SPC42xx/43xx/52xx/53xx/63xx

Intrusion Control Panel

3.6

A6V10276963
01.05.2016

Vanderbilt

Copyright

Especificaciones técnicas y disponibilidad sujetas a modificación sin previo aviso.

© Copyright Vanderbilt

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

Edition: 01.05.2016

Documento ID: A6V10276963

Contenido

1 Significado de los símbolos 11

2 Seguridad 12

2.1 Grupo objetivo 12

2.2 Instrucciones generales de seguridad 12

2.2.1 Información general 12

2.2.2 Transporte 12

2.2.3 Configuración 13

2.2.4 Funcionamiento 13

2.2.5 Servicio técnico y mantenimiento 14

2.3 Significado de los avisos escritos 14

2.4 Significado de los símbolos de peligro 14

3 Directivas y normas 15

3.1 Directivas de la UE 15

3.1.1 Información general sobre la conformidad con la norma EN50131 15

3.1.2 Conformidad con las certificaciones EN50131 19

3.1.3 Conformidad con las certificaciones EN 50136-1:2012 and EN 50136-2:2014 21

3.1.4 Conformidad con normas INCERT. 22

3.1.5 Directrices de conformidad con PD 6662:2010 23

3.1.5.1 Productos 23

3.1.5.2 Resumen de normas 23

3.1.5.3 Métodos para completar el armado y desarmado 24

3.1.5.4 Requisitos de configuración para el cumplimento de la norma PD 6662:2010. 26

3.1.5.5 Requisitos de puesta en funcionamiento adicionales para el cumplimento de la norma PD 6662:2010. 28

3.1.5.6 Información adicional 29

3.1.6 Cumplimiento de las normas VdS 29

3.1.7 Cumplimiento de las normas NF 30

4 Datos técnicos 32

4.1 SPC4000 32

4.2 SPC5000 34

4.3 SPC6000 36

5 Introducción 40

6 Montaje del equipamiento del sistema 41

6.1 Montaje de una carcasa G2 41

6.2 Montaje de una carcasa G3 42

6.2.1 Montaje del kit de tamper trasero 44

6.2.2 Instalación de la batería de conformidad con EN50131 48

6.3 Montaje de una carcasa G5 49

6.3.1 Protección de tamper 51

6.3.2 Montaje de la carcasa con protección de tamper 51

6.3.2.1 Funcionamiento del tamper 53
6.3.3 Instalación de las baterías 54
6.4 Montaje de un teclado 55
6.5 Montaje de un módulo de expansión 55
7 Fuente de alimentación inteligente 56
7.1 Fuente de alimentación inteligente SPCP355 56
7.1.1 Salidas supervisadas 58
7.1.2 Baterías 59
7.1.2.1 Instalación de las baterías 59
7.1.2.2 Comprobación de voltaje de la batería 61
7.1.2.3 Protección contra descarga mínima 61
7.1.2.4 Tiempos de espera de la batería 61
7.1.3 Cableado de la interfaz X-BUS 61
7.1.3.1 Cableado de las entradas 62
7.1.3.2 Cableado de las salidas 63
7.1.4 LED de estado de la fuente de alimentación 64
7.1.5 Recuperación del sistema 65
8 Hardware del controlador 66
8.1 Hardware del controlador 42xx\43xx\53xx\63xx 66
8.2 Hardware del controlador SPC5350 y 6350 69
9 Módulo de expansión de puerta 72
10 Cableado del sistema 73
10.1 Cableado de la interfaz X-BUS 73
10.1.1 Configuración en lazo 74
10.1.2 Configuración en punta 75
10.1.3 Configuración en estrella y multipunto 76
10.1.3.1 Ejemplos de cableado correcto 80
10.1.3.2 Ejemplos de cableado incorrecto 81
10.1.4 Apantallamiento 82
10.1.5 Mapa de cableado 83
10.2 Cableado del módulo de expansión de bifurcación 83
10.3 Cableado de la masa del sistema 84
10.4 Cableado de la salida de relé 84
10.5 Cableado de entradas de zona 85
10.6 Cableado de una sirena SAB exterior 88
10.7 Cableado de una sirena interna 89
10.8 Cableado para rotura de cristal 89
10.9 Instalación de módulos complementarios 90
11 Encendido del controlador SPC 92
11.1 Alimentación únicamente con batería 92
12 Interfaz de usuario del teclado 93
12.1 SPCK420/421 93
12.1.1 Introducción 93
12.1.2 Uso de la interfaz del teclado LCD 95
12.1.3 Introducción de datos en el teclado LCD 98

12.2 SPCK620/623 99
12.2.1 Introducción 99
12.2.2 Descripción de LED 102
12.2.3 Descripción de modo de visualización 103
12.2.4 Teclas de función en estado inactivo 104
13 Herramientas de software de apoyo 105
14 Inicio del sistema 106
14.1 Modos de técnico 106
14.1.1 Códigos técnico 106
14.2 Herramientas de programación 107
14.2.1 Programador rápido 107
14.3 Configuración de los parámetros de inicio 107
14.4 Creación de usuarios del sistema 109
14.5 Programación de Portable ACE 109
14.6 Configuración de dispositivos de mando vía radio 111
14.6.1 Borrado de alertas utilizando el mando 111
15 Programación de técnico parcial a través del teclado 113
16 Programación de técnico a través del teclado 114
16.1 Estado sistema 114
16.2 OPCIONES 115
16.3 Temp/Retardos 118
16.4 PARTICIONES 121
16.5 Grupos particiones 122
16.6 X-BUS 122
16.6.1 Direccionamiento X-BUS 122
16.6.2 Actualiz. X-Bus 123
16.6.3 RECONFIGURACIÓN 124
16.6.4 TECLADOS / MÓDULOS DE EXPANSIÓN / CONTROLADORES DE PUERTA 124
16.6.4.1 Localizar 125
16.6.4.2 Supervisión 125
16.6.4.3 EDITAR TECLADOS 126
16.6.4.4 EDITAR MÓDULOS DE EXPANSIÓN 129
16.6.4.5 EDITAR CONTROLADORES DE PUERTAS 133
16.6.5 MODO DE DIRECCIONAMIENTO 134
16.6.6 Tipo X-bus 135
16.6.7 Recuper.bus 135
16.6.8 Temp.comunic. 136
16.7 VÍA RADIO 136
16.7.1 AÑADIR DETECTORES 137
16.7.2 EDITAR DETECTORES (ASIGNACIÓN DE ZONA) 137
16.7.3 AÑADIR PAT 137
16.7.4 EDITAR PAT 138
16.8 ZONAS 139
16.9 PUERTAS 139
16.9.1 PUERTAS 139

16.10 Salidas 143
16.10.1 Tipos de salida y puertos de salida 144
16.11 Comunicación 147
16.11.1 Puertos serie 148
16.11.2 Puertos Ethernet 148
16.11.3 Módems 149
16.11.3.1 Supervisión de la transmisión del interface de red. 149
16.11.3.2 Para configurar un módem 150
16.11.4 CRAs estandar 151
16.11.4.1 AÑADIR 151
16.11.4.2 Editar 151
16.11.4.3 Borrar 152
16.11.4.4 Llamad.test 152
16.11.5 MANTENIMIENTO REMOTO 152
16.12 TEST 153
16.12.1 Test sirena 153
16.12.2 TEST INTRUSIÓN 153
16.12.3 Estado zonas 154
16.12.4 Test salidas 155
16.12.5 En pruebas 155
16.12.6 Opciones audibles 156
16.12.7 Indic. visuales 156
16.12.8 Test PAT 156
16.12.9 Test sismico 157
16.13 Utilidades 157
16.14 Aislada 158
16.15 Reg.incidenc. 158
16.16 REGISTRO DE CONTROL DE ACCESOS 158
16.17 REGISTRO ALARMAS 159
16.18 CAMBIO CÓDIGO TÉCNICO 159
16.19 USUARIOS 159
16.19.1 AÑADIR 159
16.19.2 Editar 160
16.19.2.1 CONTROL DE ACCESOS 160
16.19.3 Borrar 163
16.20 PERFILES USUARIO 163
16.20.1 AÑADIR 163
16.20.2 Editar 163
16.20.3 Borrar 164
16.21 SMS 164
16.21.1 AÑADIR 165
16.21.2 Editar 165
16.21.3 Borrar 166
16.22 X-10 166
16.23 FECHA/HORA 166
16.24 TEXTO INSTALAD. 167

16.25 CONTROL PUERTA 167
17 Programación de técnico a través del navegador 168
17.1 Información del sistema 168
17.2 Interfaz Ethernet 169
17.3 Conexión a la central a través de USB 170
17.4 Inicio de sesión en el navegador 173
17.5 SPC Home 174
17.5.1 Resumen sistema 174
17.5.2 Información general de alarmas 174
17.5.3 Visualización de vídeos 175
17.6 Estado de la central 176
17.6.1 Estado 176
17.6.2 Estado de X-BUS 177
17.6.2.1 Estado mód.exp.E/S 177
17.6.2.2 Estado de la fuente de alimentación 179
17.6.2.3 Estado del teclado 181
17.6.2.4 Estado de controlador de puerta 183
17.6.3 Vía radio 184
17.6.3.1 Registro: detector vía radio X 186
17.6.4 Zonas 186
17.6.5 Puertas 188
17.6.6 Estado FlexC 189
17.6.7 Incidencias del sistema 190
17.7 Registros 191
17.7.1 Registro del sistema 191
17.7.2 Registro acceso 192
17.7.3 Registro PAT 192
17.7.4 REGISTRO ALARMAS 193
17.8 Usuarios 193
17.8.1 Añadir/editar un usuario 194
17.8.1.1 Dispositivos desconocidos 196
17.8.2 Añadir/Editar perfiles de usuario 196
17.8.3 Configuración de SMS 201
17.8.4 Comandos de SMS 202
17.8.5 Borrado de claves web 205
17.8.6 Ajustes de configuración de técnico 205
17.8.6.1 Cambio de código de técnico y de clave web 206
17.9 Configuración 208
17.9.1 Configuración de entradas y salidas del controlador 208
17.9.1.1 Edición de una entrada 208
17.9.1.2 Edición de una salida 209
17.9.1.3 Configuración de enclavamiento del sistema y salidas de armado automático 214
17.9.1.4 Configuración de X-10: ajustes 215
17.9.2 X-BUS 217
17.9.2.1 Módulos de expansión 217

17.9.2.2 Teclados 222
17.9.2.3 Controladores de puerta 226
17.9.2.4 Mapa de cableado 227
17.9.2.5 Configuración 228
17.9.3 Vía radio 229
17.9.3.1 Registro: detector vía radio X 230
17.9.3.2 Configuración de un PAT 230
17.9.3.3 Cambio de configuración vía radio 233
17.9.4 Cambio de configuración del sistema 234
17.9.4.1 Opciones 234
17.9.4.2 Temporizaciones 244
17.9.4.3 Identificación 246
17.9.4.4 Estándares 247
17.9.4.5 Reloj 249
17.9.4.6 Idioma 250
17.9.5 Configuración de zonas, puertas y particiones 250
17.9.5.1 Edición de una zona 251
17.9.5.2 Añadir/Editar una partición 251
17.9.5.3 Edición de una puerta 261
17.9.5.4 Añadir un grupo de particiones 266
17.9.6 Calendarios 267
17.9.6.1 Añadir/Editar un calendario 267
17.9.6.2 Armado/desarmado automático de particiones 269
17.9.6.3 Armado/desarmado automático de otras operaciones en la central 270
17.9.7 Cambio propio código 270
17.9.8 Configuración de ajustes avanzados 270
17.9.8.1 Fuentes 270
17.9.8.2 Actuaciones 272
17.9.8.3 Verificación de audio/vídeo 273
17.9.8.4 Actualización de licencias de SPC 276
17.10 Configuración de las comunicaciones 277
17.10.1 Configuración de comunicaciones 277
17.10.1.1 Configuración de los servicios de red de la central 277
17.10.1.2 Ethernet 278
17.10.1.3 Transmisores 279
17.10.1.4 Puertos serie 287
17.10.1.5 Registro en el portal SPC 288
17.10.2 FlexC® 289
17.10.2.1 Modo de Operación 290
17.10.2.2 Configuración de la ATP de inicio rápido para el ATS EN50136. 290
17.10.2.3 Configuración de un ATS EN50136-1 o ATS Personalizado 292
17.10.2.4 Exportación e importación de un ATS 301
17.10.2.5 Configuración de perfiles de incidencias 302
17.10.2.6 Configuración de perfiles de comando 307
17.10.3 Transmisión 309
17.10.3.1 CRAs 309

17.10.3.2 Configuración EDP 312
17.10.4 PC Tools 319
17.10.4.1 SPC Pro / SPC Safe 319
17.10.4.2 SPC Manager 320
17.10.4.3 Mantenimiento remoto 321
17.11 Operaciones con ficheros 322
17.11.1 Operaciones para la actualización de ficheros 322
17.11.1.1 Actualización de firmware 323
17.11.1.2 Actualización de idiomas 325
17.11.2 Operaciones de gestión de ficheros 327
17.12 Uso del Programador rápido 328
17.12.1 Conexión del programador rápido a la placa base 329
17.12.2 Instalación del Programador rápido en un PC 330
17.12.3 Operaciones con archivos del Programador rápido 330
17.12.3.1 Acceso al programador rápido mediante el teclado 330
17.12.3.2 Acceso al programador rápido mediante el navegador 331
18 Acceso al servidor web de forma remota 333
18.1 Conexión RTB 333
18.2 Conexión GSM 335
19 Funcionalidad de alarma de intrusión 338
19.1 Funcionamiento en modo Financiero 338
19.2 Funcionamiento en modo comercial 338
19.3 Funcionamiento en modo doméstico 339
19.4 Alarmas completa y local 339
20 Ejemplos y situaciones del sistema 341
20.1 Cuándo utilizar una partición común 341
21 Detectores sísmicos 343
21.1 Comprobación de detectores sísmicos 344
21.1.1 Proceso de comprobación manual y automática 344
21.1.2 Comprobación automática de detectores 345
21.1.3 Comprobación manual de detectores 346
22 Funcionamiento del cierre de bloqueo 348
22.1 Cierre de bloqueo 348
22.2 Armado autorizado del cierre de bloqueo 349
22.3 Elemento de bloqueo 350
23 Apéndice 352
23.1 Conexiones de cable de red 352
23.2 Los LED de estado del controlador 352
23.3 Alimentación de módulos de expansión desde los terminales de alimentación auxiliares 353
23.4 Cálculo de los requisitos de alimentación de la batería 354
23.5 Configuración por defecto de modos doméstico, comercial y financiero 357
23.6 Cableado de la interfaz X-10 358
23.7 Códigos SIA 358
23.8 Códigos CID 362

23.9 Información general de tipos de teclados 364
23.10 Combinaciones de PIN de usuario 365
23.11 Códigos de coacción 365
23.12 Anulaciones automáticas 365
23.12.1 Zonas 366
23.12.2 Códigos de acceso 366
23.12.3 Acceso de técnico 366
23.12.4 Cierre de sesión de usuario de teclado 366
23.13 Cableado del cable de alimentación al controlador 366
23.14 Controlador de mantenimiento 367
23.15 Fuente de alimentación inteligente para mantenimiento 367
23.16 Tipos de zona 368
23.17 Atributos de zona 372
23.18 Atributos aplicables a tipos de zona 374
23.19 Niveles y especificaciones de atenuación del STA 376
23.20 Lectores de tarjeta y formatos de tarjeta admitidos 376
23.21 Soporte de SPC para dispositivos E-Bus 378
23.21.1 Configuración y direccionamiento de dispositivos E-Bus 378
23.21.1.1 Direccionamiento de transpondedores para SAP 8, SAP 14 y SAP 20 380
23.21.1.2 Direccionamiento de transpondedores para fuente de alimentación SAP 25 381
23.22 Glosario FlexC 381
23.23 Comandos FlexC 383
23.24 Tiempos de categoría ATS 384
23.25 Tiempos categoría ATP 385

1 Significado de los símbolos

En el documento hay varios símbolos:

Símbolo	Descripción
~~SPC4xxx~~	No disponible para SPC42xx, SPC43xx.
IP	Sólo disponible para controlador SPC con interfaz IP (SPC43xx/SPC53xx/SPC63xx).
	No está disponible para instalación de tipo doméstica.
	Sólo disponible en modo sin restricción.
	En el texto encontrará más información sobre el grado de seguridad, la región o el modo.
	Para más información, consulte el Apéndice.

2 Seguridad

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 se deben montar e instalar.
Personal de inicio operativo	Con formación técnica apropiada respecto a las tareas y los productos, dispositivos o sistemas que se deben poner en funcionamiento.	Puesta en funcionamiento del dispositivo o sistema recién ensamblado e instalado.	Dispositivo nuevo y recién ensamblado e instalado, o dispositivo 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 cualquier norma o reglamento de seguridad específica de su país que tenga que ver con la planificación de proyectos, el manejo y la eliminación del producto.

Declaración de responsabilidad

- No conecte el dispositivo a la red de alimentación de 230 V si está dañado o 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 sólo piezas de recambio o accesorios aprobados por el fabricante.

2.2.2 Transporte

Daños en la unidad durante el transporte

- Guarde el material de embalaje para futuros transportes.

- No exponga el dispositivo a las vibraciones mecánicas o golpes.

2.2.3 Configuración

Interferencias de radio con otros dispositivos del entorno / compatibilidad electromagnética

- Cuando manipule módulos que sean vulnerables a las descargas electrostáticas, siga las directrices sobre descargas electrostáticas.

Daños producidos por una ubicación de montaje inadecuada

- Se deben respetar las condiciones ambientales recomendadas por el fabricante.
  Consulte los datos técnicos.
- 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 voltaje de alimentación.
- Asegúrese de que el dispositivo está conectado permanentemente al suministro eléctrico; se debe utilizar un dispositivo de desconexión de fácil acceso.
- Asegúrese de que el circuito al que está conectado el dispositivo esté protegido con un fusible de 16 A (máx.). No conecte dispositivos de otros sistemas a este fusible.
- Este dispositivo está diseñado para funcionar con sistemas de alimentación TN. No conecte el dispositivo a otros sistemas de alimentación.
- La toma de tierra debe cumplir las habituales normas y regulaciones de seguridad locales.
- Los cables de alimentación primarios y los cables secundarios se deben tender de manera que no transcurran en paralelo, ni cruzados, ni se toquen entre sí dentro de la carcasa.
- Los cables de teléfono se deben insertar en la unidad por separado de los demás cables.

Riesgo de daños en los cables por tensión mecánica.

- Asegúrese de que todos los cables y conductores que salen están lo suficientemente protegidos contra los tirones.

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.

Existe peligro de explosión o riesgo de quemaduras si la batería se instala incorrectamente

- Al instalar baterías nuevas, asegúrese de respetar la polaridad.

- Utilice exclusivamente baterías aprobadas por el fabricante (tipo: célula sellada regulada por válvula).
- No acorte las clavijas de la batería.
- No exponga la batería al fuego ni a temperaturas altas.
- No desmonte la batería.
- Deseche las baterías usadas según las normas locales.
- Asegúrese de insertar la batería correctamente y de asegurarla con la correa o clip que se suministra a tal efecto.

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.
- Desconecte siempre el cable de alimentación y otros cables de la red eléctrica antes de realizar el mantenimiento.

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.
Precaucion	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

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

3.1.1 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 Sede de la sociedad: Amsterdamer Str. 174, 50735 Köln (Alemania) Director: Robert Reinermann JörgWilms-Vahrenhorst (repres.)

Los productos SPC listados han sido comprobados conforme a la norma EN50131-3:2009, y todas las especificaciones RTC relevantes.

Tipo de producto	Estándar
● SPC6350.320 ● SPC6330.320 ● SPC5350.320 ● SPC5330.320 ● SPCP355.300 ● SPCP333.300 ● SPCE652.100 ● SPCK420.100 ● SPCK421.100	EN50131 Grado 3

● SPCE452.100 ● SPCE110.100 ● SPCE120.100 ● SPCA210.100 ● SPCK620.100 ● SPCK623.100 ● SPCN110.000 ● SPCN310.000	
● 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.

Requisitos de la norma EN50131	Manual de instalación y configuración de SPC
Temperatura de funcionamiento y rango de humedad	Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36]
Pesos y dimensiones	Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36]
Detalles para la fijación	Montaje del equipamiento del sistema [→ 41]
Instrucciones de instalación, puesta en funcionamiento y mantenimiento, incluyendo la identificación de los terminales	Montaje del equipamiento del sistema [→ 41] Hardware del controlador [→ 66]
Tipo de interconexiones (consulte el apartado 8.8);	Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36] Cableado de la interfaz X-Bus [→ 73]
Detalles de los métodos de armado y desarmado posibles (véanse apartados 11.7.1 a 11.7.3 y tablas 23 a 26);	Programación de usuario a través del teclado Armado/desarmado de particiones [→ 257] Configuración de un módulo de expansión de conmutador de llave [→ 220] Configuración de un mando vía radio [→ 111] Fuentes [→ 270]
Piezas reparables	Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36]
Requisitos de alimentación si no hay alimentación integrada	Consulte las instrucciones de instalación para fuentes de alimentación de los módulos de expansión SPCP33x y SPCP43x.

Requisitos de la norma EN50131	Manual de instalación y configuración de SPC
Si la alimentación está integrada, la información requerida por la norma EN 50131-6:2008, punto 6	Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36]
Número máximo de cada tipo de ACE y dispositivo de expansión.	Cableado de la interfaz X-Bus [→ 73] Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36]
Consumo de corriente del CIE y de cada tipo de ACE y dispositivo de expansión, con y sin condición de alarma.	Consulte las instrucciones de instalación correspondientes.
Corriente máxima admisible de cada salida eléctrica	Datos técnicos SPC4000 [→ 32] Datos técnicos SPC5000 [→ 34] Datos técnicos SPC6000 [→ 36]
Funciones programables disponibles	Programación de técnico a través del teclado [→ 114] Programación de técnico a través del navegador [→ 168]
Cómo se bloquea el acceso a las indicaciones para los usuarios del nivel 1 cuando el usuario de nivel 2, 3 o 4 ya no accede a la información (véase apartado 8.5.1).	Interfaz de usuario del teclado [→ 93] Configuración del teclado estándar [→ 126] Configuración del teclado confort [→ 127] Configuración de un módulo de expansión de indicador [→ 219]
Enmascaramiento/reducción de señales/mensajes de rango procesados como incidencias de "fallo" o "enmascaramiento" (véanse apartados 8.4.1 y 8.5.1, y tabla 11);	Opciones del sistema [→ 234] Cableado de entradas de zona [→ 85] Códigos SIA [→ 358] Siempre se informa del enmascaramiento PIR como una incidencia enmascarada de zona (SIA - ZM). Además, el antienmascaramiento puede provocar una alarma, una incidencia de tamper, un problema, o ninguna acción adicional dependiendo de la configuración. Configuraciones por defecto actuales del efecto de adición de PIR: **Irlanda** Desarmado - Ninguno Armado - Alarma **GB, Europa, Suecia, Suiza, Bélgica;** Desarmado - Tamper Armado - Alarma
Priorización de procesamiento e indicaciones de señal y de mensaje (véase 8.4.1.2, 8.5.3);	Pantalla de teclado estándar [→ 95] Pantalla de teclado confort [→ 99]
Número mínimo de variaciones de códigos PIN, teclas lógicas, teclas biométricas y/o teclas mecánicas para cada usuario (véase 8.3);	Combinaciones de PIN de usuario [→ 365]
Método de WD interno limitador de tiempo para acceso de nivel 3 sin autorización de nivel 2 (véase 8.3.1);	No se admite: el técnico no puede acceder al sistema sin permiso.
Número y detalles de códigos PIN deshabilitados (véase 8.3.2.2.1);	Anulaciones automáticas [→ 365]
Detalles de todos los métodos biométricos	No aplicable

Requisitos de la norma EN50131	Manual de instalación y configuración de SPC
de autorización utilizados (véase 8.3.2.2.3);	
Método empleado para determinar el número de combinaciones de códigos PIN, teclas lógicas, teclas biométricas y/o teclas mecánicas (véase 11.6);	Combinaciones de PIN de usuario [→ 365]
Número de entradas de código no válidas antes de que se deshabilite la interfaz de usuario (véase 8.3.2.4);	Códigos de acceso [→ 366]
Detalles de medios de autorización temporal para acceso de usuario (véase 8.3.2);	Menús de usuario - Acceso permitido
Si hay una configuración automática a horas previamente determinadas, detalles de indicación previa a la configuración y cualquier anulación automática de prevención de armado (véase 8.3.3, 8.3.3.1);	Armado/desarmado de particiones [→ 257]
Detalles de condiciones proporcionadas para el estado armado (véase 8.3.3.4);	Armado y desarmado del sistema Configuración de teclado estándar [→ 126] Configuración de teclado confort [→ 127] Salidas [→ 210] Tipos de zona [→ 368]
Notificación de señales o mensajes de salida disponibles (véase 8.6);	Salidas [→ 210] Armado/desarmado de particiones [→ 257] Derechos de usuario [→ 198]
Otras configuraciones de salida a interfaz con componentes I&HAS (véase 8.2);	Salidas [→ 210] Tipos de zona [→ 368] Test [→ 153] Interfaz de usuario del teclado [→ 93]
Criterios para eliminación automática de atributo "en pruebas" (véase 8.3.9);	Temporizaciones [→ 244]
Número de incidencias que provocan la anulación automática	Anulaciones automáticas [→ 365]
Si ACE es de tipo A o de tipo B (véase 8.7) y si es portátil o desplazable (véase 11.14);	Todos los dispositivos están cableados y alimentados por fuentes de alimentación del sistema. Consulte los datos técnicos relevantes sobre las fuentes de alimentación.
Datos de componente para componentes de memoria no volátil (véase tabla 30, paso 6);	Consulte la documentación de usuario de los teclados SPCK420/421 y SPCK620/623.
Tiempo de vida de la pila de soporte de memoria (véase 8.10.1);	N/A. Almacenado en memoria no volátil.
Funciones opcionales disponibles (véase 4.1);	Programación de técnico a través del teclado Programación de técnico a través del navegador [→ 168]
Funciones adicionales disponibles (véase 4.2, 8.1.8);	Grado - Modo libre Directrices – Opciones del sistema [→ 234]
Niveles de acceso requeridos para acceder a este tipo de funciones adicionales disponibles;	Configuración de usuario (teclado) [→ 160] Configuración de usuario (navegador) [→ 194]
Detalles de cualquier instalación programable que haría que un I&HAS no	Grado - Modo libre Directrices – Opciones del sistema [→ 234]

Requisitos de la norma EN50131	Manual de instalación y configuración de SPC
cumpliera la norma EN 50131-1:2006, 8.3.13, o la cumpliera con un grado de seguridad inferior, con instrucciones sobre la eliminación consecuente del sello de conformidad (véase 4.2 y 8.3.10).	Conformidad con la norma EN50131 [→ 19]

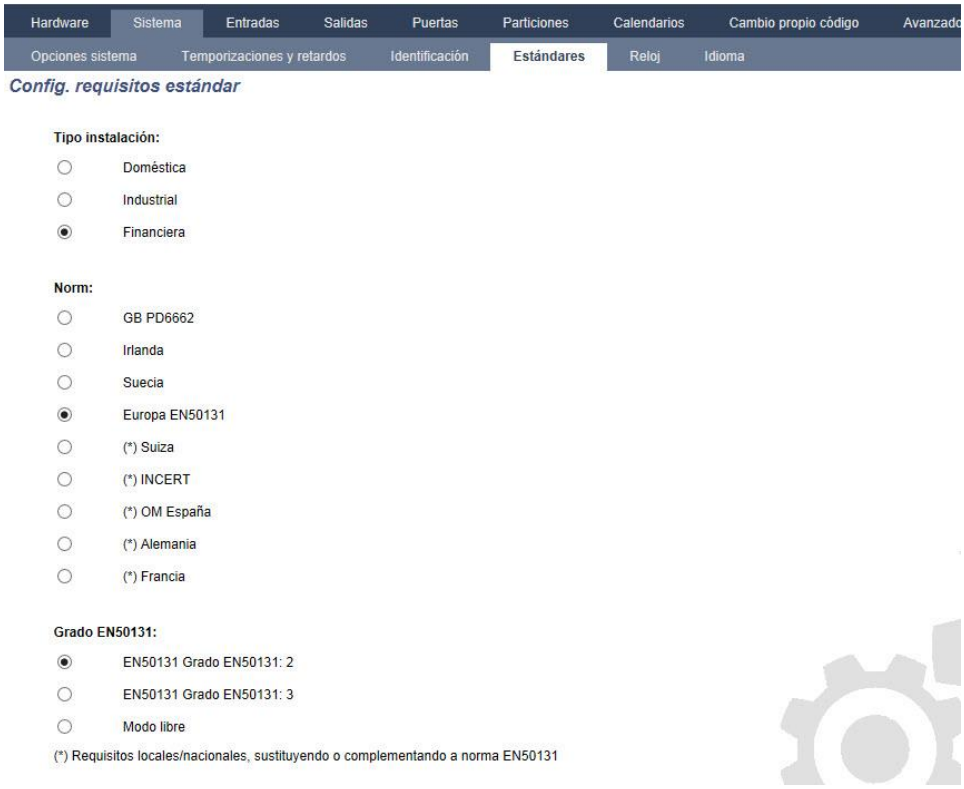
Los productos SPC listados han sido comprobados conforme a la norma EN50131-6, y todas las especificaciones RTC relevantes.

Product Type	Standard
● 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

3.1.2 Conformidad con las certificaciones EN50131

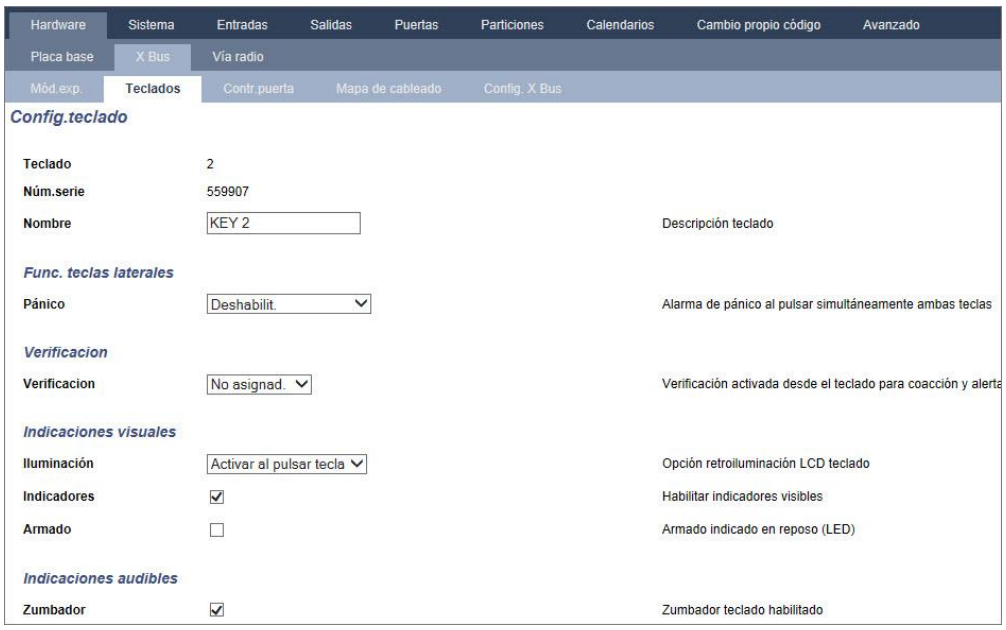
Requisitos de software

No es posible modificar el estándar ni el grado en SPC Pro. Estos ajustes solo se pueden modificar en el navegador o en el teclado.



- 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 conformidad con la norma EN50131.
- La función del vía radio "**Prevenir tiempo de armado**" debe fijarse a un valor superior a 0 e inferior a 20.
- La función del vía radio "**Tiempo dispositivo perdido**" debe fijarse a un valor inferior a 120.
- La **Configuración X-BUS**, **Reintentos**, debe fijarse a un valor de 10.
- La **Configuración X-BUS**, **Temporizador de Comunicaciones**, debe fijarse a un valor de 5.
- Seleccione **Hora de sincronización con red eléctrica** en la configuración del **reloj** para utilizar la red eléctrica como maestro para el reloj.

- NO seleccione el atributo **Estado config.** en los ajustes de configuración del **teclado** para **Indicaciones visuales**.



Requisitos de hardware

- El kit de tamper trasero (SPCY130) debe estar instalado para que las centrales y las fuentes de alimentación cumplan co

n la norma EN50131 Grado 3.

- Los componentes conformes con la norma EN50131 Grado 3 se deben instalar en sistemas que cumplan con la norma EN50131 Grado 3.
- Para los sistemas conformes con la norma EN50131 Grado 2 se deben instalar componentes que cumplan con la norma EN50131 Grado 2 ó 3.
- 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).

	AVISO
	El módulo RTB del SPCN110 y el módulo GSM/GPRS del SPCN130 se comprueban con centrales aprobadas por la norma EN50131 Grado 2 y Grado3 y se puedan utilizar con estas centrales aprobadas.

3.1.3 Conformidad con las certificaciones EN 50136-1:2012 y

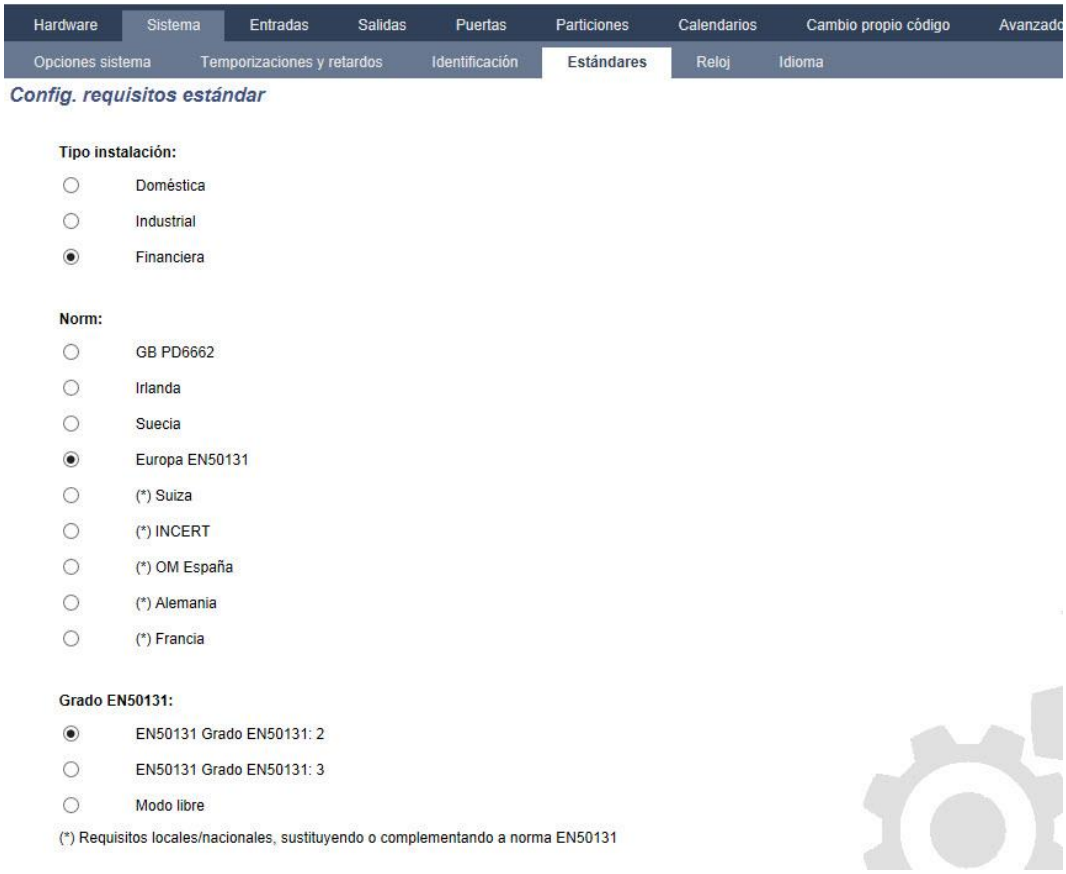
EN 50136-2:2014

Los productos SPC listados han sido comprobados conforme a la norma EN 50136-1:2012 y EN 50136-2:2014.

3.1.4 Conformidad con normas INCERT.

Requisitos de software

Si se selecciona Bélgica (*) en **Región**, se implementarán los requisitos locales o nacionales que sustituyen a los de la norma EN50131.



Si se selecciona **Grado 2** o **Grado 3**, se seleccionará la conformidad con la norma EN50131 más cualquier requisito adicional de la norma INCERT:

- Solo un técnico puede restaurar un tamper. Para INCERT, esto es aplicable en todos los grados.
  Normalmente, este requisito solo es aplicable al Grado 3 de la norma EN50131.
- Un tamper en una zona inhibida/aislada se debe enviar a la CRA y mostrarse al usuario.
  Para INCERT, los tampers se procesan para zonas aisladas. En todas las demás variaciones de la norma, los tampers se ignoran en zonas aisladas.
- Los códigos PIN de usuario se deben definir con más de 4 dígitos.

Requisitos de hardware

- La capacidad mínima de una batería para el sistema SPC42xx/43xx/52xx/53xx/63xx es de 10 Ah / 12 V. Si se usa una batería de 10 Ah, ésta se polariza hacia la izquierda de la caja y la aleta del fondo se dobla para que se ajuste a la batería.

- Fije el puente (J12) en el selector de batería para su uso con una batería de 17/10 Ah y elimine el de batería de 7 Ah.
- La cantidad de corriente de la salida auxiliar utilizando una batería de 10 Ah para el SPC42xx/SPC52xx es:

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

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

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

3.1.5 Directrices de conformidad con PD 6662:2010

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

3.1.5.1 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
Controlador de grado 3 SPC5330.320-L1
Controlador de grado 3 SPC5350.320-L1
Controlador de grado 3 SPC6330.320-L1
Controlador de grado 3 SPC6350.320-L1
Teclado LCD SPCK420/421.100
Módulo de expansión SPCE452.100, 8 salidas de relé
Módulo de expansión SPCE652.100, 8 entradas / 2 salidas,
Fuente de alimentación inteligente SPCP332.300 con módulo de expansión de E/S
Fuente de alimentación (FA) SPCP355.300 con módulo de expansión
Fuente de alimentación inteligente SPCP333.300 con módulo de expansión de E/S
Módulo RTB SPCN110.000
Módulo GSM SPCN310.000

3.1.5.2 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 4737-3.1:1977
BS EN 50136-1-5:2008
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

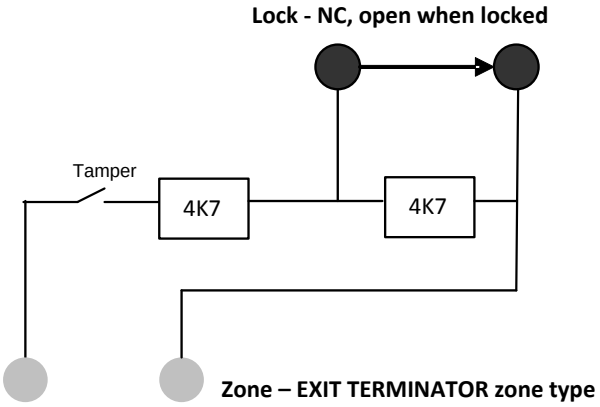
3.1.5.3 Métodos para completar el armado y desarmado

3.1.4.3.1 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 ligada 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 la siguiente sección de este manual:

Tipos de zona [→ 368]

b) Pulse el botón interruptor situado 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 la siguiente sección de este manual:

Tipos de zona [→ 368]

c) Interruptor de protección (p. ej. contacto de puerta) instalado en la puerta de salida final de las instalaciones o la partición supervisada

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 la siguiente sección de este manual:

Tipos de zona [→ 368]

Atributos de zona [→ 372]

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

Consulte la siguiente sección de este manual:

OPCIONES [→ 115] (Teclado)

Opciones [→ 234] (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.

3.1.4.3.2 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 La 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 de proximidad (p. ej. un 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 de proximidad (p. ej. un SPCK421) cerca de la puerta de entrada a unas instalaciones.

Consulte las siguientes secciones de este manual:

- Tipos de zona [→ 368]
- Atributos de zona [→ 372]

	⚠ 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 funciones en un sistema desarmado durante un período temporizado de p. ej. 30 segundos.

Consulte las siguientes secciones de este manual:

Temporizaciones [→ 118]

3.1.5.4 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 de este manual:

PARTICIONES [→ 121]

Añadir/Editar una partición [→ 251]

Temporizaciones [→ 118]

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 de este manual:

Añadir/Editar una CRA [→ 309]

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 de este manual:

SALIDAS [→ 143] (Teclado)

Configuración de entradas y salidas del controlador [→ 208] (Navegador)

Añadir/Editar una CRA [→ 309]

Intentos de retransmisión

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

Añadir/Editar una CRA [→ 309]

Edición de la configuración de EDP [→ 318]

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

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

Armados y desarmados

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 de este manual:

Temporizaciones [→ 118]

Atributos de zona [→ 372]

SALIDAS [→ 143] (Teclado)

Edición de una salida [→ 209] (Navegador)

Alarma de intrusión y de atraco confirmado (BS8243:2010 designación de señales de alarma de atraco (HUA) para la 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 una incidencia 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.

Seguridad de comunicaciones para soporte remoto y comprobaciones remotas del sistema (DD 263:2010)

Compruebe que SPC Pro se utiliza conforme a las directrices especificadas en DD 263:2010.

3.1.5.5 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.

3.1.5.6 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 máximos	M0 - M4
Tiempo de transmisión	T3 como máx.
Disponibilidad	Consulte la siguiente sección de este manual: Niveles y especificaciones de atenuación del STA [→ 376]
Nivel de seguridad de señalización	Comprobado según norma EN50136-1-1 y clasificado como "S0".

3.1.6 Cumplimiento de las normas VdS

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

This installation document encompasses the required product installation information for the following VDS Certificates:

G112104, G112124, EN-ST000055, EN-ST000056, EN-ST000057, EN-ST000058, GXXXXXX, GXXXXXX, EN-STXXXXXX, EN-STXXXXXX, EN-STXXXXXX, EN-STXXXXXX.

Software

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

1. Inicie sesión en la central con el navegador.
2. Haga clic en Modo técnico.
3. Haga clic en Configuración en el menú.
4. Haga clic en Estándares.
5. Seleccione Alemania en la lista de regiones.
6. Seleccione el grado VdS requerido por su tipo de instalación.

- Aislamientos remotos: no es posible desaislar los fallos aislados con el navegador ni con SPCPro. El desaislamiento solo se puede realizar en los teclados.
- Conexiones remotas: no es posible utilizar el navegador o SPCPro para conectar a un sistema armado.
- Alarmas confirmadas: un sistema armado internamente no puede crear una alarma confirmada.

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

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

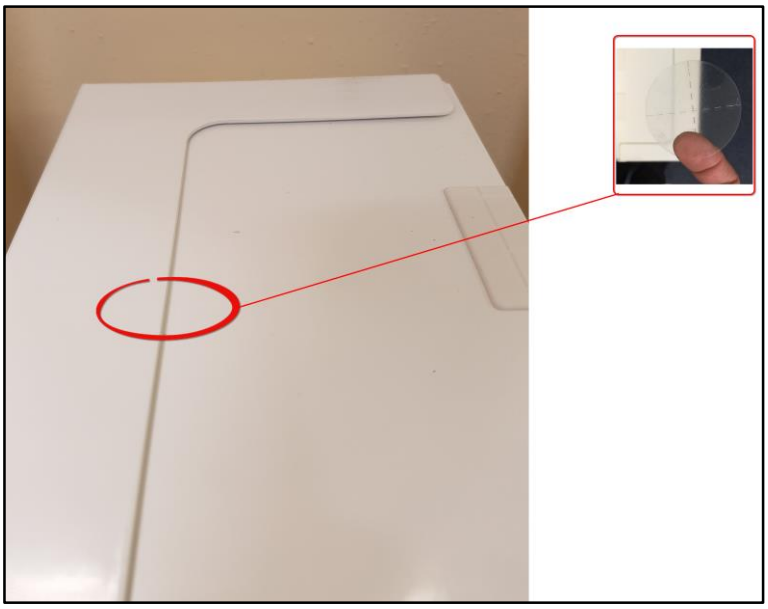
Hardware

El cumplimiento de la norma 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 (en punta)
- Las siguientes combinaciones de RFL no cumplen las normas VdS:
  - 1 k, 470 ohmios
  - 1 k, 1 k, 6k6 ohmios

3.1.7 Cumplimiento de las normas NF

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



Para cumplir con los requisitos de NF&A2P, la caja debe ser precintada tras su instalación con la etiqueta de tamper adjunta.

Los productos SPC listados han sido comprobados conforme a la norma NF324 - H58, con referencia a las certificaciones EN actuales, véase Conformidad con las certificaciones EN50131 [➔ 19] y todas las especificaciones RTC relevantes.

