sobre el estado de uno o más AS (sistemas de alarma).	SPC Com XT se instala en una CRA.
AS	**Sistema de alarma** Instalación eléctrica capaz de reaccionar de forma manual o automática ante la presencia de un riesgo. El AS (sistema de alarma) no es parte del ATS (sistema de transmisión de alarma).	Central SPC
ATE	**Equipo de transmisión de alarma** Término colectivo para describir SPT, MCT (transceptor de central de monitoreo) y RCT.	-
ATP	**Ruta de transmisión de alarma** Ruta por la que se transmite una señal de alarma entre un AS (sistema de alarma individual) y un AE (equipo de aviso) asociado. La ATP comienza en la interfaz entre el AS y el SPT, y termina en la interfaz entre el RCT y el AE. La dirección inversa también se puede utilizar para fines de notificación y vigilancia.	Ruta definida entre la central SPC y SPC Com XT. Por ejemplo, un sistema con Ethernet como ruta principal y GPRS como ruta de respaldo se considera dos ATP diferentes dentro de un mismo ATS.

Sigla	Descripción EN50136-1	Ejemplo FlexC
ATS	**Sistema de transmisión de alarma** ATE (Equipo de transmisión de alarmas) y redes usadas para transferir información concerniente a uno o más AS de las instalaciones a uno o más AE de una o más CRAs. Un ATS puede disponer de una o más ATPs.	Un sistema que combina una o más rutas entre la central SPC y SPC Com XT.
RCT	**Transceptor de central de recepción** ATE en la CRA que incluye la interfaz con uno o más AE y la interfaz con una o más redes de transmisión como parte de una o más ATP. En algunos sistemas este transceptor puede ser capaz de indicar los cambios de estado de un AS y guardarlos en un fichero de registro. Esto puede ser necesario para aumentar la disponibilidad del ATS en caso de fallo del AE	Servidor SPC Com XT
SPT	**Transceptor supervisado de la instalación** ATE del lugar supervisado que incluye el interfaz con el AS y el interfaz con una o más redes de transmisión, siendo parte de uno o más ATPs.	Integrado en la central SPC que emplea Ethernet, GPRS o PPP a través de RTB.

El protocolo FlexC emplea las siguientes siglas.

Sigla	Descripción
ASP	**Protocolos de seguridad analógicos** Los protocolos de seguridad analógicos tradicionalmente utilizados para la transmisión de alarmas a través de la red telefónica, p. ej., SIA, Contact ID.

23.23 Comandos FlexC

La siguiente tabla muestra los comandos que puede habilitar para un perfil de comandos. El perfil de comandos que asigna a un ATS define cómo controla una central desde SPC Com XT.

Filtro de comandos	Comandos
Comandos del sistema	Ver resumen de central
	Establecer la fecha y hora del sistema
	Permitir acceso al técnico
	Permitir acceso al fabricante

Filtro de comandos	Comandos
Comandos de intrusión	Ver el estado de una partición
	Ver el estado de cambio de modo de una partición
	Cambiar el modo (armado/desarmado) de una partición
	Ver el estado de alertas de central
	Ejecutar acciones ante alarmas
	Silenciar sirenas
	Ver el estado de una zona
	Controlar una zona
	Ver el registro del sistema
	Ver el registro de una zona
	Ver el registro de vía radio
Comandos de salida	Ver el estado de una puerta de mapeo
	Controlar puertas de mapeo
Comandos de usuario	Verificar un usuario en la central
	Ver la configuración de un usuario
	Añadir un usuario
	Editar un usuario
	Borrar un usuario
	Ver la configuración del perfil de un usuario
	Añadir un perfil de usuario
	Editar un perfil de usuario
	Borrar un perfil de usuario
	Cambiar el PIN de un usuario
Comandos de calendario	Obtener la configuración de un calendario
	Añadir un calendario
	Editar un calendario
	Editar una semana del calendario
	Borrar un calendario
	Añadir un día excepcional en un calendario
	Editar un día excepcional en un calendario
	Borrar un día excepcional en un calendario