Tipo de producto	Configuración	Estándar	Logo
SPC6350.320 + SPCP355.300 (Cert. XXXXXXXXXX)	60h, sin supervisión	NF Grado 3, Clase 1	
SPC5350.320 + SPCP355.300 (Cert. XXXXXXXXXX)	60h, sin supervisión		
SPC6350.320 (Cert. XXXXXXXXXX)	60h, sin supervisión		
SPC5350.320 (Cert. XXXXXXXXXX)	60h, sin supervisión		
SPC6330.320 + SPCP333.300 (Cert. 1232200003)	60h, sin supervisión	NF Grado 3, Clase 1	
SPC5330.320 + SPCP333.300 (Cert. 1232200003)	60h, sin supervisión		
SPC6330.320 (Cert. 1232200003)	30h, supervisado		
SPC5330.320 (Cert. 1232200003)	30h, supervisado		
SPC5320.320 (Cert. 1222200003)	36h, sin supervisión	NF Grado 2, Clase 1	
SPC4320.320 (Cert. 1222200003)	36h, sin supervisión		
SPCN110.000 SPCN310.000 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF Grado 2 y 3, Clase 1	

4 Datos técnicos

4.1 SPC4000

Particiones programables	4
Número máx. de códigos de usuario	100
Controles remotos	Hasta 32
Dispositivos PACE	32
Alarma de pánico vía radio	Hasta 128
Memoria de incidencias	1.000 incidencias de intrusión, 1.000 incidencias de acceso
Número de zonas incorporadas	8
Número máx. de zonas cableadas	32
Número máx. de zonas vía radio	32 (restar zonas cableadas)
Número máx. 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 (868 MHz) ● 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	Grabación de audio hasta 60 segundos antes / 60 segundos después de la incidencia
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) ● 1 programador rápido SPC ● SPC43xx: Adicionalmente 1 Ethernet (RJ45)
Contacto de tamper	Tamper con muelle frontal, 2 entradas auxiliares de

	contacto de tamper
Suministro eléctrico	Tipo A (por EN50131-1)
Voltaje de red	230 V CA, +10 %/ -15 %, 50 Hz
Fusible de red	250 mA T (pieza reemplazable en bloque de terminales de red)
Consumo de energía	SPC42xx: Máx. 160 mA a 230 V CA SPC43xx: Máx. 200 mA a 230 V CA
Corriente de funcionamiento	Controlador SPC42xx: Máx. 160 mA a 12 V CC Controlador SPC43xx: Máx. 200 mA a 12 V 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 (red conectada y batería totalmente cargada), mín. 10,5 V CC cuando ha sido encendida por dispositivo secundario (antes de cerrarse el sistema como protección contra la 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. 750 mA a 12 V CC
Tipo de batería	SPC422x/4320: YUASA NP7-12FR (7 Ah), batería no incluida
Cargador de batería	SPC422x/4320: Máx. 72 h para el 80 % de capacidad de la batería
Protección de la batería	Corriente limitada a 1 A (protegida por fusible), protección contra descarga mínima a 10,5 V 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 funcionamiento	-10 ~ +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 mm x 82 mm)
Coeficiente IP	30

1) Máx. 400 m entre dispositivos / tipos de cable IYSTY 2 x 2 x Ø 0,6 mm (mín.), UTP cat5 (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
Número máx. de códigos de usuario	500
Controles remotos	Hasta 100
Dispositivos PACE	250
Alarma de pánico vía radio	Hasta 128
Memoria de incidencias	10.000 incidencias de intrusión, 10.000 incidencias de acceso
Número de zonas incorporadas	● SPC5320\5330 — 8 ● SPC5350 — 16
Número máx. de zonas cableadas	128
Número máx. de zonas vía radio	120 (restar zonas cableadas)
Número máx. 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 (intercambiables de polo único, 30 V CC / máx. 1 A corriente de conmutación resistiva)
Salidas electrónicas	● SPC5320\5330 — 5 salidas: – 2 sirenas internas/externas – 3 programables. Máximo 400 mA 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	Grabación de audio hasta 60 segundos antes / 60 segundos después de la incidencia
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 o 1 lazo), ● 2 RS232 ● 1 USB (conexión a PC), ● 1 programador rápido SPC, ● 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/posterior
Suministro eléctrico	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. 200 mA a 230 V CA ● SPC5350: Máx. 500 mA a 230 V CA
Corriente de funcionamiento	● SPC5320/5330: Controlador: Máx. 200 mA a 12 V CC ● SPC5350: Máx. 210 mA a 12 V 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 (red conectada y batería totalmente cargada), mín. 10,5 V CC cuando ha sido encendida por dispositivo secundario (antes de cerrarse el sistema como protección contra la 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. 750 mA a 12 V CC ● SPC5350: Máx. 2200 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 (12V 27Ah) 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 funcionamiento	-10 ~ +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 mm x 82 mm) ● SPC5350: 4 módulos de expansión adicionales (150 x 82 mm)
Coeficiente IP / IK	30 / 06

1) Máx. 400 m entre dispositivos / tipos de cable IYSTY 2 x 2 x Ø 0,6 mm (mín.), UTP cat5 (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
Número máx. de códigos de usuario	2500
Controles remotos	Hasta 100
Dispositivos PACE	250
Alarma de pánico vía radio	Hasta 128
Memoria de incidencias	10.000 incidencias de intrusión, 10.000 incidencias de acceso
Número de zonas incorporadas	● SPC6320\6330 — 8 ● SPC6350 — 16
Número máx. de zonas cableadas	512

Número máx. de zonas vía radio	120 (restar zonas cableadas)
Número máx. 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 (intercambiables de polo único, 30 V CC / máx. 1 A corriente de conmutación resistiva)
Salidas electrónicas	● SP6320\6330 — 5 salidas: – 2 sirenas internas/externas – 3 programables. Máximo 400 mA 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	Grabación de audio hasta 60 segundos antes / 60 segundos después de la incidencia
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 o 1 lazo), ● 2 RS232 ● 1 USB (conexión a PC), ● 1 programador rápido SPC, ● 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/posterior
Suministro eléctrico	Tipo A (por EN50131-1)
Voltaje de red	230 V CA, + 10%/ -15% / 50 Hz
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. 200 mA a 230 V CA ● SPC6350: Máx. 500 mA a 230 V CA
Corriente de funcionamiento	● SPC6330: Máx. 200 mA a 12 V CC ● SPC6350: Máx. 210 mA a 12 V 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 (red conectada y batería totalmente cargada), mín. 10,5 V CC cuando ha sido encendida por dispositivo secundario (antes de cerrarse el sistema como protección contra descarga mínima de batería) ● SPC6350: 13-14 V CC en condiciones normales (red conectada y batería totalmente cargada), mín. 10,5 V CC cuando ha sido encendida por 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. 750 mA a 12 V CC ● SPC6350: Máx. 2200 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 (12V 27Ah) 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 funcionamiento	-10 ~ +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 mm x 82 mm) ● SPC6350: 6 módulos de expansión adicionales (150 mm x 82 mm) o 1 controlador adicional + 4 módulos de expansión
Coeficiente IP / IK	30 / 06

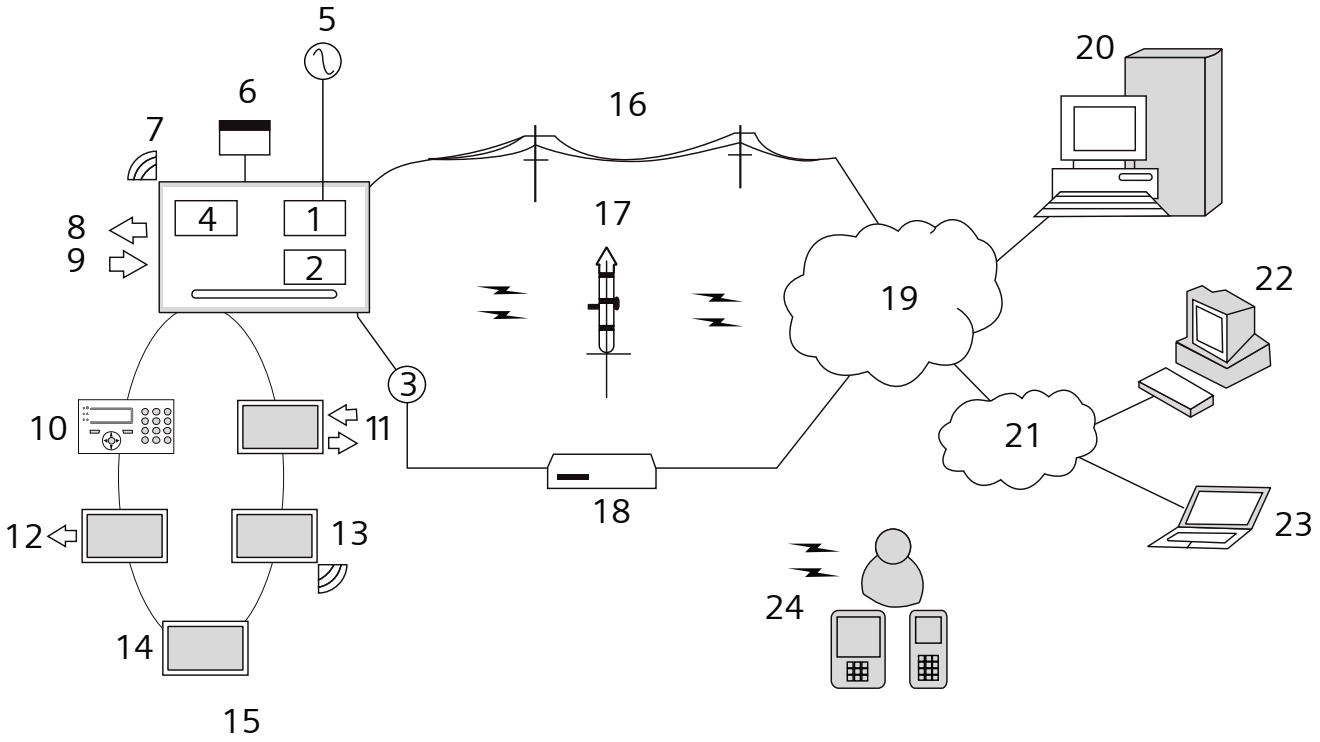
1) Máx. 400 m entre dispositivos / tipos de cable IYSTY 2 x 2 x Ø 0,6 mm (mín.), UTP cat5 (núcleo sólido) o Belden 9829.

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.

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 relacionar los componentes funcionales (RTB/GSM/RF), mejorando la capacidad del sistema. Gracias a este enfoque, un instalador puede garantizar una instalación eficaz con el cableado mínimo.



Visión general

1	RTB	13	Módulo de expansión vía radio
2	GSM	14	F.A.
3	Ethernet	15	Configuración en lazo
4	Receptor vía radio	16	Red RTB
5	Toma de CA general	17	Red GSM
6	Batería de 12 V	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 del equipamiento del sistema

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.

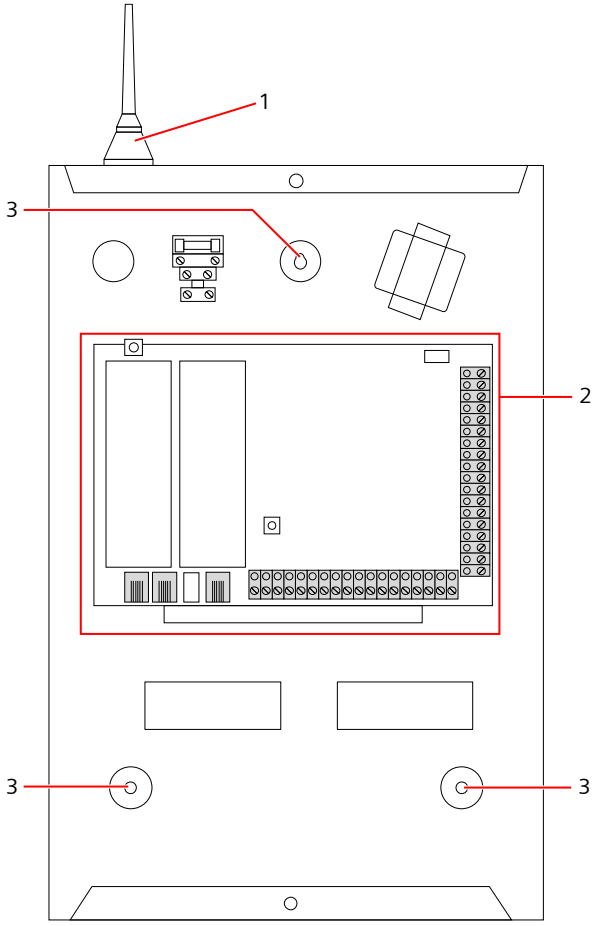
Para abrir la carcasa, retire ambos tornillos con el destornillador adecuado y levante la cubierta directamente desde la base.

La carcasa G2 incluye la **P**laca de **C**ircuito **I**mpreso (PCI) 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 de 7 Ah (máx.) bajo el 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 mural 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 del bastidor. 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.



Carcasa estándar

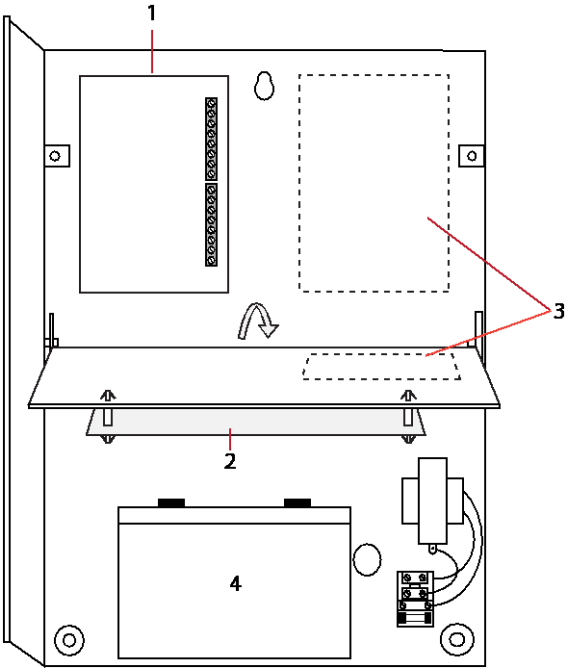
1	Antena vía radio
2	Controlador SPC
3	Orificios de los tornillos para el montaje mural

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.



1 Módulos de expansión / fuente de alimentación

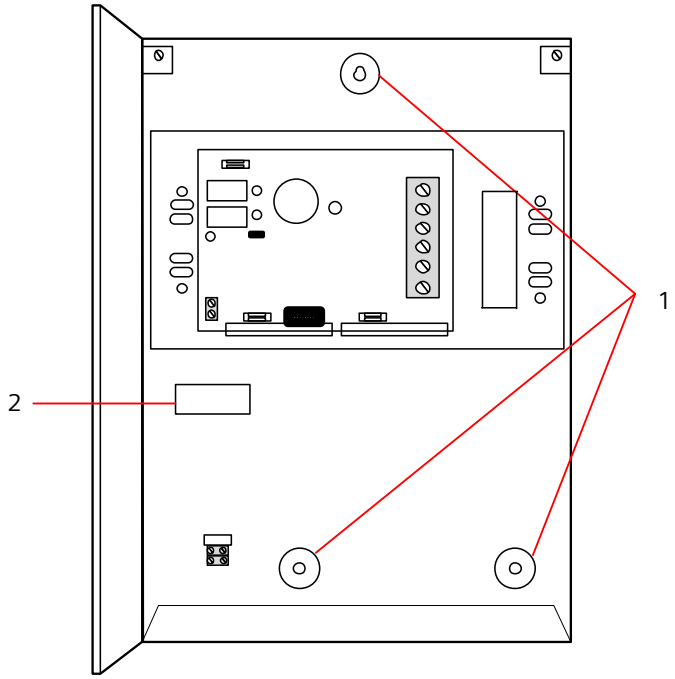
2 Controlador

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 mural de la unidad (véase elemento 1 en la siguiente figura).



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 del bastidor.
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 del kit de tamper trasero

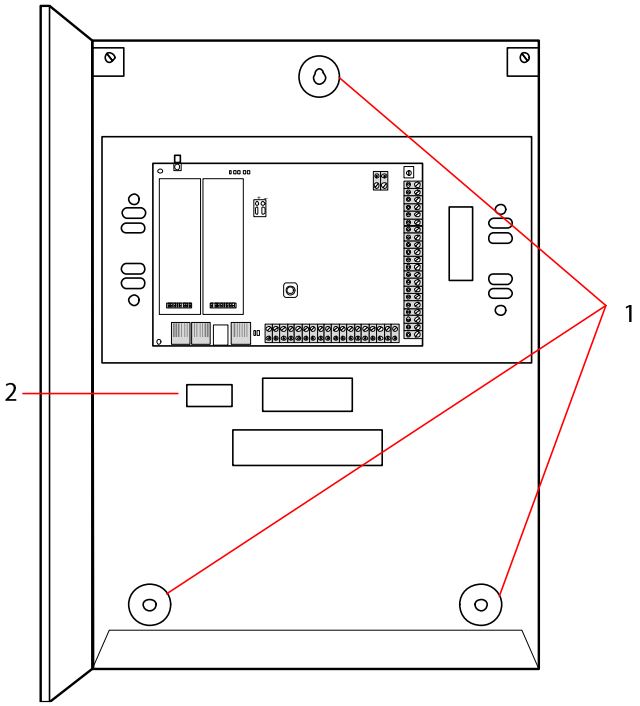
El kit de tamper trasero del SPC proporciona a las centrales SPC y a las fuentes de alimentación la opción de disponer tanto de tamper trasero como de tamper delantero.

El kit de tamper trasero se compone de las siguientes piezas:

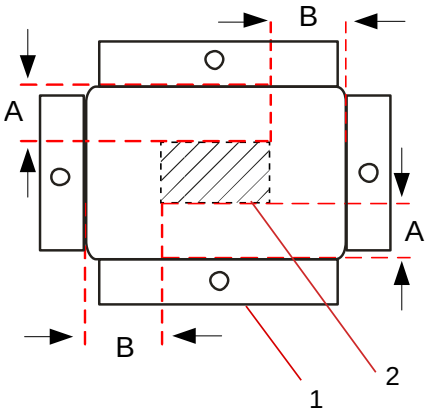
- Interruptor de tamper
- Conductores para conectar el interruptor de tamper trasero al controlador
- Placa de fijación a la pared

Montaje de la placa de fijación a la pared

1. Monte el SPC en la pared, en la posición adecuada, mediante las tres fijaciones (véase elemento 1 en la siguiente figura).



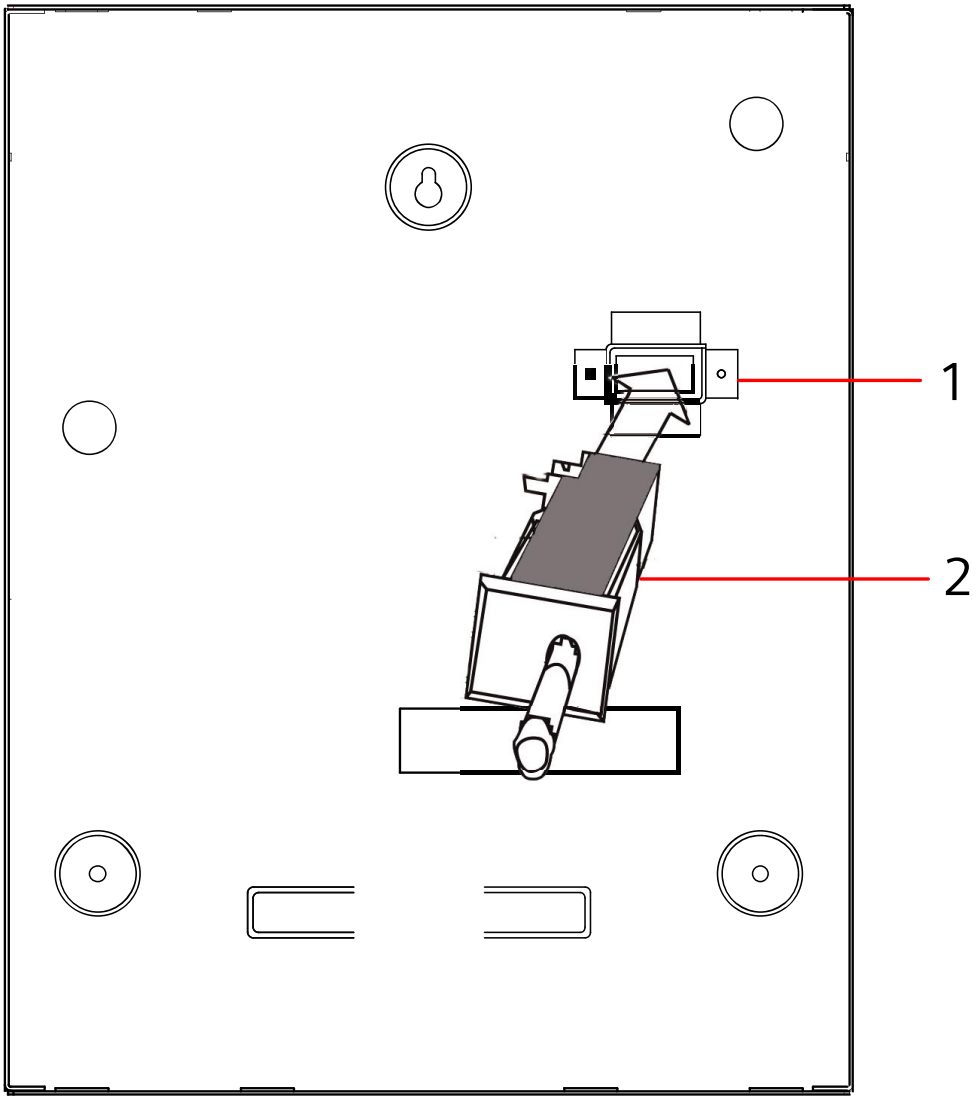
2. Dibuje una línea alrededor del interior de la sección prevista para el tamper trasero (véase elemento 2 en la figura anterior). Esta línea servirá de guía para colocar la placa de pared. Retire la caja de la pared.
3. Coloque la placa de pared (véase elemento 1 en la siguiente figura) en la pared, centrándola exactamente alrededor del rectángulo previamente dibujado (véase elemento 2 en la siguiente figura).



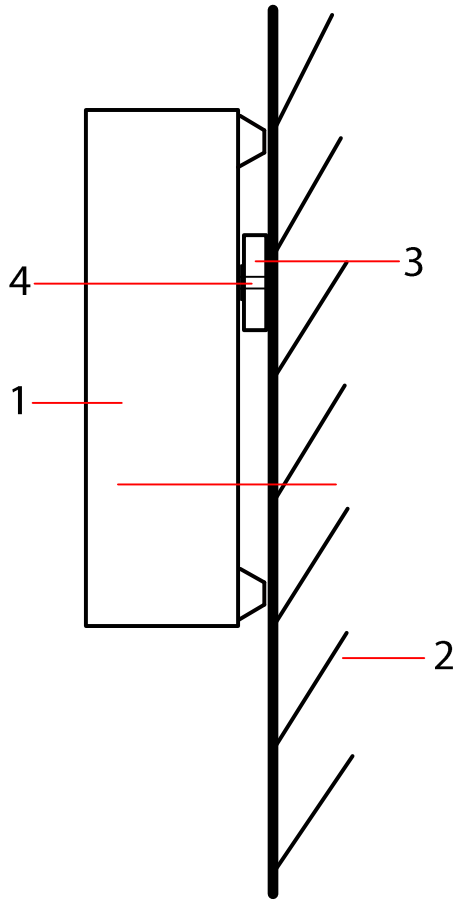
4. Asegúrese de que los cuatro apoyos en la placa de la pared queden a ras con la pared.
5. Marque las cuatro fijaciones sobre la placa de la pared.
6. Taladre y utilice tornillos adecuados (máx. 4 mm) para la superficie de la pared.
7. Fije la placa a la pared.

Fijación del interruptor de tamper trasero

1. Inserte el interruptor de tamper (véase elemento 2 en la siguiente figura) en la parte trasera de la caja de modo que el émbolo quede mirando hacia fuera (véase elemento 1 en la siguiente figura).



2. Fije la parte trasera de la caja sobre la pared utilizando las tres fijaciones retiradas anteriormente (véase elemento 2 en la siguiente figura). Compruebe visualmente que la placa de la pared y la estructura metálica de la carcasa quedan a ras.



1 Carcasa

2 En pared

3 Placa de fijación a la pared

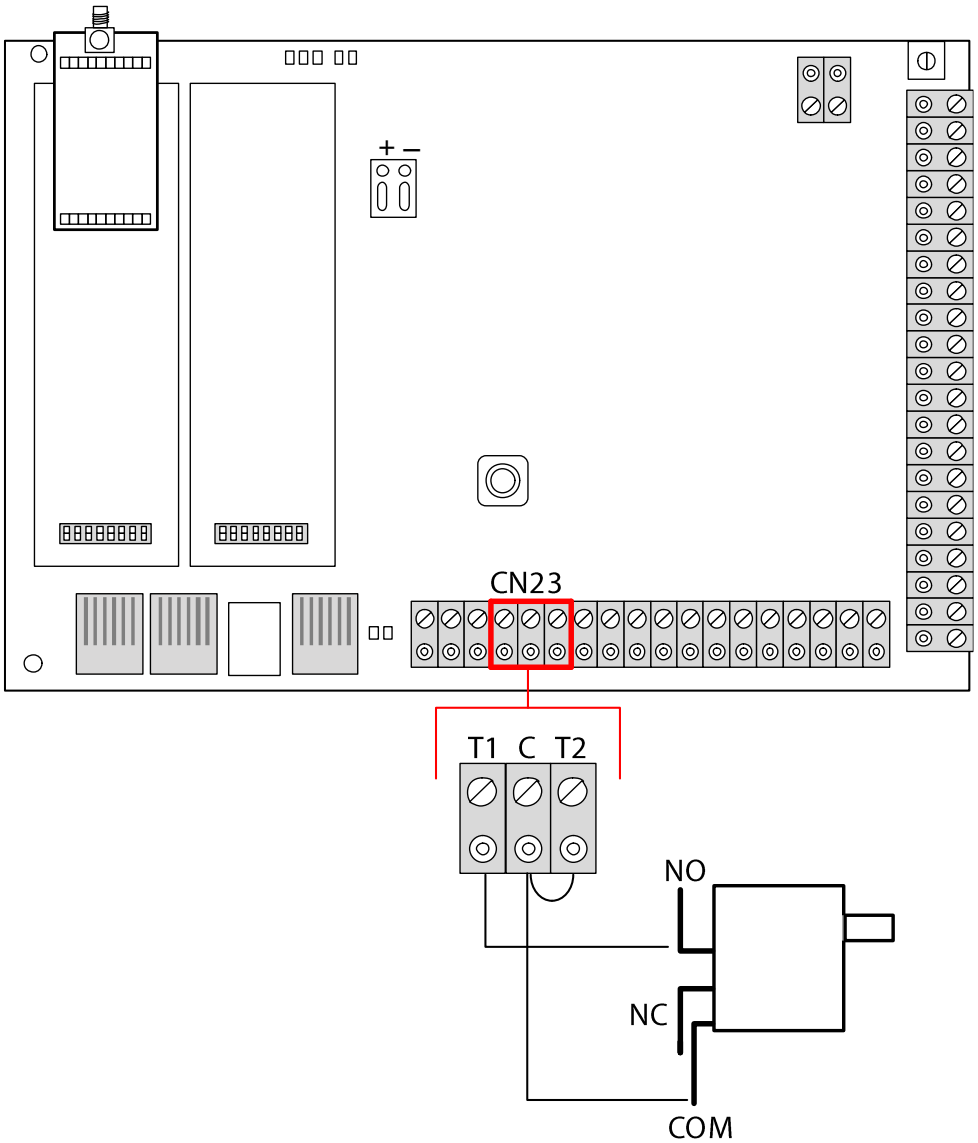
4 Interruptor de tamper

	⚠ ADVERTENCIA
	Si la placa de fijación a la pared no está alineada exactamente, la carcasa no quedará asentada correctamente en sus fijaciones.

Cableado del interruptor de tamper trasero a la central

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

El sistema se referirá a 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 que no se ha retirado el jumper T2.
3. Una vez cableado el interruptor de tamper, el controlador se puede poner en funcionamiento normalmente.

6.2.2 Instalación de la batería de conformidad con EN50131

Para cumplir con los estándares EN50131, la batería se debe mantener sujeta dentro de la carcasa para evitar que se mueva. Esto se consigue doblando hacia el exterior las aletas de la parte trasera de la carcasa con bisagras, de tal forma que la batería queda retenida.

Si se usa una batería de 7 Ah, ésta se polariza hacia la izquierda de la caja y la aleta del fondo se dobla para que se ajuste a la batería.

Si se usa una batería de 17 Ah, ésta se polariza hacia la derecha de la caja y la aleta central se dobla para que se ajuste a la batería.

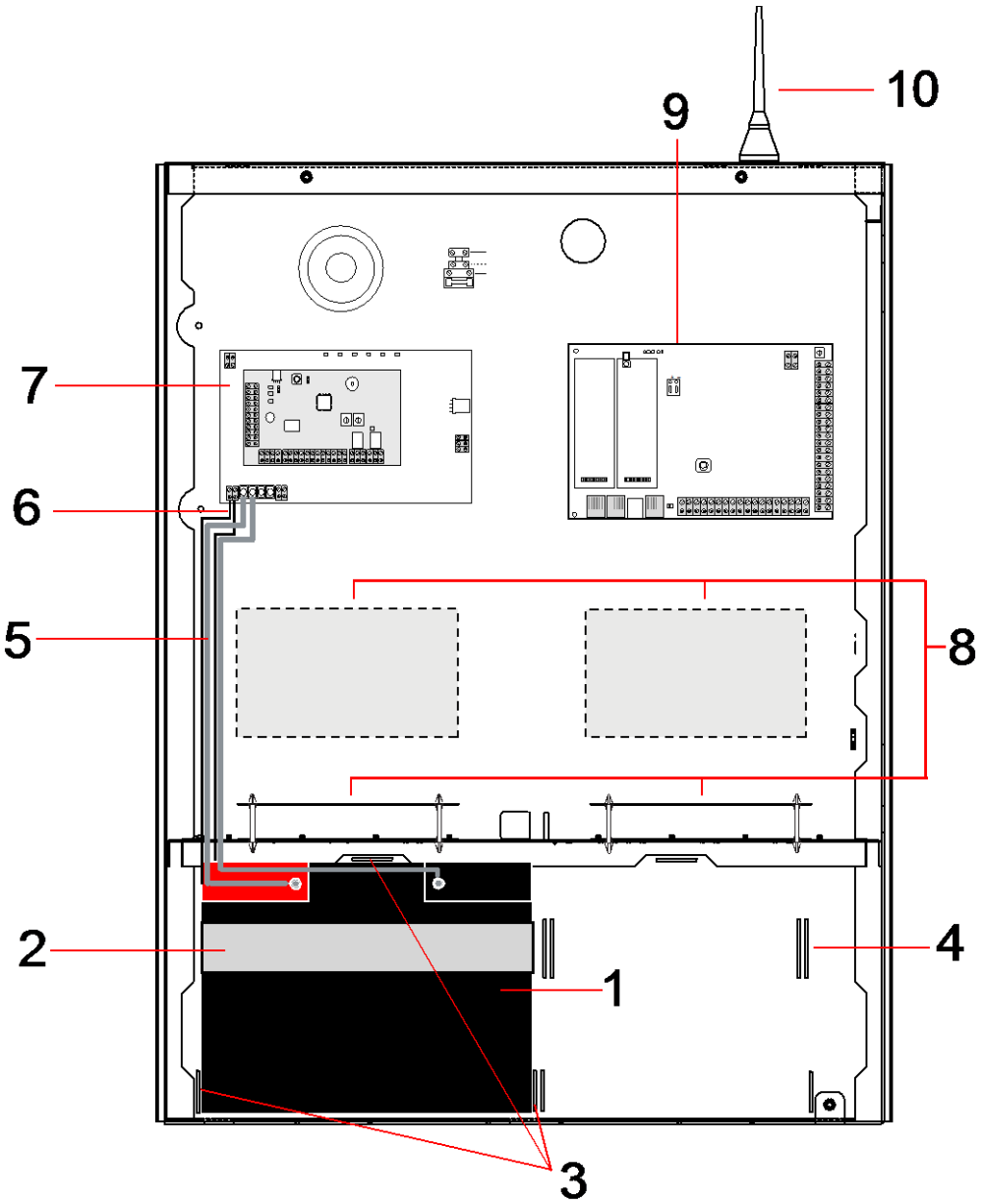
Las aletas de la batería se deben doblar con cuidado para no dañar la batería. Si existe algún indicio de daños en la batería o alguna fuga del electrolito, la batería se deberá desechar, conforme a las regulaciones actuales, debiéndose colocar una nueva.

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 **P**laca de **C**ircuito **I**mpreso (PCI) del controlador y la fuente de alimentación inteligente SPCP355, 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 extra 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.



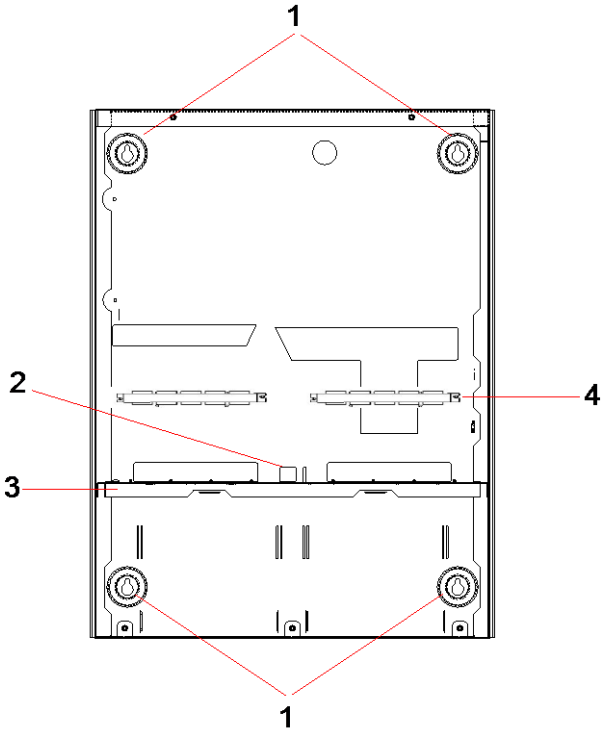
Número	Descripción	Número	Descripción
1	Batería	6	Conductores de temperatura de la batería
2	Correa para la batería	7	F.A.
3	Lengüetas de fijación	8	Posiciones para módulos de expansión opcionales
4	Orificios para la correa	9	Controlador
5	Conductores de la batería	10	Antena

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.

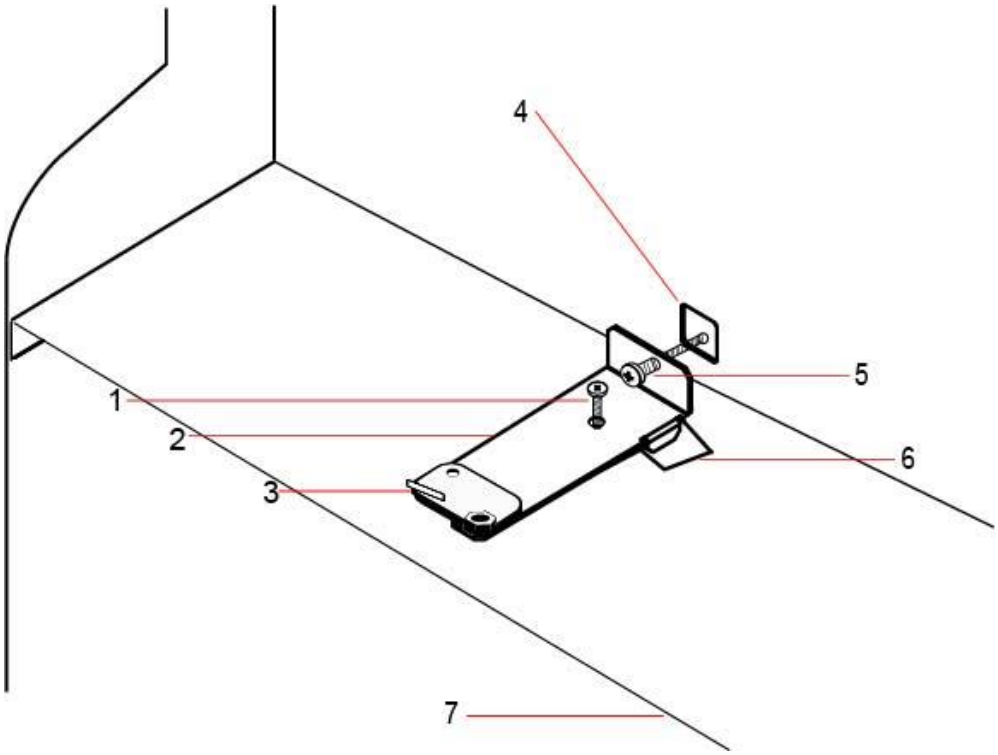
El soporte de tamper queda fijado firmemente a su sitio mediante un tornillo de fijación. Recuerde retirar este tornillo si el sistema se pone en servicio con protección de tamper trasero. No retire este tornillo si se utiliza únicamente el tamper frontal.

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 (véase 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 1 mm para activar el interruptor de tamper.

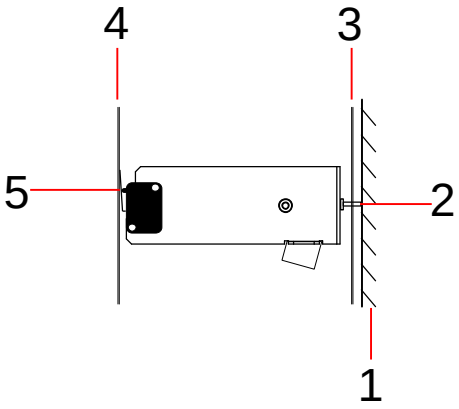


Número	Descripción	Número	Descripción
1	Tornillo de fijación de tamper frontal	5	Tornillo de tamper trasero
2	Soporte de tamper	6	Ranura de orientación
3	Interruptor de tamper	7	Estante de separación del compartimento de la batería
4	Abertura para el tamper trasero		

	⚠ 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



1 Pared

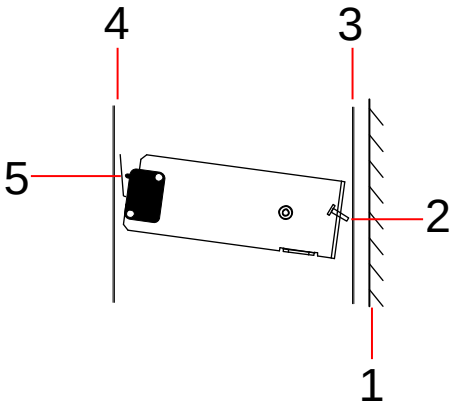
2 Tornillo de tamper trasero

3 Pared trasera de la carcasa

4 Tapa de la carcasa

5 Contacto del interruptor de tamper cerrado

Interruptor de tamper – desplazado



1 Pared

2 Tornillo de tamper trasero

3 Pared trasera de la carcasa

4 Tapa de la carcasa

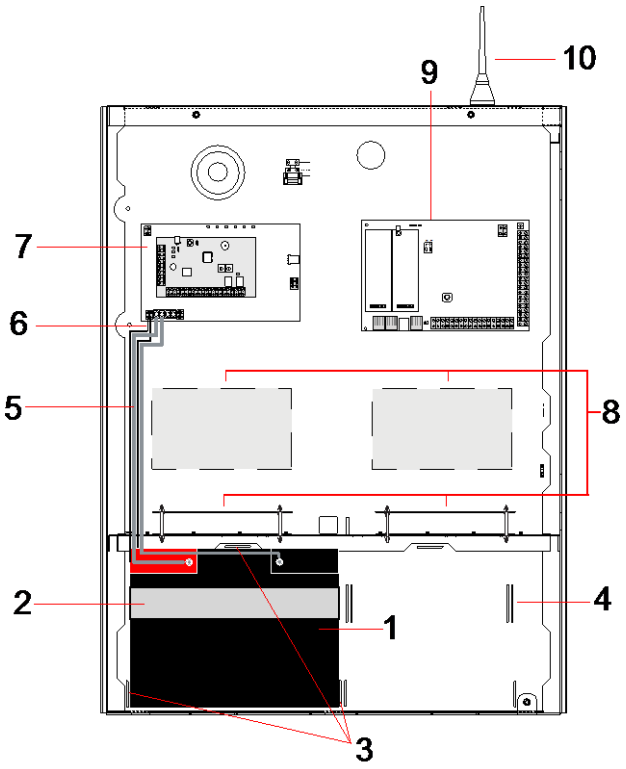
5 Contacto del interruptor de tamper abierto

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

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



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

	⚠ ATENCIÓN
	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.

6.5 Montaje de un módulo de expansión

Consulte las instrucciones de instalación correspondientes.

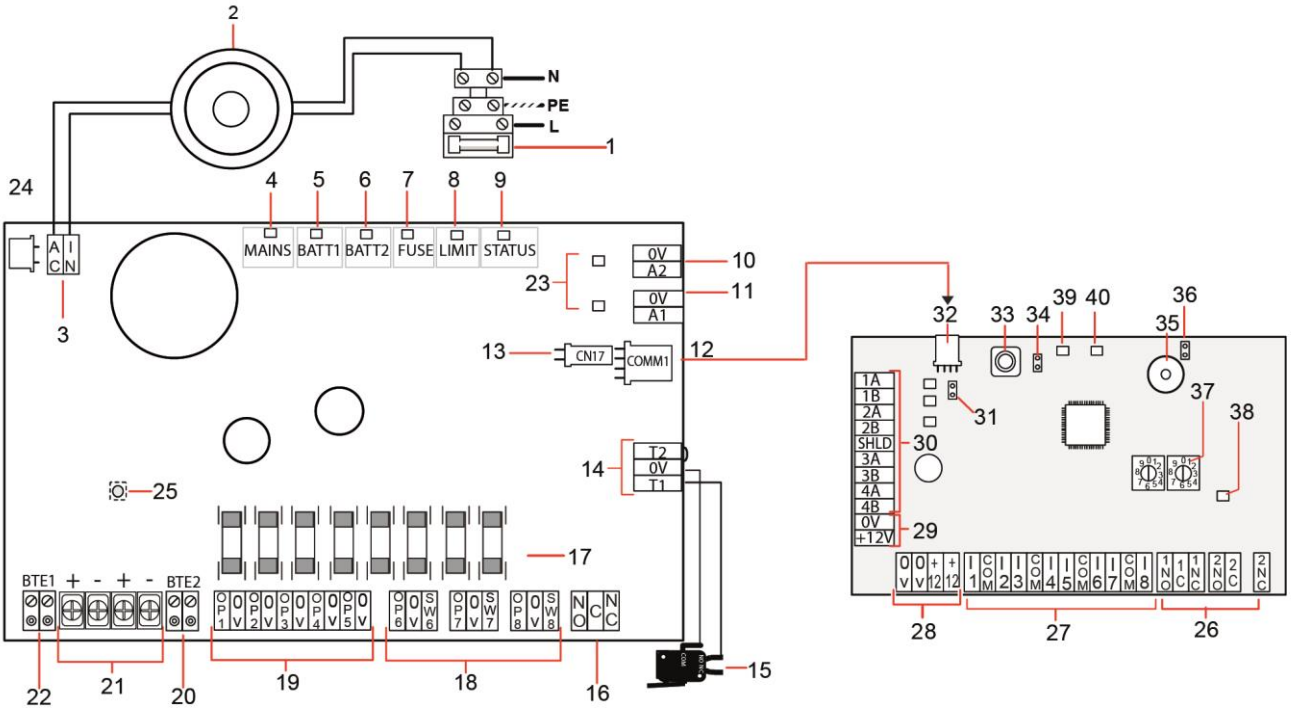
7 Fuente de alimentación inteligente

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

7.1 Fuente de alimentación inteligente SPCP355

La fuente de alimentación inteligente SPCP355 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	
1	Entrada de red C.A. y bloque de fusibles
2	Transformador de entrada
3	**AC IN**: Entrada de alimentación de C.A.
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
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.

Número	Descripción
	● 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. Véase Montaje de la carcasa con protección de tamper [→ 51]
15	Interruptor de tamper frontal/trasero. Véase Montaje de la carcasa con protección de tamper [→ 51]
16	NA/NC: Salida de relé lógica configurable NA/NC. Para más información, véase Cableado de las salidas [→ 63].
17	Fusibles de cristal: fusibles T de 400 mA para salidas 1-8.
18	OP 6 – 8 y SW 6 – 8: Salidas de alimentación combinadas (OP) y salidas lógicas (SW). 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, véase nota de advertencia debajo de la 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 más información, véase Recuperación del sistema [→ 65].
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 más información, véase Recuperación del sistema [→ 65].
25	Interruptor de arranque de fuente de alimentación: Para más información, véase Recuperación del sistema [→ 65].
Módulo de expansión	
26	NA/NC: Salidas de relé lógicas. El módulo de expansión cuenta con dos salidas de relé lógicas configurables NA/NC. Para más información, véase Cableado de las entradas [→ 62]
27	I Entradas 1 – 8: El módulo de expansión cuenta con 8 entradas incorporadas que se pueden configurar como zonas de alarma de intrusión en el sistema SPC. Para más información, véase Cableado de las entradas [→ 62]
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.
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.
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.

Número	Descripción
	Para más información, véase Cableado de la interfaz X-BUS [→ 61].
32	Interfaz de 4 clavijas de fuente de alimentación: Se conecta con COMM1 en la fuente de alimentación inteligente SPCP355 (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 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. Para más información, véase el menú de X-BUS Localizar [→ 125].
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

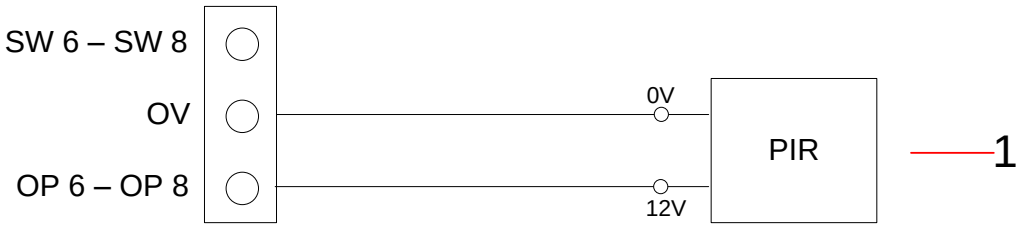
La corriente de carga máxima combinada absorbida desde todas las salidas de 12 V C.C. (OP 1 - 8) más COMM1 no debe sobrepasar los 2,4 A. Cada salida individual, y la salida A2, no debe sobrepasar los 300 mA. Si la corriente del dispositivo requiere más de 300 mA, se recomienda disponer las salidas en paralelo.

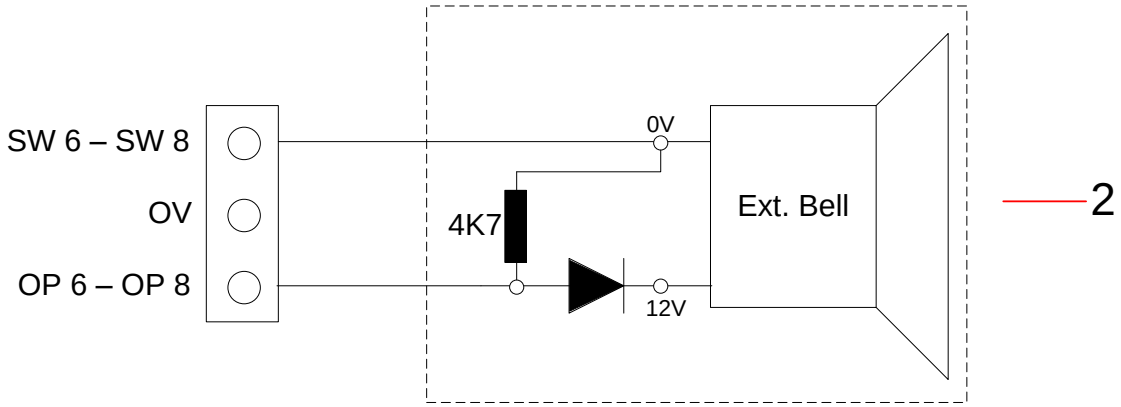
Añadir módulos de expansión adicionales

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, el tamper frontal y trasero se manipula mediante la propia cubierta y la fuente de alimentación inteligente SPCP355.

7.1.1 Salidas supervisadas

La fuente de alimentación inteligente SPCP355 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.



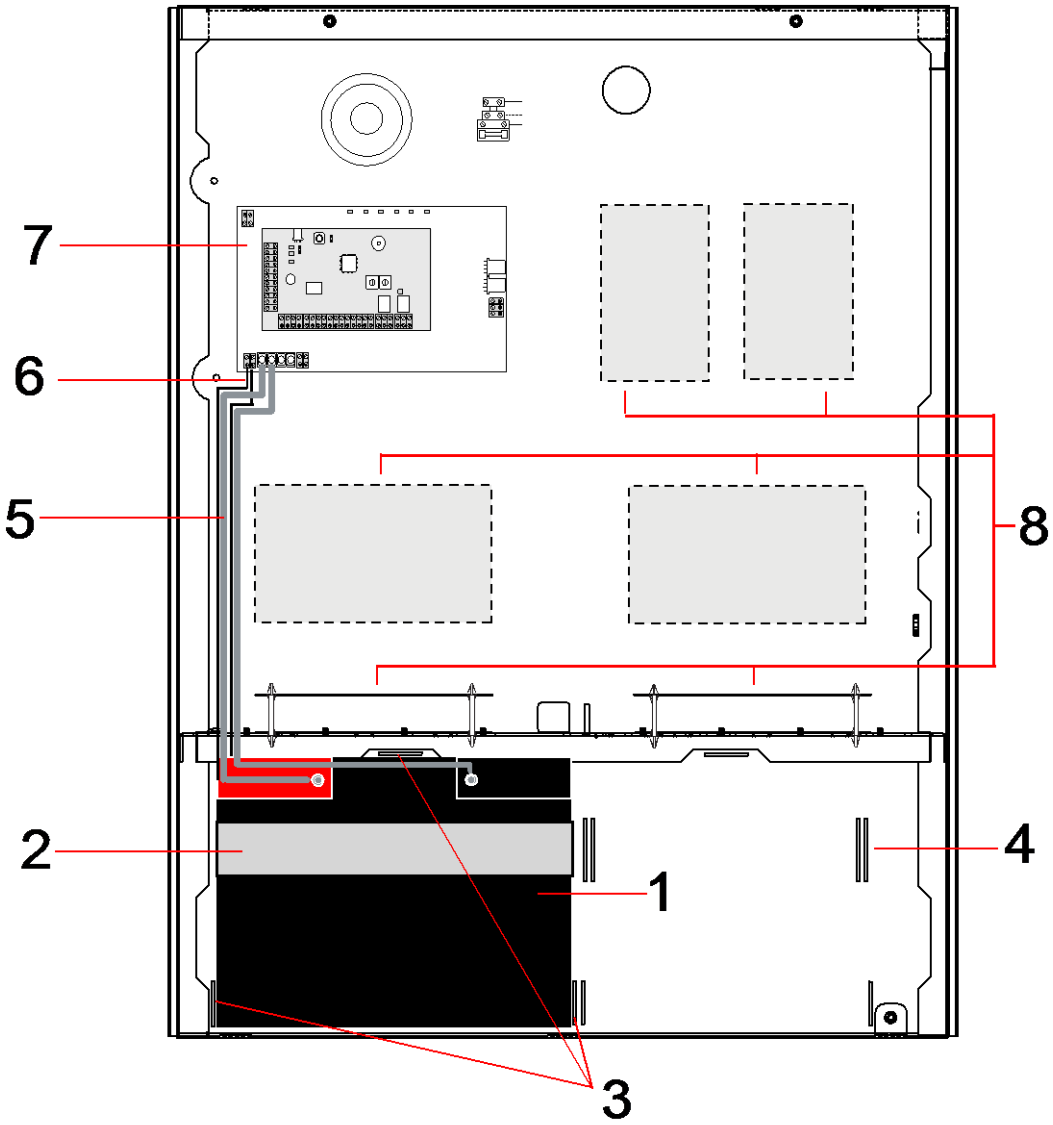


Número	Descripción
1	Salida de alimentación estándar de 12 V
2	Salida lógica conmutada configurable y supervisada de 12 V C.C.

7.1.2 Baterías

7.1.2.1 Instalación de las baterías

En esta sección se describe la instalación de baterías para la fuente de alimentación inteligente SPCP355 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 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 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 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 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

Para obtener información sobre el estado de espera de la batería, consulte el apartado Cálculo de los requisitos de alimentación de la batería [→ 354].

7.1.3 Cableado de la interfaz X-BUS

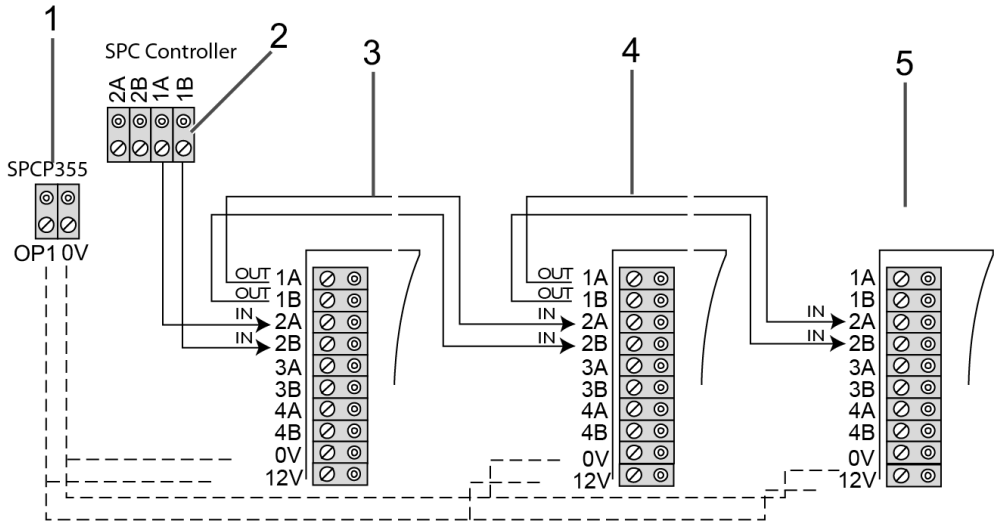
La interfaz X-BUS permite conectar módulos de expansión y teclados al controlador SPC. El X-BUS se puede cablear con un gran número de configuraciones diferentes según los requisitos de la instalación.

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
2	Controlador SPC
3	Módulo de expansión de entrada/salida SPCP355
4	Módulo de expansión posterior
5	Módulo de expansión posterior

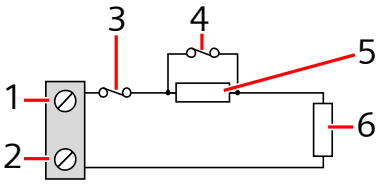
7.1.3.1 Cableado de las entradas

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
- PIR antienmascaramiento

Configuración por defecto

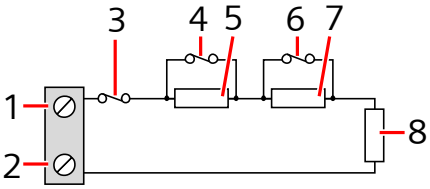
En el siguiente diagrama se muestra la configuración por defecto, 2 RFL 4K7:



Número	Descripción
1	Entrada 1
2	COM
3	Tamper
4	Alarma
5	4K7
6	RFL 4K7

PIR antienmascaramiento

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



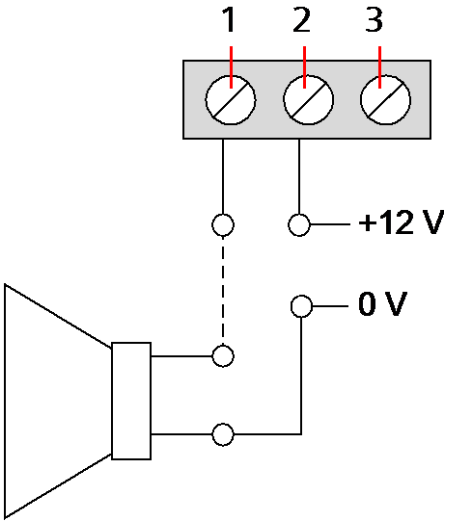
Número	Descripción
1	Entrada 2
2	COM
3	Tamper
4	Alarma
5	4K7
6	Fallo de detector
7	2K2
8	RFL 4K7

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 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				Parpadeando

7.1.5 Recuperación del sistema

Fallo de red y batería

En caso de avería tanto en la red de C.A. como en la batería, el interruptor de arranque de la fuente de alimentación (elemento 25 en Fuente de alimentación inteligente SPCP355 [→ 56]) permite reiniciar el sistema si solo se restablece la alimentación de la batería. Para arrancar el sistema, haga lo siguiente:

▷ 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.

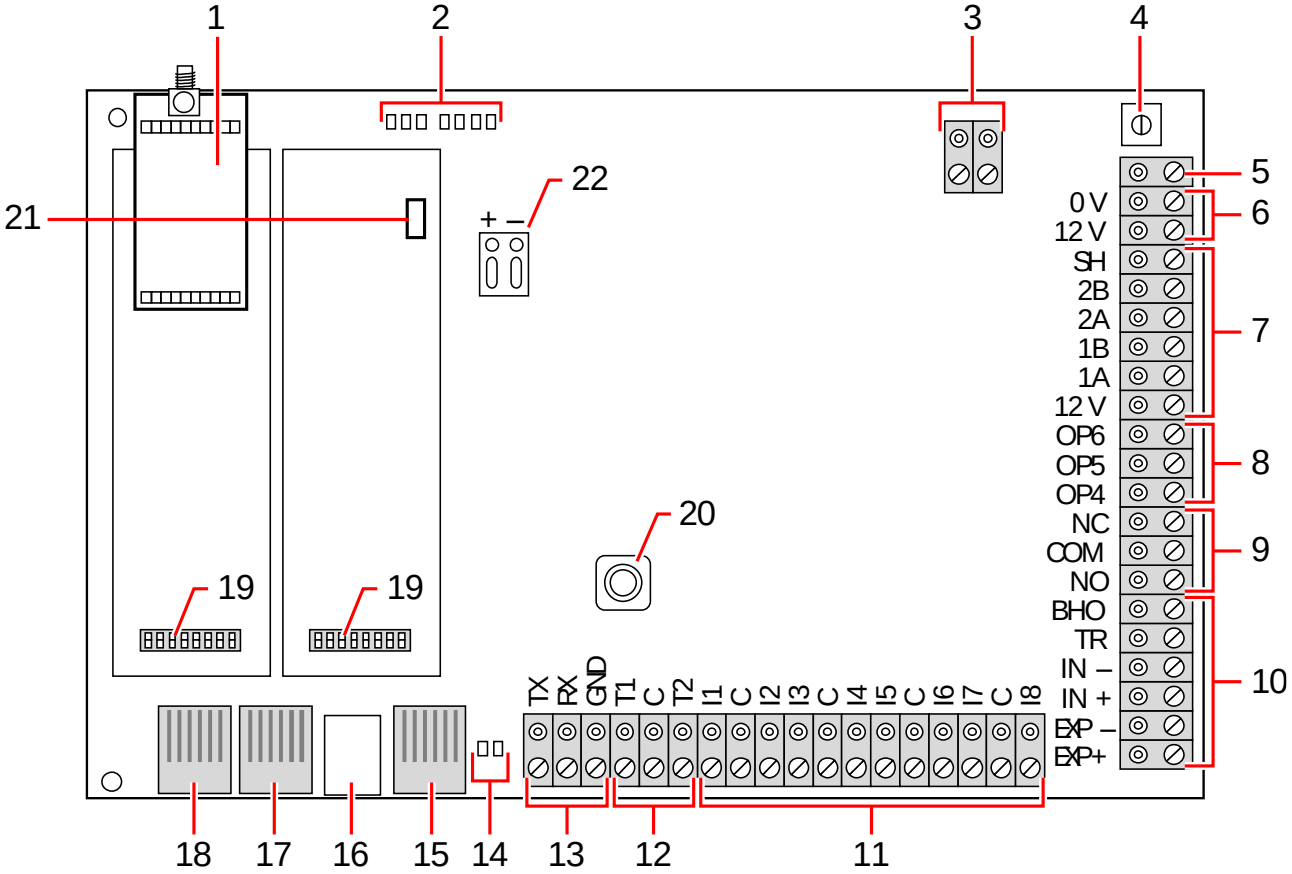
Ver también

- Alimentación de módulos de expansión desde los terminales de alimentación auxiliares [→ 353]
- Cableado de la interfaz X-BUS [→ 73]
- Cableado de una sirena interna [→ 89]
- Cableado de entradas de zona [→ 85]
- Los LED de estado del controlador [→ 352]
- Los LED de estado del controlador [→ 352]
- Alimentación de módulos de expansión desde los terminales de alimentación auxiliares [→ 353]
- Cableado de la interfaz X-BUS [→ 73]
- Cableado de una sirena interna [→ 89]
- Cableado de entradas de zona [→ 85]

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

En esta sección se describe el controlador para los modelos SPC42xx, 43xx, 53xx y 63xx. El SPC5350 y el 6350 se describen en el apartado Hardware del controlador SPC5350 y 6350 [→ 68].

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



1	Módulo vía radio	La placa del controlador puede estar equipada de fábrica con un módulo

	opcional	vía radio para su uso con detectores vía radio (868 MHz).
2	Indicadores LED de estado del SPC	Estos 7 LED muestran el estado de diversos parámetros del sistema como se describe en la página [→ 352].
3	Entrada de alimentación de CA	Entrada de red 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 caja del SPC. La toma de tierra de la red de CA se ha cableado a un punto de conexión en la caja 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 restablecer el controlador: – pulse este interruptor una vez. ● Para restablecer la configuración de programación por defecto y reiniciar el controlador: – mantenga pulsado el botón hasta que se le pregunte si desea restablecer la configuración predeterminada de fábrica. – Seleccione YES (sí) para restablecer la configuración predeterminada de fábrica. **Advertencia:** Si el controlador vuelve a los ajustes de fábrica, se borrarán todos los ficheros de configuración guardados en el controlador, incluyendo las copias de seguridad. 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 está habilitado el bloqueo de técnico.
5	Terminal de conexión a tierra	Este terminal no es necesario y no se debe conectar.
6	Salida auxiliar de 12 V	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 la página [→ 353]. La corriente máxima que se puede suministrar es de 750 mA. **Nota**: la cantidad de corriente absorbida depende del tiempo que se deba mantener funcionando con batería.
7	Interfaz X-BUS	Es el bus de comunicaciones del SPC que se utiliza para conectar entre sí los módulos de expansión en el sistema. Consulte la página [→ 73]. SPC4000 solo tiene una interfaz de X-BUS.
8	Salidas incorporadas	Las salidas OP4, OP5 y OP6 son salidas resistivas de colector abierto de 12 V que comparten una corriente de 400 mA con la salida auxiliar de 12 V. Si las salidas no están conectadas a los 12 V del controlador y son alimentadas desde una fuente de alimentación externa, los 0 V de la fuente de alimentación se deben conectar a los 0 V del controlador, y la fuente de alimentación externa no podrá sobrepasar 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.
10	Sirena interior / sirena exterior	Las salidas de sirenas interiores y exteriores (INT+, INT-, EXT+, EXT-) son salidas resistivas con una corriente de 400 mA. Las salidas BHO (**B**ell **H**old **O**ff), **TR** (**T**amper **R**eturn) y EXT se utilizan para conectar una sirena exterior al controlador. Los terminales INT+ e INT- se utilizan para conectar con los dispositivos internos, como una sirena interna. Consulte la página [→ 89].
11	Entradas de zona	El controlador proporciona ocho entradas de zona incorporadas que se pueden supervisar mediante diferentes configuraciones de supervisión. Estas configuraciones se pueden programar en la programación del sistema. La configuración predeterminada es 2 **R**esistencias **F**inales **de L**ínea (2 RFL) a través de los valores de resistencia de 4K7. Consulte la página [→ 85].
12	Terminales de tamper	El controlador incluye dos terminales de entrada de tamper adicionales que se pueden conectar a los dispositivos de tamper auxiliares para proporcionar una protección de tamper mejorada. Estos terminales se

		deben puentear cuando no estén en uso.
13	Bloque de terminales del puerto serie 2: ~~4000~~	El bloque de terminales del puerto serie 2 (TX, RX, GND) se puede utilizar como interfaz a un módem externo o programa del terminal del PC. El puerto serie 2 comparte un canal de comunicaciones con el módem de copia de seguridad. Si se instala un módem de copia de seguridad, asegúrese de que no haya dispositivos conectados al puerto serie.
14	IP LED de conectividad Ethernet	Los dos LED de Ethernet indican el estado de la conexión Ethernet. El LED izquierdo indica la actividad de datos en el puerto Ethernet; el LED derecho indica que el enlace Ethernet está activo.
15	IP Interfaz Ethernet	La interfaz Ethernet permite 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 a un programa del terminal.
17	Puerto serie 2 ~~4000~~	Este puerto serie RS232 puede utilizarse como interfaz para un módem externo o programa del terminal de PC. El puerto serie 2 comparte un canal de comunicaciones con el módem de copia de seguridad. Si se instala un módem de back-up, asegúrese de que no haya dispositivos conectados al puerto serie.
18	Puerto serie 1	Este puerto serie RS232 puede utilizarse como interfaz para un dispositivo de protocolo X-10.
19	Módulos complementarios opcionales	Es posible conectar un módulo principal (ranura izquierda) y un módulo de copia de seguridad (ranura derecha) al controlador. Estos módulos pueden ser módems GSM o RTB y ofrecen más funciones de comunicación. El módem de copia de seguridad no se debe conectar si la interfaz del puerto serie 2 está conectada a un módem externo o a otro dispositivo.
20	Tamper frontal	Este tamper frontal incorporado (interruptor + interruptor) proporciona la protección de tamper de la caja. **Nota:**El tamper frontal no se utiliza en la carcasa G5.
21	Selector de batería	J12: Fijar jumper para uso de batería de 17 Ah y retirar el de para 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**.

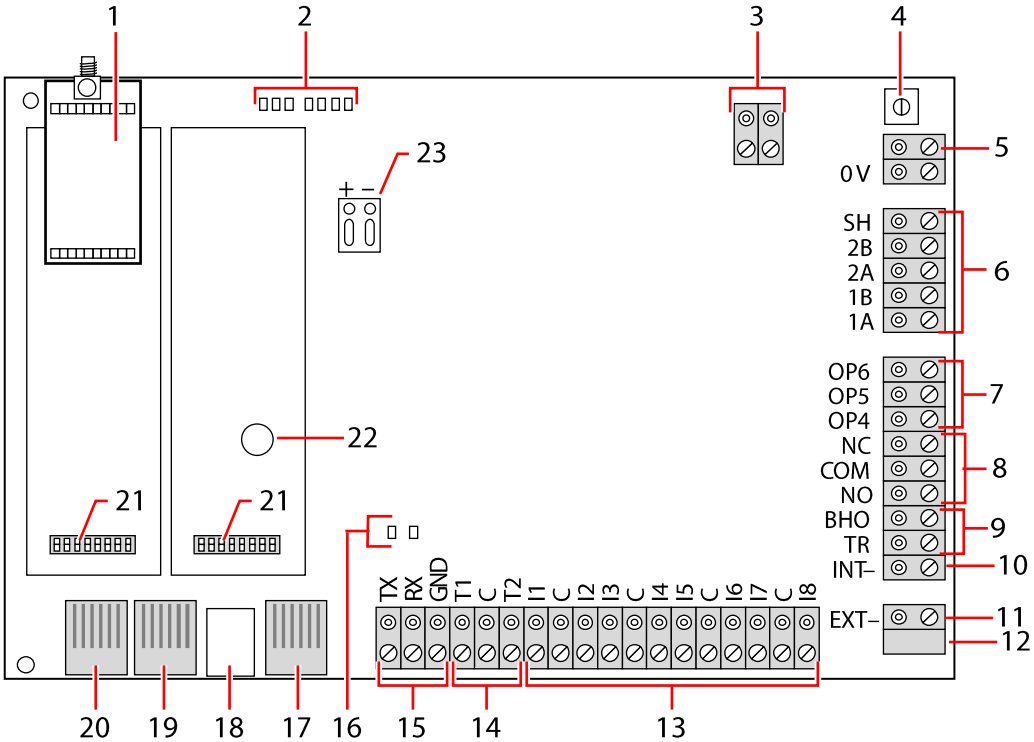
* Configuración por defecto para centrales SPC5350 y SPC5360

** 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 de 8Z/2S que viene de serie en el modelo G5 está direccionado como “01” y no puede ser modificado.



1	Módulo vía radio opcional	La placa del controlador puede estar equipada de fábrica con un módulo vía radio para su uso con detectores vía radio (868 MHz).
2	Indicadores LED de estado del SPC	Estos 7 LED muestran el estado de diversos parámetros del sistema como se describe en la página [→ 352].
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.
4	Botón de Reset	● Para restablecer el controlador: – pulse este interruptor una vez. ● Para restablecer la configuración de programación por defecto y reiniciar el controlador: – mantenga pulsado el botón hasta que se le pregunte si desea restablecer la configuración predeterminada de fábrica. – Seleccione YES (sí) para restablecer la configuración predeterminada de fábrica. **Advertencia:** Si el controlador vuelve a los ajustes de fábrica, se borrarán todos los ficheros de configuración guardados en el controlador, incluyendo las copias de seguridad. 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 está habilitado el bloqueo de técnico.
5	Terminal de conexión a tierra	Este terminal no es necesario y no se debe conectar.

6	Interfaz X-BUS	Es el bus de comunicaciones del SPC que se utiliza para conectar entre sí los módulos de expansión en el sistema. Consulte la página [→ 73]. Las terminales 1B y 1A se deben conectar a los terminales del módulo de expansión de E/S SPCP355 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 incorporadas	Las salidas OP4, OP5 y OP6 son salidas resistivas de colector abierto de 12 V con una corriente de 300 mA. La carga de OP4 se debe conectar a la fuente de alimentación inteligente SPCP355.
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 (**B**ell **H**old **O**ff) y **TR** (**T**amper **R**eturn) (y EXT) se utilizan para conectar una sirena exterior al controlador. Consulte la página [→ 89].
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.
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.
12	No utilizar.	No utilizar.
13	Entradas de zona	El controlador proporciona ocho entradas de zona incorporadas que se pueden supervisar mediante diferentes configuraciones de supervisión. Estas configuraciones se pueden programar en la programación del sistema. La configuración predeterminada es 2 **R**esistencias **F**inales **de** **L**ínea (2 RFL) a través de los valores de resistencia de 4K7. Consulte la página [→ 85].
14	Terminales de tamper	El controlador incluye dos terminales de entrada de tamper adicionales que se pueden conectar a los dispositivos de tamper auxiliares para proporcionar una protección de tamper mejorada. Estos terminales se deben puentear cuando no estén en uso.
15	Bloque de terminales del puerto serie 2:	El bloque de terminales del puerto serie 2 (TX, RX, GND) se puede utilizar como interfaz a un módem externo o programa del terminal del PC. El puerto serie 2 comparte un canal de comunicaciones con el módem de copia de seguridad. Si se instala un módem de copia de seguridad, asegúrese de que no haya dispositivos conectados al puerto serie.
16	LED de conectividad Ethernet	Los dos LED de Ethernet indican el estado de la conexión Ethernet. El LED izquierdo indica la actividad de datos en el puerto Ethernet; el LED derecho indica que el enlace Ethernet está activo.
17	Interfaz Ethernet	La interfaz Ethernet permite 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 a un programa del terminal.
19	Puerto serie 2	Este puerto serie RS232 puede utilizarse como interfaz para un módem externo o programa del terminal de PC. El puerto serie 2 comparte un canal de comunicaciones con el módem de copia de seguridad. Si se instala un módem de back-up, asegúrese de que no haya dispositivos conectados al puerto serie.
20	Puerto serie 1	Este puerto serie RS232 puede utilizarse como interfaz para un dispositivo de protocolo X-10.
21	Módulos complementarios opcionales	Es posible conectar un módulo principal (ranura izquierda) y un módulo de copia de seguridad (ranura derecha) al controlador. Estos módulos pueden ser módems GSM o RTB y ofrecen más funciones de comunicación. El módem de copia de seguridad no se debe conectar si la interfaz del puerto serie 2 está conectada a un módem externo o a 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.

Ver también

Alimentación de módulos de expansión desde los terminales de alimentación auxiliares [→ 353]

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 por medio de la E/S de dos puertas. Cada una de las E/S de dos puertas es responsable de la funcionalidad de dos entradas y una salida del controlador de puertas. Se puede asignar un número de puerta específico a una E/S de puerta, lo que proporciona la funcionalidad predefinida a las entradas y las salidas. Si no se asigna ningún número de puerta a ninguna de las E/S de puertas (opción "Zonas" seleccionada), las entradas y salidas del controlador de puertas se pueden utilizar como entradas y salidas en la central de control. De este modo, no habrá ninguna funcionalidad de acceso disponible en este controlador de dos puertas.

Si se asigna un número de puerta solamente a la E/S de la primera 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 utilizará como lector de salida para la puerta configurada. Dos entradas y una salida poseen una funcionalidad predefinida, y dos entradas y una salida pueden ser configuradas por el usuario. Además, la entrada del sensor de posición de la puerta de la primera puerta se puede utilizar como zona de intrusión, pero sólo 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 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 poseen una funcionalidad predefinida. Las entradas del sensor de posición de puerta de las dos puertas también se pueden utilizar como zonas de intrusión, pero sólo con funcionalidad limitada.

Para más información sobre los lectores de tarjetas y formatos de tarjetas soportados actualmente, consulte el apéndice [→ 376].

Todos los números de zona libres se pueden asignar a las zonas. Sin embargo, la asignación no es fija. Si el número 9 estaba asignado a una zona, la zona y un módulo de expansión de entrada con la dirección 1 están conectados al X-Bus (el cual está utilizando los números de zona 9-16). La zona asignada desde el controlador de dos puertas se desplazará al siguiente número de zona libre. La configuración se adaptará consecuentemente.

10 Cableado del sistema

10.1 Cableado de la interfaz X-BUS

La interfaz del X-BUS permite conectar módulos de expansión al controlador. El X-BUS se puede cablear en una serie de configuraciones diferentes según los requisitos de la instalación. La velocidad en baudios de la interfaz del X-BUS es de 307 kb.

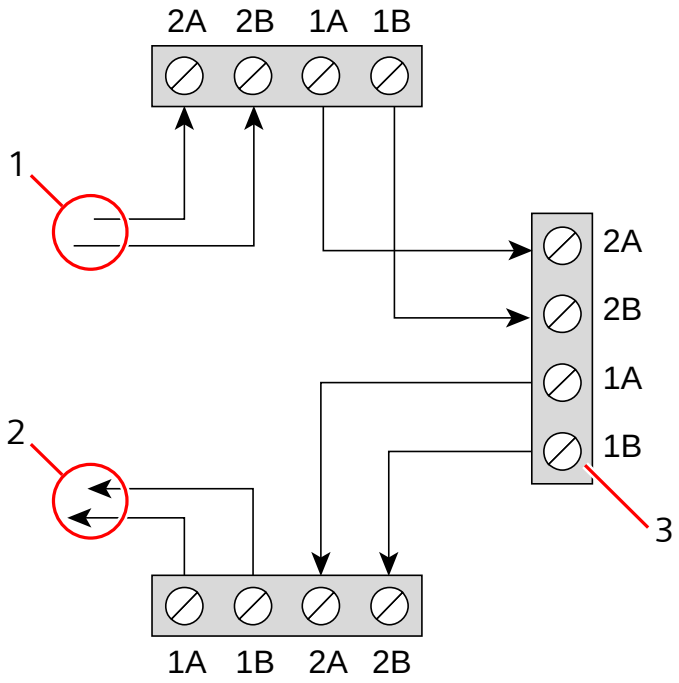
	AVISO
	El X-BUS es un bus RS-485 con una velocidad de baudios de 307 kb. El rendimiento completo sólo se admite en una configuración de cableado en lazo [→ 74] y punta [→ 75] (la mejor calidad de señal debido a la configuración en cadena de tipo margarita de secciones aisladas con 1 transmisor / 1 receptor y resistencias de terminación equilibradas en cada extremo). El rendimiento en el cableado con configuración en estrella [→ 76] o multipunto [→ 76] 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 encarecidamente el uso de la configuración en lazo [→ 74] o en punta [→ 75].

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

Tipo de cable	Distancia
Cable de alarma estándar CQR	200 m
Categoría UTP: 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 del X-BUS. El controlador inicia un proceso de detección al encenderse para determinar el número de módulos de expansión conectados al sistema y la topología según la cual lo están.



Cableado de módulos de expansión

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

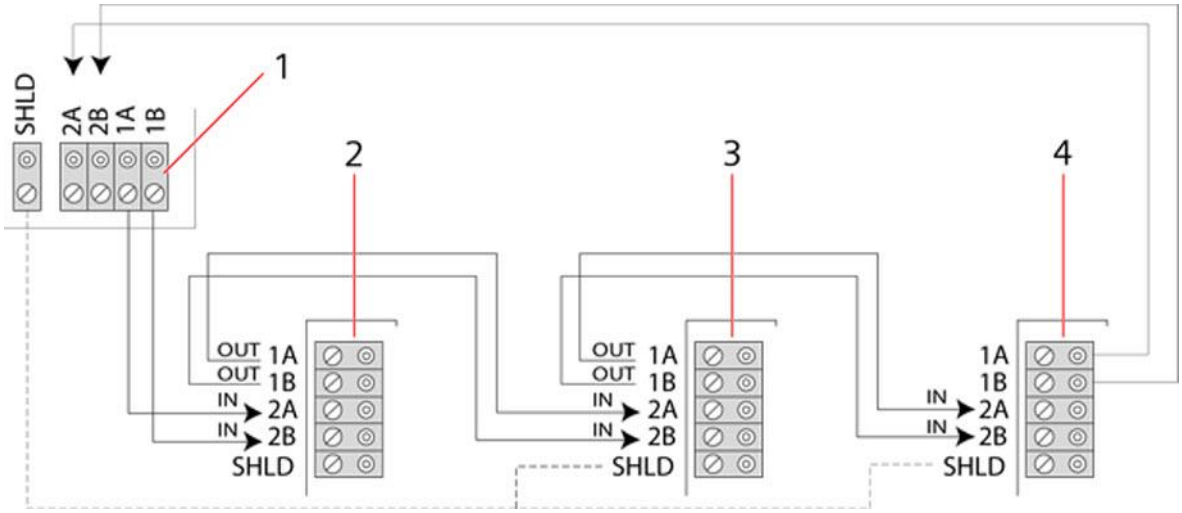
La mayoría de los módulos de expansión están equipados con terminales adicionales 3A/3B y 4A/4B para el cableado de un módulo de expansión de bifurcación. Consulte la página [→ 83] para obtener instrucciones sobre el cableado del módulo de expansión de bifurcación.

10.1.1 Configuración en lazo

i	*AVISO*
	~~4000~~ El SPC42xx/43xx no admite la configuración en lazo (sólo 1 puerto X-BUS).

i	*AVISO*
	Todos los teclados / módulos de expansión están equipados, por defecto, con un jumper de terminación. En la configuración en lazo, es imprescindible contar con 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 son controlados. Esto se consigue conectando los terminales 1A, 1B del controlador a los 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 la de 1A, 1B del último módulo de expansión a 2A, 2B en el controlador. Vea la configuración del cableado en la figura que aparece a continuación.



1	Controlador
2-4	Módulos de expansión

10.1.2 Configuración en punta

i	*AVISO*
	El SPC52xx/53xx/63xx admite 2 puntas (2 puertos X-BUS). El SPC42xx/43xx admite 1 punta (1 puerto X-BUS).

i	*AVISO*
	Todos los teclados / módulos de expansión están equipados, por defecto, con un jumper de terminación. En la configuración en punta, es imprescindible tener estos jumpers puestos.

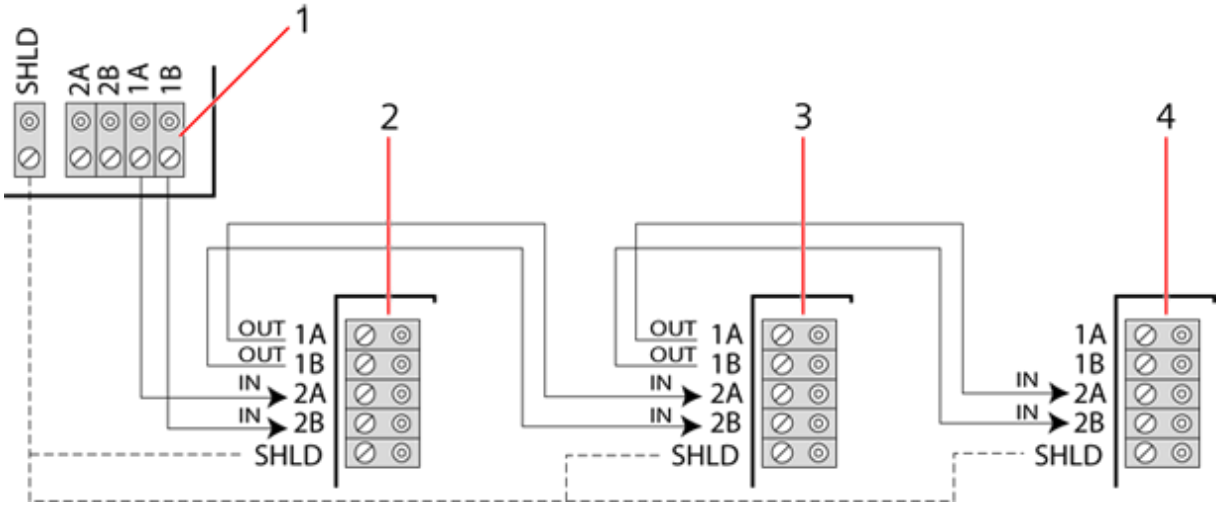
El método de cableado en punta (o de lazo abierto) ofrece un alto nivel de tolerancia a fallos y puede ser más adecuado en ciertas instalaciones. En caso de fallo o discontinuidad de un X-BUS, todos los módulos de expansión y detectores hasta el punto del fallo continúan siendo supervisados.

En esta configuración, el controlador SPC utiliza un único puerto X-BUS (1A/1B ó 2A/2B) para admitir un grupo de módulos de expansión. Vea la configuración del cableado en la figura que aparece a continuación. El último módulo de expansión en una configuración de lazo abierto no está conectado al controlador y se puede identificar por el LED parpadeando rápidamente (una vez cada 0,2 segundos aprox.) cuando se utiliza la programación en el modo técnico total.

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

Todos los teclados y módulos de expansión están equipados, por defecto, con jumpers de terminación, lo que permite la terminación en todos los dispositivos. Esto es necesario para la configuración en punta (cadena), pues el jumper actúa como terminador de resistencia, eliminando los ecos en la línea.

En la configuración de cableado en lazo, todos los teclados y módulos de expansión están equipados, por defecto, con un puente que permite la terminación en el dispositivo.



Configuración en punta

1	Controlador
2-4	Módulos de expansión

10.1.3 Configuración en estrella y multipunto

	AVISO
	Por favor, lea esta sección para ver ejemplos de cableado [→ 81] y la sección Apantallamiento [→ 82] antes de comenzar con la instalación.

Los métodos de cableado en estrella y multipunto permiten sustituir los cableados existentes por cables de cuatro hilos en edificios pequeños (normalmente en

casas) con entornos de bajo ruido eléctrico. Estos métodos de cableado se limitan a las especificaciones que se indican a continuación:

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

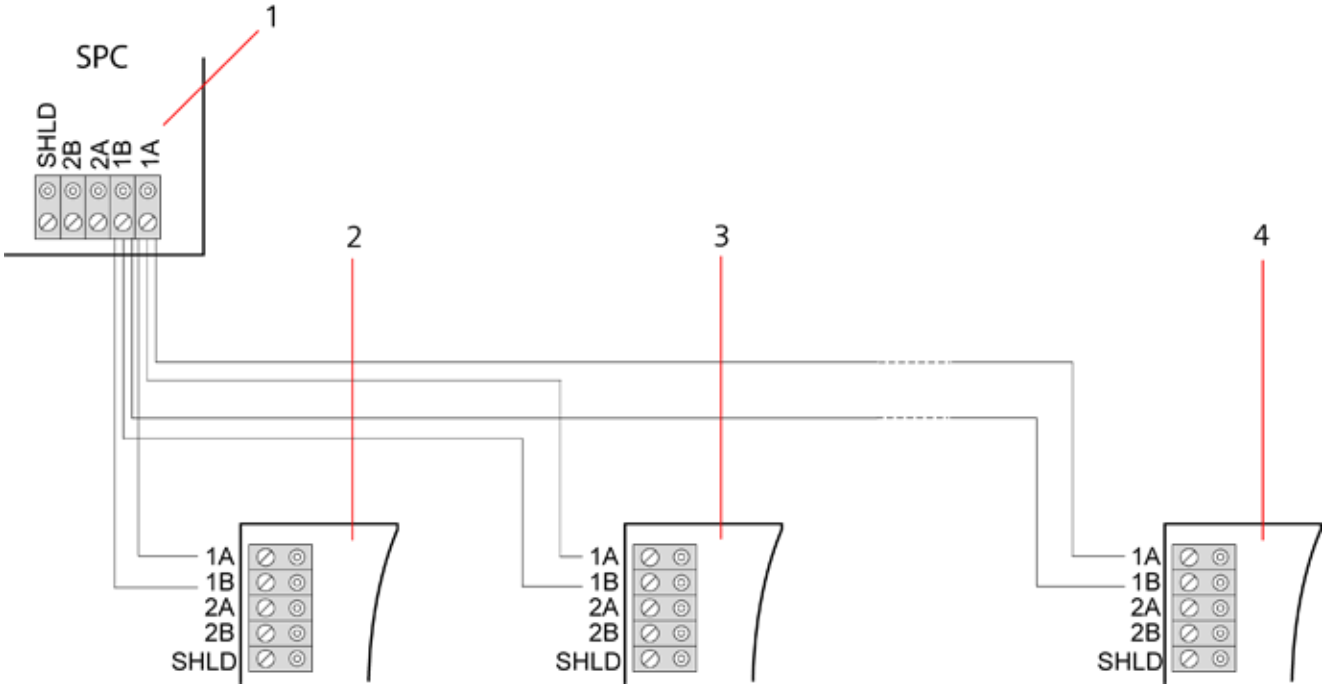
	AVISO
	El rendimiento en el cableado con configuración en estrella o multipunto es limitado debido a que las condiciones de la especificación de bus RS-485 no son las óptimas (calidad de la señal reducida debido a múltiples receptores / transmisores en paralelo con resistencias de terminación no equilibradas).

Configuración en estrella

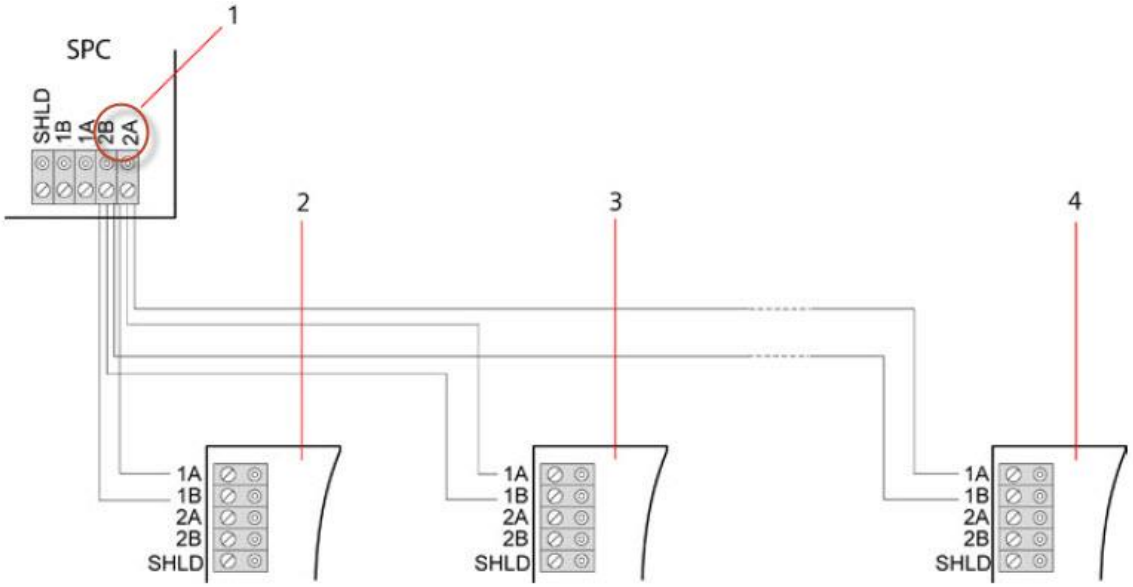
	AVISO
	Todos los teclados / módulos de expansión están equipados, por defecto, con un jumper de terminación. En la configuración en estrella, es imprescindible **retirar** estos jumpers.

Una configuración en estrella se establece cuando varios módulos de expansión se vuelven a conectar al mismo puerto X-BUS en el controlador SPC. Dependiendo del tipo de controlador, puede haber 2 puertos (1A/1B, 2A/2B), pero sólo se puede utilizar un puerto (1A/1B) en 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. Un cortocircuito en el cable desactiva todos los módulos de expansión.



Configuración en estrella



Configuración en estrella 2

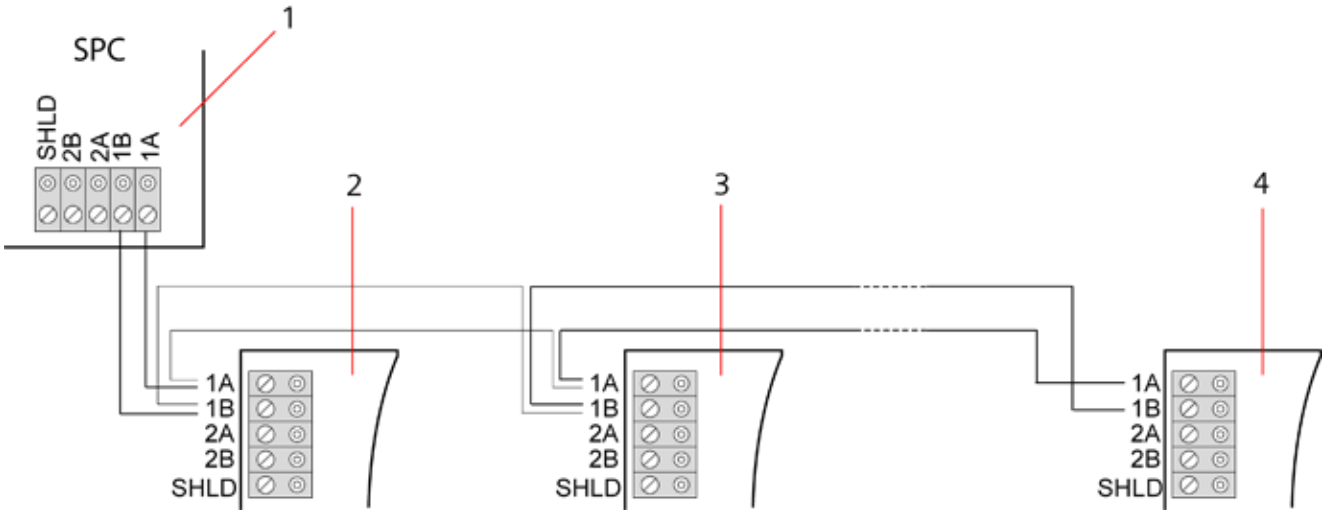
1	Controlador SPC
2-4	Módulos de expansión

Configuración multipunto

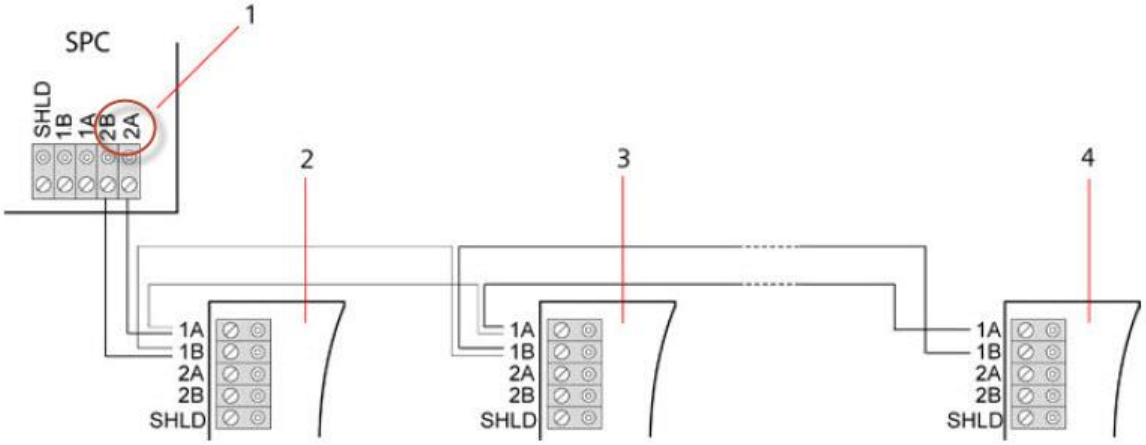
	AVISO
	Todos los teclados / módulos de expansión están equipados, por defecto, con un jumper de terminación. En la configuración multipunto, es imprescindible **retirar** estos jumpers a excepción del último teclado o módulo de expansión.

La configuración multipunto se diferencia de la configuración en estrella en que cada módulo de expansión utiliza el mismo canal de comunicación para conectarse al siguiente, de manera que todos los módulos de expansión utilizan el mismo canal de entrada. Vea la configuración multipunto en la segunda figura.

En caso de discontinuidad de un X-BUS, todos los módulos de expansión y detectores hasta el punto del fallo continúan siendo supervisados. Un cortocircuito en el cable desactiva todos los módulos de expansión.