Filtro de comandos	Comandos
Comandos de comunicación	Ver el estado de Ethernet
	Ver el estado de un módem
	Ver el registro para un módem
	Ver el registro para receptor de la CRA
Comandos FlexC	Ver el estado de un ATS FlexC
	Ver el registro de red para un ATS FlexC
	Ver el registro de incidencias para un ATS FlexC
	Ver el registro para una ATP FlexC
	Ver el registro de red para una ATP FlexC
	Exportar el archivo de configuración de un ATS FlexC
	Importar el archivo de configuración de un ATS FlexC
	Borrar un ATS FlexC
	Borrar una ATP FlexC
	Borrar un perfil de incidencias de FlexC
	Borrar un perfil de comandos de FlexC
	Solicitar una llamada de test para una ATP FlexC
Comandos de control de accesos	Ver la configuración para una puerta
	Obtener el estado para un puerta
	Controlar una puerta
	Ver el registro de acceso
Comandos de verificación	Obtener la imagen de una cámara
	Ver el estado de una zona de verificación
	Ver datos para una zona de verificación
	Enviar datos a una zona verificación
Comandos de teclado virtual	Controlar el teclado

Filtro de comandos	Comandos
Comandos de archivo	Actualizar el firmware de la central
	Actualizar el firmware de periféricos
	Cargar el firmware de periféricos
	Actualizar el progreso de PFW
	Cargar un archivo
	Descargar un archivo
	Salva la configuración de la central
	Resetear la central
Comandos heredados	Ver información de la central
	Ver el estado de la central
	Ver encabezados de ficheros de configuración
	Ver la configuración de idioma
	Ver la configuración de intrusión
	Ver el estado de dispositivos X Bus
	Ver la configuración de una partición

23.24 Tiempos categorías ATS

Esta tabla describe los tiempos de las categorías ATS EN50136-1 estipulados en el estándar y cómo la implementación FlexC cumple con estos estándares en las categorías SP1-SP6, DP1-DP4.

		Requisitos de tiempos de categoría ATS EN50136-1				Implementación FlexC de requisitos de tiempos de categoría ATS			
Categoría ATS	Interfaces por defecto	Tiempo de espera de incidencia	Tiempo de espera de polling primario	Tiempo de espera de polling ATP de respaldo (primario OK)	Tiempo de espera de polling ATP de respaldo (primario caído)	Tiempo de espera de incidencia	Tiempo de espera de polling primario	Tiempo de espera de polling ATP de respaldo (primario OK)	Tiempo de espera de polling ATP de respaldo (primario caído)
SP1	Cat 1 [Ethernet]	8 min	32 días	-	-	2 min	30 días	-	-
SP2	Cat 2 [Ethernet]	2 min	25 h	-	-	2 min	24 h	-	-
SP3	Cat 3 [Ethernet]	60 s	30 min	-	-	60 s	30 min	-	-
SP4	Cat 4 [Ethernet]	60 s	3 min	-	-	60 s	3 min	-	-
SP5	Cat 5 [Ethernet]	30 s	90 s	-	-	30 s	90 s	-	-

		Requisitos de tiempos de categoría ATS EN50136-1				Implementación FlexC de requisitos de tiempos de categoría ATS			
Categoría ATS	**Interfaces por defecto**	**Tiempo de espera de incidencia**	**Tiempo de espera de polling primario**	**Tiempo de espera de polling ATP de respaldo (primario OK)**	**Tiempo de espera de polling ATP de respaldo (primario caído)**	**Tiempo de espera de incidencia**	**Tiempo de espera de polling primario**	**Tiempo de espera de polling ATP de respaldo (primario OK)**	**Tiempo de espera de polling ATP de respaldo (primario caído)**
SP6	Cat 6 [Ethernet]	30 s	20 s	-	-	30 s	20 s	-	-
DP1	Cat 2 [Ethernet] Cat 2 [Módem]	2 min	25 h	50 h	25 h	2 min	24 h	24 h 30 min	24 h 10 min
DP2	Cat 3 [Ethernet] Cat 3 [Módem]	60 s	30 min	25 h	30 min	60 s	30 min	24 h 30 min	30 min
DP3	Cat 4 [Ethernet] Cat 4 [Módem]	60 s	3 min	25 h	3 min	60 s	3 min	24 h 30 min	3 min
DP4	Cat 5 [Ethernet] Cat 5 [Módem]	30 s	90 s	5 h	90 s	30 s	90 s	4 h 10 min	90 s