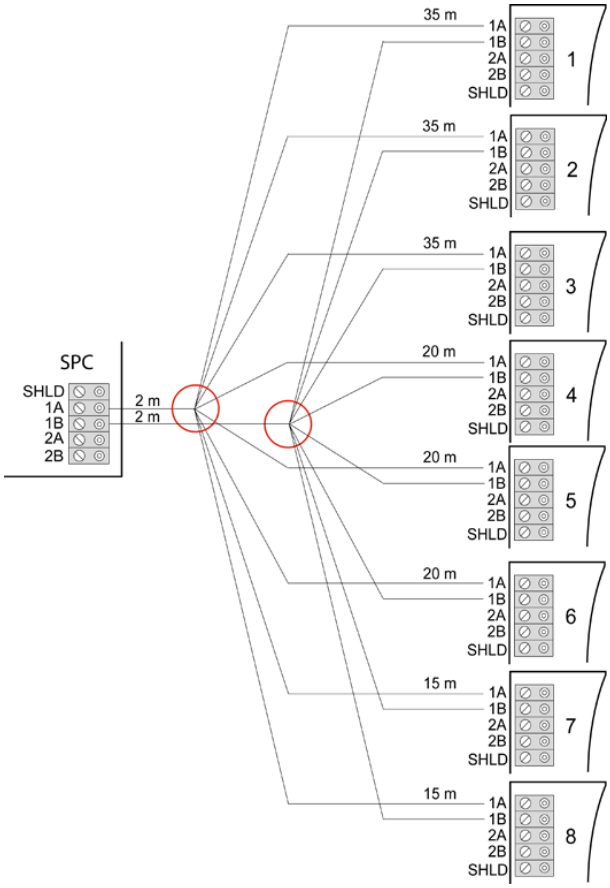
Configuración multipunto



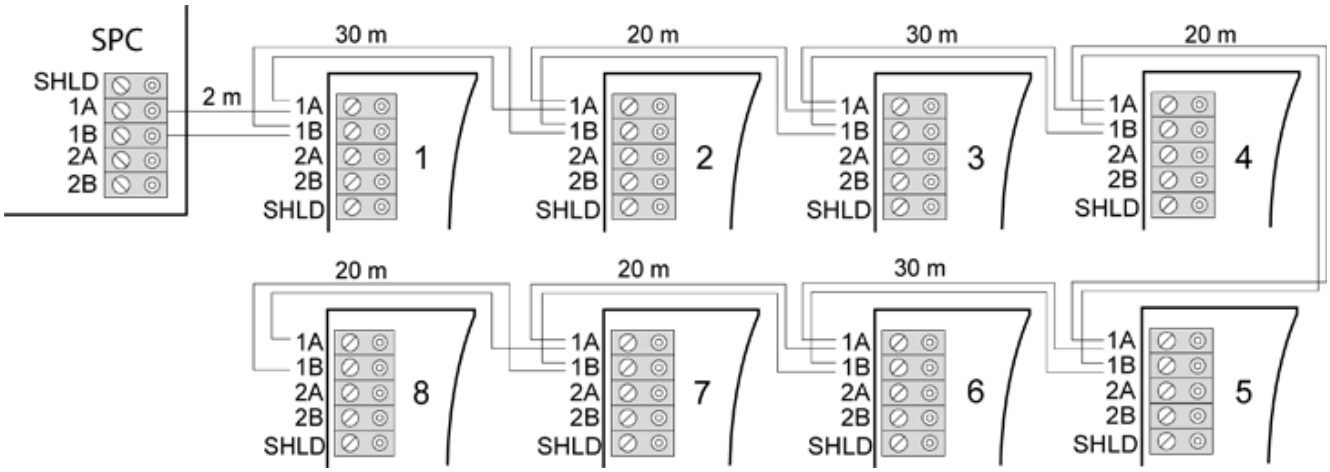
Configuración multipunto 2

1	Controlador SPC
2-4	Módulos de expansión

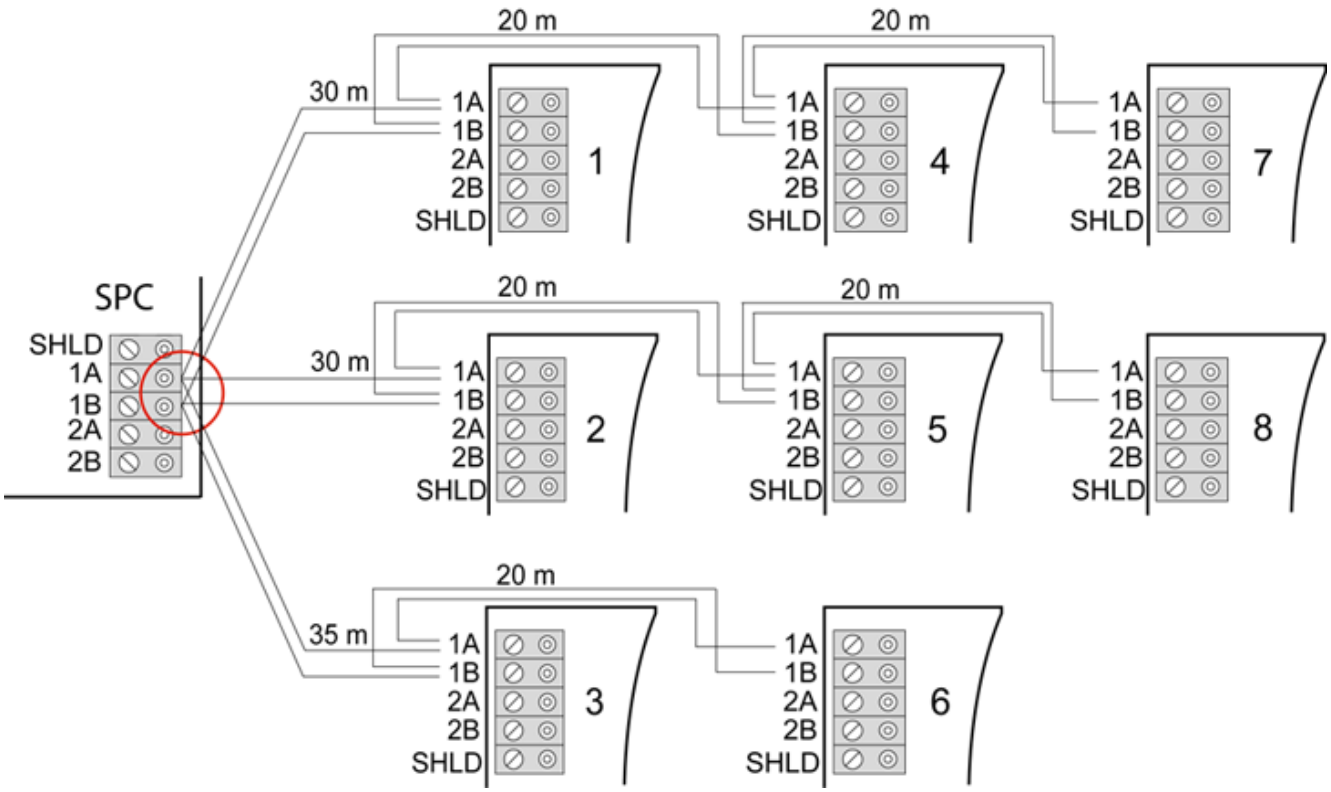
10.1.3.1 Ejemplos de cableado correcto



Cableado en estrella



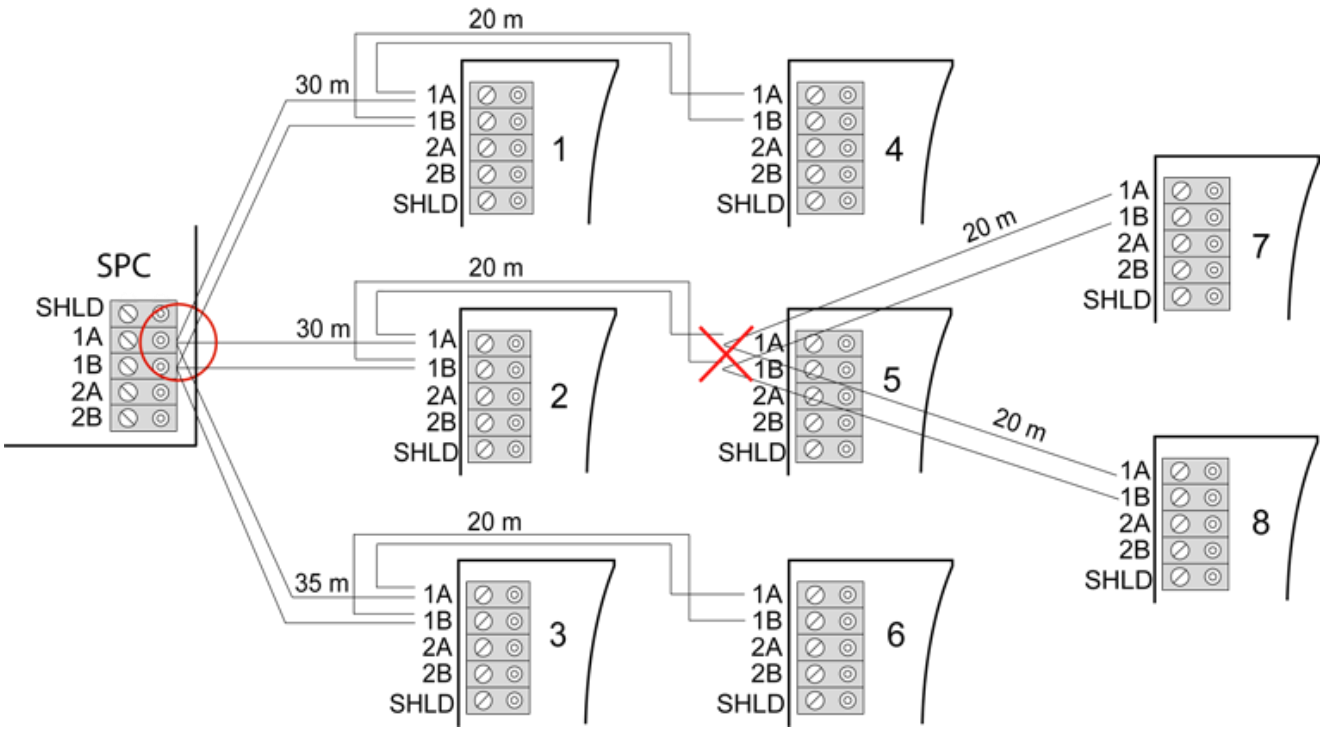
Cableado multipunto



Cableado mixto

10.1.3.2 Ejemplos de cableado incorrecto

	AVISO
	Sólo se permite una mezcla de configuración en estrella y multipunto si el punto de la estrella se encuentra en el puerto X-BUS del controlador. En ese caso, todos los módulos de expansión / teclados se deben cablear con una configuración multipunto sin ningún otro punto de estrella en el cableado.



No está permitido el cableado con un segundo punto de estrella

	AVISO
	Si la mezcla de configuración en estrella y multipunto no está cableada correctamente, la reducción en la calidad de la señal puede provocar que el tiempo de reacción de los dispositivos conectados sea lento (p. ej. funcionamiento del teclado) o, incluso, que se pierda la comunicación con los dispositivos. Si se observa este comportamiento, se recomienda encarecidamente realizar el cableado con configuración en lazo O BIEN en estrella.

10.1.4 Apantallamiento

Los terminales de apantallado (SHLD) deben utilizarse únicamente para los tipos de cable con apantallado (p. ej. 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 el apantallado debe estar conectado a tierra, se deberá conectar un cable del terminal SHLD del controlador al saliente de tierra del chasis. NO conecte a tierra el terminal SHLD de ninguno de los módulos de expansión.

	AVISO
	Para cableado en estrella y multipunto En la configuración del cableado en estrella y multipunto no se recomienda utilizar cables apantallados debido a sus características eléctricas poco ventajosas (mayor capacitancia). Sin embargo, si se requiere apantallado (es decir, en instalaciones con muchas interferencias eléctricas), se deberá realizar un nuevo cableado, en punta o en lazo según sea lo más adecuado, con una configuración apropiada de los cables de instalación.

10.1.5 Mapa de cableado

La identificación y orden de numeración de los módulos de expansión y teclados varía dependiendo de si el direccionamiento de los módulos de expansión es automático o manual. Para obtener información sobre la configuración manual y automática, consulte la página [→ 122].

En un sistema con direccionamiento manual, los módulos de expansión y teclados tienen una secuencia de numeración distinta y las define el técnico manualmente. Por ejemplo, los módulos de expansión se numeran como 01, 02, 03 y, así, sucesivamente, según se desee. Los teclados se pueden numerar, según se desee, utilizando los mismos números.

En la configuración manual, el sistema asigna zonas de forma automática a cada módulo de expansión. Por esta razón, los dispositivos sin zonas, como los módulos de expansión de 8 salidas deben direccionarse los últimos.

Para un sistema con direccionamiento automático, los módulos de expansión y teclados pertenecen al mismo grupo de numeración y los asigna el controlador. Por ejemplo, los módulos de expansión y teclados se numeran juntos como 01, 02, 03 en el orden en el que se detectan en relación con la ubicación del controlador.

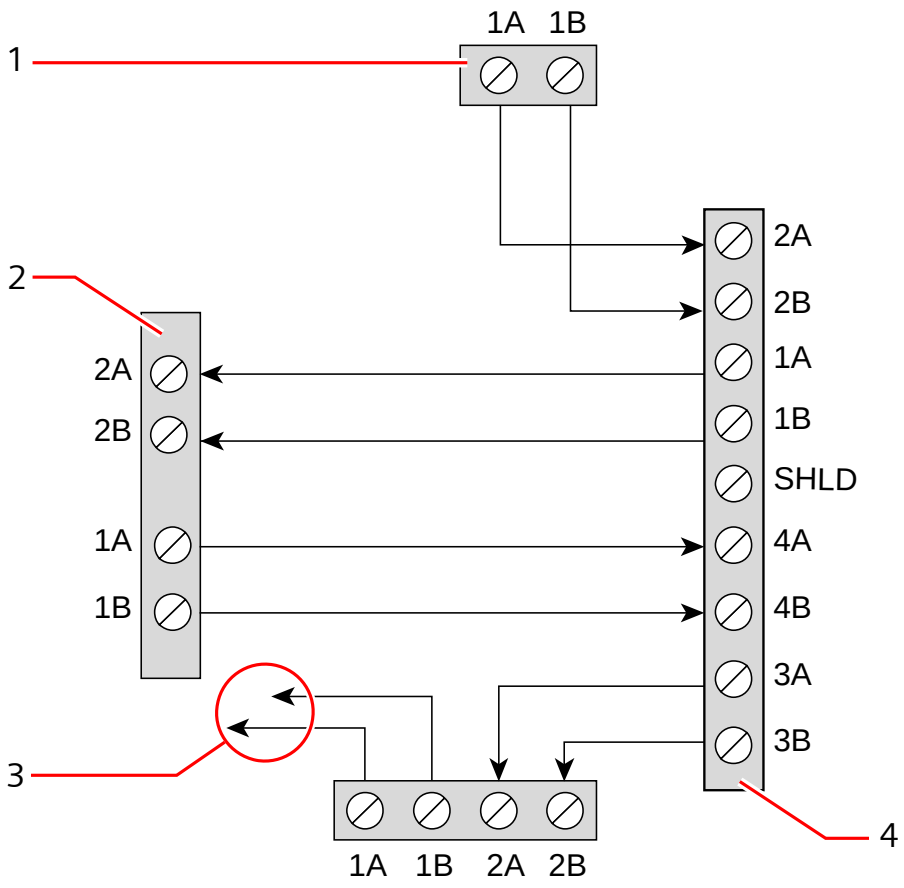
10.2 Cableado del módulo de expansión de bifurcación

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 la bifurcación no se utiliza, los terminales 1A/1B se emplean para conectarse con el siguiente módulo de expansión/teclado. Entonces, los terminales 3A/3B 4A/4B no se utilizan.

Los módulos siguientes tienen la opción de cableado de módulo de expansión 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

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

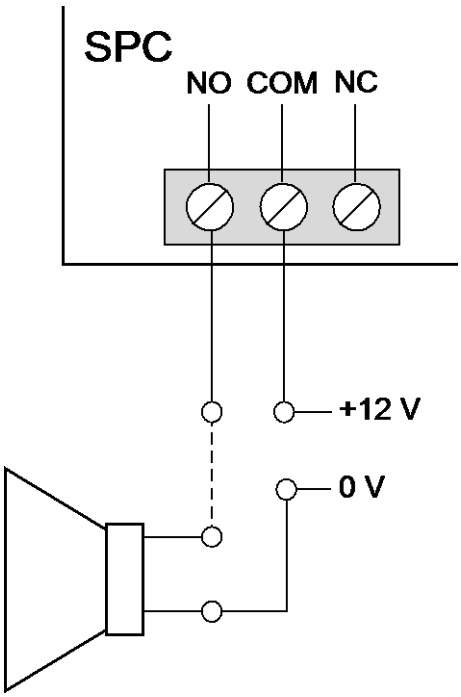
10.3 Cableado de la masa del sistema

Los terminales de 0 V de las fuentes de alimentación inteligentes, teclados y módulos de expansión deben estar conectados al terminal de 0 V del controlador SPC (masa del sistema).

10.4 Cableado de la salida de relé

El controlador SPC dispone de 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 puede conmutar un voltaje nominal de 30 V c. c. (carga no inductiva).

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



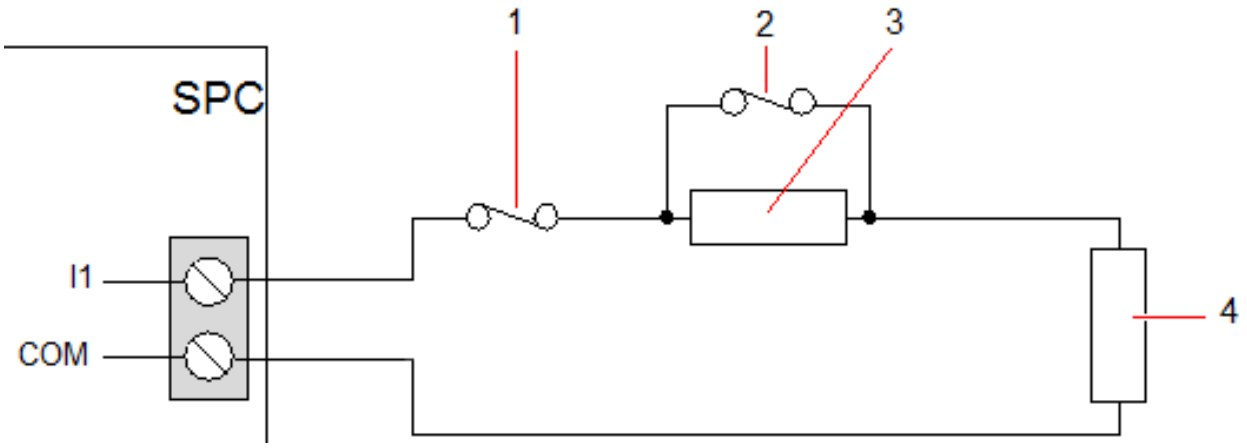
Cableado estándar

NA	Terminal Normalmente Abierto
COM	Conexión de terminal común
NC	Terminal Normalmente Cerrado

10.5 Cableado de entradas de zona

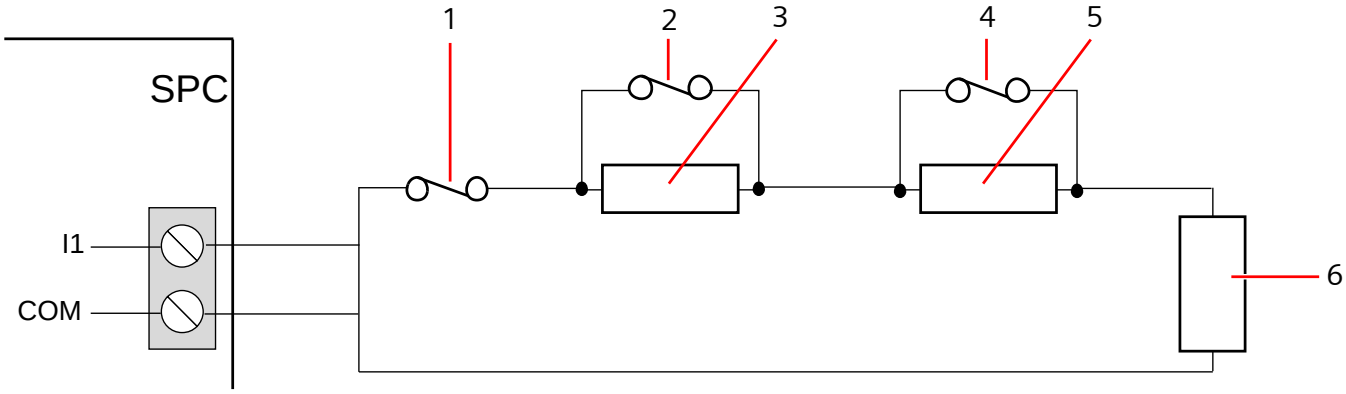
El controlador SPC cuenta con 8 entradas de zona incorporadas. Por defecto, estas entradas se vigilan mediante la supervisión RFL. El instalador puede elegir entre cualquiera de las siguientes configuraciones a la hora de cablear las entradas:

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



Configuración predeterminada (2 RFL 4K7)

1	Tamper
2	Alarma
3	RFL 4K7
4	RFL 4K7



Configuración de PIR antienmascaramiento

1	Tamper
2	Alarma
3	RFL 4K7
4	Fallo
5	RFL 2K2
6	RFL 4K7

En la siguiente tabla figuran los rangos de resistencia asociados a cada configuración.

1 RFL

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	1 kΩ	1,3 kΩ	23 kΩ	N/A	Infinito

	(-30%)		(+30%)			
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
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

2 RFLs 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	2700 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%)

2 RFLs

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%)
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	3,0 kΩ	3,9 kΩ	4,5 kΩ	6 kΩ	7,5 kΩ

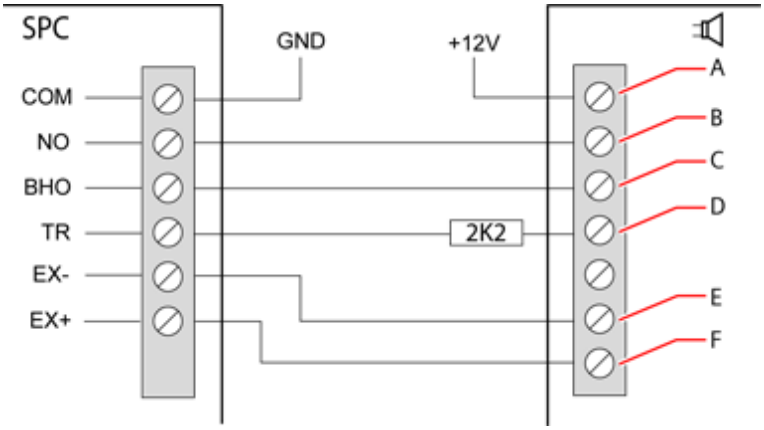
	(-30%)		(+30%)	(-25%)		(+25%)
DUAL_3K3_3K3	2,3 kΩ (-26%)	3,3 kΩ	4,3 kΩ (+31%)	4,9 kΩ (-26%)	6,6 kΩ	8,3 kΩ (+26%)
DUAL_3K9_8K2	7,0 kΩ (-15%)	8,2 kΩ	9,5 kΩ (+16%)	10,5 kΩ (-14%)	12,1 kΩ	13,8 kΩ (+15%)
DUAL_4K7_2K2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	5 kΩ (-28%)	6,9 kΩ	8,8 kΩ (+28%)
DUAL_4K7_4K7	3,3 kΩ (-30%)	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 **B**ell **H**old **O**ff (BHO) y **TR** (**T**amper Return) conectadas a sus entradas respectivas en la interfaz de la sirena exterior.

La placa del controlador dispone de una resistencia (2K2) premontada entre los terminales BHO y TR. Al cablear una sirena exterior, debe conectar esta resistencia en serie desde el terminal TR del controlador al terminal TR de la interfaz de la sirena exterior.



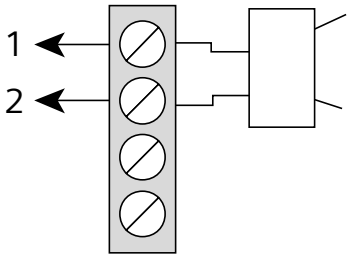
Cableado de la sirena exterior

A	Flash +
B	Flash –
C	Hold Off
D	Retorno tamper

E	Sirena -
F	Sirena +

10.7 Cableado de una sirena interna

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



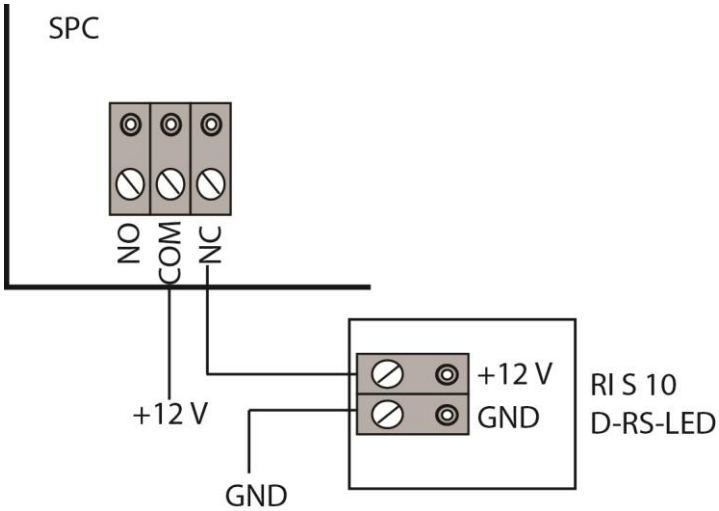
Cableado de la sirena interna (12 V)

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.

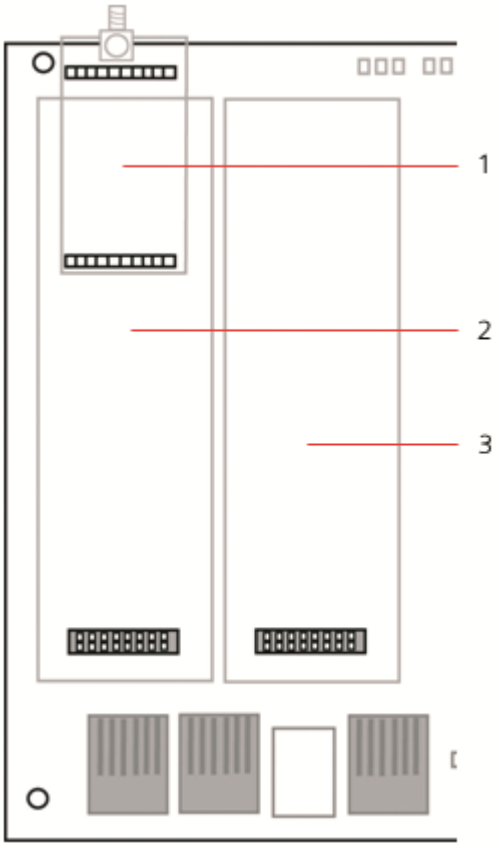
Para más información sobre el cableado de los sensores de rotura de cristal a la interfaz de rotura de cristal, véase la documentación específica del producto.

10.9 Instalación de módulos complementarios

Se pueden instalar dos módems (RTB o GSM) en la placa del controlador para mejorar la funcionalidad. La siguiente figura muestra las dos ranuras disponibles para cada módem: la ranura principal (izquierda) y la ranura de copia de seguridad (derecha).

Si están disponibles ambas ranuras del módem, instale siempre el módulo complementario en la ranura principal; el sistema siempre intenta realizar llamadas RTB o GSM en un módem instalado en la ranura principal antes de probar a hacerlo en la ranura de copia de seguridad.

	⚠ 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 complementarios

1	Ranura de receptor vía radio
2	Ranura del módem principal
3	Ranura del módem de copia de seguridad

Consulte las instrucciones en el correspondiente manual de instalación.

11 Encendido del controlador SPC

El controlador SPC posee dos fuentes de alimentación: la red eléctrica y la batería integral en espera. Un técnico en electricidad cualificado deberá realizar la conexión a la red, y la red eléctrica se deberá conectar desde una punta que se pueda aislar. Consulte la página [→ 366] para obtener más detalles sobre tamaños de conductores, especificaciones de fusibles, etc.

El controlador SPC debe recibir la alimentación, en primer lugar, de la red eléctrica y, a continuación, de la batería interna en espera. Para cumplir con los estándares EN, únicamente se debe colocar una batería con la capacidad adecuada.

11.1 Alimentación únicamente con batería

Se recomienda que, al suministrar energía a un sistema únicamente desde una batería, ésta debe estar en estado completamente cargado (>13,0 V). El sistema no se encenderá si se utiliza una batería con menos de 12 V y no está conectada la red eléctrica.

	AVISO
	La batería seguirá suministrando energía al sistema hasta que se detecte el nivel de descarga mínimo (entre 10,5 V y 10,8 V). El tiempo que el sistema aguante con la batería dependerá de la carga externa y el amperaje de dicha 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

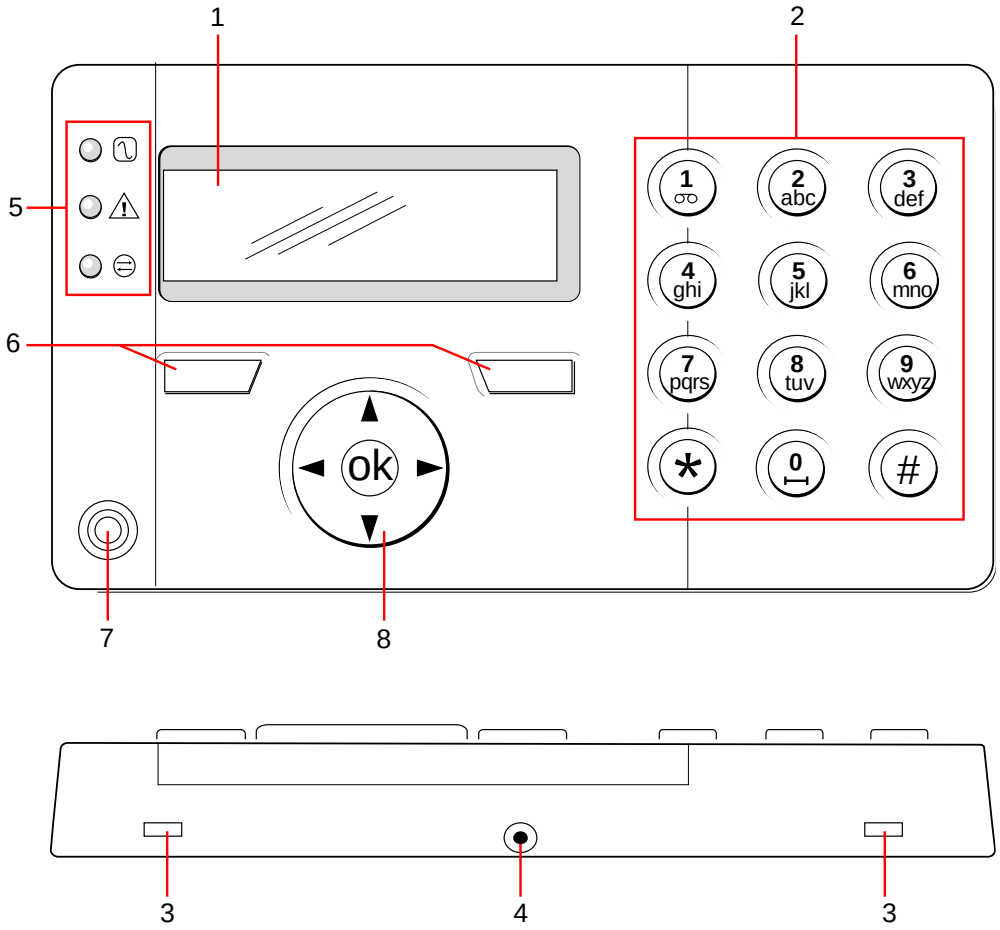
12.1.1 Introducción

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 el Manual de usuario del SPCK420/421 para más información sobre la programación de usuario).

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 proximidad de dispositivos Portable ACE (PACE) (consulte la página [→ 364]).



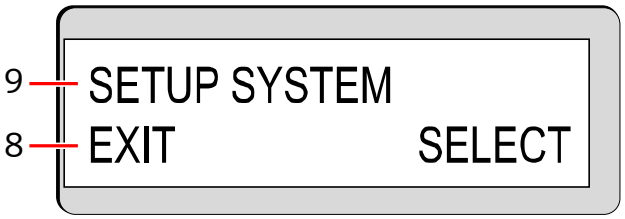
Teclado LCD

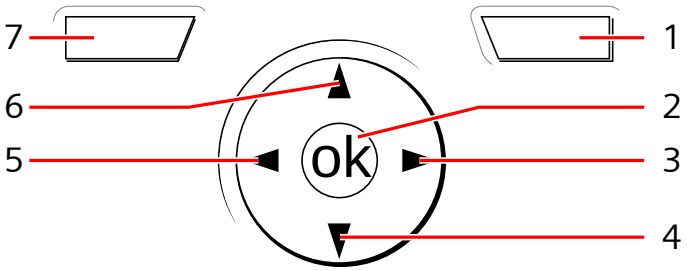
1	Pantalla LCD	La pantalla del teclado (2 líneas de 16 caracteres) muestra todos los mensajes de incidencias y de advertencia, además de proporcionar una interfaz visual para la programación del sistema (sólo programación de técnico). De la pantalla se puede ajustar el contraste y las condiciones en 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.
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 está equipado con un receptor de dispositivo en proximidad (consulte la página [→ 364]), los usuarios deberán colocar el mando Portable ACE dentro de un área de 1 cm para ARMAR/DESARMAR el sistema.
8	Tecla multifunción de	La tecla multifunción de navegación, en combinación con la pantalla del teclado, proporciona una interfaz para programar el sistema.

	navegación	

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 alimentación de CA FIJO: alimentación 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. OFF: 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 de X-BUS (Rojo)		Indica el estado de las comunicaciones de X-BUS durante la programación en modo técnico total 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 del controlador X-BUS, el LED permanece en estado ON.

12.1.2 Uso de la interfaz del teclado LCD





Pantalla del teclado

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 mostrada en la línea superior → ENTER para introducir los datos que aparecen en la línea superior → SIGUIENTE para ver la siguiente alerta después de la que se muestra en la línea superior → BORRAR para borrar la alerta que se muestra en la línea superior → SALVAR para guardar 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 la sección sobre priorización de mensajes en pantalla)
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. (Véase Priorización de mensajes en pantalla más 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 c.a.
  - Batería
  - Fallo Fuente alimentación

  - Fallo Aux
  - Fusible sirena exterior
  - Fusible sirena interior
  - Tamper de sirena
  - Tamper de caja
  - Tamper auxiliar 1
  - Tamper auxiliar 2
  - Interferencia vía radio
  - Transmisor 1
  - Línea transmisor 1
  - Fallo transmisor 2
  - Línea transmisor 2
  - Comunicación
  - Pánico usuario
  - Fallo cable XBUS
  - Fallo comunicación XBUS
  - Fallo c.a. XBUS
  - Fallo batería XBUS
  - Fallo fuente alimentación XBUS
  - Fallo fusible XBUS
  - Fallo tamper XBUS
  - Fallo antena XBUS
  - Interferencia vía radio XBUS
  - Pánico XBUS
  - Incendio XBUS
  - Alarm.médica XBUS
  - Enlace fuente alimentación XBUS
  - Tamper de salida XBUS
  - Bajo voltaje XBUS
  - Reset de técnico requerido
  - Autoarmado
- Información del sistema
  - Zonas en pruebas
  - Zonas abiertas
  - Estado de partición
  - Batería baja (detector)
  - Detector perdido
  - Batería baja PAT
  - PAT perdido
  - Test PAT retrasado
  - Cámara fuera de línea
  - Mando batería baja
  - Corriente excesiva XBUS
  - Nombre instalador
  - Teléfono instalador

- Técnico habilitado
- Fabr.habilitado
- Reiniciar
- Fallo hardware
- Sobrecorriente aux.
- Baja batería
- Link 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. Más abajo se detalla el uso de la interfaz para cada tipo de operación.

Introducción de valores numéricos

En el modo de entrada numérica sólo se pueden introducir dígitos numéricos (0 - 9).

- Para mover la posición del cursor un carácter a la izquierda y a la derecha, pulse las flechas izquierda y derecha respectivamente.
- Para salir de la función sin guardar, pulse la tecla de menú ATRÁS.
- Para guardar la configuración programada pulse ENTER u OK.

Introducción de texto

En el modo de entrada de texto, se pueden introducir tanto caracteres alfabéticos (A-Z) como dígitos numéricos (0 – 9).

- Para introducir un carácter alfabético, pulse la tecla correspondiente el número de veces que sea necesario.
- 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 pulsada la tecla correspondiente durante dos segundos y, a continuación, suéltela.
- Para mover la posición del cursor un carácter a la izquierda y a la derecha, pulse las flechas izquierda y derecha respectivamente.
- Para salir de la función sin guardar, pulse ATRÁS.
- Para guardar la configuración programada pulse ENTER u OK.
- Para cambiar entre mayúsculas o minúsculas en un carácter alfabético, pulse las flechas arriba o abajo cuando el carácter se encuentra resaltado por el cursor.
- Para cambiar entre mayúsculas y minúsculas con los caracteres siguientes, pulse almohadilla (#).
- Para eliminar un carácter a la izquierda del cursor, pulse asterisco (*).

Selección de una opción de programación

En el modo de navegación, el usuario/técnico selecciona una de las opciones de programación predefinidas de una lista.

- Para desplazarse por la lista de opciones disponibles, pulse la flecha hacia arriba o hacia abajo.
- Para salir de la función sin guardar, pulse ATRÁS.

- Para guardar la opción seleccionada, pulse SALVAR u OK.

12.2 SPCK620/623

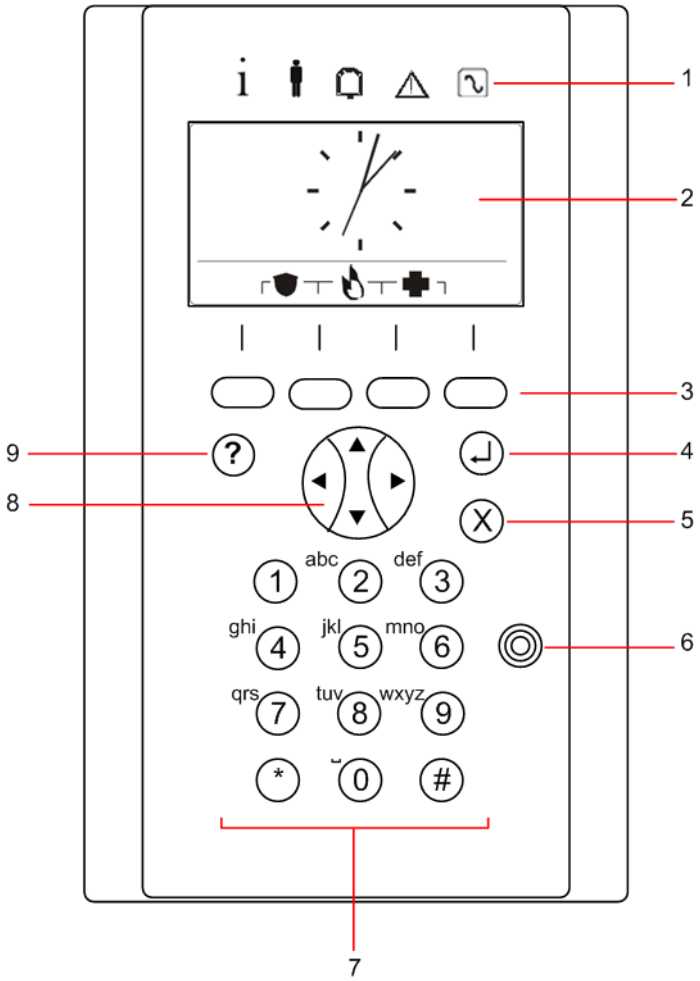
12.2.1 Introducción

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 el Manual de usuario del SPC620/623 para más información sobre la programación de usuario).

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.



1	LED indicadores de estado	Los LED indicadores de estado proporcionan información acerca del estado actual del sistema, como se describe en la siguiente tabla.
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 la sección sobre priorización de mensajes en pantalla). De la pantalla se pueden configurar las condiciones en las que se produce la retroiluminación.
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 proximidad de dispositivos, los usuarios deben ubicar el Portable ACE Fob dentro de una distancia de un 1 cm sobre esta área.
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. (Véase Priorización de mensajes en pantalla más 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 c.a.
  - Batería
  - Fallo Fuente alimentación
  - Fallo Aux
  - Fusible sirena exterior
  - Fusible sirena interior
  - Tamper de sirena
  - Tamper de caja
  - Tamper auxiliar 1
  - Tamper auxiliar 2
  - Interferencia vía radio
  - Transmisor 1
  - Línea transmisor 1
  - Fallo transmisor 2
  - Línea transmisor 2
  - Comunicación
  - Pánico usuario
  - Fallo cable XBUS
  - Fallo comunicación XBUS
  - Fallo c.a. XBUS
  - Fallo batería XBUS
  - Fallo fuente alimentación XBUS
  - Fallo fusible XBUS
  - Fallo tamper XBUS
  - Fallo antena XBUS
  - Interferencia vía radio XBUS

  - Pánico XBUS
  - Incendio XBUS
  - Alarm.médica XBUS
  - Enlace fuente alimentación XBUS
  - Tamper de salida XBUS
  - Bajo voltaje XBUS
  - Reset de técnico requerido
  - Autoarmado
- Información del sistema
  - Zonas en pruebas
  - Zonas abiertas
  - Estado de partición
  - Batería baja (detector)
  - Detector perdido
  - Batería baja PAT
  - PAT perdido
  - Test PAT retrasado
  - Cámara fuera de línea
  - Mando batería baja
  - Corriente excesiva XBUS
  - Nombre instalador
  - Teléfono instalador
  - Técnico habilitado
  - Fabr.habilitado
  - Reiniciar
  - Fallo hardware
  - Sobrecorriente aux.
  - Baja batería
  - Link Ethernet
  - Nombre del sistema

12.2.2 Descripción de LED

Descripción	Símbolo	Color	Funcionamiento	Descripción
Información	i	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 inactivo. 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

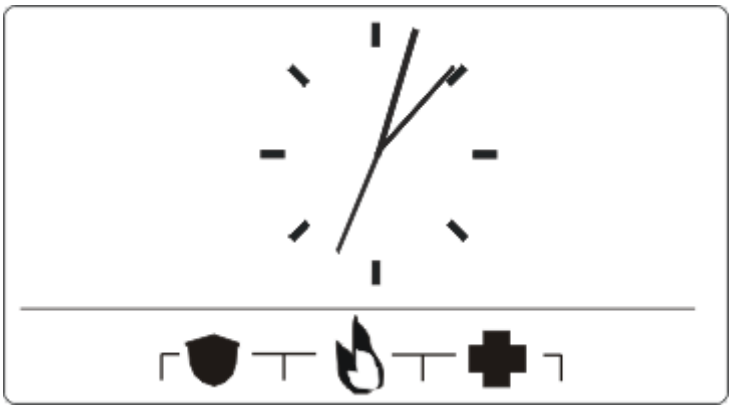
Existen dos modos de visualización (automático):

- Vista multipartición: el usuario tiene acceso a varias particiones. La visualización de las particiones se realiza mediante grupos de partición. Si no hay ningún grupo de partición configurado, sólo se visualiza el grupo general "Todas mis particiones".
- Vista de partición única: el usuario únicamente posee atribuciones para 1 partición. En la vista de partición única, sólo se muestra una partición en fuentes de gran tamaño pudiéndose controlar directamente.

	AVISO
	Las atribuciones de un usuario se pueden restringir mediante la configuración de usuario o la configuración del teclado en el que el usuario está iniciando sesión. La partición sólo se muestra si el usuario y el teclado que se está utilizando para iniciar la sesión tienen atribuciones para esa partición. Si el usuario posee atribuciones para varias particiones pero el teclado sólo tiene atribuciones para una partición, el usuario también verá la vista de partición única.

12.2.4 Teclas de función en estado inactivo

Emergencia

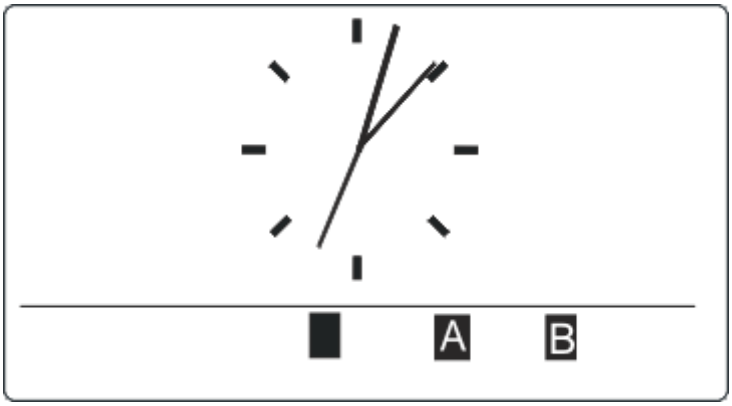


Las teclas de emergencia se muestran en función de la configuración. Al pulsarse simultáneamente las teclas se activa una llamada de emergencia.

	Alarma de pánico
	Alarma incendio
	Alarma medica

El proceso activado depende de la configuración del sistema. Para más información, consulte al instalador.

Configuración directa



Dependiendo de la configuración, se visualiza la opción de armado directo. Para la partición asignada al teclado es posible realizar un armado forzado / armado parcial sin PIN.

13 Herramientas de software de apoyo

Las siguientes herramientas de software para PC están disponibles 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.
- SPC Safe
  Proporciona administración automatizada de sitios remotos de un sistema SPC.
- SPC Remote Maintenance
  Proporciona supervisión y servicio técnico remoto automatizado de un sistema SPC.

14 Inicio del sistema

!	⚠ ATENCIÓN
	El sistema SPC debe ser instalado por un técnico instalador autorizado.

1. Para ello, conecte el teclado a la interfaz X-BUS del controlador.
2. Para acceder a la programación del técnico, introduzca el código de técnico por defecto (1111). Para más información, consulte Códigos de técnico [→ 106].

14.1 Modos de técnico

El sistema SPC funciona con dos modos de programación para técnicos instaladores autorizados: completo y parcial. En el navegador, sólo se puede cerrar sesión en el modo Técnico parcial.

Modo Técnico total

Se deben aislar o borrar todas las alertas, fallos y tampers antes de poder salir del modo Técnico total.

El modo Técnico total ofrece una funcionalidad completa para programar. Sin embargo, la programación con el modo Técnico total deshabilita la configuración de todas las alarmas, informes y la programación de salida del sistema. Para una revisión completa de las opciones de menú del modo Técnico total, consulte la página [→ 114].

Modo Técnico [parcial]

El modo Técnico parcial proporciona menos funciones de programación y no afecta a ninguna de las salidas programadas en el sistema. Para una visión completa de las opciones de menú del modo Técnico parcial, consulte la página [→ 113].

14.1.1 Códigos técnico

El código de programación del técnico es, por defecto, "1111".

Si una instalación ha cambiado de Grado 2 a Grado 3 en algún momento después del inicio, todos los códigos tendrán el prefijo 0. Por lo tanto, el código de técnico por defecto será "01111".

Al aumentar el número de dígitos para el código (véase Opciones del sistema [→ 234]) se añadirá el número de ceros correspondiente delante del código existente (por ejemplo, 001111 para un código de 6 dígitos)

!	*Aviso*
	Si el código por defecto 1111 está habilitado, por ejemplo, en una nueva instalación SPC, deberá cambiar el código de técnico en la central. Si no cambia su código, recibirá un mensaje de información que le obligará a cambiar su código por defecto antes de que cierre la sesión en modo técnico completo.

14.2 Herramientas de programación

Teclado

El teclado proporciona acceso rápido in situ a los menús y a la programación del sistema. El técnico autorizado para realizar instalaciones debe establecer la configuración inicial por defecto con el teclado. La programación del lector de tarjetas o dispositivos en proximidad, y la asignación a los usuarios también se deben realizar con el teclado.

SPC Pro

SPC Pro es una aplicación de software que le permite configurar sistemas SPC tanto en línea como fuera de línea. La herramienta de programación SPC Pro ofrece comunicación avanzada adicional y funcionalidad X-10 que no está disponible en el teclado. Las actualizaciones de firmware también se pueden realizar mediante el SPC Pro.

SPC Pro admite la conectividad con un controlador SPC a través de USB, puerto de serie, Ethernet y módem RTB/GSM.

14.2.1 Programador rápido

El Programador rápido del SPC es un dispositivo de almacenamiento portátil que ofrece al técnico la posibilidad de cargar y descargar ficheros de configuración de forma rápida y eficaz. El Programador rápido se puede utilizar junto con todas las herramientas de programación anteriormente indicadas. Para obtener más detalles, consulte la página [→ 328].

El Programador rápido puede realizar actualizaciones de firmware.

14.3 Configuración de los parámetros de inicio

La siguiente configuración de inicio se puede modificar en un momento posterior cuando se 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 en el teclado.
   - Después de cada ajuste, pulse NEXT (siguiente) para desplazarse al siguiente ajuste.
2. Seleccione el IDIOMA en el que se mostrará el asistente de configuración.
3. Seleccione la REGIÓN correspondiente.
   - EUROPA, SUECIA, SUIZA, BÉLGICA, ESPAÑA REINO UNIDO, IRLANDA, ITALIA, , , , CANADÁ, EE.UU.
4. Seleccione un 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 el autoarmado, bloqueos temporales, grupos de particiones interrelacionadas y tipo de zona sísmica.

Para más información sobre descripciones de zona por defecto, consulte Configuración por defecto de modos doméstico, comercial y financiero [→ 357].

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, consulte las secciones correspondientes en "Actualizar idiomas" para el teclado, el navegador y el SPC Pro.
8. Introduzca la FECHA y la HORA.
   ⇨ El sistema explora el X-BUS en busca de módems.
9. Seleccione el modo de direccionamiento X-BUS:
   - MANUAL: recomendado para la mayoría de los tipos de instalación, especialmente cuando se realiza una preconfiguración.
   - AUTO: se recomienda solo para instalaciones muy pequeñas.
10. Seleccione la topología de la instalación: LAZO (anillo) o PUNTA (cadena).
    ⇨ El sistema busca la cantidad de teclados, módulos de expansión, controladores de puerta y entradas de zona disponibles.
11. Pulse SIGUIENTE para explorar todos los dispositivos X-BUS.
    ⇨ Se mostrará MODO PROGRAMAC.
    ⇨ La configuración de inicio se ha completado.
12. Compruebe las alertas en el menú ESTADO SISTEMA > ALERTAS. De lo contrario, no podrá salir del modo técnico.

13. Configure el sistema mediante teclado, SPC Pro o navegador web.

Ver también

- Configuración por defecto de modos doméstico, comercial y financiero [→ 357]

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

Consulte la sección Añadir Usuarios:

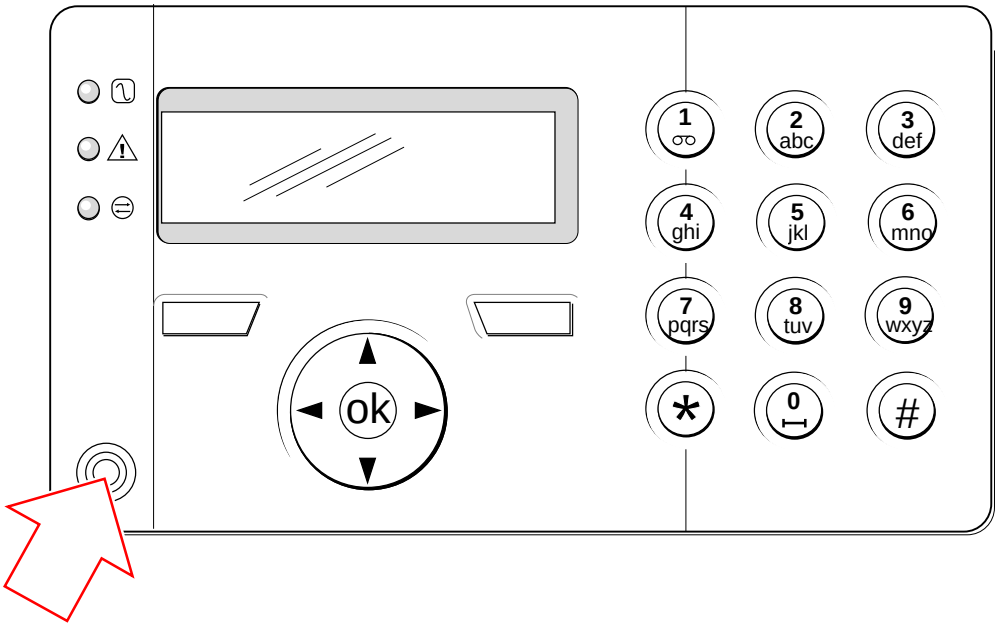
La capacidad de permitir al fabricante el acceso al sistema (es decir, a realizar una actualización de firmware de la central) se configura como un derecho del usuario para un perfil de usuario. Si a un usuario se le va a permitir actualizar el firmware, asegúrese de que dicho usuario posee el perfil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

Ver también

- Códigos técnico [→ 106]

14.5 Programación de Portable ACE

El teclado del SPC se puede configurar con un lector de tarjetas o de dispositivos de proximidad. Los usuarios cuyos perfiles estén configurados de esa forma pueden ARMAR o DESARMAR el sistema, así como realizar la programación, en función del nivel del perfil. Cuando se ha programado un dispositivo de proximidad en el teclado, el usuario tiene la posibilidad de armar o desarmar el sistema o de introducir la programación del usuario colocando el dispositivo a 1 cm del área del receptor del teclado.



Área del receptor del teclado

Para programar un Portable ACE en el teclado:

1. Introduzca el código de programación de técnico. (El código por defecto es 1111. Consulte Códigos de técnico [→ 106])
2. Desplácese a USUARIOS.
3. Pulse SELECC.
4. Seleccione EDITAR y a continuación seleccione USER1 de la lista.
5. Desplácese a PACE y pulse SELECC.
6. Seleccione HABILITAR o DESHABILITAR la función PACE.
   ⇨ El teclado mostrará PASO ACTUAL parpadeando en la línea superior de la pantalla.
7. Coloque el mando PACE a 1 cm dentro del área del receptor del teclado.

⇨ El teclado indica que el dispositivo se ha registrado mostrando el texto PASO CONFIGURADO.

Para deshabilitar un Portable ACE en el sistema:

1. Introduzca el código de programación de técnico. (El código por defecto es 1111. Consulte Códigos de técnico [→ 106])
2. Desplácese a USUARIOS.
3. Pulse SELECC.
4. Seleccione EDITAR y a continuación seleccione USER1 de la lista.
5. Desplácese a PACE y pulse SELECC.
6. Cambie a la opción DESHABILITADO.

⇨ El teclado indica 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 a través del teclado.

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

1. Introduzca el código de programación de técnico (el código por defecto es 1111. Consulte Códigos de técnico [→ 106]).
2. Con los botones de flecha arriba/abajo, desplácese a 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 VÍA RADIO y pulse SELECC.
7. Desplácese hasta la opción HABILITADO y pulse SELECC.
   ⇨ El mensaje PULSE TECL. MANDO parpadeará en la línea superior de la pantalla.
8. Coloque el mando dentro de un radio de 8 metros de distancia del teclado y pulse una de las teclas.

⇨ Se mostrará el mensaje MANDO CONFIGURD. para indicar que el dispositivo ha quedado registrado.

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

1. Introduzca el código de programación de técnico (el código por defecto es 1111. Consulte Códigos de técnico [→ 106]).
2. Con los botones de flecha arriba/abajo, desplácese a 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 VÍA RADIO y pulse SELECC.
6. Cambie a la opción DESHABILITADO y pulse SALVAR.

Si no se detecta ningún receptor vía radio de 868 MHz en el sistema, la opción MANDO VÍA RADIO no aparece en el menú del teclado.

Número de mandos vía radio por usuario: Sólo se puede programar un dispositivo de mando por cada usuario. Para cambiar los dispositivos de mando entre usuarios, repita el procedimiento de programación para cada nuevo dispositivo. Los dispositivos de mando antiguos se pueden preparar para que puedan ser utilizados por diferentes usuarios.

14.6.1 Borrado de alertas utilizando el mando

Las alertas en el sistema SPC se borran normalmente mediante la opción RESTAURAR del teclado. El borrado de alertas también se puede realizar utilizando 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 a RESTAUR.TECLADO y pulse SELECC.
5. Cambie la configuración a HABILITADO y pulse SALVAR.

15 Programación de técnico parcial a través del teclado

Esta sección proporciona opciones de programación de técnico [parcial] empleando el teclado LCD.

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

1. Introduzca un código de técnico válido (el código de técnico por defecto es 1111. Para más información, consulte Códigos de técnico [→ 106]).
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.

1	ARMADO	Realiza un desarmado, armado total o armado parcial en el sistema. Consulte la página
2	INHIBIDA	Muestra una lista de las zonas anuladas en el sistema. Consulte la página
3	AISLADA	Permite al técnico aislar zonas en el sistema. Consulte la página [→ 158]
4	REG. INCIDENC.	Muestra una lista de las incidencias más recientes del sistema. Consulte la página [→ 158]
5	REGISTRO ACCESO	Muestra una lista de los accesos más recientes del sistema. Consulte la página
6	REGISTRO ALARMAS	Muestra una lista de alarmas recientes.
7	CAMBIO COD.TECN.	Permite al técnico cambiar el código del técnico. Consulte la página [→ 159]
8	USUARIOS	Permite al técnico añadir, editar o eliminar usuarios. Consulte la página [→ 159]
9	SMS	Permite al usuario añadir, editar o borrar detalles de SMS para usuarios. Consulte SMS [→ 164]

Ver también

- TEST [→ 153]
- CONTROL PUERTA [→ 167]
- Programación de técnico a través del teclado [→ 114]
- TEXTO INSTALAD. [→ 167]
- FECHA/HORA [→ 166]
- SMS [→ 164]

16 Programación de técnico a través del teclado

Esta sección proporciona opciones de programación de técnico [total] empleando el teclado LCD.

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

1. Introduzca un código de técnico válido (el código de técnico por defecto es 1111. Para más información, consulte Códigos de técnico [→ 106]).
2. Pulse SELECC. para escoger la programación TÉCNICO TOTAL.
3. Con las flechas arriba/abajo, desplácese hasta la opción de programación deseada.
4. Se ha implementado una función de selección rápida. Pulse # para seleccionar un parámetro (p. ej. un atributo de zona). El parámetro seleccionado aparece con un * (p. ej. *Anulación).

⇨ Tras finalizar con las opciones de programación, el teclado muestra ACTUALIZADO momentáneamente.

16.1 Estado 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 pruebas.
ELEM. 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	Se muestra el tiempo de batería remanente, la tensión y la corriente de la batería. Deberá introducir los valores de **capacidad de la batería** y **Máxima corriente** en OPCIONES para poder ver el tiempo de batería remanente en el teclado, en el caso de producirse un fallo de la red de alimentación. Esto se indica en el menú ESTADO - BATERÍA - DURACIÓN BATERÍA. Este menú también indica si hay un fallo de batería.
AUX	Se muestra el voltaje y la corriente de la alimentación auxiliar.

	AVISO
	Los usuarios no pueden salir de la programación TÉCNICO TOTAL si existen condiciones de fallo. El primer fallo se mostrará en el teclado cuando intente salir del modo Técnico. Puede ver e inhibir todos los fallos dentro del menú de estado del sistema, en Alertas y Zonas abiertas.

16.2 OPCIONES

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

⇨ Las opciones de programación que se muestran en el menú OPCIONES varían en función del grado de seguridad del sistema (vea la columna de la derecha).

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

Variable	Descripción	Por defecto
Grado EN50131	Determina el grado de seguridad de la instalación SPC. ● Irlanda y Europa: – EN50131 Grado 2 – EN50131 Grado 3 – Modo libre ● Reino Unido: – PD6662 (basada en EN50131 Grado 2) – PD6662 (basada en EN50131 Grado 3) – Modo libre ● Suecia: – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Modo libre ● Bélgica: – TO-14 (basada en EN50131 Grado 2) – TO-14 (basada en EN50131 Grado 3) – Modo libre ● Suiza: – SWISSI Cat 1 – SWISSI Cat 2 – Modo libre ● España – EN50131 Grado 2 – EN50131 Grado 3 ● Alemania – VdS Clase A – VdS Clase C	Grado: 2 País: n/d

Variable	Descripción	Por defecto
	– Modo libre ● Francia – NF tipo 2 – NF tipo 3 – Modo libre	
REGIÓN	Determina los requisitos regionales específicos que cumple la instalación. Las opciones son GB, IRLANDA, EUROPA, SUECIA, SUIZA, BÉLGICA, ALEMANIA y FRANCIA	
TIPO INSTALACIÓN	Determina si SPC se está instalando para utilizar en un negocio comercial o en una residencia privada. Elija entre COMERCIAL (consulte la página [→ 339]), DOMÉSTICA (consulte la página [→ 338]) o FINANCIERA.	Doméstica

Consulte la sección Opciones del sistema [→ 234] para más información sobre las siguientes OPCIONES.

ARMADO PARCIAL A	Renombrar Temporizado Acceso a E/S E/S con alarma LOCAL
ARMADO PARCIAL B	Renombrar Temporizado Acceso a E/S E/S con alarma LOCAL
Mens.llam.CRA	MOSTRAR MENSAJE (HABILITADO/DESHABILITADO)
Confirmación	VDS DD243: GARDA EN50131-9
Confirm.zonas	Seleccionar Nº DE ZONAS.
Auto reset	HABILITADO/DESHABILITADO
Reset al desrm.	HABILITADO/DESHABILITADO
CÓDIGO COACCIÓN	Deshabilitar Código + 1 Código + 2
Redisp. sirena	HABILITADO/DESHABILITADO
Sirena primero	HABILITADO/DESHABILITADO
Sir.fall.armd.	HABILITADO/DESHABILITADO
Flash fall.ar.	HABILITADO/DESHABILITADO
Alarma al salir	HABILITADO/DESHABILITADO Solo disponible en modo Configur.técnico pues la configuración no cumple con la norma EN50131.
IDIOMA	Idioma sistema IDIOMA EN REPOSO
Dígitos códigos	4 DÍGITOS 5 DÍGITOS 6 DÍGITOS

	7 DÍGITOS 8 DÍGITOS
Restaur. coded	HABILITADO/DESHABILITADO
Acc.web.perm.	HABILITADO/DESHABILITADO Permite/restringe el acceso al navegador web.
ZON.ABIER.	HABILITADO/DESHABILITADO
Acceso técnico	HABILITADO/DESHABILITADO
Acceso fabrican. *	HABILITADO/DESHABILITADO
Ver estado.sist.	HABILITADO/DESHABILITADO
Resist.fin línea	Ninguna 1 RFL 1K 1 RFL 1K5 1 RFL 2K2 1 RFL 4K7 1 RFL 10K 1 RFL 12K 2 RFLs 1K / 470R 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.
Tarjeta y código	HABILITADO/DESHABILITADO
Rest.con des.	HABILITADO/DESHABILITADO **Nota:**Para cumplir la norma PD6662 se debe deshabilitar esta opción.
Restaur.técnico	HABILITADO/DESHABILITADO
Tamp.fuera línea	HABILITADO/DESHABILITADO
BLOQUEO TÉCNICO	HABILITADO/DESHABILITADO Si está habilitado, el sistema no se puede restaurar con el botón amarillo del controlador, a no ser que se introduzca un código de técnico en el teclado.
Código generado	HABILITADO/DESHABILITADO
Config.reloj	DST automático SINC HORA RED CA
SOSPECHA AUDIBLE	HABILITADO/DESHABILITADO
Ver cámaras	HABILITADO/DESHABILITADO

Test sísmicos ON	HABILITADO/DESHABILITADO
Arm.prohb.alert.	HABILITADO/DESHABILITADO
Arm. antienmasc.	Deshabilitar TAMPER Fallo Alarma
Des.antienmasc.	Deshabilitar TAMPER Fallo Alarma
REDISPARO INTIMIDACIÓN	HABILITADO/DESHABILITADO
Rearme pánico	HABILITADO/DESHABILITADO
Silenc.ver.audio	HABILITADO/DESHABILITADO
Salir modo Ing.	HABILITADO/DESHABILITADO

* No disponible para SPC42xx, SPC43xx.

16.3 Temp/Retardos

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

Temporizaciones

Designación de las funciones en el siguiente orden:

- 1.ª fila: Web/SPC Pro
- 2.ª fila: Teclado

Temporizador	Descripción	Por defecto
Audible		
Sirenas interiores Tiempo Sirena interior	Tiempo que sonarán las sirenas interiores cuando la alarma esté activada. (1 – 15 minutos: 0 = nunca))	15 min.
Sirenas exteriores Tiempo Sirena exterior	Retardo activación sirenas exteriores. (1 – 15 minutos: 0 = nunca)	15 min.
Retardo sirena exterior Retardo.sir.ext.	Provocará una activación retardada de la sirena exterior. (0 – 600 segundos)	0 segundos
Chime TEMP.CHIME	Número de segundos que se activará la salida de chime cuando se abra una zona con atributo CHIME. (1 – 10 segundos)	2 segundos
Confirmación		
Confirmar TIEMPO CONFIRM.	● **Nota**: Solo disponible cuando el grado de seguridad es "Libre" y se ha seleccionado "DD243" para la variable "Confirmación". (Consulte Opciones del sistema [→ 234]) Este temporizador se aplica a la función de confirmación de alarma y se define como el tiempo máximo entre alarmas de zonas diferentes no solapadas para generar una alarma confirmada. (30 – 60 minutos)	30 min.
Atraco confirmado	Este temporizador se aplica a la función de atraco confirmado y se define como el tiempo máximo entre alarmas de zonas diferentes no solapadas para generar una alarma confirmada.	480 min.

Temporizador	Descripción	Por defecto
	(480 - 1200 minutos)	
Retardo TX RETARDO TX	Cuando está programado, el retardo de marcación inicia un período de retardo predefinido (de 0 a 30 segundos) antes de que el sistema llame a un CRA. Esta opción está específicamente diseñada para reducir respuestas sin fiabilidad de CRAs y comisarías de policía. En caso de que salte una zona posterior, el periodo de retardo del marcador se ignora y éste llama inmediatamente. (0 – 30 segundos)	30 segundos
Abortar alarma ABORTAR ALARMA	Tiempo tras transmitirse una alarma en el que se puede transmitir un mensaje de interrupción de alarma. (0 – 999 segundos)	30 segundos
Armado		
Autorización de armado AUTORIZ. ARMADO	Período durante el cual es válida la autorización de armado. Introduzca un valor entre 10 y 250 segundos.	20 segundos
Fin de salida FIN DE SALIDA	El tiempo de fin de salida es el número de segundos que se retarda el armado después de que una zona programada con el atributo Fin de salida se cierre. (1 – 45 segundos)	7 segundos
Sirena con armado total SIR.ARM.TOTAL	Activa la sirena exterior momentáneamente para indicar un estado totalmente armado. (0 – 10 segundos)	0 segundos
Flash con armado total FLAH.ARM.TOTAL	Activa el flash en la sirena exterior momentáneamente para indicar un estado totalmente armado. (0 – 10 segundos)	0 segundos
Fallo al armar FALLO AL ARMAR	Núm. de seg. para mostrar el mensaje de fallo al armar en teclados (0: Hasta introducir código válido). (0 – 999 segundos)	10 segundos
Alarma		
Doble detección DOBLE DETECCIÓN	Máximo retardo entre activaciones de zonas con doble detección para generar alarma. (1 – 99 segundos)	10 segundos
Pruebas Zonas en pruebas	Número de días en test de zona antes de retornar automáticamente al modo normal. (1 – 99 días)	14 días
Intervalo test sísmico AUTOTEST SÍSMICO	El tiempo medio entre tests automáticos de detector sísmico (12 – 240 horas) **Nota**: Para habilitar la comprobación automática, el atributo **test de detector automático** debe estar habilitado para una zona sísmica.	168 horas.
Duración test sísmico T TEST SÍSMICO	Tiempo máximo de alarma (seg) en respuesta a un test. (3 - 120 segundos)	30 segundos
Bloqueo post-alarma BLOQUEO POST-ALARMA	Tiempo tras alarma en el que el acceso es denegado.	0 minutos
Flash sirena exterior Flash	Tiempo que el flash estará activo cuando se active una alarma. (1 – 15 minutos: 0 = indefinidamente)	15 min.
Incidencias		
Retardo red c. a. RETAR.FALLO C.A.	El tiempo que transcurre desde que se detecta un fallo de corriente antes de que el sistema active una alerta. (0 – 60 minutos)	0 min.
Técnico		
Acceso de técnico ACCESO DE TÉCNICO	El temporizador para el acceso a técnico comienza en cuanto el usuario habilita el acceso al técnico. (0 – 999 minutos. "0" indica que no hay limitación para acceso al sistema).	0 min.
Salida modo técnico automática SAL.AUTO.M.TÉC.	Tiempo de inactividad tras el cual el técnico finalizará la sesión automáticamente	0 minutos
Teclado		

Temporizador	Descripción	Por defecto
Retorno teclado a normal T.fallo.comunic.teclado	El número de segundos que esperará un RKD la introducción de la clave antes de salir del menú actual (10 – 300 segundos)	30 segundos
Idioma teclado Idioma teclado	Tiempo que espera el teclado en reposo antes de pasar al idioma por defecto (0 - 9999 segundos; 0 = nunca).	10 segundos
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. (1 – 999 segundos) Véase Edición de una zona [→ 251].	30 segundos
Reconocimiento alarma incendio RECONOCIMIENTO ALARMA INCENDIO	Tiempo adicional que se debe esperar antes de notificar una alarma de incendio para zonas con los atributos "Prealarma incendio" y "Reconocimiento alarma incendio" seleccionados. (1 – 999 segundos). Véase Edición de una zona [→ 251].	120 segundos
PIN		
PIN válido PIN VÁLIDO	Periodo en el que el PIN es válido en días (1 - 330)	30 días
Límite cambios de PIN LÍMITE CAMBIOS DE PIN	Número de cambios dentro de un periodo válido (1 - 50)	5
Aviso PIN AVISO EXP. PIN	Tiempo para expiración del PIN mostrado mediante aviso en display (1 - 14)	5 días
Configuración general		
Tiempo salida RF SALIDA RF	Tiempo en que permanece activa la salida RF del sistema (0 – 999 segundos)	0 segundos
Límite tiempo sincronismo LÍMITE TIEMPO SINCRONISMO	Límite de tiempo durante el cual no se notificará ninguna incidencia. (0 – 999 s) La sincronización de tiempo solo se produce si la hora del sistema y la hora de actualización están fuera de este límite.	0 segundos
T. fallo link T.ENLAC.EXC.	Tiempo de espera para fallo de Link Ethernet (0 = Deshabilitado) (0 - 250)	0 segundos
Cámara fuera de línea CAM.NO EN LÍNEA	Tiempo para cámara fuera de línea (10 - 9999)	10 segundos
Retardo técnico RETARDO TÉCNICO	Número de segundos de retardo para zonas técnicas con el atributo "retardo técnico". (0 – 9999 segundos)	0 segundos
Supervisada SUPERVISADA (!)	Este atributo sólo se aplica al Mantenimiento remoto. El número de horas que una zona debe abrirse por dentro si la zona está programada con el atributo **Uso frecuente**. (1 – 9999 horas)	336 horas (2 semanas)
Coacción silenciosa	Tiempo durante el cual la coacción permanecerá silenciosa y sin poderse restaurar desde el teclado (0 - 999).	0 minutos
Silencio con atraco/pánico	Número de minutos que un atraco/pánico permanecerá en silencio y sin poderse restaurar desde el teclado (0 - 999).	0 minutos

Los tiempos por defecto dependen de la configuración del técnico. Los tiempos por defecto indicados pueden permitirse o no y dependen de la configuración que realice el técnico.

16.4 PARTICIONES

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

AÑADIR	Para modo doméstico y comercial, el tipo de partición por defecto es estándar. En modo Financiero, seleccione el tipo de partición ESTÁNDAR, CAJERO AUTOMÁTICO, CÁMARA ACORAZADA o AVANZADO. Introduzca el nombre de la partición y la hora de entrada/salida preferida.
Editar	Edite los parámetros siguientes: ● DESCRIPCIÓN ● Robo E/S – Tiempo entrada – Tiempo salida – Sin temp.salida – Pul.v.rad.activ. ● A.parc.A/B – HABILITADO/DESHABILITADO – Temporizado – Acceso a E/S – E/S con alarma – LOCAL – Sin sirenas ● Partic.ligadas – Partición – Arm. total – Todo armad.total – Impedir a.total – IMPED.A.TOT.TODAS – Desarmado – Todo desarmado – Impedir desarmd. – Imped.desar.todo ● Automatiz. – Calendario – Arm/Desarmado automático – Bloqueo tiempo – Acceso cámara ● TX incidenc. – Armado prematuro – Armado tarde – Desarm.prematuro – Desarmado tarde ● Arm/Desarmado – Aviso autoarmado – Cancel.autoarm. – Retard.autoarm. – Conmut.llave – Interval.retraso – Contador retraso – Retard.desarmado

	– Duración desarm. – INTERBLOQ. – Código doble ● Salida RF
Borrar	Seleccione la partición que desee borrar.

Consulte Añadir/Editar una partición [→ 251] para más información sobre estas opciones.

16.5 Grupos particiones

1. Desplácese hasta GRUPOS PARTICIONES y pulse SELECC.
2. Desplácese a 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 desee borrar.

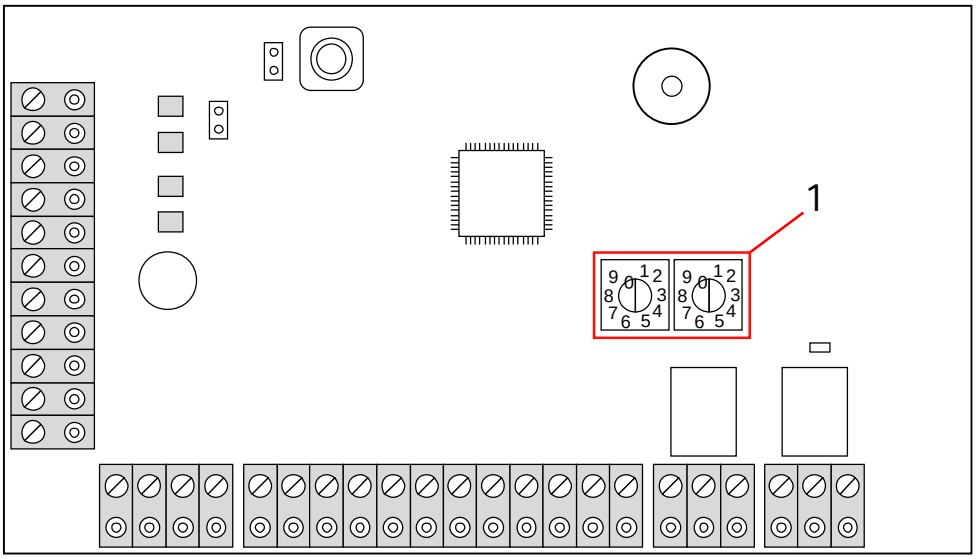
16.6 X-BUS

1. Desplácese a XBUS y pulse SELECC.
2. Desplácese a las opciones de programación deseadas como se muestra a continuación.

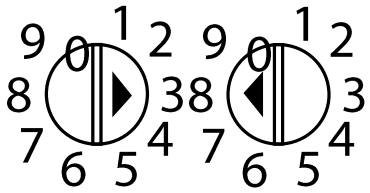
16.6.1 Direccionamiento X-BUS

Los módulos de expansión, teclados y zonas posteriores se pueden configurar, ubicar y vigilar siguiendo los pasos indicados en esta sección. En este menú también se accede a la configuración de X-BUS como tipo, tiempos de comunicación y reintentos.

La siguiente figura muestra cada conmutador rotativo con un símbolo de flecha que señala un número de identificación (p. ej. 3, 8). El conmutador derecho corresponde al dígito de las unidades y el de la izquierda al de las decenas. El módulo de expansión en la siguiente figura se identifica con el número 38.



Conmutadores rotativos

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, se asignan zonas a cada módulo de expansión de entrada.

El SPC41xx no admite módulos de expansión de direccionamiento automático.

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 el número 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 RECONFIGURACIÓN

	AVISO
	Una reconfiguración sólo se aplica a zonas cableadas en un módulo de expansión. Las zonas inalámbricas en un módulo de expansión y las zonas del controlador no se colocarán en línea tras una reconfiguración. Para colocar zonas de controlador en línea, se debe aplicar un tipo de zona que no sea "Sin utilizar" por medio del menú de zonas en el teclado o en el navegador web.

Si hay una mezcla de tipos de módulos de expansión (con y sin conmutadores rotativos) en el sistema, éste sólo puede ser reconfigurado automáticamente. Si el sistema tiene todos los módulos de expansión con conmutadores rotativos, también se puede reconfigurar automáticamente; el sistema omite la configuración de los conmutadores rotativos y asigna direcciones a todos los módulos de expansión del sistema.

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

Para reconfigurar teclados/módulos de expansión:

1. Desplácese a RECONFIGURAR.
2. Pulse SELECC.
   ⇨ Se muestra el número de teclados en línea.
3. Pulse SIGUIENTE.
   ⇨ Se muestra el número de módulos de expansión en línea.
4. Pulse SIGUIENTE
   ⇨ Se muestra el número de zonas en línea.
5. Pulse ATRÁS para salir.

16.6.4 TECLADOS / MÓDULOS DE EXPANSIÓN /

CONTROLADORES DE PUERTA

	AVISO
	Debe actualizar a la versión 1.1 del firmware antes de añadir controladores de puertas. Con versiones de firmware anteriores, los controladores de puertas son vistos por la central como módulos de expansión de E/S normales, por lo que las puertas se deben añadir manualmente.

16.6.4.1 Localizar

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

1. Desplácese a TECLADOS, MÓDULOS DE EXPANSIÓN o CONTROLADORES DE PUERTA y pulse SELECC.
2. Desplácese hasta LOCALIZAR y pulse SELECC.
3. Desplácese al módulo de expansión / teclado / controlador de puerta que desee localizar y pulse SELECC.
   ⇨ El dispositivo seleccionado emite una señal sonora y el LED parpadea para que el técnico pueda localizarlo.
4. Pulse ATRÁS para salir.

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

16.6.4.2 Supervisión

Para obtener una vista general de los módulos de expansión, teclados o controladores de puerta conectados al sistema:

1. Desplácese a TECLADOS, MÓDULOS DE EXPANSIÓN o CONTROLADORES DE PUERTA y pulse SELECC.
2. Desplácese a MONITOR y pulse SELECC.
3. Desplácese a la opción de programación de Monitor que desee.
4. Pulse SELECC.
   ⇨ Se muestra una lista de los teclados o módulos de expansión detectados.
5. Desplácese por la lista hasta el módulo de expansión / teclado / controlador de puerta que prefiera y pulse SELECC.
   ⇨ En la tabla que figura a continuación se muestran los parámetros y datos, si procede, para la edición:
6. Pulse ATRÁS para salir.

ESTADO	En línea o fuera de línea
Nº serie	Número de serie (para seguimiento e identificación)
Ver.	Versión de firmware

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 puertas.
Fusible auxiliar	El estado del fusible auxiliar en el módulo de expansión / controlador de puertas
F.A.	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 zona	Estado de entrada de cada zona asociada a un módulo de expansión de la forma siguiente: C: Cerrada, O: Abierta, D: Desconectada, S: Corta (sólo módulos de expansión con entradas)

16.6.4.3 EDITAR TECLADOS

Para editar teclados:

1. Desplácese a TECLADOS > EDITAR.
2. Pulse SELECC.
3. Desplácese al dispositivo que desee editar y pulse SELECC.
   ⇨ Los ajustes de configuración para un teclado estándar y un teclado confort se describen en las siguientes secciones.
4. Pulse ATRÁS para salir del menú.

Configuración del teclado LCD

Configure los siguientes ajustes para el teclado.

Descripción	Introduzca una descripción única para identificar el teclado.
Func. teclas laterales	
Pánico	Seleccione Habilitar, Deshabilitar o Habilit.silencio Cuando está habilitada, la alarma de pánico se activa pulsando las dos teclas programables al mismo tiempo.
Verificación	Si asigna una zona de verificación al teclado, cuando se dispare una alarma de pánico al pulsar 2 teclas programables simultáneamente o al introducir un código de coacción, se activarán las incidencias de audio y vídeo.
Indicaciones visuales	
Iluminación	Seleccione cuándo estará encendida la iluminación. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Indicadores	Habilite o deshabilite los LED en el teclado.
Estado de configuración	Seleccione si el estado de configuración se debe indicar en modo inactivo.
Indicaciones audibles	
Zumbador	Habilite o deshabilite el zumbador en el teclado.
Zumb.arm.parcial	Habilite o deshabilite el zumbador durante el tiempo de salida en armado parcial.
Pulsac.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 un calendario. Consulte Calendario [→ 267].
Actuaciones	Seleccione si el teclado debe estar limitado por una salida de sistema.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador de llave.
Entrada CCAA	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay una tarjeta configurada en el teclado.
Particiones	
Localización	Seleccione la partición segura donde se encuentra localizado el teclado.
Particiones	Particiones controladas por el teclado
Opciones	
Retardo arm.total	Seleccione esta opción para configurar un armado retardado en todos los teclados. La ubicación del teclado se ignora, y todas las particiones realizarán una cuenta atrás de tiempo de salida completo.

	AVISO
	Solo se debe asignar una partición a un teclado si el teclado se encuentra dentro de la partición asignada, y si se ha definido una ruta de entrada/salida. Si se asigna una partición, cuando se arma o se desarma esa partición en particular, se utilizan los temporizadores de entrada y salida (siempre y cuando estén configurados). También quedan disponibles otras funciones relacionadas con rutas de entrada/salida. Si no hay ninguna partición asignada, la partición se arma o se desarma inmediatamente y otras funciones de entrada/salida dejan de estar disponibles.

Configuración del teclado confort

Configure los siguientes ajustes para el teclado confort.

Descripción	Introduzca una descripción única para identificar el teclado.
Func. teclas laterales	
Pánico	Seleccione Habilitar, Deshabilitar o Habilit.silencio Cuando está habilitada, la alarma de pánico se activa pulsando las teclas programables F1 y F2 al mismo tiempo.
Incendio	Habilite esta opción para permitir que se active la alarma de incendio pulsando las teclas programables F2 y F3 al mismo tiempo.
Alarma médica	Habilite esta opción para permitir que se active la alarma médica pulsando las teclas programables F3 y F4 al mismo tiempo.
Armado total	Habilite esta opción para permitir que se active el armado total pulsando dos veces la tecla F2.
Armado parcial A	Habilite esta opción para permitir que se active el armado parcial A pulsando dos veces la tecla F3.
Armado parcial B	Habilite esta opción para permitir que se active el armado parcial B pulsando dos veces la tecla F4.
Verificación	Si asigna una zona de verificación al teclado de confort, cuando se dispare una Alarma médica, una incidencia de Pánico o de Incendio, o si un usuario introduce un código de coacción, entonces se activarán las incidencias de audio y vídeo.
Indicaciones visuales	

Iluminación	Seleccione cuándo estará encendida la iluminación. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Nivel retroilum.	Seleccione la intensidad de la retroiluminación. Intervalo del 1 al 8 (alta).
Indicadores	Habilite o deshabilite los LED en el teclado.
Estado de configuración	Habilite esta opción si, estando en reposo, se desea indicar el estado de configuración. (LED)
Logo	Habilite esta opción si, estando en reposo, se desea que se vea el logotipo.
Reloj analógico	Seleccione la posición del reloj en caso de verse estando en reposo. Las opciones son: Situado a la izquierda, Alineado centro, Situado a la derecha o Deshabilitado.
Emergencia	Habilite esta opción si desea que las teclas de función Pánico, Incendio y Médico se indiquen en la pantalla LCD.
Armado directo	Habilite esta opción si desea que las teclas de función Armado total y Armado parcial se indiquen en la pantalla LCD.
Indicaciones audibles	
Alarmas	Seleccione el volumen del altavoz para indicaciones de alarma o desactive el sonido.
Entrada/salida	El intervalo es de 0 a 7 (volumen máximo)
Chime	Seleccione el volumen del altavoz para indicaciones de entrada y salida, o desactive el sonido.
Pulsac.tecla	El intervalo es de 0 a 7 (volumen máximo)
Mensajes hablados	Seleccione el volumen del altavoz para la función Chime o desactive el sonido.
Zumb.arm.parcial	El intervalo es de 0 a 7 (volumen máximo)
Desactivación	
Calendario	Seleccione si el teclado debe estar limitado por un calendario. Consulte Calendario.
Actuaciones	Seleccione si el teclado debe estar limitado por una salida de sistema.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador de llave.
Entrada CCAA	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay una tarjeta configurada en el teclado.
Particiones	
Localización	Seleccione la partición segura donde se encuentra localizado el teclado.
Particiones	Particiones controladas por el teclado
Opciones	
Retardo arm.total	Seleccione esta opción para configurar un armado retardado en todos los teclados. La ubicación del teclado se ignora, y todas las particiones realizarán una cuenta atrás de tiempo de salida completo.

	AVISO
	Solo se debe asignar una partición a un teclado si el teclado se encuentra dentro de la partición asignada, y si se ha definido una ruta de entrada/salida. Si se asigna una partición, cuando se arma o se desarma esa partición en particular, se utilizan los temporizadores de entrada y salida (siempre y cuando estén configurados). También quedan disponibles otras funciones relacionadas con rutas de entrada/salida. Si no hay ninguna partición asignada, la partición se arma o se desarma inmediatamente y otras funciones de entrada/salida dejan de estar disponibles.

16.6.4.4 EDITAR MÓDULOS DE EXPANSIÓN

Para editar módulos de expansión:

1. Desplácese a MÓD.EXPANSIÓN > EDITAR.
2. Pulse SELECC.
3. Desplácese al dispositivo que desee 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 tanto, cualquier módulo de expansión designado o identificado por un número superior a 63 no tiene zonas asignadas.

16.6.4.4.1 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.

16.6.4.4.2 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.
Zona	Seleccione la zona.

Nombre	Descripción
Límite volumen	Seleccione el límite de volumen.

16.6.4.4.3 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.

16.6.4.4.4 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.

16.6.4.4.5 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.
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: ● Ninguna ● 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	Le permite asignar un comportamiento específico a cada LED del módulo indicador Cada LED tiene las siguientes opciones:

Nombre	Descripción
(sólo en modo flexible)	● Función: Están disponibles las siguientes opciones: – Conmutador llave: Seleccione un conmutador de llave y la posición de la llave. – Deshabilitar: Seleccione esta opción para deshabilitar el LED. – Sistema: Seleccione el tipo de alarma que accionará el LED. – Particiones: Seleccione la partición que activará el LED. – Zonas: Seleccione la zona que activará el LED – Puerta: Seleccione la puerta y la opción de puerta que activará 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: Varíe la velocidad 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: Varíe la velocidad 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,
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.
Modo	Seleccione Ligado o Flexible. El modo Ligado reduce el número de opciones disponibles en el menú de Editar módulo de expansión.
Zona	Seleccione la zona

16.6.4.4.6 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.

Nombre	Descripción
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 de llave y la posición de la llave. – Deshabilitar: Seleccione esta opción para deshabilitar el LED. – Sistema: Seleccione el tipo de alarma que accionará el LED. – Particiones: Seleccione la partición que activará el LED. – Zonas: Seleccione la zona que activará el LED – Puerta: Seleccione la puerta y la opción de puerta que activará 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: Varíe la velocidad 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: Varíe la velocidad del parpadeo.
Desactivación (sólo en modo flexible)	Seleccione un método de desactivación de entre las opciones disponibles: ● Calendario: Seleccione un calendario.
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 más información sobre controladores de puertas, consulte la página [→ 72].

1. Desplácese a CONTROL.PUERTA > EDITAR.
2. Pulse SELECC.
3. Desplácese al dispositivo que desee editar y pulse SELECC.

⇨ En la tabla que figura a continuación se muestran los parámetros y datos, si procede, para la edición:

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

Para editar una E/S de puerta:

1. Desplácese a PUERTAS.
2. Pulse SELECC.
3. Desplácese a la E/S de puerta que desee editar y pulse SELECC.

⇨ En la tabla que figura a continuación se muestran los parámetros y datos, si procede, para la edición:

ZONAS	No se ha realizado ninguna funcionalidad de acceso. Las entradas y salidas se pueden utilizar normalmente.
PUERTA 1 – PUERTA 64	El número de puerta seleccionada está asignado a la E/S PUERTA.

Si la opción "ZONAS" está seleccionada 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 a la E/S de puerta que desee editar y pulse SELECC.
   ⇨ La opción "Zonas" queda seleccionada.
2. Pulse SELECC.
3. Seleccione qué zona se debe editar (Zona pos.puerta o Zona lib.puerta).
4. Pulse SELECC.

⇨ En la tabla que figura a continuación se muestran los parámetros y datos, si procede, para la edición:

Sin asignar	Esta zona no está asignada y no se puede usar.
ZONA 1 – ZONA 512	La zona que está editada se asigna a este número de zona. Si la zona se asigna a un número de zona específica, se puede configurar como una zona normal.

Las zonas se pueden asignar a cada número de zona que esté libre. Sin embargo, la asignación no es fija. Si la zona tenía asignado el número de zona 9 y un módulo de expansión de entrada con la dirección 1 está conectado al X-Bus (el cual está utilizando los números de zona 9-16), la zona asignada desde el controlador de dos puertas se desplazará al siguiente número de zona libre. La configuración se adaptará de acuerdo con esto.

Para editar un PERFIL DE LECTOR:

1. Desplácese a LECTORES.
2. Pulse SELECC.
3. Desplácese al LECTOR que desee editar y pulse SELECC.

⇨ Seleccione alguno de los siguientes perfiles para el lector.

1	Para lectores con un LED verde y otro rojo.
2	Para lectores de VANDERBILT con un LED amarillo (AR618X).
3	El perfil 3 se utiliza con lectores de HID que envían un código al panel como lectura de tarjeta con un código local predefinido (0)
4	El perfil 4 se utiliza con lectores de HID que envían un código al panel como lectura de tarjeta con un código local predefinido (255).
5	Seleccionar para activar los lectores Sesam. Para poder cumplir las normas VdS, asegúrese de seleccionar la opción **Anulación LEDs lector** del navegador para proporcionar información durante el proceso de configuración.

Ver también

Módulo de expansión de puerta [→ 72]

16.6.5 MODO DE DIRECCIONAMIENTO

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

Direccionamiento automático

El direccionamiento automático se puede realizar mediante una combinación de conmutador rotativo y sin módulos de expansión de conmutador rotativo. Con el direccionamiento automático, el controlador anula los conmutadores rotativos y asigna automáticamente módulos de expansión y teclados en los ID exclusivos del sistema en orden numérico.

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 para la ID se pueden calcular empleando la siguiente fórmula ((valor ID × 8)+1)= número de primera zona y, después, las 7 zonas siguientes secuenciales. Por ejemplo ((ID2 × 8)+1)=17. La zona 17 está asignada a la entrada 1 en ID2. Cada entrada tiene la siguiente zona secuencial asignada a ella, en este caso hasta la zona 24. Nota: Límite de ID para asignación de zona SPC 4000: ID expansión 1 – 3. SPC 5000: ID expansión 1 – 15. SPC 6000: ID expansión 1 – 63.

ID	Zone	ID	Zone	ID	Zones	ID	Zones	ID	Zones
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

Si dos dispositivos del mismo tipo (p. ej. módulos de expansión) se configuran con el mismo ID, ambos emitirán una señal sonora y un LED parpadeante indicará el conflicto. Restablezca los conmutadores y las reexploraciones del sistema.

Si los dos conmutadores rotativos de un dispositivo se configuran en cero (0, 0), toda la configuración será de direccionamiento automático.

Para seleccionar el MODO DE DIRECCIONAMIENTO:

1. Desplácese a MODO 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 X-bus

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

1. Desplácese a Tipo XBUS.
2. Pulse SELECC.
3. Desplácese a la configuración deseada:
   - Lazo cerrado
   - Lazo abierto
4. Pulse SELECC. para actualizar la configuración.

16.6.7 Recuper.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 a RECUPER.BUS.
2. Pulse SELECC.

3. Introduzca, según sus preferencias, el número de veces que el sistema debe retransmitir los datos.
4. Pulse SELECC. para actualizar la configuración.

16.6.8 Temp.comunic.

Para designar el periodo de tiempo antes de registrar un fallo de comunicación:

1. Desplácese a Temp.comunic.
2. Pulse SELECC.
3. Introduzca el ajuste de tiempo preferido.
4. Pulse SELECC. para actualizar el parámetro.

16.7 VÍA RADIO

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

Detectores	Puede que sea necesario cambiar el tipo de detector dado de alta en el sistema si dicho tipo de detector se identificó de forma incorrecta en el proceso de alta. Si no hay detectores vía radio dados de alta, el teclado muestra NO DET.ACTIVADOS. Para los detectores se dispone de las siguientes opciones: ● AÑADIR Consulte AÑADIR DETECTORES [→ 137] ● EDITAR (cambiar asignación de zona) Consulte EDITAR DETECTORES (ASIGNACIÓN DE ZONA) [→ 137] ● ELIMINAR Seleccione el dispositivo o detector que desee borrar.
PAT	Añada, edite o elimine un PAT (pulsador atraco vía radio). ● AÑADIR Consulte AÑADIR PAT [→ 137] ● EDITAR Consulte EDITAR PAT [→ 138] ● ELIMINAR Seleccione el PAT que desee eliminar.
Antena exterior	Habilitar o deshabilitar la antena exterior.
SUPERVISIÓN	Habilitar o deshabilitar la supervisión de tamper.
FILTRO SE. BAJA	Habilitar o deshabilitar el filtro de señal baja (niveles de RF 0 y 1).
DETEC.INTERF.RF	Habilitar o deshabilitar las interferencias RF.
Panico usuario	Habilite o deshabilite la función Pánico usuario o habilite el modo silencio para Pánico usuario.
Config.test del PAT	Introduzca un período máximo (en días) entre tests de PAT. El máximo es 365 días.
T prev.via radio	Introduzca un tiempo en minutos tras el cual, si no hay señales del detector o del PAT, se evita un armado para la partición en la que se encuentra la zona vía radio. El máximo es de 720 minutos.
T v.radio perd.	Introduzca el número de minutos tras el cual se considerará perdido un dispositivo vía radio si no envía señales dentro de dicho intervalo

	de tiempo. (Mínimo 20 minutos, máximo 720 minutos).

16.7.1 AÑADIR DETECTORES

Para añadir un dispositivo detector vía radio:

1. Desplácese a AÑADIR y pulse SELECC.
   ⇨ Se muestra el mensaje ALTA FUNCIÓN.
2. Pulse SELECC.
   ⇨ En la línea superior de la pantalla parpadea el texto ACTIVAR DISPOS.
3. Active el dispositivo vía radio entre 3 y 5 veces sucesivamente para permitir que el receptor del teclado detecte la transmisión vía radio del dispositivo.
   ⇨ La pantalla indica que el dispositivo ha sido detectado mostrando el texto parpadeante DETEC.ENCONTRADO. El TIPO de dispositivo y la información de ID se muestran de forma alterna.
4. Pulse ALTA.

⇨ Se muestra un mensaje para seleccionar el tipo de zona.

1. Pulse SELECC.
2. Desplácese al tipo de zona requerida y pulse SELECC.

Para añadir un dispositivo mediante ALTA TAMPER, desplácese a dicha opción en el paso 2. El proceso de alta es idéntico, excepto que se muestra un mensaje para definir un tipo de partición antes del mensaje de tipo de zona.

16.7.2 EDITAR DETECTORES (ASIGNACIÓN DE ZONA)

Puede que sea necesario cambiar la asignación de zona del detector dado de alta en el sistema.

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

1. Desplácese hasta EDITAR y pulse SELECC.
2. Desplácese al detector que desee modificar y pulse SELECC.
3. Desplácese a ZONA.
4. Desplácese al número de zona correspondiente (sólo se muestran los números de zona sin ocupar).
5. Pulse SELECC.

16.7.3 AÑADIR PAT

!	*AVISO*
	Sólo se puede configurar un PAT o comprobar su estado en el teclado si hay un módulo vía radio montado en el panel o en alguno de sus módulos de expansión, y si el panel cuenta con licencia para el tipo de módulo(s) instalado(s).

Un PAT no se asigna a un usuario. Normalmente, un PAT es compartido por varias personas, como por ejemplo guardas de seguridad que trabajan por turnos; como alternativa, los PAT pueden estar situados de forma permanente en una superficie, como por ejemplo debajo de un escritorio o detrás de una caja registradora.

Se permite un máximo de 128 PAT por panel.

Para configurar un PAT con el teclado:

1. Seleccione VÍA RADIO y a continuación PAT.
2. Seleccione AÑADIR para añadir un PAT.
3. Seleccione MANUAL para introducir manualmente un ID de PAT.
   El ID también puede ser introducido automáticamente por el panel seleccionando la opción ALTA PAT. Cuando se muestra el mensaje ACTIVAR PAT, se debe pulsar uno de los botones PAT para que el panel pueda identificarlo. El panel no aceptará un PAT si su ID es idéntico al de un PAT que ya se encuentre configurado.
4. Salga del menú AÑADIR y seleccione el menú EDITAR para configurar el PAT.