23.25 Tiempos categorías ATP

La siguiente tabla muestra la configuración aplicada para los tiempos de espera de incidencias, intervalos de polling (activo y no activo) y tiempos de espera de polling (activo y no activo) para cada categoría ATP. Para los fines del uso de Ethernet, el intervalo de polling y el intervalo de reintento son idénticos. Para reducir los costos relacionados con las llamadas GPRS, el intervalo y el intervalo de reintento para las rutas GPRS difieren, por ejemplo: Cat 3 [módem] realiza el polling cada 25 minutos y, luego, cada 60 segundos durante 5 minutos hasta caducar a los 30 minutos. Para obtener una descripción general visual del intervalo de polling configurado, vaya a **Estado > FlexC > Registro de red**.

Si una ATP está activa y luego cae, continuará en las tasas de polling activo durante otros dos ciclos de polling antes de continuar con los intervalos de polling **ATP con fallo**.

Categorías ATP Ethernet		Polling con ATP activa			Polling con ATP no activa			Polling con ATP caída	
Categoría de ATP	**Tiempo de espera de incidencia**	**Intervalo test**	**Intervalo de reintentos**	**Margen fallo test**	**Intervalo test**	**Intervalo de reintentos**	**Margen fallo test**	**Intervalo test**	**Timeout**
Cat 6 [Ethernet]	30 s	8 s	30 s	20 s	8 s	30 s	20 s	30 s	30 s
Cat 5 [Ethernet]	30 s	10 s	30 s	90 s	10 s	30 s	90 s	30 s	30 s

Categorías ATP Ethernet		Polling con ATP activa			Polling con ATP no activa			Polling con ATP caída	
Categoría de ATP	**Tiempo de espera de incidencia**	**Intervalo test**	**Intervalo de reintentos**	**Margen fallo test**	**Intervalo test**	**Intervalo de reintentos**	**Margen fallo test**	**Intervalo test**	**Timeout**
Cat 4 [Ethernet]	60 s	30 s	30 s	3 min	30 s	30 s	3 min	30 s	30 s
Cat 3 [Ethernet]	60 s	60 s	60 s	30 min	60 s	60 s	30 min	60 s	30 s
Cat 2A [Ethernet]	2 min	2 min	2 min	4 h	2 min	2 min	4 h	2 min	30 s
Cat 2 [Ethernet]	2 min	2 min	2 min	24 h	2 min	2 min	24 h	2 min	30 s
Cat 1 [Ethernet]	2 min	2 min	2 min	30 días	2 min	2 min	30 días	2 min	30 s
Categorías ATP módem									
Cat 5 [Módem]	30 s	10 s	30 s	90 s	4 h	2 min	4 h 10 min	10 min	90 s
Cat 4A [Módem]	60 s	60 s	60 s	3 min	4 h	2 min	4 h 10 min	30 min	90 s
Cat 4 [Módem]	60 s	60 s	60 s	3 min	24 h	2 min	24 h 30 min	1 h	90 s
Cat 3 [Módem]	60 s	25 min	60 s	30 min	24 h	2 min	24 h 30 min	4 h	90 s
Cat 2A [Módem]	2 min	4 h	2 min	4 h 10min	24 h	2 min	24 h 30 min	4 h	90 s
Cat 2 [Módem]	2 min	24 h	2 min	24 h 10 min	24 h	2 min	24 h 30 min	24 h	90 s
Cat 1 [Módem]	2 min	24 h	10 min	25 h	30 días	10 min	30 días 1 h	7 días	90 s

24 Notas

Publicado por Vanderbilt International (IRL) Ltd.
Clonshaugh Business and Technology Park
Clonshaugh
Dublin 17
D17 KV 84
Ireland

www.vanderbiltindustries.com

ID del documento: A6V10276959-c
Versión del documento: X.X
Fecha de edición: 31.08.2017

VANDERBILT