16.7.4 EDITAR PAT

Para configurar un PAT con el teclado:

1. Seleccione VÍA RADIO y a continuación PAT.
2. Seleccione EDITAR para configurar un PAT.

DESCRIPCIÓN	Introduzca un nombre para identificar inequívocamente el PAT.
ID transmisor	Introduzca el ID del PAT. El panel no aceptará un PAT si su ID es idéntico al de un PAT que ya se encuentre configurado.
Func. a pulsad.	Utilice esta sección para asignar funciones a combinaciones de botones. Las funciones disponibles son Pánico, Pánico silencioso, Atraco, Sospecha, Salida RF usuario, Alarma médica. Se puede seleccionar más de una combinación de botones para una 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 una activación. Consulte Activaciones [→ 270]
SUPERVISAR	El dispositivo WPA puede configurarse para que envíe señales de supervisión periódicas. Si la supervisión está habilitada en el PAT (con el puente), el PAT envía un mensaje de supervisión aprox. cada 7,5 minutos. El tiempo entre mensajes es aleatorio para disminuir las posibilidades de que los envíos coincidan con los de otros PAT. La función de supervisión también se debe habilitar en el panel para ese PAT en concreto para que la supervisión funcione correctamente. Si el panel no recibe una señal de supervisión, se activa una alarma que se indica en el teclado y queda registrada. Si no se activa esta función, cada 24 horas aproximadamente el dispositivo WPA envía un mensaje de supervisión para comunicar al panel el nivel de carga de la pila. Este mensaje también es aleatorio para disminuir las posibilidades de que los envíos coincidan con los de otros PAT. Seleccione HABILITAR si se ha habilitado la supervisión para ese

	PAT en particular.
TEST	Permite comprobar la señal del PAT.

Consulte también

Fuentes [→ 270]
Configuración de temporizadores de PAT [→ 136]
Comprobación de un PAT desde el teclado [→ 156]

16.8 ZONAS

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

DESCRIPCIÓN	Se utiliza para ayudar a identificar la zona; introduzca un nombre específico y descriptivo
Tipo	Determina el tipo de zona. Consulte la página [→ 368].
Atributos	Determina los atributos de la zona. Consulte la página [→ 372].
A partición	Determina qué zona se asigna a qué partición. Esta opción del menú sólo se muestra si hay varias particiones definidas en el sistema. La selección de este parámetro permite a los usuarios crear un conjunto de zonas que se identifiquen con una partición concreta del edificio.

El número y tipo de atributos que se muestran en los menús del teclado para una zona concreta varían en función del tipo de zona que se seleccione. Consulte la página.

16.9 PUERTAS

16.9.1 PUERTAS

1. Desplácese hasta PUERTAS y pulse SELECC.
2. Desplácese hasta la puerta que desee 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 puerta
   - Atributos puerta
   - Temporizadores puerta
   - Información del lector (mostrar únicamente - formato de la última tarjeta utilizada con el lector configurado)

Entradas de puerta

Cada puerta tiene 2 entradas con funcionalidad predefinida. Estas dos entradas, el sensor de posición de la puerta y el interruptor de liberación de la puerta se pueden configurar.

Nombre	Descripción
Zona	El interruptor de liberación de la puerta también se puede utilizar para la parte de intrusión. Si la entrada del sensor de posición de la puerta también se utiliza para la parte de intrusión, se debe seleccionar el número de zona que tiene asignado. Si el sensor de posición de la puerta se utiliza únicamente para la parte de acceso, se debe seleccionar la opción "SIN ASIGNAR". Si el sensor de posición de la puerta está asignado a una zona de intrusión, se puede configurar como una zona normal pero sólo con funcionalidad limitada (p. ej. no se pueden seleccionar todos los tipos de zona). Si una partición o el sistema están armados con el lector de tarjetas, la entrada del sensor de posición de la puerta se debe asignar a un número de zona y a la partición o al sistema que se deben armar.
Descripción (Solo web y SPC Pro)	Descripción de la zona a la que está asignado el sensor de posición de la puerta.
Tipo de zona (Solo web y SPC Pro)	Tipo de zona de la zona a la que está asignado el sensor de posición de la puerta (no todos los tipos de zonas están disponibles).
Atributos de zona (Solo web y SPC Pro)	Los atributos de la zona a la que está asignado el sensor de posición de la puerta se pueden modificar.
Partición (Solo web y SPC Pro)	La partición a la que están asignados la zona y el lector de tarjetas. (Si el lector de tarjetas se usa para armar y desarmar, esta partición se armará o desarmará).
Posición de puerta (web) RFL posic.puerta (teclados) RFL posición puerta (SPC Pro)	La resistencia usada con el sensor de posición de la puerta. Elija el valor / la combinación de la resistencia usada.
DPS Normalmente abierto	Seleccione si el interruptor de liberación de la puerta debe ser una entrada normalmente abierta o normalmente cerrada.
Liberar puerta (web) RFL LIBER.PUERTA (teclados) RFL posición puerta (SPC Pro)	La resistencia usada con el interruptor de liberación de la puerta. Elija el valor / la combinación de la resistencia usada.
Liberación puerta NA	Seleccione si el interruptor de liberación de la puerta es una entrada normalmente abierta o no.
Sin DRS (Solo web y SPC Pro)	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) (Solo web y SPC Pro)	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 (no disponible en SPC Pro).

Todos los números de zona libres se pueden asignar 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 desplazará al siguiente número de zona libre. La configuración se adaptará consecuentemente.

Grupos de puertas

Las diferentes puertas se pueden asignar a grupos de puertas. Esto es necesario si está activada alguna de las siguientes funcionalidades:

- Responsable
- Registro retorno
- Evitar retorno
- Interrelacionada

Atributos de puerta

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

Atributo	Descripción
Nulo	La tarjeta está bloqueada temporalmente.
Grupo de puerta	Se utiliza cuando hay múltiples puertas asignadas a la misma partición y/o se requiere la funcionalidad antirretorno, responsable o interbloqueo.
Tarj. y código	Se requiere tarjeta y código PIN para entrar.
Sólo código	Se requiere el código PIN. No se acepta ninguna tarjeta.
Código o tarjeta	Se requiere código o tarjeta para entrar
Código para salir	Se requiere código en lector de salida. Se requiere puerta con lector de entrada y salida.
Código para desarmar	Se requiere código para armar y desarmar la partición vinculada. La tarjeta se debe presentar antes de introducir el código.
Desarmado desde exterior (navegador) Desarmado en lector de entrada (SPCPro)	Desarmado central/partición al presentar tarjeta en lector acceso.
Desarmado desde interior (navegador) Desarmado en lector de salida (SPCPro)	Desarmado central/partición al presentar tarjeta en lector salida.
Inhibir alarma	Se garantiza el seguimiento si hay una partición armada y la puerta es un tipo de zona de alarma o de entrada.
Armado total desde exterior (navegador) Armado total en lector de entrada (SPCPro)	Armado total central/partición al presentar 2 veces tarjeta en lector acceso.
Armado total desde interior	Armado total central/partición al presentar 2 veces

Atributo	Descripción
Armado total en lector de salida (SPCPro)	tarjeta en lector salida.
Forzar armado total	Si el usuario tiene permisos, puede forzar el armado desde el lector de entrada.
Emergencia	El bloqueo de la puerta se abre si se detecta una alarma de incendio dentro de la partición asignada.
Cualquier emergencia	Un incendio en cualquier partición desbloqueará la puerta.
Visita	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 el "atributo de acompañante" 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 la atribución de Visita se puede configurar individualmente para cada puerta.
Evitar retorno*	Se debe imponer el antirretorno 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 tarjetas deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta ha presentado su tarjeta de acceso para entrar en un grupo de puertas y no la ha presentado para salir de él, dicho titular habrá violado las normas antirretorno. La próxima vez que el titular de tarjeta intente entrar en el mismo grupo de puertas se activará una alarma Hard antirretorno y no se le permitirá entrar en el grupo de puertas.
Registr.retorno*	Las violaciones del antirretorno solamente quedan registradas. 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 tarjetas deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta ha presentado su tarjeta de acceso para entrar en un grupo de puertas y no la ha presentado para salir de él, dicho titular habrá violado las normas antirretorno. La próxima vez que un titular de tarjeta intente entrar en el mismo grupo de puertas se activará una alarma Soft de antirretorno. No obstante, al titular de la tarjeta se le seguirá permitiendo la entrada al grupo de puertas.
Responsable*	La función de responsable permite al titular de una tarjeta con atributo de responsable (el responsable de custodia) proporcionar acceso a otros titulares de tarjetas (no responsables de custodia). El responsable debe ser el primero en entrar en la estancia. Sólo podrán entrar personas no responsables de custodia si el responsable de custodia está en la estancia. El responsable de custodia no podrá salir hasta que todas las personas no responsables de custodia hayan salido de la estancia.
Sirena puerta	La sirena montada en la placa del controlador de puerta suena cuando se producen alarmas en puertas.

Atributo	Descripción
Forzado ignorado	La puerta abierta de forma forzada no se procesa.
Interrelacionada* (navegador) Límite acceso a puerta interrelacionada (SPCPro)	Solo se permite una puerta abierta al mismo tiempo en una partición. Se requiere un grupo de puertas.
Configurando prefijo	Autorización con prefijo de clave (A,B,* o #) para armar el sistema.
* Se requiere un grupo de puertas	

Temporizadores puerta

Temporizador	Mín.	Máx.	Descripción
Autorización acceso	1 s	255 s	El tiempo que el bloqueo permanecerá abierto tras la autorización de acceso.
Acceso denegado	1 s	255 s	Temporización para que el controlador esté listo para leer la siguiente incidencia tras una denegación de acceso.
Apertura puerta	1 s	255 s	Temporización para cerrar la puerta y evitar alarma de "Puerta abierta demasiado tiempo".
Puerta dejada abierta	1 min	180 min	Temporización para cerrar la puerta y evitar alarma de "Puerta dejada abierta".
Extendido	1 s	255 s	Tiempo adicional tras acceso autorizado a tarjeta con atributo "Extendido"
Visita	1 s	30 s	Período de tiempo tras presentarse una tarjeta con atributo de acompañante en el que un usuario sin atributo de acompañante puede acceder a la puerta.

16.10 Salidas

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, por ejemplo al abrirse una puerta o una ventana, al detectarse humo, detectarse 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 al módulo de expansión o a la salida que desee programar y pulse SELECC.

   ⇨ Si las activaciones de salida se graban en el registro de incidencias del sistema (por ejemplo: habilitado, elementos registrados / deshabilitados, elementos), estarán disponibles las siguientes opciones de programación que se muestran en la siguiente tabla.

Nombres	Se utiliza para ayudar a identificar la salida; introduzca un nombre específico y

	descriptivo.
Tipo salida	Determina el tipo de salida; consulte la página [→ 144] para ver una descripción de los tipos de salidas.
Modo salida	Determina el estilo de la salida: Continua, Temporizada o Impulso.
Polaridad	Determina si la salida está activada con una polaridad positiva o negativa.
REGISTRO	Determina si el registro del sistema está habilitado o deshabilitado.

Para obtener información sobre el procedimiento de prueba de una salida, consulte la página [→ 155].

16.10.1 Tipos de salida 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 o informar sobre ello a estaciones centrales remotas si fuera necesario.

Todos los puertos de salida de los módulos de expansión son salidas de tipo relé de polo único (NA, COM, NC); por tanto, los dispositivos de salida pueden necesitar fuentes de alimentación externas para activarse si están conectados a salidas de módulos de expansión.

La activación de un tipo de salida concreto depende del tipo de zona (consulte la página [→ 368]) o de condición de la alerta que provoca la activación. Si se definen varias particiones en el sistema, las salidas del 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 alimentación) mientras que las salidas de partición indican incidencias detectadas en una o más de las particiones definidas en el sistema. Cada partición cuenta con su propio conjunto de salidas de partición. Si una de ellas es una partición común para otras, sus salidas indicarán el estado de todas las particiones para las que es común, incluyendo su propio estado. Por ejemplo, si la partición 1 es común para las particiones 2 y 3, y Sirena Exterior está activada para la partición 2, la salida Sirena Exterior de la partición 1 también estará activada.

Algunos tipos de salida sólo pueden indicar incidencias que afectan a todo el sistema (no de particiones específicas). Consulte la tabla que figura 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 estará activa cuando cualquier sirena exterior de una partición también lo esté. Por defecto, esta salida se asigna a la primera salida de la placa del controlador (EXT+, EXT-). **Nota**: Una salida de sirena exterior se activa automáticamente siempre que una zona programada como Alarma active una alarma en los modos Armado total o Armado parcial.
Flash sirena exterior	Este tipo de salida se utiliza para activar el flash en la sirena exterior del sistema, y está activo cuando cualquier flash de partición lo esté. Por defecto, esta salida se asigna a la salida del relé del flash (Salida 3) en la placa del controlador (NA, COM, NC). **Nota**: Una salida de flash de sirena exterior se activa automáticamente siempre que una zona programada como Alarma active una alarma en los modos Armado total o Armado parcial. El flash de la sirena exterior se activa en una condición de "Fallo al

	armar" si en las opciones del sistema está seleccionada la opción "Fallo al armar".
Sirena interior	Este tipo de salida se utiliza para activar la sirena interior del sistema y estará activa cuando cualquier sirena interior de una partición también lo esté. Por defecto, se asigna a la segunda salida de la placa del controlador (INT+, INT-). Nota: Una salida de sirena interior se activa automáticamente siempre que una zona programada como Alarma active una alarma en los modos 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".
Robo inst.	Esta salida se enciende tras la activación de una zona de alarma en el sistema o desde cualquier partición definida en el sistema.
Alarma confirmada	Esta salida se enciende cuando se ha confirmado una alarma. Una alarma se confirma cuando 2 zonas independientes del sistema (o dentro de la misma partición) se activan en un periodo de tiempo establecido.
Pánico*	Esta salida se enciende tras la activación, desde cualquier partición, de tipos de zona de Alarma de pánico. También se genera una salida de Alarma de pánico si se produce una incidencia de coacción de usuario o si la opción de pánico está habilitada para el teclado.
Atraco	Esta salida se enciende cuando una zona programada como de tipo Atraco activa una alarma desde cualquier partición.
Incendio	Esta salida se enciende tras la activación de una zona de incendio en el sistema (o desde cualquier partición).
Tamper	Esta salida se enciende cuando se detecta una condición de tamper desde cualquier parte del sistema. Para un sistema de grado 3, si se pierde la comunicación con un dispositivo XBUS durante más de 100 s, se genera un tamper y las incidencias SIA y CIR de las que se informa envían un tamper.
Alarma médica	Esta salida se enciende cuando se activa una zona médica.
Fallo	Esta salida se enciende cuando se detecta un fallo técnico.
Técnico	Esta salida sigue a la actividad en una zona técnica.
Fallo de red c. a.*	Esta salida se activa cuando se desconecta la alimentación.
Fallo batería*	Esta salida se activa cuando hay un problema con la batería de reserva. Esta salida se activa si el voltaje de la batería desciende por debajo de 11 V. La opción de "Restaurar" para este fallo sólo se presenta cuando el nivel de voltaje supera los 11,8 V.
Armado parcial A	Esta salida se activa si el sistema o cualquier partición definida en el mismo está en modo Armado parcial A.
Armado parcial B	Esta salida se activa si el sistema o cualquier partición definida en el mismo 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 el sistema, o cualquier partición definida en el mismo, ha fallado al armar, y se borra cuando se restaura la alerta
Entrada/salida	Esta salida se activa si se ha activado una zona de E/S, p. ej. si está funcionando un temporizador de Entrada o Salida de un sistema o partición.
Enclavamiento	Esta salida se enciende tal como se haya definido en la configuración del enclavamiento de salidas del sistema (consulte Configuración del enclavamiento y autoarmado de salidas del sistema [→ 214]). Esta salida se puede utilizar para resetear los detectores de enclavamiento, como detectores de humo o inerciales.
Salida de incendio	Esta salida se ENCIENDE si se activa cualquier zona Inc.X en el sistema.
Chime	Esta salida se enciende momentáneamente cuando se abre cualquier zona del sistema con el atributo Chime.
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 enciende momentáneamente cuando un test de intrusión está operativo y una zona se activa. Esta salida se puede utilizar, por ejemplo, para activar pruebas funcionales de detectores conectados (si está disponible).
Autoarmado	Esta salida se enciende si la función de autoarmado se ha activado en el sistema.
Código coacción usuario	Esta salida se enciende si se ha activado un estado de coacción del usuario (se ha introducido el código PIN + 1 en el teclado).
PIR enmascarado	Esta salida se enciende si hay alguna zona PIR con máscara en el sistema. Esto genera una salida de fallo en el LED del teclado. Esta salida se bloquea y permanecerá activa hasta que sea restablecida por un usuario de nivel 2. El enmascaramiento PIR está conectado por defecto. El número de entradas de registro no excede las 8 entre períodos de armado.
Zona omitida	Esta salida se enciende si hay zonas anuladas, inhibidas o con test de intrusión en el sistema.
Comunicación	Esta salida se enciende si hay un fallo en la comunicación con la estación central.
Test hombre caído	Esta salida enciende un dispositivo vía radio de "hombre caído" que se activa durante un test de "hombre caído".
Desarmado	Esta salida se activa si el sistema está en modo Desarmado.
Abortar alarma	Esta salida se activa si se produce una incidencia de abortar alarma, es decir, cuando se introduce un código de usuario válido a través del teclado tras una alarma confirmada o sin confirmar. Se utiliza, por ejemplo, con marcadores telefónicos externos (SIA, CID, FF)
Test sísmico	Esta salida se utiliza para activar un test manual o automático en una zona sísmica. Los detectores sísmicos tienen un pequeño vibrador que se instala en la misma pared que el detector y se conecta mediante un cable a una salida en el panel o en alguno de sus módulos de expansión. Durante el test, el panel espera hasta 30 segundos a que se abra la zona sísmica. Si no se abre, el test se considera fallido. Si se abre en un plazo de 30 segundos, el panel espera a que la zona se cierre en un plazo de 10 segundos. Si no ocurre así, el test se considera fallido. A continuación, el panel espera otros 2 segundos antes de informar sobre el resultado del test. El resultado del test, tanto manual como 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 Fob o PAT.
Fallo línea TX 1	Esta salida se activa cuando hay un fallo de línea en el 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 de línea en el módem secundario.
Fallo TX 2	Esta salida se activa cuando falla el módem secundario.
Baja batería	Esta salida se activa cuando la carga de la batería está baja.
Estado entradas	Esta salida se activa cuando se implementa un procedimiento de entrada "Todo OK" y no se genera ninguna alarma, es decir, que el botón "Todo OK" se pulsa dentro del tiempo configurado después de introducirse el código de usuario.
Estado aviso	Esta salida se activa cuando se implementa un procedimiento de entrada "Todo OK" y se genera una alarma silenciosa, es decir, que el botón "Todo OK" no se pulsa dentro del tiempo configurado después de introducirse el código de usuario.
Listo para armar	Esta salida se activa cuando una partición está lista para el armado.
Config. ACK (SPC Pro — Armado completo)	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

(SPC Pro — Armado con éxito)	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.
Atraco confirmado	Se activa en los siguientes escenarios para la conformidad con PD6662: ● dos activaciones de zona de atraco separadas entre sí más de dos minutos ● una activación de zona de atraco y de zona de pánico separadas entre sí más de dos minutos ● Si en el periodo de dos minutos se produce una activación de zona de atraco y de zona de tamper o una activación de zona de pánico y de zona de tamper
Modo técnico	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).*

Ver también

🗎 Configuración de enclavamiento del sistema y salidas de armado automático [→ 214]

16.11 Comunicación

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

16.11.1 Puertos serie

Los puertos serie permiten a un PC antiguo conectarse al sistema o a otros periféricos como impresoras.

1. Desplácese a PUERTOS SERIE.
2. Pulse SELECC.
3. Desplácese al puerto serie que desee programar.
4. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.
5. Pulse ATRÁS para salir.

Tipo	Determina si el tipo es TERMINAL (información del sistema) o IMPRESORA (registro de incidencias del SPC)
Baudios	Determina la velocidad de la comunicación entre la central y el equipo periférico. Tenga en cuenta que debe establecerse la misma tasa de baudios en ambos componentes del equipo.
Bits datos	Determina la longitud del paquete de datos que se transferirá entre la central y el equipo periférico. Tenga en cuenta que deben establecerse los mismos bits de datos para ambos componentes del equipo.
Bits de parada	Determina el número de bits de parada al final del paquete de datos. Tenga en cuenta que deben establecerse los mismos bits de parada para ambos componentes del equipo.
Paridad	Determina la paridad (par / impar) del paquete de datos. Tenga en cuenta que la paridad debe ser la misma para ambos componentes del equipo.
Control de flujo	Determina si los datos están bajo control del hardware (RTS, CTS) o del software (ninguno). Tenga en cuenta que debe establecerse el mismo control de flujo para ambos componentes del equipo.

16.11.2 Puertos Ethernet

Para programar el puerto Ethernet:

1. Desplácese a PUERTO ETHERNET.
2. Pulse SELECC.
   ⇨ La opción de Dirección IP muestra XXX.XXX.XXX.XXX Para números de una cifra, se necesitan ceros delante. P. ej., 001
3. Pulse SELECC. e introduzca la dirección IP que prefiera.
   ⇨ Cuando se pulsa la tecla ENTER, el sistema emite dos sonidos e indica ACTUALIZADO si la dirección IP es válida. Si la dirección IP se asigna manualmente, ésta debe ser exclusiva en la LAN o VLAN conectada a la central. No se introduce ningún valor cuando se utiliza la opción DCHP.
4. Desplácese a MASC.SUBRED.
5. Pulse SELECC. e introduzca la MÁSCARA SUBRED con formato XXX.XXX.XXX.XXX. (Para números de una cifra, se necesitan ceros delante, p. ej. 001). Cuando se utiliza la tecla ENTER, el sistema emite dos sonidos e indica ACTUALIZADO si la MÁSCARA SUBRED es válida.
6. Desplácese a PUERTA DE ENLACE. Tenga en cuenta que la puerta de enlace tiene que programarse para un acceso fuera de la red (para el 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, p. ej.

001). Cuando se utiliza la tecla ENTER, el sistema emite dos sonidos e indica ACTUALIZADO si la PUERTA DE ENLACE es válida.

8. Desplácese a DHCP. DHCP está activado si la LAN cuenta con un servidor DHCP para asignar la dirección IP. La dirección IP debe activarse manualmente. Tenga en cuenta que la puerta de enlace tiene que programarse si la central necesita tener acceso fuera de la red (para el 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, p. ej., 001)
   - ⇨ Cuando se pulsa la tecla ENTER, el sistema emite dos sonidos e indica ACTUALIZADO si la dirección PUERTA DE ENLACE es válida.
   - ⇨ Se muestra la opción DHCP.
10. Alterne entre DHCP HABILITADO y DESHABILITADO según la opción que prefiera.
11. Pulse SELECC.

16.11.3 Módems

El sistema SPC es compatible con los módems inteligentes del SPC para comunicaciones con líneas analógicas y conexionado de redes móviles para comunicaciones y conectividad mejoradas. El sistema SPC debe configurarse en consecuencia.

16.11.3.1 Supervisión de la transmisión del interface de red.

El sistema de alarma SPC envía un mensaje de prueba (poll) al SPC COM XT, el cual responde con un reconocimiento del mismo (poll ACK). Cuando el sistema de alarma SPC recibe el ACK válido actualiza su estado a OK (correcto), y reinicia su contador de tiempo de intervalos de mensaje de prueba (dependiendo de la categoría del ATP)

Si el sistema de alarma SPC no recibe respuesta a su mensaje de test mediante el ACK, dentro de un intervalo de tiempo (dependiente de la categoría del ATP), el sistema de alarma SPC actualiza su estado a DOWN (Caido).

SPC soporta los siguientes interfaces de transmisión:

- Ethernet
- GSM con GPRS activo
- Modem 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 (alimentación de CA y batería) o la tarjeta no se activará.

	AVISO
	Tras un retorno a la configuración predeterminada de fábrica, durante el proceso de configuración inicial del sistema con el teclado, el panel detecta si hay un módem principal o de reserva instalado y, en ese caso, muestra su tipo y lo(s) habilita automáticamente con la configuración por defecto. En esta fase no se permite ninguna otra configuración de módem.

16.11.3.2 Para configurar un módem

Para configurar un módem GSM o RTB:

1. Desplácese a MÓDEMS y pulse SELECCIONAR.
2. Cambie entre TX PRIMARIO y TX DE BACKUP para elegir la ranura de módem correcta y pulse SELECC.
   ⇨ Se muestra la opción Habilitación TX.
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 CONTESTADOR	Elija esta opción para seleccionar el modo en que el módem responderá a las llamadas entrantes. NO DESCOLGAR o DESCOLG.SIEMPRE
RESP.ACC.TÉCNICO	Seleccione HABILITAR para responder sólo con código de técnico autorizado.
SMS	Seleccione HABILIT. SMS para habilitar el SMS para este módem. (Sólo para 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 el SMS en intervalos de tiempo 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 LÍNEA	**Para RTB**: Habilite esta función para controlar el voltaje de la línea conectada al módem. **Módem GSM:** Habilite esta característica para supervisar el nivel de señal de la antena GSM conectada al módem. Seleccione un MODO de control (SIEMPRE ACTIVADO,

Opción de menú	Descripción
	ARMADO TOTAL, DESHABILITAR) La opción ARMADO TOTAL solo permite esta función cuando el sistema está en Armado total. Introduzca el número de segundos para la TEMPORIZACIÓN 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 activada. (Consulte Opciones del sistema).

Sólo módem GSM. Si el SMS está habilitado, y se envía un código PIN incorrecto a la tarjeta SIM tres veces, la tarjeta SIM se bloqueará. En este caso, se recomienda que se extraiga la tarjeta SIM y que se desbloquee utilizando un teléfono móvil. Si se cambia la tarjeta SIM en el módulo GSM o se está utilizando una tarjeta SIM con código PIN, se recomienda programar el código PIN antes de colocarlo en el soporte de la tarjeta SIM para asegurarse de que no se envían códigos PIN incorrectos. Se debe desconectar cualquier tipo de alimentación (red de c. a. o batería) cuando se cargue la tarjeta SIM en el soporte de la misma.

16.11.4 CRAs estandar

16.11.4.1 AÑADIR

Para programar los parámetros de la estación central:

1. Desplácese a ESTACIÓN CENTRAL > AÑADIR.
2. Pulse SELECC.
3. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.
4. Una vez finalizada la programación, se muestra en el teclado la opción de realizar una llamada de prueba a la estación.

Código abonado	Esta información debe estar disponible desde la estación receptora y se utiliza para identificar a los usuarios cada vez que se realiza una llamada a la CRA.
Nombre abonado	Descripción de la CRA remota
Protocolo	El protocolo de comunicación que se utilizará (SIA, ID de contacto, Formato rápido)
Teléfono 1	El primer número que hay que marcar para contactar con la CRA.
Teléfono 2	El segundo número que hay que marcar para contactar con la CRA; el sistema sólo intenta contactar con la CRA en este número si no ha podido establecer conexión con el primer número de contacto.
Prioridad	El módem (primario o de copia de seguridad) que se utilizará para comunicarse con el CRA.

16.11.4.2 Editar

Par editar la configuración de la estación central:

1. Desplácese a CRAs estandar >Editar.
2. Pulse SELECC.
3. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.
4. Una vez finalizada la programación, se muestra en el teclado la opción de realizar una llamada de prueba a la estación.

Código abonado	Esta información debe estar disponible desde la estación receptora y se utiliza para identificar a los usuarios cada vez que se realiza una llamada a la CRA.
Nombre abonado	Descripción de la CRA remota
Protocolo	El protocolo de comunicación que se utilizará (SIA, ID de contacto, Formato rápido)
Teléfono 1	El primer número que hay que marcar para contactar con la CRA.
Teléfono 2	El segundo número que hay que marcar para contactar con la CRA; el sistema sólo intenta contactar con la CRA en este número si no ha podido establecer conexión con el primer número de contacto.
Intentos marcac.	Introduzca el número de veces que el sistema intentará realizar una llamada al receptor.
Interv.marcacion	Introduzca el número de segundos entre intentos de marcación fallidos. (0 - 999)
Partic.asignadas	Asigne las particiones para las que se enviarán incidencias a la CRA.
Envio incidenc.	Defina los tipos de incidencias enviadas a la CRA.
Prioridad	El módem (primario o de copia de seguridad) que se utilizará para comunicarse con el 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.

16.11.4.3 Borrar

Le permite borrar una CRA configurada.

16.11.4.4 Llamad.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 MANTENIMIENTO REMOTO

1. Desplácese a MANTENIMIENTO REMOTO > MANTENIMIENTO REMOTO HABILITADO
2. Pulse Seleccionar.
3. Alterne entre HABILITADO y DESHABILITADO.

4. Seleccione la opción de programación deseada que se muestra en la siguiente tabla.

Identificación	ID mantenimiento remoto. Debe coincidir con el del SPC Pro (1 - 999999).
Clave	Clave mantenimiento remoto Debe coincidir con la del SPC Pro.
Ent.config.com.	Configuración de conexiones entrantes. Puede habilitar ENT.HABILIT.IP para permitir las conexiones IP entrantes desde el servidor de mantenimiento remoto. Si no están habilitadas, sólo son posibles las conexiones de módem. Introduzca el puerto TCP/IP de entrada en el que la central escuchará las conexiones IP entrantes desde el servidor de mantenimiento remoto.
Sal.config.com.	Config. conexiones salientes. Seleccione cómo realizar conexiones salientes con el servidor de mantenimiento remoto desde las opciones INHIBIDO, VÍA MÓDEM o VÍA IP.

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 a TEST > TEST SIRENA.
2. Pulse SELECC.

⇨ Cuando se selecciona TEST SIRENA, estarán disponibles las siguientes opciones: 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 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 Estado zonas

La opción Estado zonas muestra información sobre el estado de cada una de las zonas del sistema.

Para ver información sobre el estado de las zonas:

1. Desplácese a TEST > ESTADO ZONAS.
2. Pulse SELECC.
3. Desplácese a la zona que prefiera y pulse SELECC.
   ⇨ Se muestra el estado de la zona y el valor de resistencia asociado a la misma.
4. Pulse SIGUIENTE para ubicar la zona (ej. CONTROLADOR 1 = primera zona del controlador).

⇨ Consulte la tabla siguiente para correlacionar la información sobre los demás estados (válida para resistencias RFL duales).

Estado de zona	Abreviatura
Desconocd.	GB
REPOSO	CE
Alarma	Ab
CORTO	CC
DESCONECTADO	DI
IMPULSO	PU
DET.VIBRACIÓN	GR
ENMASCARADO	AM
FALLO	FA
SUSTITUCIÓN C.C.	DC
FUERA LÍMITES	OB
ENTRADA ZONA INESTABLE	IN

Todas las zonas de un sistema pueden controlarse para verificar un funcionamiento correcto a través de un test de control.

Para realizar un test de control de zona:

1. Desplácese a ESTADO ZONAS.
2. Pulse SELECC.
3. Desplácese a la zona que prefiera y pulse SELECC. o introduzca el número de la zona directamente.

⇨ Si la zona está ubicada cerca del teclado, puede verse el estado de éste a medida que cambia. El estado de zona y su valor de resistencia se muestran en la parte superior derecha.

4. Cambie el estado del detector; p. ej. para un detector de contacto de puerta, abra la puerta.

⇨ El zumbador del teclado suena y el estado del detector cambia de Ce (cerrado) a Ab (abierto). El valor de resistencia correspondiente cambia a otro que depende del esquema de resistencia RFL.

Es recomendable verificar el funcionamiento de todas las zonas del sistema una vez finalizada la instalación. Para ubicar la zona, seleccione SIGUIENTE (parte inferior derecha) en el teclado. Un valor de estado de zona CC o DE indica que la zona está cortocircuitada o desconectada.

16.12.4 Test salidas

Para realizar un test de salidas:

1. Desplácese a TEST SALIDAS.
2. Pulse SELECC.
3. Alterne entre CONTROLADOR y MÓDULO DE EXPANSIÓN según la opción que prefiera.
4. Si está probando las salidas del controlador, desplácese a la salida que prefiera y pulse SELECC. Si está probando las salidas del módulo de expansión, seleccione el módulo de expansión y, a continuación, la salida.

   ⇨ La pantalla del teclado indica el estado actual de la salida en la línea superior.

5. Active el estado ON/OFF de la salida.
6. Compruebe que el dispositivo conectado a la salida seleccionada cambie al estado correspondiente.

16.12.5 En pruebas

La función En pruebas proporciona un método para poner a prueba las zonas seleccionadas. Las zonas en pruebas no producen ninguna alarma pero se graban en el registro de incidencias. Las zonas en pruebas permanecerán de esta forma hasta que finalice el temporizador de pruebas por defecto (14 días).

Para realizar pruebas:

1. Desplácese a EN PRUEBAS y pulse SELECC.
2. Alterne entre HABILIT.PRUEBAS y CANCELAR PRUEBAS según la opción que prefiera.
3. Desplácese a la zona que prefiera y pulse SELECC.

⇨ Se mostrará un mensaje para confirmar que la zona está en pruebas.

	AVISO
	Todos los tipos de zona se pueden incluir como zona en pruebas.

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: TODAS, SIRENA INTERIOR, SIRENA EXTERIOR, TECLADO
4. Pulse SALVAR.
5. Pulse ATRÁS para salir.

16.12.7 Indic. 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*
	Este test solo puede ser realizado por un técnico o un usuario con autorización para realizar el "Test PAT". Véase Atribuciones de usuario.

Para comprobar el PAT desde el teclado:

1. Desplácese a TEST PAT y pulse SELECC.
2. Cuando se le solicite mediante ACTIVAR PAT, pulse los tres botones del PAT simultáneamente.

⇨ Si el test es satisfactorio, aparecerá un mensaje de PAT *n* OK, siendo n el número de PAT que se está comprobando.

1. Repita el test si es necesario.
2. Pulse ATRÁS o X para finalizar el test.

16.12.9 Test sismico

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 Comprobación de detectores sísmicos [→ 344].

16.13 Utilidades

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

Versión software	Para ver la versión de software actual.
PARÁM.FÁBRICA	Para restablecer los usuarios o devolver el sistema a su configuración de fábrica.
CONFIG.BACKUP	Para realizar una copia de seguridad de una configuración.
Restaur.config.	Para restaurar una configuración.
PROGRAMADOR RÁPIDO	● Central - Progr.: Transferir datos del controlador al Programador rápido. Se le solicitará que confirme si el nombre del nuevo archivo de configuración es igual que un nombre de archivo ya existente en el programador rápido para evitar que los archivos de configuración se sobrescriban. ● Progr. - Central: Transferir datos al controlador desde el Programador rápido. ● Borrar ficheros: ● ACTUALIZACIÓN FIRMWARE. Nota: Si instala una versión anterior del firmware, el sistema restablecerá toda 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. ● ACTUALIZACIÓN PERIFÉRICO: ● ACTUALIZACIÓN IDIOMA:
SPC PRO/SPC SAFE	Para programar las siguientes opciones del SPC Pro: ● HABILIT. ACCESO**:** Determina si el SPC Pro está habilitado o deshabilitado. ● ACCESO TÉCNICO**:** Determina si el acceso del técnico está habilitado o deshabilitado. ● CLAVE**:** Edite la clave existente del sistema. ● HABILIT. IP: Habilite para conectar al sistema a través de IP. ● PUERTO IP: Seleccione a través de qué puerto IP se conectará el SPC Pro/SDK.

REPOS.SISTEMA	Para reiniciar el sistema.
LICENCIA	Introduzca un número de licencia para cambiar la clave de licencia del SPC. El sistema no registra los cambios de licencia ni informa sobre ellos.

16.14 Aislada

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 com. XBUS ● FALLO FUSIBLE XBUS (sólo módulos de expansión) ● TAMPER X-BUS
Ver aislam.	Para ver una lista de las zonas inhibidas, alertas del sistema y alertas de dispositivos X-BUS.

16.15 Reg.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 **Reg > Registro seguridad > Reg. alarmas**.

En este registro se muestran los siguientes tipos:

- Zonas
  - Robo inst.
  - Pánico
- Incidencias del sistema
  - Alarma confirmada
  - Código coacción usuario
  - Pánico XBUS
  - Pánico usuario
  - Pánico RPA

16.18 CAMBIO CÓDIGO 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 con un número menor de dígitos que el que se ha configurado.
3. Confirme el código nuevo pulsando 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

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

16.19.1 AÑADIR

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 – Atribut.tarjeta (véase 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.

16.19.2.1.1 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.

16.19.2.1.2 ALTA TARJETA

i	*AVISO*
	Sólo se pueden dar de alta tarjetas con formatos admitidos.

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.

i	*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.

16.19.2.1.3 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 siguiente tabla.
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
Visita	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 Acompañante para permitir abrir la puerta a otros titulares de tarjeta sin esta atribución. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con la atribución de Acompañante 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 estancia. 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.

16.19.2.1.4 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.

16.19.2.1.5 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 USUARIO

Ver también

🗎 Añadir/Editar perfiles de usuario [→ 198]

16.20.1 AÑADIR

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 pesonalizado 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 pefil 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. Véase Derechos de usuario [→ 198].

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 SMS

El sistema SPC admite la comunicación de alertas por SMS desde la central al técnico y a teléfonos móviles de usuarios seleccionados (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 AUTENTIFICACIÓN SMS seleccionado (véase el menú OPCIONES [→ 115], la autentificación se puede configurar para que se utilicen diferentes combinaciones del código e identificador llamada del usuario, o del código de SMS y 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
- Habilita / deshabilita el 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
- Anulac. e inhibiciones
- Todos los demás tipos de incidencias

16.21.1 AÑADIR

▷ Hay un módem instalado e identificado por el sistema.

▷ La función **Autentificación SMS** está activada en OPCIONES [→ 115].

1. Desplácese a 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

▷ Hay un módem instalado e identificado por el sistema.

▷ La función **Autentificación SMS** está activada en OPCIONES [→ 115].

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

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.
Usuario	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. Véase Comandos de SMS [→ 202]

!	*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 Identidad de Línea Llamante (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 a 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

La versión 3.4 no admite el X-10. Esta funcionalidad se mantiene en el producto para conservar la compatibilidad retroactiva.

La X-10 es una tecnología que permite al sistema controlar dispositivos periféricos, como luces o aparatos, y las incidencias del sistema se pueden utilizar para activar 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 a X-10 y pulse SELECC.
2. Desplácese a la opción de programación deseada:

HABILITAR X-10	Para habilitar o deshabilitar la funcionalidad X-10 en el sistema.
Dispositivos	Para añadir, editar, borrar o probar dispositivos X-10.
Registrando	Para habilitar o deshabilitar el registro de X-10.

16.23 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 INSTALAD.

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

1. Desplácese hasta Textos personlz. y pulse SELECC.
2. Desplácese a la opción de programación deseada:

Nombre sistema	Se utiliza para ayudar a identificar el sistema; utilice un nombre claro y descriptivo para la instalación.
ID sistema	Se utiliza para ayudar a identificar la instalación cuando está conectada a una estación central (máx. 10 dígitos).
Nombr.instalador	Se utiliza para fines de contacto.
ID sistema	Se utiliza para fines de contacto.
Instalador Sistema	Parámetro para mostrar información del instalador durante su estado inactivo.

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

16.25 CONTROL PUERTA

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.

17 Programación de técnico a través del navegador

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

Para acceder a la programación del técnico a través del navegador, introduzca el código de técnico por defecto (1111). Para más información, consulte Códigos de técnico [→ 106].

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 de técnico del SPC se dividen en las siguientes categorías:

Funciones de software técnico

Estas funciones pueden programarse sin necesidad de desactivar el sistema de alarma; se accede a ellas directamente al entrar en el modo técnico.

Funciones de técnico total

Estas funciones requieren que el sistema de alarma se desactive antes de que pueda comenzar la programación; se puede acceder a ellas desde el menú técnico total.

!	*AVISO*
	Si la opción "Salida técnico" está habilitada en Opciones del sistema, el técnico puede salir del modo Técnico total con alertas activas, pero deberá confirmar todas las alertas listadas en el teclado o en el navegador antes de pasar del modo Técnico total al Modo normal.

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

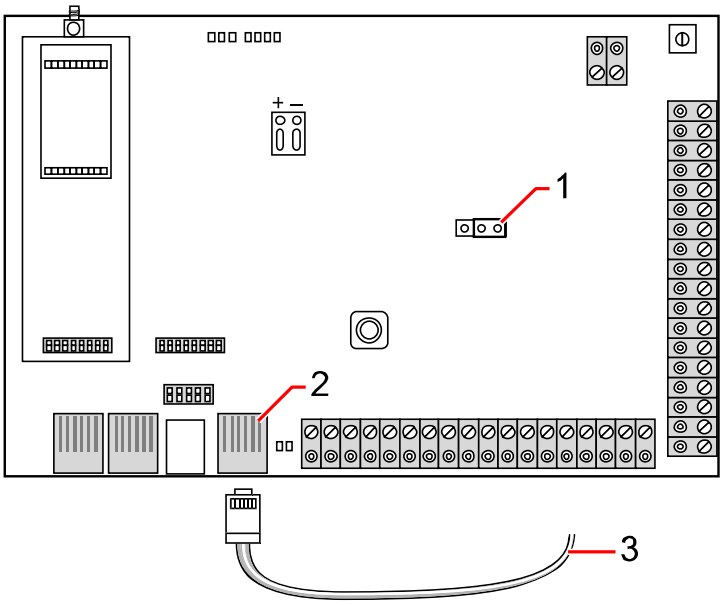
Si se está programando con una interfaz de navegador, haga clic en **Salvar** cuando se realicen cambios.
Haga clic en **Actualizar** para ver los valores de programación actuales en una página web.

17.1 Información del sistema

Haga clic en el icono **?** para ver el menú de ayuda que le proporcionará información actualizada sobre la central y sobre la funcionalidad autorizada actualmente en el sistema.

17.2 Interfaz Ethernet

IP



Conectar

1	JP9 ~~SPC4xxx~~
2	Puerto Ethernet
3	Al puerto Ethernet del ordenador

Si la interfaz de 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

Conexión del cable

- Conecte un cable Ethernet desde la interfaz Ethernet del PC al puerto Ethernet de la placa del controlador,
  O BIEN
  si se conecta directamente desde un PC, debe utilizarse un cable cruzado.
  Consulte la página [→ 352].

  ⇨ Los LED en la derecha de la interfaz Ethernet indican una conexión de datos (LED derecho encendido) y un tráfico de datos Ethernet (LED izquierdo parpadeando) correctos.

Determinación de la dirección IP controlador SPC

1. Entrando en el modo Técnico (consulte Códigos de técnico [→ 106]).
2. Con los botones de flecha arriba/abajo, baje hasta la opción COMUNICACIÓN y pulse SELECCIONAR.
3. Desplácese a la opción PUERTO ETHERNET y pulse SELECCIONAR.

4. Desplácese a DIRECCIÓN IP y pulse SELECCIONAR.

17.3 Conexión a la central a través de USB

Si se restaura la central mientras el cable USB está conectado, dicho cable se debe desenchufar y volver a enchufar.

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.

▷ SPC Pro debe estar instalado en su PC.

▷ 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.
   ⇨ Se muestra el asistente de **Nuevo hardware encontrado**.
2. Pulse **Siguiente**.
   ⇨ Windows XP detecta una unidad USB genérica.
3. Haga clic en Finalizar.
   ⇨ Windows XP detecta el 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:
   ⇨ **Vanderbilt Intrunet SPC USB Local Connection**
7. Haga clic en **Siguiente**.
   ⇨ 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.
8. Haga clic en **Continuar de todas formas**.
   ⇨ 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 nueva conexión**.
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 solicita el nombre de usuario y la clave para la conexión USB. Introduzca los detalles siguientes:
    - Nombre de usuario: SPC
    - Clave: password (por defecto)
11. Haga clic en **Conectar**.
    ⇨ El PC inicia un enlace de datos con el controlador. Cuando se ha establecido el enlace, aparece un icono de conexión en la barra de tareas de la parte inferior de la pantalla del PC.
12. Haga clic con el botón derecho sobre el enlace y seleccione **Estado**.
    ⇨ Se mostrará una dirección IP del servidor en la ventana de detalles.
13. Introduzca esta dirección en la barra de direcciones del navegador de Internet utilizando un "protocolo de hipertexto seguro" (p. ej. 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

▷ Ejecute todas las acciones descritas en Conexión USB en Windows 7 para SPCPro

▷ 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 abre la ventana de **Teléfono y módem**.
3. Seleccione la pestaña **Módems** y haga clic en **Añadir**.
   ⇨ Se abrirá la ventana **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 **Siguiente**.
7. Seleccione el puerto COM asignado en Conexión USB en Windows 7 para SPCPro.
8. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.
9. Vuelva a la pestaña **Módems** en la ventana de **Teléfono y módem**.
10. Seleccione el nuevo módem y haga clic en **Propiedades**.
    ⇨ Se abre la ventana **Cable de comunicaciones entre dos ordenadores - Propiedades**.
11. En la pestaña **General**, haga clic en **Cambiar configuración** para que se puedan editar las propiedades.
12. Seleccione la pestaña **Módem**.
13. Modifique el valor de **Velocidad máxima del puerto** a **115200** y haga clic en **Aceptar**.
14. En el **Panel de control**, abra **Centro de redes y recursos compartidos**.
15. Haga clic en **Cambiar configuración del adaptador**. Si hay un nuevo módem en la lista de conexiones disponibles, continúe con el paso 23. Si el módem *no* está presente, continúe con los siguientes pasos.
16. En el **Centro de redes y recursos compartidos**, haga clic en **Configurar una nueva conexión o red**.
17. Seleccione **Configurar una conexión de acceso telefónico** y haga clic en **Siguiente**.
18. 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**.
19. Haga clic en **Conectar**.
    ⇨ Windows 7 crea la conexión.
20. Sáltese el proceso de **Comprobación de la conexión a Internet**.
21. Haga clic en **Cerrar**.
22. En el **Centro de redes y recursos compartidos**, haga clic en **Cambiar configuración del adaptador**.
23. Haga doble clic en el nuevo módem.
    ⇨ Se abre la ventana **Conectar** *Nombre de conexión*, siendo *Nombre de conexión* el nombre que usted ha definido para el módem.
24. Haga clic en **Propiedades**.
25. Compruebe que el campo **Conectarse mediante:** contiene la información correcta, por ejemplo Cable de comunicación entre dos ordenadores (COM3).
26. Abra su navegador e introduzca la dirección IP del controlador, con https como protocolo de conexión.
27. Si el navegador muestra una página de error de certificado, haga clic en Continuar de todos modos.
28. 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 de Internet utilizando un "protocolo de hipertexto seguro".(p. ej. https:// 192.168.1.100) Consulte la siguiente tabla.
   ⇨ Se mostrará una ventana con un mensaje de seguridad.
3. Haga clic en **Continuar a este sitio web**.
   ⇨ Aparecerá la pantalla de inicio de sesión.

4. Introduzca los siguientes datos:
   - **Id usuario**: Nombre de usuario o de técnico
   - **Clave**: Código de usuario o de técnico.
5. Seleccione un idioma en el que mostrar las pantallas 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 **Inicio de sesión**.

Configuración por defecto para dirección de servidor WEB

Conexión	Dirección IP de servidor web
Ethernet	192.168.1.100 (por defecto)
RS232	192.168.2.1 (fija)
Módem de backup / RS232	192.168.3.1 (fija)
Módem principal	192.168.4.1 (fija)
USB	192.168.5.1 (fija)

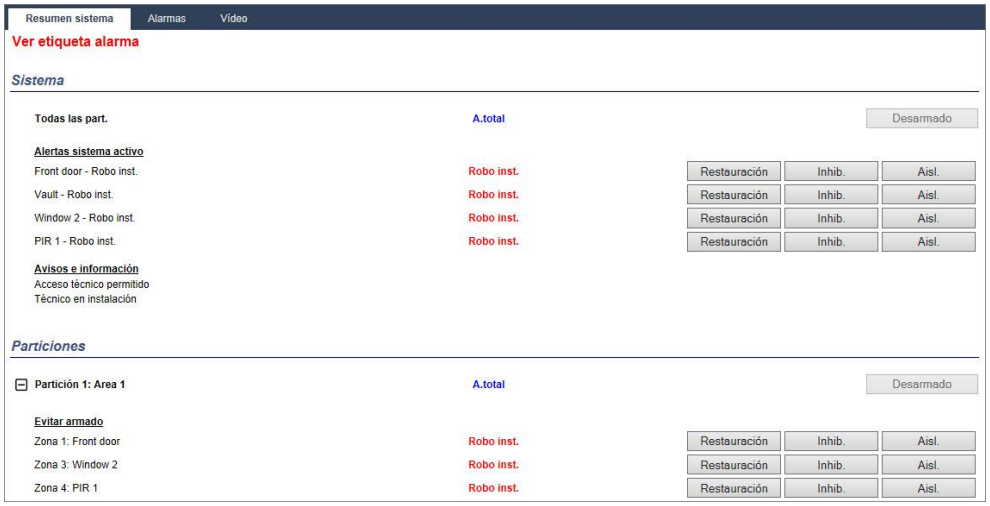
17.5 SPC Home

La página SPC Home posee las pestañas **Resumen sistema**, **Alarmas** y **Vídeo**.

17.5.1 Resumen sistema

La pestaña **Resumen sistema** se divide en las siguientes tres secciones:

- **Sistema:** muestra el estado de todas las áreas, alertas y advertencias de sistema activos e información del sistema.
- **Particiones:** muestras el estado de cada área definida en el sistema con hasta 20 incidencias de alarma. Puede armar y desarmar una partición y aquí se muestra el estado de la misma.
- **Inhibiciones y aislamientos:** Muestra una lista de todas las zonas aisladas y le permite restaurar o inhibir antes de armar.



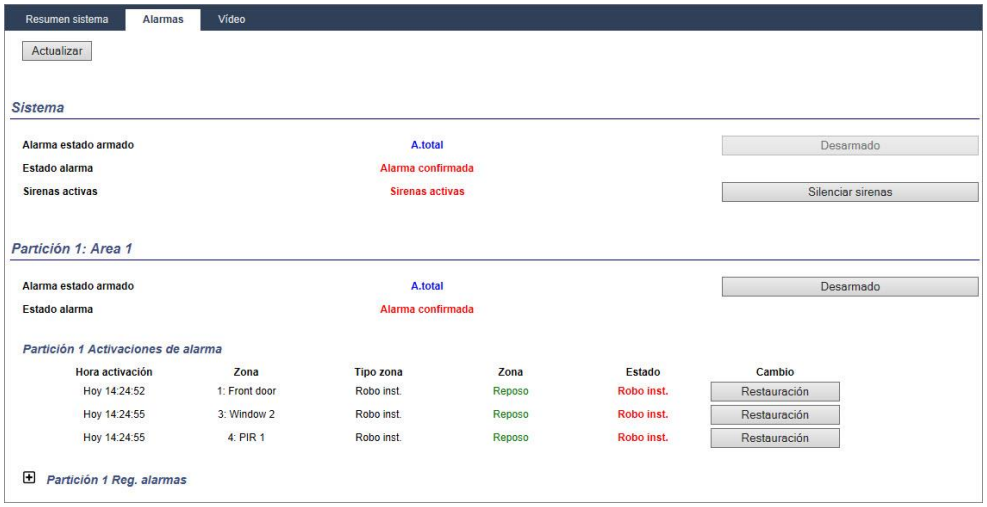
!	*AVISO*
	Si hay alarmas en el sistema, se muestra el mensaje **Ver etiqueta alarma**.

17.5.2 Información general de alarmas

La pestaña **Alarmas** muestra la siguiente información de sistema:

- **Alarma estado armado** - muestra si el sistema posee un armado parcial o completo en el momento en el que se disparó la alarma.
- **Estado 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.

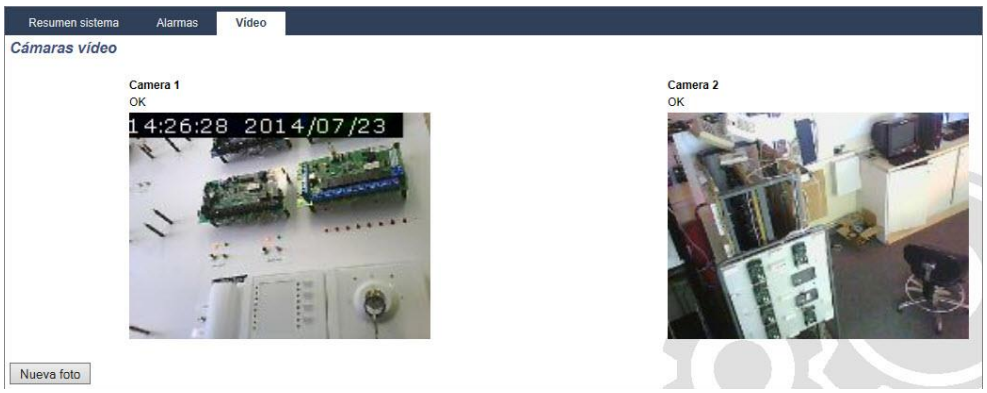
Para cada una de las particiones se muestra **Alarma estado armado**, **Estado alarma**, **Activaciones de alarma** y **Reg. alarmas**. **Activaciones de alarma** muestra una lista de zonas con estado de alarma ordenadas según activación. Haga clic en el botón **Restauración** para borrar. El **Reg. alarmas** muestra hasta 20 incidencias.



17.5.3 Visualización de vídeos

La pestaña **Vídeo** muestra imágenes de hasta 4 cámaras IP.

- En Modo técnico, Modo normal y Modo usuario, seleccione **SPC Home > Vídeo**.
  - ⇨ Todas las cámaras configuradas y operativas (hasta un máximo de cuatro) se muestran en la página **Cámaras vídeo**. En el siguiente ejemplo solo hay dos cámaras disponibles.



Las imágenes se actualizan automáticamente en función de la configuración de intervalo para la cámara. (Véase Configuración de vídeo [→ 273])

Haga clic en el botón **Nueva foto** para retener la imagen actual en pantalla y hacer una pausa en la actualización. Haga clic en el botón **Resumir actualización** para que la central reanude la actualización de las imágenes.

Nota: Compruebe que se ha seleccionado una resolución de 320 x 240 para las cámaras que se mostrarán en el navegador; de lo contrario, es posible que las imágenes no se muestren correctamente. Para el funcionamiento con SPC Pro y SPC Com se puede utilizar la resolución más alta de 640 x 480.

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

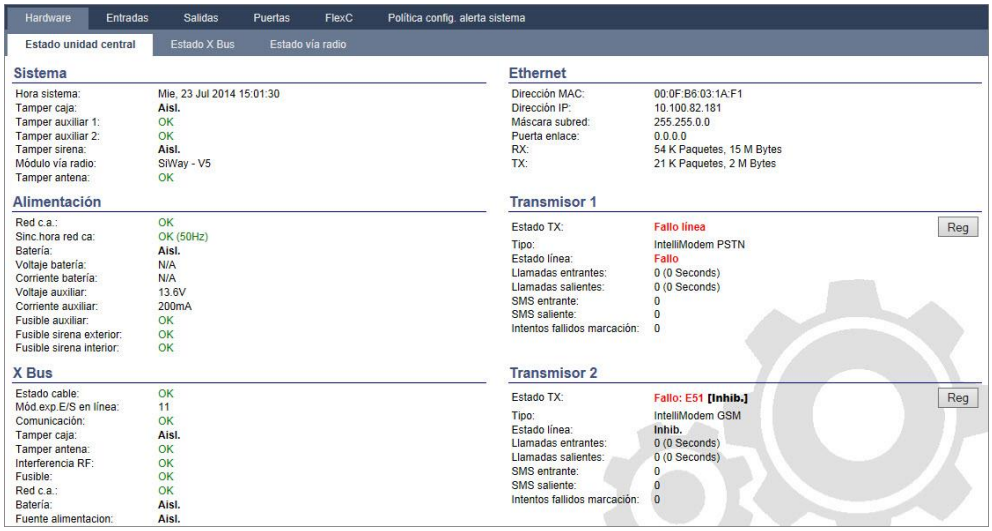
Mensaje	Descripción
Socket no válido	Error de manipulación de ranura interna
Imagen demasiado pequeña	Imagen recibida demasiado pequeña
Búfer demasiado pequeño	La imagen recibida es demasiado grande. Baje la resolución en la configuración de la cámara.
Formato incorrecto	Formato recibido no válido.
Abortar	Conexión TCP desconectada
Zona	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.
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

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 unidad central**.
2. Consulte las tablas a continuación para obtener más información.



Se pueden realizar las siguientes acciones

Las siguientes acciones solo son posibles si se ha establecido una conexión.

Reset incidencias (Pro)	Restaura todas las incidencias activas en la central. Estos mensajes de incidencia se muestran en texto rojo frente al elemento relevante.
Actualizar	Actualiza los cambios en el estado de la central. Para mostrar el estado real de la central en cualquier momento, debe actualizar la ventana de estado.

Técnico total / Técnico parcial	Para alternar entre los modos Técnico parcial y Técnico total. El modo Técnico total deshabilita las alarmas e impide la presentación de informes de incidencias a una estación central.

17.6.2 Estado de X-BUS

1. Seleccionar **Estado > Hardware > Estado X-Bus**.

   ⇨ Se muestra la siguiente ventana con el estado de los diferentes dispositivos X-Bus. Todos los módulos de expansión detectados aparecen listados por defecto.

ID	Nombre	Estado	Tipo	Núm.serie	Firmware	Lector	Vía radio	F.A.
1	IO 1	En línea	E/S [8 Zona / 2 Salida]	11327907	1.11 [07AUG13]	Inexistente	Inexistente	Type 1 - V4
2	AEX 2	En línea	Audio [4 Zona]	1434900	1.03 [13MAR13]	Inexistente	Inexistente	Inexistente
3	AEX 3	En línea	Audio [4 Zona / 1 Salida]	37070907	1.03 [13MAR13]	Inexistente	Inexistente	Inexistente
4	WIR 4	En línea	Vía radio	489907	1.11 [07AUG13]	Inexistente	SiWay - V5	Inexistente
5	IOA 5	En línea	E/S analizada [8 Zona / 2 Salida]	165074801	2.00 [09Apr14]	Inexistente	Inexistente	Inexistente
6	IO 6	En línea	E/S [8 Salida]	443907	1.11 [07AUG13]	Inexistente	Inexistente	Inexistente
7	KSW 7	En línea	Llave desarmado [1 Salida]	226593801	1.01 [11NOV10]	Inexistente	Inexistente	Inexistente
8	IND 8	En línea	Indicador [1 Zona]	223387801	1.03 [13MAR13]	EM4100	Inexistente	Inexistente

2. Seleccione una de las siguientes pestañas:
   - Módulos de expansión (para programar módulos de expansión, consulte la página [→ 217]).
   - Teclados (para programar teclados, consulte la página [→ 222]).
   - Controladores de puerta (para programar controladores de puerta, consulte la página [→ 226]).
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 mód.exp.E/S

1. Seleccione **Estado > Hardware > Estado X-Bus**.
2. Seleccione la pestaña **Mód. 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 exclusivo para el módulo de expansión.
Descripción	Descripción de texto del módulo de expansión. Este texto también aparecerá en el navegador y en el teclado.
Tipo	El tipo de módulo de expansión detectado (E/S, F.A., teclado, etc.).

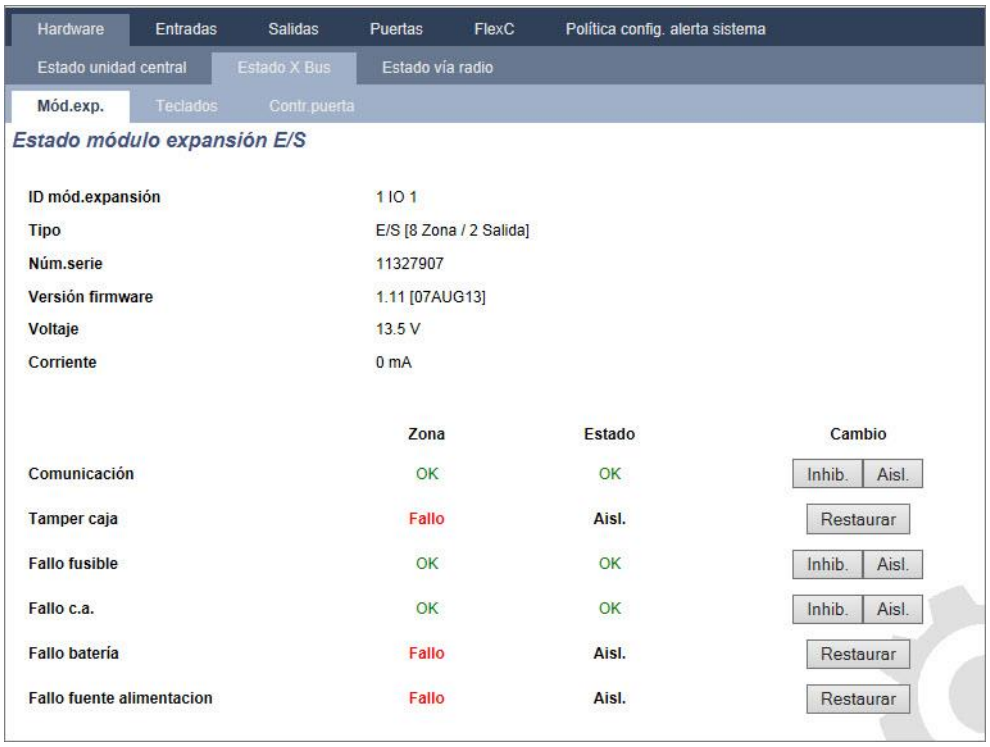
Núm. serie	El número de serie del módulo de expansión.
Versión	La versión de firmware del módulo de expansión.
Comunicación	El estado del módulo de expansión (en línea o fuera de línea).
Estado	El estado del módulo de expansión (OK, Fallo, Ab, Tamper).
F.A.	El tipo de fuente de alimentación conectada al módulo de expansión, si procede. Haga clic en la fuente de alimentación para ver su estado.

Se pueden realizar las siguientes acciones

Actualizar	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, Inhibido, Anulado) de la conexión del cable del X-BUS al módulo de expansión.
Tamper caja	El estado físico y programado del tamper de caja 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

Nombre	Descripción
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.

Se pueden realizar las siguientes acciones

Nombre	Descripción
Reset incidencias	Haga clic en este botón para restaurar todas las incidencias en la central.
Inhib. ⓘ	Haga clic en este botón para anular 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.

Ver también

Estado de la fuente de alimentación [→ 179]

17.6.2.2 Estado de la fuente de alimentación

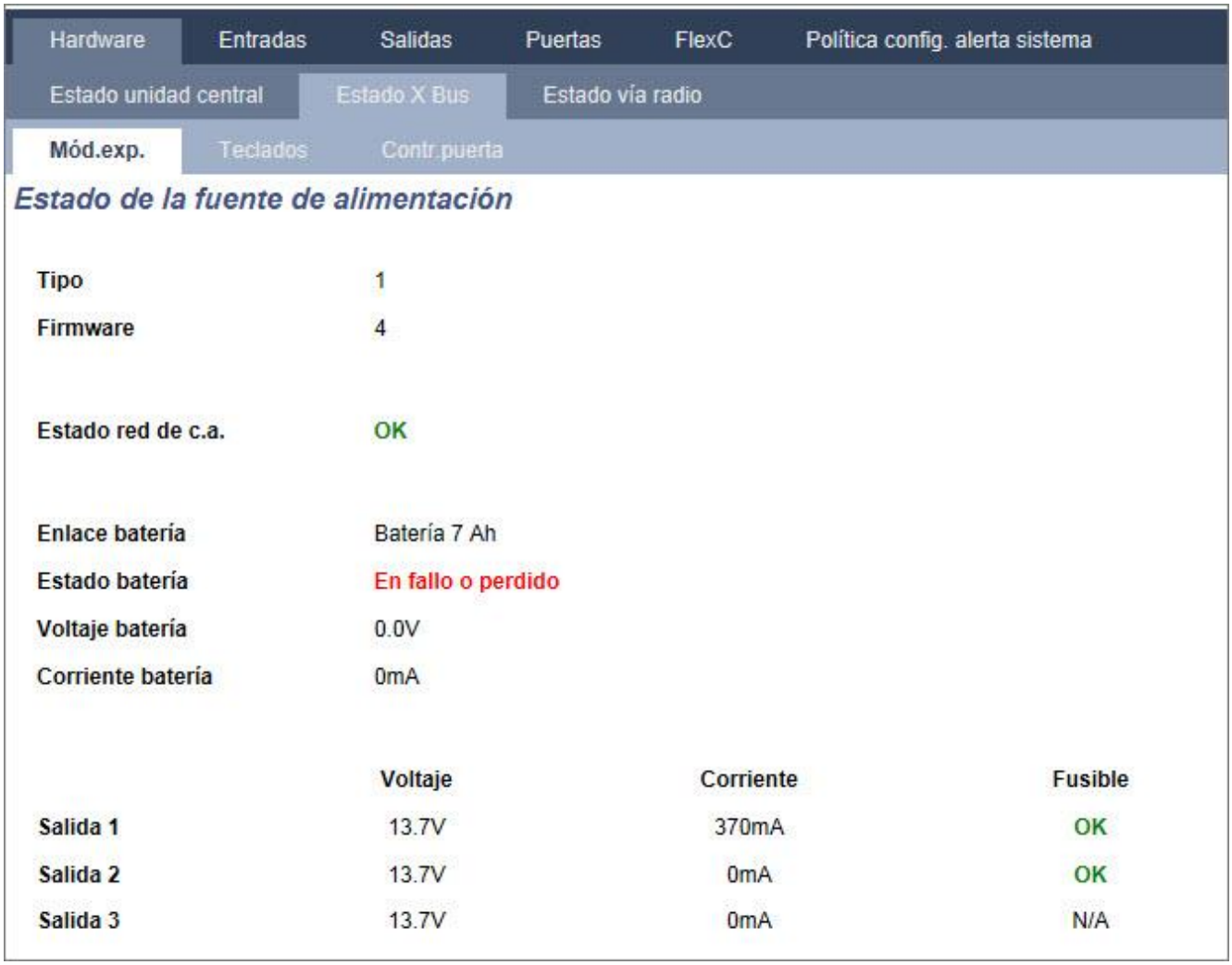
La ventana **Estado de la fuente de alimentación** muestra detalles sobre el estado actual de la fuente de alimentación y sus salidas, además de sobre el estado de cualquiera de las baterías conectadas.

Son compatibles los siguientes tipos de fuentes de alimentación:

- Fuente de alimentación inteligente SPCP332/333
- Fuente de alimentación inteligente SPCP355

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.
Salidas	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

En la siguiente imagen se muestra el estado de la fuente de alimentación inteligente SPCP355.

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.
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.
Salidas	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. Seleccionar **Estado > Hardware > Estado X-Bus**.
2. Seleccione la pestaña **Teclados**.
   ⇨ Se muestra una lista de teclados detectados.

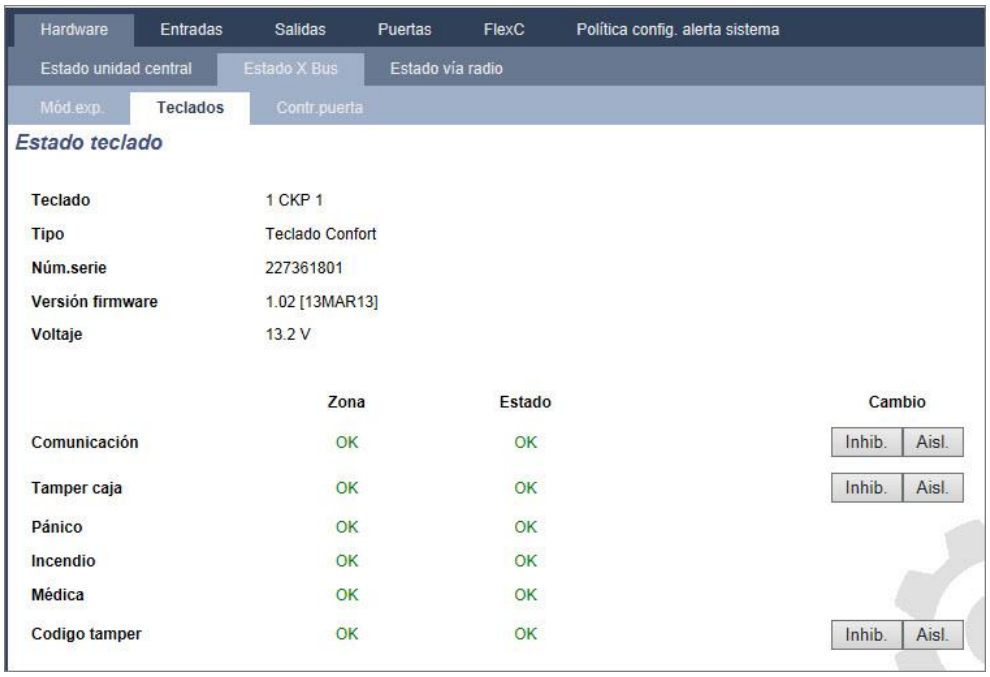
Nombre	Descripción
ID mód. expansión	Este número de ID es un identificador exclusivo para el teclado.
Descripción	Descripción de texto del teclado (máx. 16 caracteres).
Tipo	El tipo de módulo de expansión detectado (= teclado)
Núm.serie	El número de serie del teclado.
Versión	La versión de firmware del teclado.
Comunicación	El estado del teclado (en línea o fuera de línea).
Estado	El estado del teclado (OK, Fallo).

Se pueden realizar las siguientes acciones

Actualizar	Haga clic en el botón de 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, nombre, tipo, número de serie) para ver más información sobre su estado.



Comunicación	El estado físico (OK, Fallo) y el estado programado (OK, Inhibido, Anulado) de la conexión del cable del teclado al módulo de expansión.
Tamper caja	El estado físico y programado del tamper de caja del módulo de expansión.

ACCESO TARJETA	Se aplica sólo a los teclados con un receptor de tarjeta 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

Se pueden realizar las siguientes acciones

Reset incidencias	Haga clic en este botón para restaurar todas las incidencias en la central.
Inhib. ⓘ	Haga clic en este botón para anular 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. Seleccionar **Estado > Hardware > Estado X-Bus**.
2. Seleccione la pestaña **Contr. puerta**.
   ⇨ Se muestra una lista de controladores de puerta detectados.

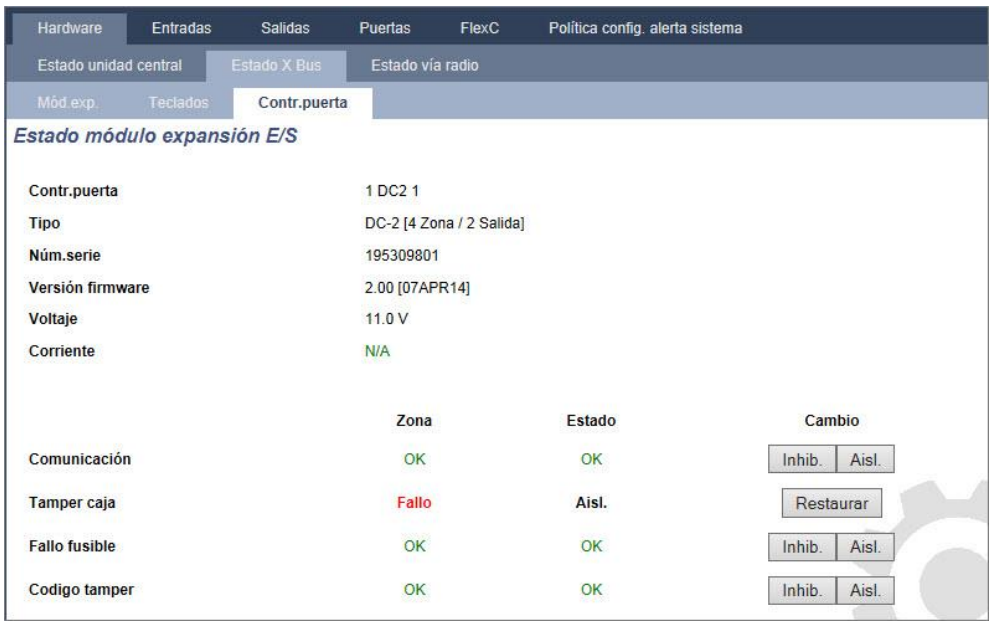
ID mód. expansión	Este número de ID es un identificador exclusivo para el controlador de puerta.
Descripción	Descripción de texto del controlador de puerta (máx. 16 caracteres).
Tipo	El tipo de módulo de expansión detectado (= controlador de puerta)
Núm.serie	Número de serie del controlador de puerta.
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.A.	Especifica si el controlador de puerta tiene una fuente de alimentación.

Se pueden realizar las siguientes acciones

Actualizar	Haga clic en el botón de actualización para actualizar el estado de las incidencias del sistema.

Para ver más información de estado:

- Haga clic en los parámetros de identificación de un controlador de puerta (ID, nombre, tipo, número de serie) para ver más información sobre su estado.



Comunicación	El estado físico (OK, Fallo) y el estado programado (OK, Inhibido, Anulado) de la conexión del cable del teclado al módulo de expansión.
Tamper caja	El estado físico y programado del tamper de caja del módulo de expansión.
Fallo fusible	El estado físico y programado del fusible del controlador de la puerta.
Código tamper	Estado del código de usuario. Múltiples intentos fallidos provocan una incidencia.

Se pueden realizar las siguientes acciones

Reset incidencias	Haga clic en este botón para restaurar todas las incidencias en la central.
Inhib. ⓘ	Haga clic en este botón para anular 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 mediante detectores vía radio (868 MHz) en la central SPC se realiza mediante módulos receptores vía radio que pueden venir montados de fábrica en el teclado, o instalando un módulo de expansión vía radio.

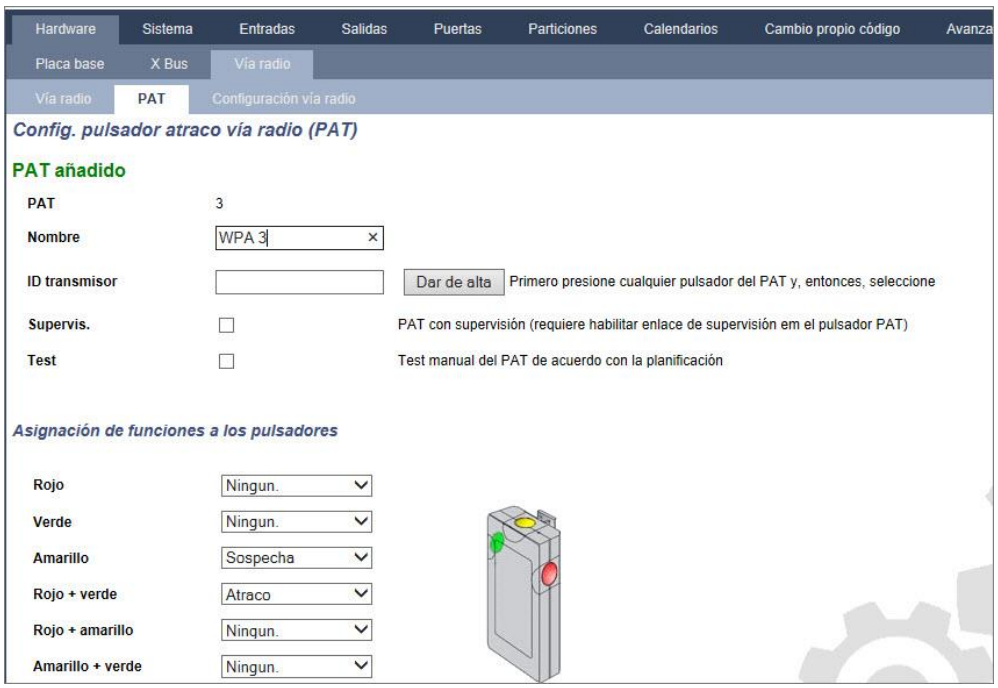
1. Seleccionar **Configuración > Hardware > Vía radio > Vía radio**.
2. Consulte la tabla a continuación para obtener más información.

Detector	El número del sensor dado de alta en el sistema (1 = primero, 2 = segundo, etc.)
ID	Un número de identificación exclusivo para ese detector.
Tipo	El tipo de detector vía radio detectado (contacto magnético, inercial/de impacto, etc.)
Zona	La zona en la que se ha dado de alta el detector.
Batería	El estado de la batería del detector (si está montada).
Supervisar	El estado de la operación de supervisión (OK = señal de supervisión recibida, No supervisado = 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 pierden la conexión.

Se pueden realizar las siguientes acciones

Registro	Haga clic para ver el registro del detector vía radio. Consulte la página [→ 186].
Dar de alta	Haga clic para abrir la lista de dispositivos vía radio sin estar dados de alta.

1. Seleccione **Estado > Hardware > Vía radio > PAT**.
2. Se muestra la identidad de cada PAT dado de alta así como su estado.



17.6.3.1 Registro: detector vía radio X

Para ver un registro rápido de las incidencias de un detector vía radio:

1. Haga clic en el botón **Registro**.
2. Consulte la tabla a continuación para obtener más información.
3. Cree un fichero de texto del registro haciendo clic en **Fichero de texto**.

Fecha/hora	La fecha y la hora de la incidencia registrada.
Receptor	La ubicación del receptor vía radio, es decir, 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 detector (OK, Fallo).

17.6.4 Zonas

Para ver la configuración, consulte la página [→ 251].

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 las tablas a continuación para obtener más información.

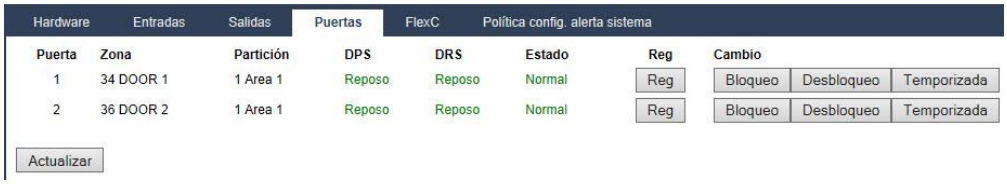
Actualización autom. estado Pro	Marque esta casilla para activar una actualización automática del estado de las zonas. Esto sólo se puede realizar para todas las zonas, y no para zonas filtradas.
Descripción de zona	Descripción de texto de la zona (máx. 16 caracteres).
Partición	Particiones a las que se asigna esta zona.
Tipo de zona	El tipo de zona (alarma, entrada/salida, etc.)
Calidad de 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 [→ 85].
Entrada	El estado de entrada detectado de esa zona (Desconocida, Abierta, Reposo, Desconectada, Corto, Pulso, Det. vibración, Enmascarada, Fallo, Fuera límites, Inestable, Sustitución c.c, Ruidoso.) Sustitución c.c. es una entrada de alerta de tamper. Sustitución c.c. realiza una comprobación periódica para garantizar que no se están aplicando tensiones eléctricas externas a dicho circuito. Inestable: Un estado inestable se produce cuando el valor de resistencia de entrada de zona no permanece estable durante un periodo de muestreo definido. Ruidoso: Un estado ruidoso se produce cuando se induce una interferencia externa en el circuito de entrada durante un periodo de muestreo definido. Fuera de límites: Se producirá un estado fuera de límites cuando el valor de resistencia en la entrada de zona no tiene lugar dentro de las tolerancias aceptadas para los valores RFL actuales.
Estado	El estado programado de dicha zona. Un valor de estado de Normal significa que la zona está programada para funcionar con normalidad. A continuación se indica la lista completa de los posibles valores: Aislada, Pruebas, Inhibida, Tamper, Alarma, Salida emergencia, Fallo aviso, Fallo atraco, Fallo detector, Fallo de línea, Pánico, Atraco, Alarma técnica, Alarma médica, Bloqueo, Incendio, Problema, PIR enmascarado, Normal, Activada, Tamper , Post Alarma. Una zona se encontrará en el estado Post alarma si se ha producido una alarma y la alarma confirmada ha excedido el tiempo. Esto restituye la zona, pero también indica que se produjo una alarma.

Se pueden realizar las siguientes acciones

Actualizar	Se 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 dicha zona.
Inhibir ⓘ	Haga clic en este botón para anular 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 inhibir 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 inhibir 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 Pro	Haga clic en este botón para iniciar una comprobación del detector sísmico seleccionado. Para más información sobre detectores sísmicos, véase Detectores sísmicos [→ 343].
Ocultar en reposo	Haga clic en este botón para ocultar todas las entradas cerradas.
Filtrado estado zonas Pro	Seleccione un tipo de zona en el menú desplegable. Sólo se mostrará el resumen de este tipo de zona.

17.6.5 Puertas

1. Seleccione **Estado > Puertas**.
2. Consulte las tablas a continuación para obtener más información.



Puerta	Este número de ID es un identificador exclusivo para la puerta.
Zona	El número de zona a la que está conectado el sensor de posición de la puerta (sólo si el sensor de posición de la puerta también se utiliza como zona de intrusión).
Partición	La partición a la que están asignadas la entrada del sensor de posición de la puerta y el lector de tarjetas.
DPS	Estado del sensor de posición de la puerta.
DRS	Estado del interruptor de liberación de la puerta.
Estado	El estado de la puerta (OK, Fallo).
Modo puerta Pro	Especifica el modo de funcionamiento de la puerta.

Se pueden realizar las siguientes acciones

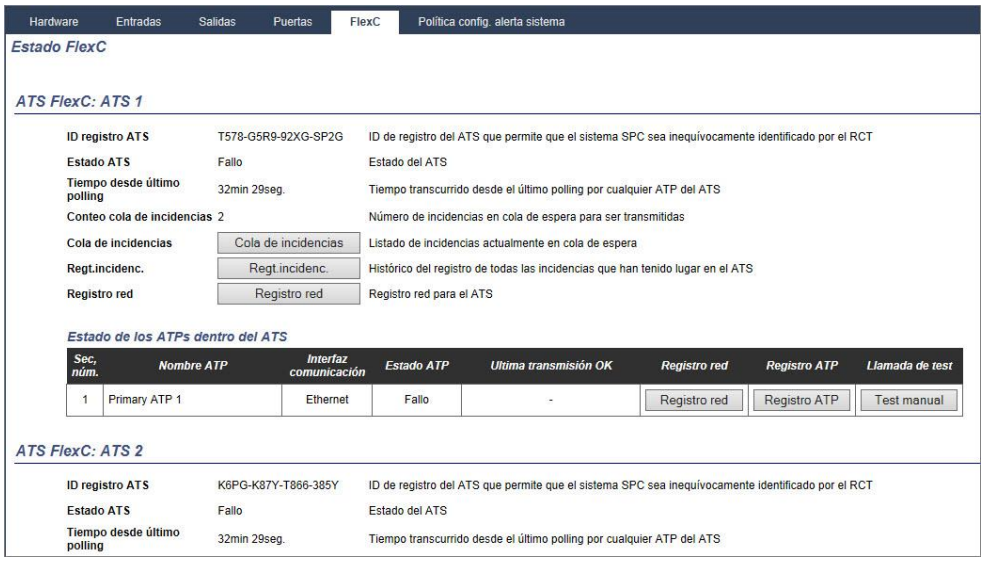
Actualizar	Actualiza el índice de puertas.
Registro	Muestra un registro de incidencias para la puerta seleccionada.
Bloqueo	Bloquea la puerta seleccionada.
Desbloqueo	Desbloquea la puerta seleccionada.
Normal	Devuelve la puerta al control normal del sistema.

Temporizada	Desbloquea la puerta durante un período temporizado.

17.6.6 Estado FlexC

Esta pantalla muestra el estado de cada ATS configurada en su sistema.

1. Para ver el estado de una ATS, vaya a **Estado - FlexC**.
2. La tabla abajo indicada describe los criterios de estado disponibles para cada ATS.



ID registro ATS	El ID de registro único de la ATS permite a la central ser identificada inequívocamente en el RCT.
Estado ATS	El estado de la ATS, por ejemplo, inicializando.
Tiempo desde último polling	Tiempo transcurrido desde el último polling en cualquier ATP del ATS.
Conteo cola de incidencias	Número de incidencias en la cola de incidencias que se encuentran a la espera de ser transmitidas.
Conteo cola de incidencias	Número de incidencias en la cola de incidencias que se encuentran a la espera de ser transmitidas.
Cola de incidencias	Lista de incidencias actualmente en la cola de incidencias. La tabla muestra lo siguiente: ● Secuencia de incidencias núm. ● Fecha/hora incidencia ● Descripción incidencia ● Info incidencia adicional ● Inicio fechado ● Duración TX
Regt.incidenc.	Historial del registro de incidencias para todas las incidencias que se han producido en la ATS. La tabla muestra los mismos campos que muestra arriba la cola de incidencias más el siguiente campo adicional:

	● Secuencia de incidencias núm. ● Fecha/hora incidencia ● Descripción incidencia ● Info incidencia adicional ● Resultado ● ATP enviada ● Inicio fechado ● ACK o fallo fechado ● Duración TX
Registro red	Registro de red para la ATS que muestra el intervalo test configurado.
Estado de la ATP dentro de la ATS	Esta tabla muestra cada ATP en la 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 realizada con éxito, el registro de red, el registro de ATP y el botón llamada de test. **Registro red:** Haga clic en este botón para mostrar el registro de red. **Registro ATP:** Muestra una lista de transmisiones de test. Haga clic en el botón **Actualizar** para actualizar el registro. Haga clic en el botón **Último el más reciente** para cambiar el orden de la vista. Por defecto, la incidencia más reciente se muestra en primer lugar. 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 Incidencias del sistema

1. Seleccione **Estado > Incidencias sistema**.
2. Consulte las tablas a continuación para obtener más información.

Alerta	Zona	Estado	Cambio
Red c.a. central	OK	OK	Inhib. Aisl.
Fallo batería	Fallo	Aisl.	Restaurar
Fallo fuente alimentacion	OK	OK	Inhib. Aisl.
Fusible central	OK	OK	Inhib. Aisl.
Fallo fusible sirena exterior	OK	OK	Inhib. Aisl.
Fallo fusible sirena interior	OK	OK	Inhib. Aisl.
Tamper sirena	Fallo	Aisl.	Restaurar
Tamper caja central	Fallo	Aisl.	Restaurar
Tamper auxiliar 1	OK	OK	Inhib. Aisl.
Tamper auxiliar 2	OK	OK	Inhib. Aisl.
Tamper antena	OK	OK	Inhib. Aisl.
Interferencia	OK	OK	Inhib. Aisl.
Fallo transmisor 1	OK	OK	Inhib. Aisl.
Fallo transmisor 2	Fallo	Inhib.	Restaurar Aisl.
Comunicación	OK	Alerta	Restauración
Código coacción usuario	OK	OK	
Mando pánico vía radio	OK	OK	
Alarma hombre caído	OK	OK	
Fallo cable X-Bus	OK	OK	Inhib. Aisl.
Codigo tamper	OK	OK	Inhib. Aisl.

Alerta	Descripción de la incidencia del sistema.
Zona	El estado actual de la incidencia detectado en la central (OK, Fallo).
Estado	El estado programado de la incidencia del sistema, es decir, si la incidencia ha sido inhibida o anulada. Si no se ha deshabilitado de ninguna manera la condición de la

⚠	incidencia, el valor que se muestra en el estado es OK (consulte la página).

Se pueden realizar las siguientes acciones

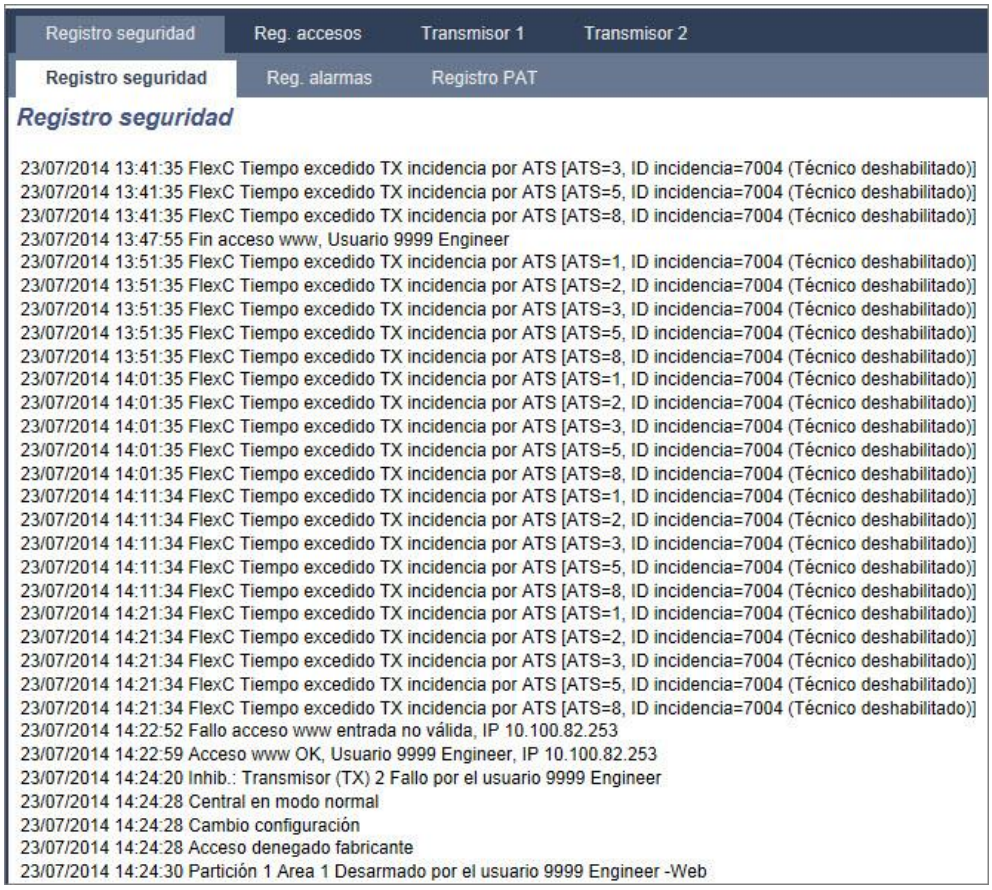
Actualizar	Haga clic en este botón para actualizar el estado de las incidencias del sistema.
Restaurar	Haga clic en este botón para restaurar una alerta en la central
Inhibir ⓘ	Haga clic en este botón para anular una condición de fallo. La operación de anulación deshabilitará dicho fallo o zona sólo 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 inhibir la zona. Al inhibir 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 inhibir zonas, ya que dichas zonas no estarán activas siempre que el sistema esté ARMADO.

17.7 Registros

17.7.1 Registro del sistema

Este registro muestra todas las incidencias del sistema SPC.

1. Seleccione **Registro > Registro seguridad > Registro seguridad**.
2. Cree un archivo de texto del registro haciendo clic en **Fichero 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 acceso

El registro recoge todas las incidencias de acceso del sistema SPC.

- Seleccione **Registro > Registro acceso**.

⇨ Se mostrará la siguiente ventana:

Registro seguridad | Reg. accesos | Transmisor 1 | Transmisor 2

Reg. accesos

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 fichero de texto del registro haciendo clic en el botón **Fichero de texto**.

17.7.3 Registro PAT

Este registro muestra todas las incidencias de PAT en el sistema.

- Seleccione **Registro seguridad > Registro PAT**.

  ⇨ Se mostrará la siguiente ventana:

17.7.4 REGISTRO ALARMAS

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

- Seleccione **Reg > Registro seguridad > Reg. alarmas**.

En este registro se muestran los siguientes tipos:

- Zonas
  - Robo inst.
  - Pánico
- Incidencias del sistema
  - Alarma confirmada
  - Código coacción usuario
  - Pánico XBUS
  - 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:

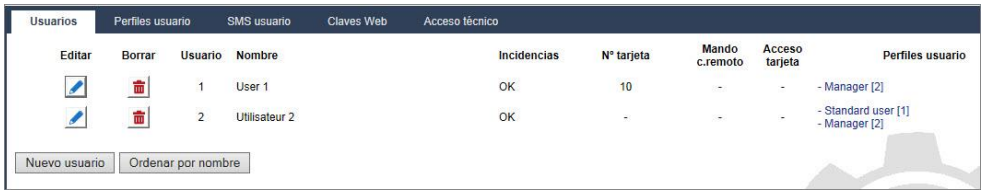
N.º máximo	SPC4xxx	SPC5xxx	SPC6xxx
Usuarios	100	500	2500
Perfiles de usuario	100	100	100
Perfiles de usuario por Usuario	5	5	5
Dispositivos PACE	32	250	250
ID SMS	32	50	100
Claves web	32	50	100
Mandos vía radio	32	50	100
Dispositivos HCD	32	32	32

	⚠ 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 usuario, no se asignará ningún perfil (véase Perfiles de usuario [→ 196]). Por favor, 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

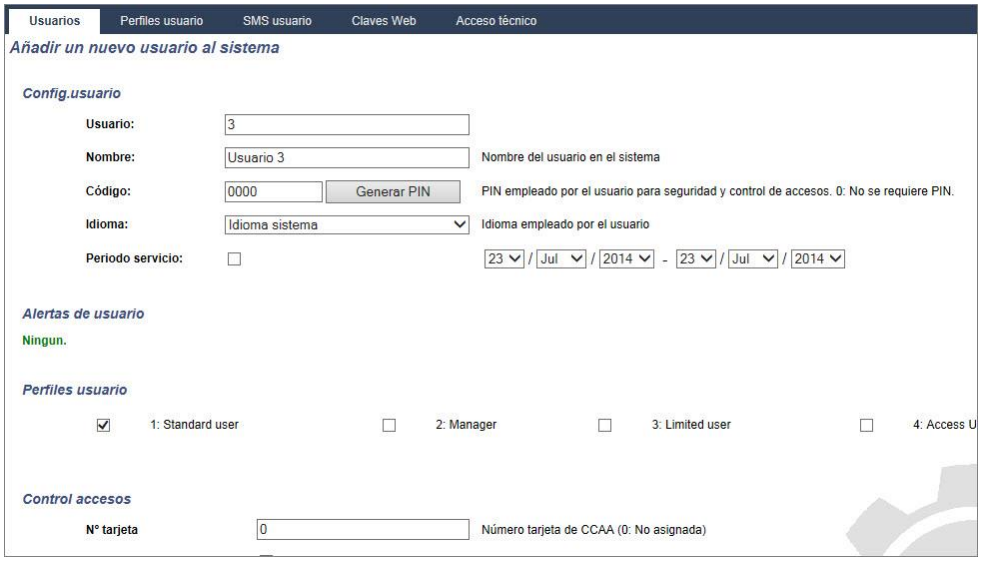
1. Seleccione **Usuarios > Usuarios> Añadir usuario**.

   ⇨ Se muestra una lista de usuarios configurados.



2. Haga clic en el botón **Añadir** o en el botón **Editar** del usuario deseado.

   ⇨ Aparecerá la siguiente pantalla.



3. Introduzca un **ID de usuario** que no se esté utilizando actualmente. Si introduce un ID de usuario que ya se haya utilizado, se mostrará el mensaje "ID no disponible".

4. Proporcione un **Nombre de usuario** (16 caracteres como máximo y con distinción de mayúsculas y minúsculas).

5. Para generar automáticamente un **Código** para un usuario nuevo, haga clic en el botón **Generar 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. Seleccione el Perfil de usuario [→ 196] adecuado para este usuario.
8. Seleccione **Cód. intimidación** para este usuario si es necesario. El número de PINs asignados para intimidación (PIN+1 o PIN+2) está configurado en Opciones del sistema [→ 234].

La opción de intimidación solo está disponible en esta pantalla si "Alarma de intimidación" está habilitado para el sistema en Opciones del sistema. Si la opción de intimidación está habilitada para este usuario, no se permiten códigos de usuario consecutivos (p. ej. 2906, 2907), ya que al introducir este código desde el teclado se 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
Visita	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 Acompañante para permitir abrir la puerta a otros titulares de tarjeta sin esta atribución. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con la atribución de Acompañante 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

Atributo	Descripción
	estancia. 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**
- 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:

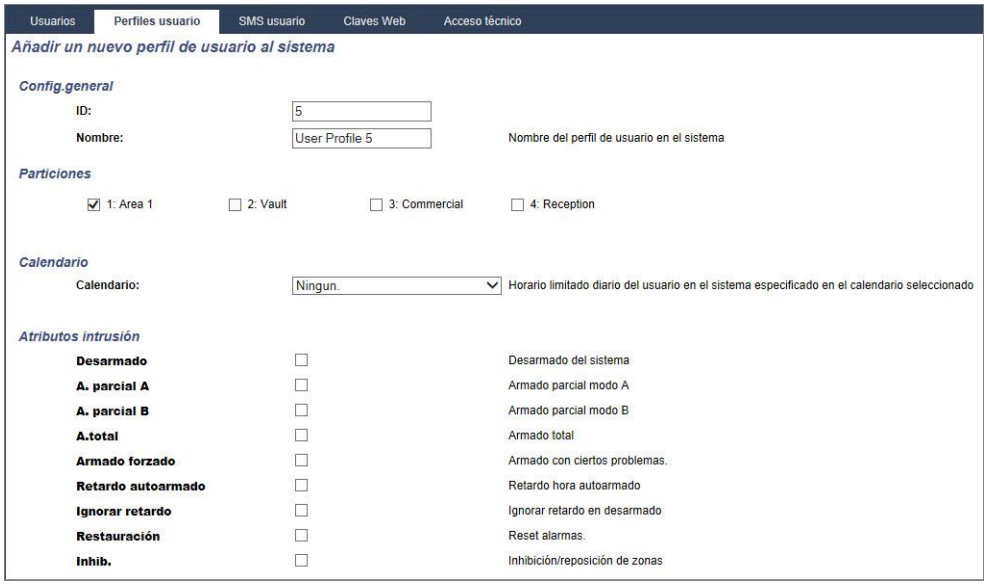
1. Cambie el número de tarjeta a cero (0).
2. Haga clic en **Guardar**.
   La tarjeta se desasigna del usuario y también se borra del sistema.
3. Para volver a añadir la tarjeta, deberá volver a escanearla.

17.8.2 Añadir/Editar perfiles de usuario

!	*AVISO*
	Los perfiles de usuario globales no se pueden editar en el navegador ni en el SPC Pro, sino que deben editarse en el 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. Seleccione **Añadir perfil de usuario** o haga clic en el botón **Editar** del perfil requerido.
   Se muestra la siguiente pantalla 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 de usuario que ya se haya utilizado, se mostrará 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.

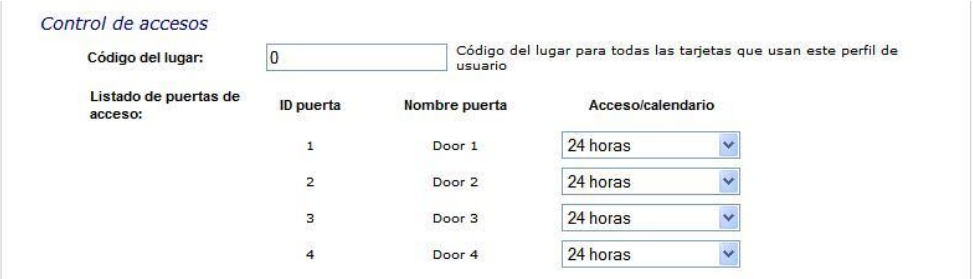
Atributos de usuario

Derecho	Tipo de perfil de usuario por defecto	Descripción
Atributos de usuario: Intrusión		
Armado total	Maestro estándar limitado	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.
Armado parcial A	Maestro estándar	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	Maestro estándar	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	Maestro estándar limitado	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	Maestro* estándar	El usuario puede retrasar o cancelar el autoarmado.
Ignorar retardo	Maestro estándar	El usuario puede anular automáticamente el Retardo desarmado. Sólo disponible para instalaciones Financieras. Consulte Armado/desarmado [→ 257]
Restaurar	Maestro estándar	Con la función RESTAURAR se restaura la condición de alerta en el sistema y se 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.

Derecho	Tipo de perfil de usuario por defecto	Descripción
Inhibir	Maestro estándar	Al anularse 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	Maestro* estándar	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.
Atributos de usuario: Sistema		
Acceso web	Maestro* estándar	El usuario puede acceder a la central a través del navegador web.
Registro de incidencias	Maestro estándar	Esta opción de menú muestra la incidencia más reciente en la pantalla del teclado. El registro de incidencias [→ 158] informa sobre la hora y la fecha de cada incidencia registrada.
Usuarios	Maestro	Este usuario puede crear y editar otros usuarios en la central, pero solo con los mismos derechos o menos que él.
SMS	Maestro* estándar	Esta característica permite a los usuarios configurar el servicio de mensajes SMS si se ha instalado un módem en el sistema.
Configurar Fecha	Maestro estándar	Utilice esta opción de menú para programar la hora y la fecha en el sistema [→ 166]. 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	Maestro estándar	Esta opción de menú permite a los usuarios cambiar sus códigos de usuario [→ 159]. **Nota**: Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.
Ver vídeo / Vídeo en navegador	Maestro estándar	El usuario puede ver imágenes de vídeo mediante el navegador web. Nota: para esta función también debe estar habilitado el derecho de Acceso web.
Chime	Maestro estándar	Todas las zonas con el atributo CHIME generan, al abrirlas, una ráfaga corta de tonos acústicos 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	Maestro	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.

Derecho	Tipo de perfil de usuario por defecto	Descripción
Actualizar	Maestro	El usuario puede autorizar al fabricante el acceso a la central para actualizar el firmware.
Atributos de usuario: Control		
Salidas	Maestro estándar	Activación/desactivación de las salidas configuradas (actuaciones). Véase Edición de una salida [→ 209].
X-10	Control de acceso Maestro estándar	Activación y desactivación de los dispositivos X-10 configurados. **Nota:**X-10 ya no es compatible. Esta funcionalidad solo se mantiene en el sistema para soporte de legado.
Control de puertas	Control de acceso Maestro estándar*	El usuario puede bloquear/desbloquear puertas.
Control RF	Control de acceso Maestro estándar	El usuario puede controlar la salida RF
Atributos de usuario: Test		
Test sirena(s):	Maestro estándar	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	Maestro estándar	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	Maestro estándar	El usuario puede comprobar un PAT.
Test sísmico	Maestro estándar	El usuario puede comprobar el detector sísmico.
Atributos de usuario: Técnico		
Config. de usuarios (master)		El usuario puede crear y editar otros usuarios en el sistema sin restricción de los atributos de usuario.
Config. perfiles usuario		El usuario puede crear y editar perfiles de usuario en el sistema.
Configurar calendarios		El usuario puede configurar calendarios.
Config. puertas		El usuario puede editar puertas.
* 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 que usan este perfil de usuario. Consulte la sección correspondiente del apéndice en Lectores y formatos de tarjetas [→ 376].
2. Seleccione los derechos de **Acceso** de este perfil de usuario para las puertas configuradas en el sistema. Las opciones son:
   - Sin acceso
   - 24 horas (es decir, sin límite de tiempo)
   - 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.

Ver también

🗎 Añadir/Editar perfiles de usuario [→ 198]
🗎 Añadir/Editar una partición [→ 251]

17.8.3 Configuración de SMS

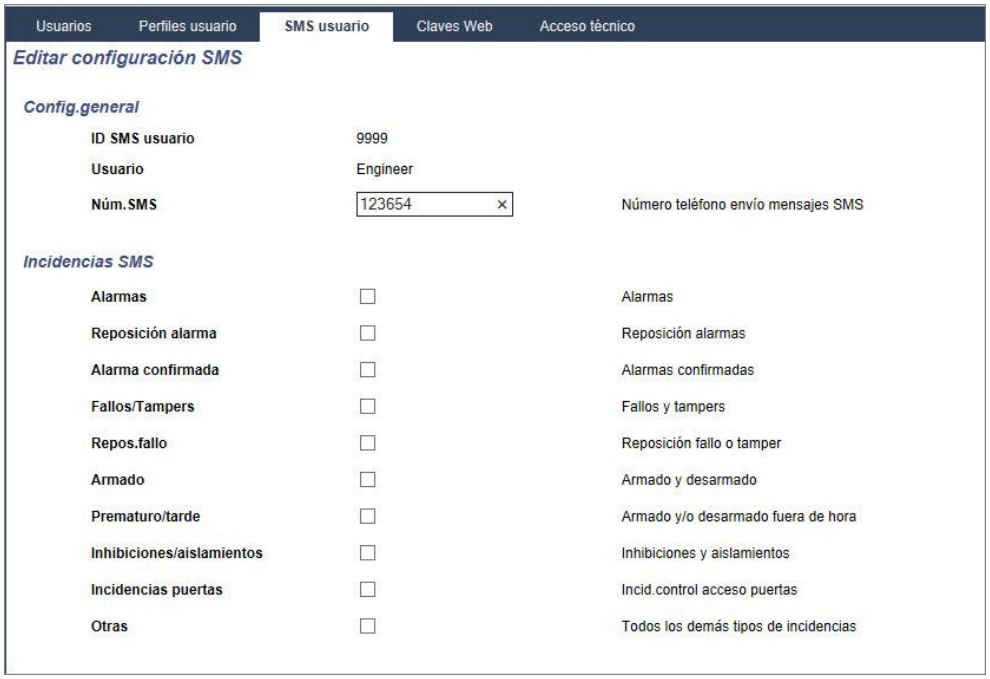
El sistema SPC permite la mensajería remota (SMS) en sistemas que tengan un módem instalado.

▷ Hay un módem instalado e identificado por el sistema.

▷ La función **Autentificación SMS** está activada. Consulte página [→ 234].

1. Seleccione **Usuarios > SMS usuario**.
   ⇨ 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.
Usuario	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. Véase Comandos de SMS [→ 202]

!	*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 Identidad de Línea Llamante (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 ****.ATOT	ATOT Arm. 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
**** DESM ****.DESM ****. DESM	DESM Desarmado	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 (X10) ****.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 (Permitir técnico) ****.ATEC.ON	ATEC.ON	Habilitar acceso de técnico	Acceso a técnico
**** ATEC.OFF	ATEC.OFF	Deshabilita el acceso del técnico	Acceso retirado a técnico

****.ATEC.OFF			
**** AFAB.ON ****.AFAB.ON		Habilita el acceso de fabricante	Estado de fabricante
**** AFAB.OFF ****.AFAB.OFF		Deshabilita el acceso de fabricante	Estado de fabricante
**** ABT.5.ON ****.ABT.5.ON ****. Salida		Cuando la salida de usuario se identifica como "ABT.5", 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 se identifica como "ABT.5", está desactivado	Estado de "ABT.5" Por ejemplo: Salida ABT.5 desactivada
****.APA (Armado parcial A)		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 ventana de Opciones. Véase Opciones [→ 234]	Sistema armado.
****.APB ARMADO PARCIAL B)		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 ventana de Opciones. Véase Opciones [→ 234] Por ejemplo: ****.APA Noche	Sistema armado.
****.BORR ****. Restaurar		Permite el borrado de alertas por SMS	

Para el reconocimiento de SMS, la identificación de la salida de usuario utiliza el formato ONNN, donde O se refiere a la salida de usuario y NNN son los espacios numéricos (no todos son necesarios).
(Ejemplo: ABT.5 es la salida de usuario 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 con 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 proveedores de servicios sólo permiten los SMS a un teléfono registrado en el mismo país. (Esto se debe a problemas derivados de la facturación)

17.8.5 Borrado de claves web

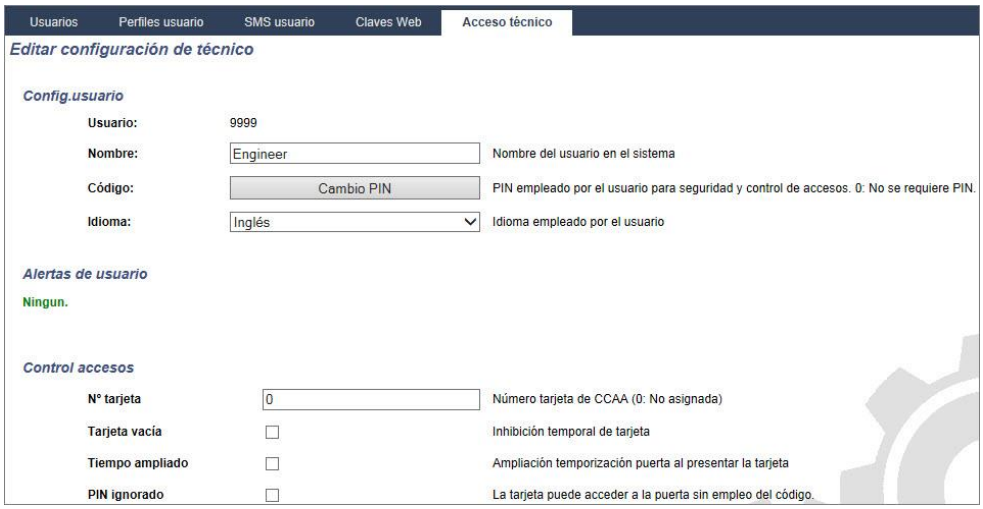
En esta pantalla aparece una lista de claves de técnico y de cualquier otro usuario, así como la clave de técnico que se ha creado para acceder al navegador de Internet.

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 Cambio PIN [→ 206] para cambiar el código de técnico.
   ⇨ **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; véase Actualizar idiomas [→ 325]).

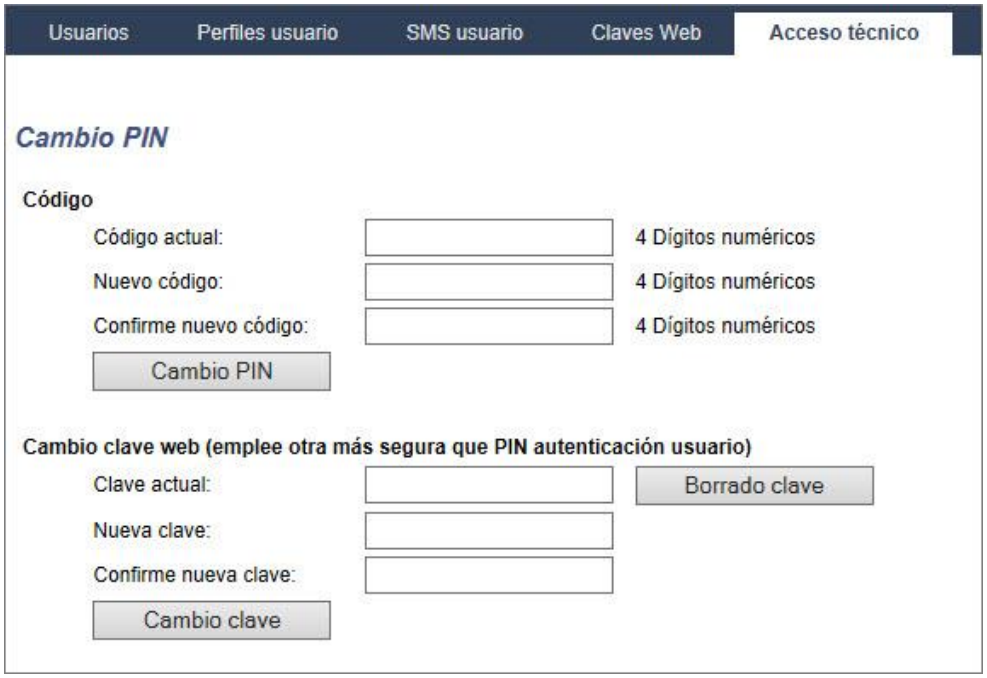
Control de accesos

Atributo	Descripción
Número tarjeta	Número de la tarjeta de CCAA Introduzca 0 para dejar sin asignar esta tarjeta.

Atributo	Descripción
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
Visita	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 Acompañante para permitir abrir la puerta a otros titulares de tarjeta sin esta atribución. El período de tiempo durante el cual los titulares de tarjetas pueden presentar sus tarjetas después de haberse presentado otra con la atribución de Acompañante 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 estancia. 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 pantalla 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).



- Cambie el código PIN como se indica a continuación:

Código actual	Introduzca el código PIN actual del técnico. (solo dígitos numéricos)
Nuevo código	Introduzca el nuevo código PIN del técnico. (solo dígitos numéricos)
Confirme nuevo código	Vuelva a introducir el nuevo código PIN del técnico.

1. Haga clic en el botón **Cambio PIN** para activar el nuevo código PIN.

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**.

2. Cambie la clave web por otra 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.

- Haga clic en el botón **Cambio clave** para activar la nueva clave.

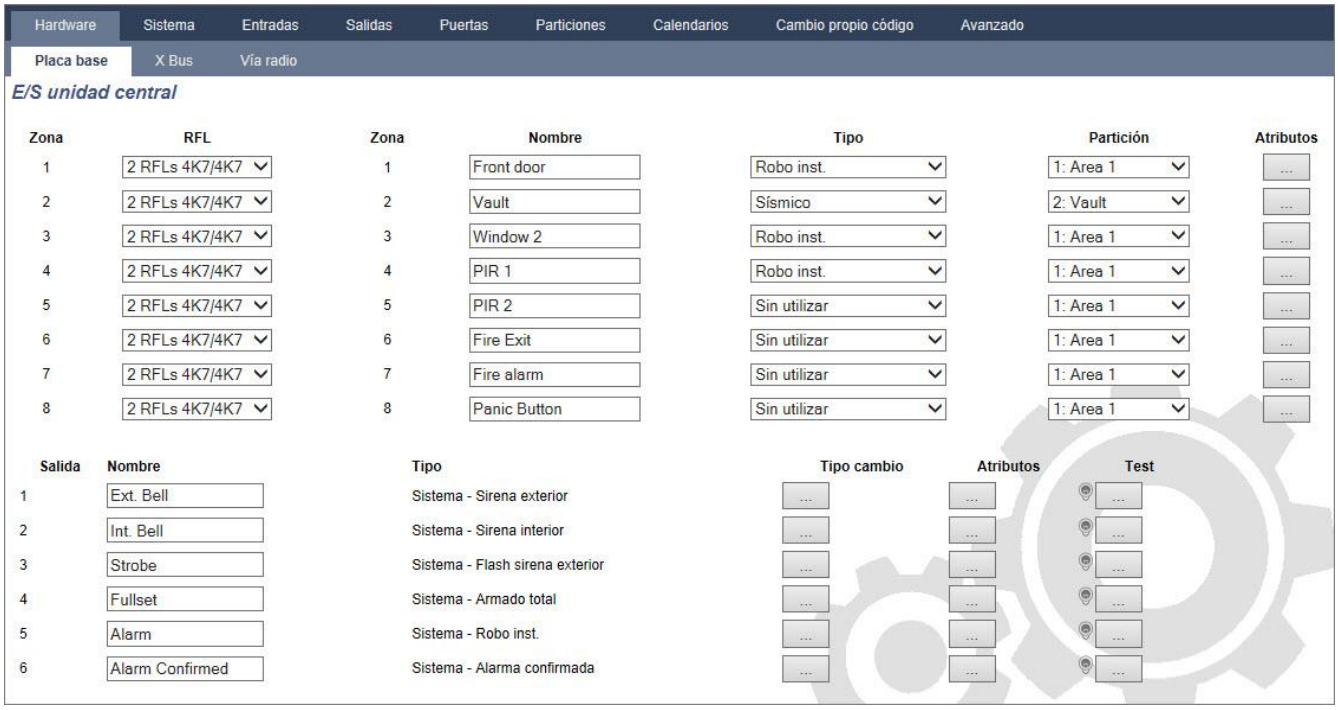
Esta clave distingue entre mayúsculas y minúsculas; así pues, compruebe si introduce caracteres en mayúsculas o en minúsculas en su nueva clave.

17.9 Configuración

17.9.1 Configuración de entradas y salidas del controlador

17.9.1.1 Edición de una entrada

1. Seleccione **Configuración > Hardware > Placa base**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.



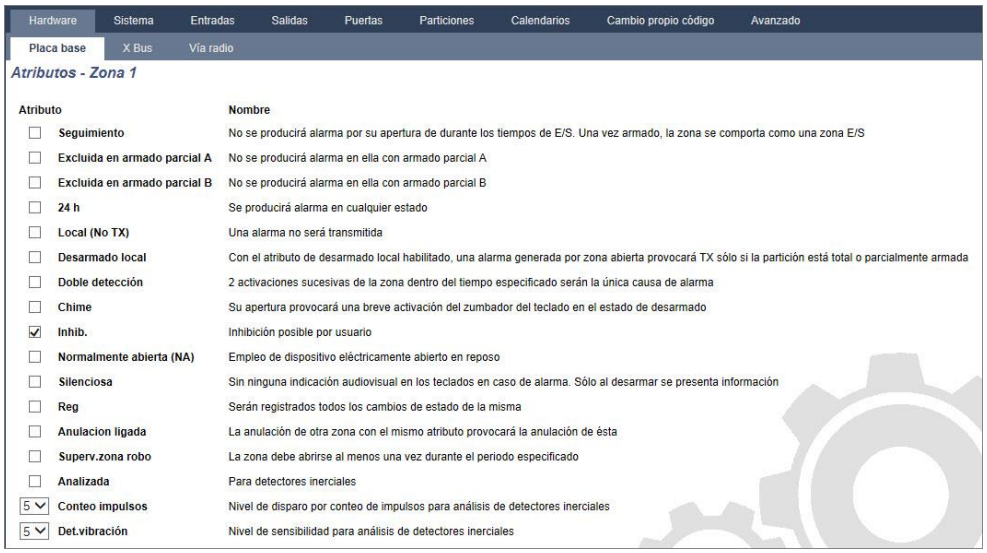
Entrada	El número se presenta para referencia y no se puede programar.
RFL	Seleccione RFL para la entrada de zona (por defecto: 4K7).
Analizado (Pro)	Muestra si el detector es de tipo inercial/shock
Conteo de impulsos (Pro)	Recuento de impulsos programado en la central que activará una alarma desde un detector inercial / de shock.
Ataque serio (Pro)	La sensibilidad programada en la central que activará una alarma desde un detector inercial / de shock.
Zona	Número de la zona en la central.
Descripción	Introduzca un texto que describa la entrada (máx. 16 caracteres). Este texto también aparecerá en el navegador y en el teclado.
Tipo	El tipo de zona (consulte la página [→ 368]).
Partición	Sólo si la función de particiones (múltiples) está activada en el menú Config. central > Config. sistema > Opciones. Seleccione las particiones a las que se ha asignado esta zona.
Atributos	Un icono en este campo indica que se han programado atributos para esta zona. (consulte la página [→ 209]).

17.9.1.1.1 Zonas de entrada: atributos

Se puede asignar a cada zona del SPC un atributo que determine las propiedades de la misma.

Para asignar un atributo a una zona:

1. Seleccione **Configuración > Hardware > Placa base > Atributos**.
   ⇨ Se mostrará la siguiente ventana:

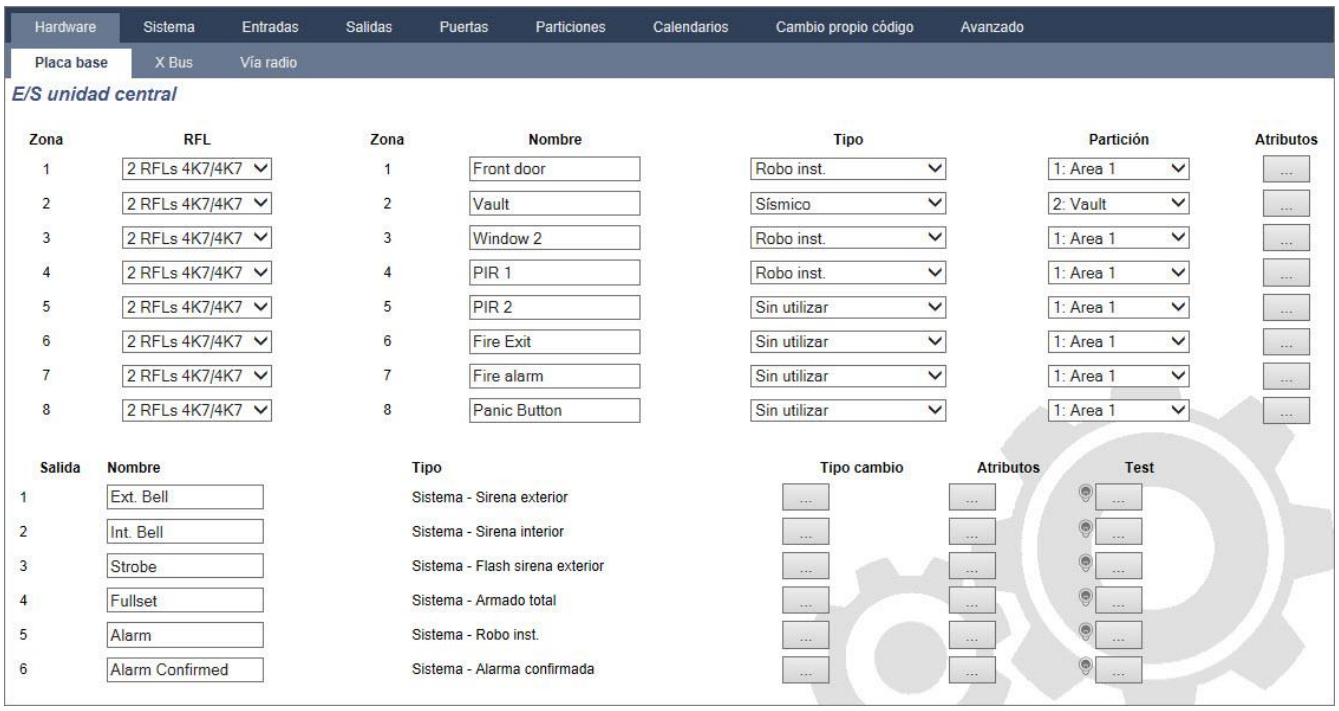


2. Marque la casilla junto al atributo preferido.

Los atributos que se presentan en esta página dependerán del tipo de zona seleccionada. Encontrará una lista de atributos asignables en la página [→ 374].

17.9.1.2 Edición de una salida

1. Seleccione **Configuración > Hardware > Placa base**.
2. Configure los campos tal como se describe en la siguiente tabla.



Tipo de salida	● **Salida sistema**: Seleccione el tipo en el menú desplegable. (Véase Tipos de salida y puertos de salida [→ 211]) ● **Salida 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 dicha partición. (Véase Tipos de salida y puertos de salida [→ 211]) ● **Asig. a zona**: Seleccione qué zona se debe asignar. ● **Salida sistema**: Seleccione qué salida del sistema se debe asignar. ● **Salida puerta**: Seleccione el número de puerta y el tipo de salida del sistema para dicha puerta. (Véase Tipos de salida y puertos de salida [→ 211]) ● **Conmutador llave**: Seleccione el ID de nodo para el conmutador de llave requerido y la posición de llave requerida para asignar a esta salida.
Descripción	Introduzca un texto que describa la salida (máx. 16 caracteres). Este texto también aparecerá en el navegador y en el teclado.
Configuración salidas	● **Modo**: Seleccione el modo de funcionamiento. Continuo, sigue el tipo de salida; intermitente, se activa y desactiva con tipo de salida activo; de una activación, genera un impulso cuando se activa el tipo de salida. ● **Reactivación**: Marque esta casilla para reactivar salidas de una única activación. ● **En hora**: Introduzca el modo En hora que se aplica a salidas de una única activación e intermitentes. ● **Fuera de hora**: Introduzca el modo Fuera de hora que se aplica a salidas intermitentes. ● **Inversa**: Marque esta casilla para invertir la salida física. ● **Registro**: Marque esta casilla para registrar los cambios en el estado de la salida en el registro de incidencias. ● **Calendario**: Si es necesario, seleccione el calendario deseado. Consulte la página [→ 267].

Ver también

🗎 Calendarios [→ 267]

17.9.1.2.1 Tipos de salida 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 o informar sobre ello a estaciones centrales remotas si fuera necesario.

Todos los puertos de salida de los módulos de expansión son salidas de tipo relé de polo único (NA, COM, NC); por tanto, los dispositivos de salida pueden necesitar fuentes de alimentación externas para activarse si están conectados a salidas de módulos de expansión.

La activación de un tipo de salida concreto depende del tipo de zona (consulte la página [→ 368]) o de condición de la alerta que provoca la activación. Si se definen varias particiones en el sistema, las salidas del 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 alimentación) mientras que las salidas de partición indican incidencias detectadas en una o más de las particiones definidas en el sistema. Cada partición cuenta con su propio conjunto de salidas de partición. Si una de ellas es una partición común para otras, sus salidas indicarán el estado de todas las particiones para las que es común, incluyendo su propio estado. Por ejemplo, si la partición 1 es común para las particiones 2 y 3, y Sirena Exterior está activada para la partición 2, la salida Sirena Exterior de la partición 1 también estará activada.

Algunos tipos de salida sólo pueden indicar incidencias que afectan a todo el sistema (no de particiones específicas). Consulte la tabla que figura 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 estará activa cuando cualquier sirena exterior de una partición también lo esté. Por defecto, esta salida se asigna a la primera salida de la placa del controlador (EXT+, EXT-). Nota: Una salida de sirena exterior se activa automáticamente siempre que una zona programada como Alarma active una alarma en los modos Armado total o Armado parcial.
Flash sirena exterior	Este tipo de salida se utiliza para activar el flash en la sirena exterior del sistema, y está activo cuando cualquier flash de partición lo esté. Por defecto, esta salida se asigna a la salida del relé del flash (Salida 3) en la placa del controlador (NA, COM, NC). Nota: Una salida de flash de sirena exterior se activa automáticamente siempre que una zona programada como Alarma active una alarma en los modos Armado total o Armado parcial. El flash de la sirena exterior se activa en una condición de "Fallo al armar" si en las opciones del sistema está seleccionada la opción "Fallo al armar".
Sirena interior	Este tipo de salida se utiliza para activar la sirena interior del sistema y estará activa cuando cualquier sirena interior de una partición también lo esté. Por defecto, se asigna a la segunda salida de la placa del controlador (INT+, INT-). Nota: Una salida de sirena interior se activa automáticamente siempre que una zona programada como Alarma active una alarma en los modos 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".
Robo inst.	Esta salida se enciende tras la activación de una zona de alarma en el sistema o desde cualquier partición definida en el sistema.
Alarma confirmada	Esta salida se enciende cuando se ha confirmado una alarma. Una alarma se confirma cuando 2 zonas independientes del sistema (o dentro de la misma partición) se activan en un periodo de tiempo establecido.

Pánico*	Esta salida se enciende tras la activación, desde cualquier partición, de tipos de zona de Alarma de pánico. También se genera una salida de Alarma de pánico si se produce una incidencia de coacción de usuario o si la opción de pánico está habilitada para el teclado.
Atraco	Esta salida se enciende cuando una zona programada como de tipo Atraco activa una alarma desde cualquier partición.
Incendio	Esta salida se enciende tras la activación de una zona de incendio en el sistema (o desde cualquier partición).
Tamper	Esta salida se enciende cuando se detecta una condición de tamper desde cualquier parte del sistema. Para un sistema de grado 3, si se pierde la comunicación con un dispositivo XBUS durante más de 100 s, se genera un tamper y las incidencias SIA y CIR de las que se informa envían un tamper.
Alarma médica	Esta salida se enciende cuando se activa una zona médica.
Fallo	Esta salida se enciende cuando se detecta un fallo técnico.
Técnico	Esta salida sigue a la actividad en una zona técnica.
Fallo de red c. a.*	Esta salida se activa cuando se desconecta la alimentación.
Fallo batería*	Esta salida se activa cuando hay un problema con la batería de reserva. Esta salida se activa si el voltaje de la batería desciende por debajo de 11 V. La opción de "Restaurar" para este fallo sólo se presenta cuando el nivel de voltaje supera los 11,8 V.
Armado parcial A	Esta salida se activa si el sistema o cualquier partición definida en el mismo está en modo Armado parcial A.
Armado parcial B	Esta salida se activa si el sistema o cualquier partición definida en el mismo 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 el sistema, o cualquier partición definida en el mismo, ha fallado al armar, y se borra cuando se restaura la alerta
Entrada/salida	Esta salida se activa si se ha activado una zona de E/S, p. ej. si está funcionando un temporizador de Entrada o Salida de un sistema o partición.
Enclavamiento	Esta salida se enciende tal como se haya definido en la configuración del enclavamiento de salidas del sistema (consulte Configuración del enclavamiento y autoarmado de salidas del sistema [→ 214]). Esta salida se puede utilizar para resetear los detectores de enclavamiento, como detectores de humo o inerciales.
Salida de incendio	Esta salida se ENCIENDE si se activa cualquier zona Inc.X en el sistema.
Chime	Esta salida se enciende momentáneamente cuando se abre cualquier zona del sistema con el atributo Chime.
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 enciende momentáneamente cuando un test de intrusión está operativo y una zona se activa. Esta salida se puede utilizar, por ejemplo, para activar pruebas funcionales de detectores conectados (si está disponible).
Autoarmado	Esta salida se enciende si la función de autoarmado se ha activado en el sistema.
Código coacción usuario	Esta salida se enciende si se ha activado un estado de coacción del usuario (se ha introducido el código PIN + 1 en el teclado).
PIR enmascarado	Esta salida se enciende si hay alguna zona PIR con máscara en el sistema. Esto genera una salida de fallo en el LED del teclado.

	Esta salida se bloquea y permanecerá activa hasta que sea restablecida por un usuario de nivel 2. El enmascaramiento PIR está conectado por defecto. El número de entradas de registro no excede las 8 entre períodos de armado.
Zona omitida	Esta salida se enciende si hay zonas anuladas, inhibidas o con test de intrusión en el sistema.
Comunicación	Esta salida se enciende si hay un fallo en la comunicación con la estación central.
Test hombre caído	Esta salida enciende un dispositivo vía radio de "hombre caído" que se activa durante un test de "hombre caído".
Desarmado	Esta salida se activa si el sistema está en modo Desarmado.
Abortar alarma	Esta salida se activa si se produce una incidencia de abortar alarma, es decir, cuando se introduce un código de usuario válido a través del teclado tras una alarma confirmada o sin confirmar. Se utiliza, por ejemplo, con marcadores telefónicos externos (SIA, CID, FF)
Test sísmico	Esta salida se utiliza para activar un test manual o automático en una zona sísmica. Los detectores sísmicos tienen un pequeño vibrador que se instala en la misma pared que el detector y se conecta mediante un cable a una salida en el panel o en alguno de sus módulos de expansión. Durante el test, el panel espera hasta 30 segundos a que se abra la zona sísmica. Si no se abre, el test se considera fallido. Si se abre en un plazo de 30 segundos, el panel espera a que la zona se cierre en un plazo de 10 segundos. Si no ocurre así, el test se considera fallido. A continuación, el panel espera otros 2 segundos antes de informar sobre el resultado del test. El resultado del test, tanto manual como 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 Fob o PAT.
Fallo línea TX 1	Esta salida se activa cuando hay un fallo de línea en el 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 de línea en el módem secundario.
Fallo TX 2	Esta salida se activa cuando falla el módem secundario.
Baja batería	Esta salida se activa cuando la carga de la batería está baja.
Estado entradas	Esta salida se activa cuando se implementa un procedimiento de entrada "Todo OK" y no se genera ninguna alarma, es decir, que el botón "Todo OK" se pulsa dentro del tiempo configurado después de introducirse el código de usuario.
Estado aviso	Esta salida se activa cuando se implementa un procedimiento de entrada "Todo OK" y se genera una alarma silenciosa, es decir, que el botón "Todo OK" no se pulsa dentro del tiempo configurado después de introducirse el código de usuario.
Listo para armar	Esta salida se activa cuando una partición está lista para el armado.
Config. ACK (SPC Pro — Armado completo)	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 (SPC Pro — Armado con éxito)	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.
Atraco confirmado	Se activa en los siguientes escenarios para la conformidad con PD6662: ● dos activaciones de zona de atraco separadas entre sí más de dos minutos ● una activación de zona de atraco y de zona de pánico separadas entre sí más de dos minutos ● Si en el periodo de dos minutos se produce una activación de zona de atraco y de zona de tamper o una activación de zona de pánico y de zona de tamper
Modo técnico	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).*

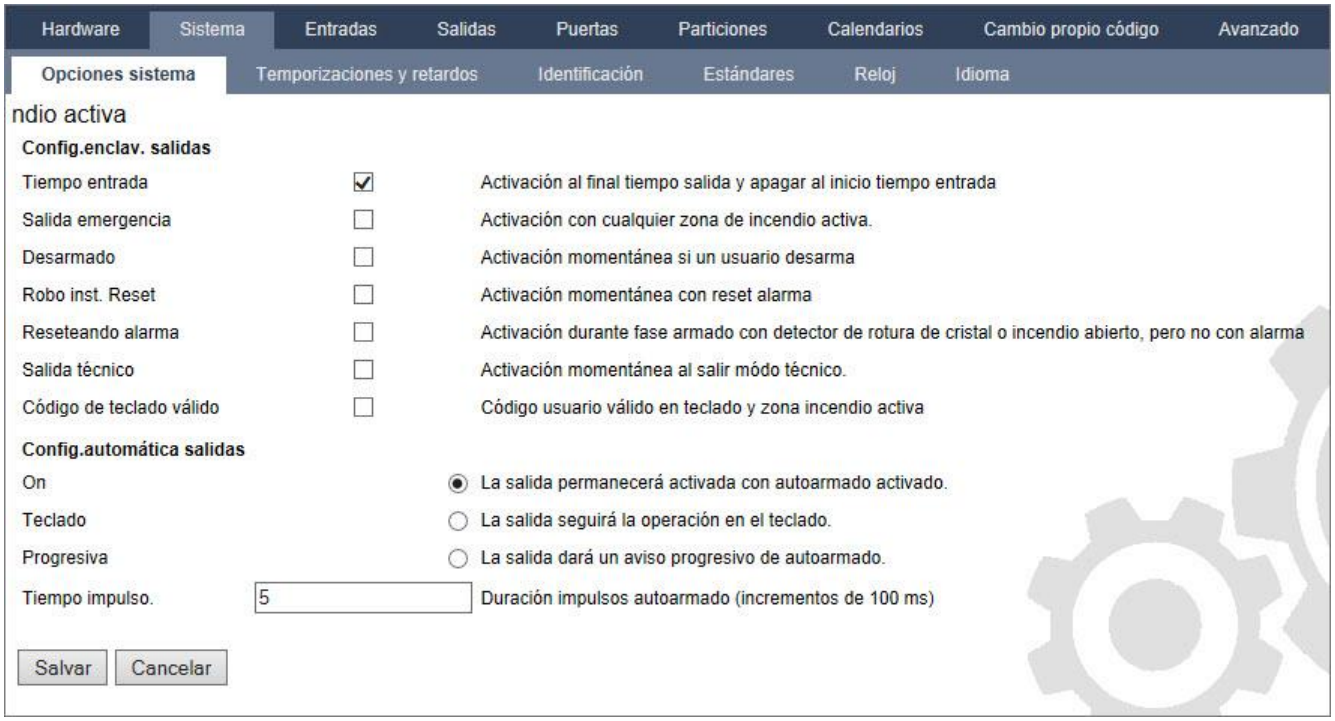
Ver también

🗎 Configuración de enclavamiento del sistema y salidas de armado automático [→ 214]

17.9.1.3 Configuración de enclavamiento del sistema y salidas de armado automático

- En **Política**, haga clic en el botón **Editar** para la opción **Configuración salidas** en **Opciones del sistema**.

⇨ Aparecerá la siguiente pantalla:



- Seleccione la condición bajo la que se activará la salida de enclavamiento:

Tiempo de entrada	La salida se enciende al final del tiempo de salida, y se apaga al inicio del tiempo de entrada.
Salida de incendio	La salida se enciende si hay alguna zona de salida de incendio activa.
Desarmado	La salida se enciende si algún usuario desarma el sistema temporalmente
Reset alarma	La salida se activa si se restablece una alarma temporalmente.
Reseteando alarma	La salida se activa durante la fase de armado si un detector de rotura de cristal o incendio está abierto pero no en alarma.
Salida técnico	La salida se activa cuando un técnico sale temporalmente del modo técnico.
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.

- Seleccione el comportamiento de la salida.

On	La salida permanecerá activada con autoarmado activado.
Teclado	La salida seguirá la operación en el teclado.
Progresiva	La salida dará un aviso progresivo de autoarmado.
Tiempo impulso.	Seleccione la duración que la salida de autoarmado permanecerá activa cuando se pulse.

17.9.1.4 Configuración de X-10: ajustes

La ventana de configuración del X-10 permite configurar el funcionamiento del X-10 en la central.

1. Seleccione **Configuración> Salidas > X-10**.
   ⇨ Se mostrará la siguiente ventana:

2. Active la casilla **Habilitar** para habilitar el funcionamiento del X-10 en la central.
3. Active la casilla **Registro** para habilitar el registro de todas las incidencias del X-10 en la central.
4. Haga clic en **Salvar**.
5. Para programar las funciones del dispositivo X-10, haga clic en una pestaña alfabética (A-P).
   ⇨ Se mostrará una lista de funciones de dispositivos programables (1-16) para ese carácter alfabético:

Número de unidad	Es el número (1-16) que se asigna al dispositivo.
Activo	Este campo indica si el dispositivo está activo o no.
Descripción	Este campo muestra una descripción que ayuda a identificar el dispositivo; p. ej. luz de piso inferior (máximo 16 caracteres).
Tecla rápida	Este campo indica si el dispositivo X-10 se puede activar o desactivar introduciendo un código desde el teclado.

Para editar un dispositivo X-10

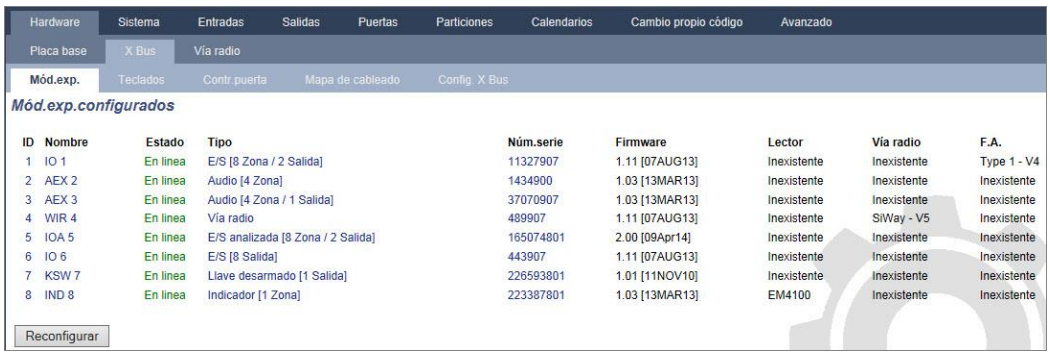
1. Haga clic en **Editar**.
   ⇨ Se mostrará la siguiente ventana:

2. Para más información sobre programación, consulte la página [→ 270].

17.9.2 X-BUS

17.9.2.1 Módulos de expansión

1. Seleccione **Configuración > Hardware > X-Bus > Mód.exp.**.
   ⇨ Se mostrará la siguiente ventana:



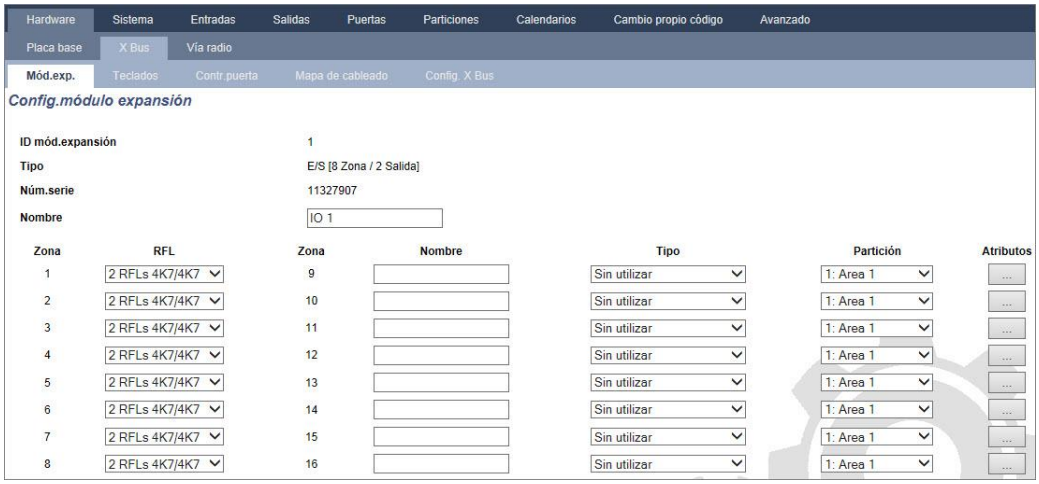
ID	Nombre	Estado	Tipo	Núm.serie	Firmware	Lector	Vía radio	F.A.
1	IO 1	En linea	E/S [8 Zona / 2 Salida]	11327907	1.11 [07AUG13]	Inexistente	Inexistente	Type 1 - V4
2	AEX 2	En linea	Audio [4 Zona]	1434900	1.03 [13MAR13]	Inexistente	Inexistente	Inexistente
3	AEX 3	En linea	Audio [4 Zona / 1 Salida]	37070907	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 darles nombre e identificarlos:

En una configuración de lazo, cada módulo de expansión se numera de forma consecutiva desde el primero (conectado a 1A 1B en el controlador SPC) al último (conectado a 2A 2B en el controlador).

Ejemplo para SPC63xx: Cuando están numerados del 1 al 63, se asignan zonas a los módulos de expansión (en grupos de 8) en identidades consecutivas de 1 a 512 (el número más alto en la identificación de zona es 512). Por tanto, cualquier módulo de expansión designado o identificado por un número superior a 63 no tiene zonas asignadas.

2. Haga clic en alguno de los parámetros de identificación del módulo de expansión para que aparezca la pantalla de **Configuración de módulo de expansión**.



- Configure los siguientes campos:

Descripción	Para mostrarse en los LED de dispositivo.
Límite de volumen	**Solo módulo de expansión de audio:** Volumen del altavoz para el módulo de expansión de audio y satélites (WAC 11). Todos están cableados en paralelo. Observe que el altavoz en WAC 11 tiene un potenciómetro para ajustar el volumen con precisión. El intervalo es 0 min. - 7 máx., o deshabilitado.
Canal auxiliar	**Solo módulo de expansión de audio:**Esta opción se debe habilitar si se conectan satélites (WAC11) a este módulo de expansión. **Nota**: Esta opción, si está habilitada, alimenta a los micrófonos satélite. Los altavoces satélite siempre están habilitados independientemente de este ajuste.
RFL	Seleccione el RFL correcto (por defecto: 2 RFL 4K7). Esta configuración debe coincidir con el cableado real de la entrada del controlador o módulo de expansión. Consulte la página [→ 73].
Descripción (de zona)	Proporciona una descripción de la zona asignada.
Tipo (de zona)	Seleccione el tipo de zona. Consulte la página [→ 372].
Partición	Seleccione la partición.
Atributos	Asigne atributos según desee. Consulte la página [→ 368].
Salidas / Salidas de fuente de alimentación (visibles SOLO para fuente de alimentación inteligente SPCP355)	
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 conectarse la resistencia en paralelo, el diodo y la carga requerida. El SPCP355 debe realizar una calibración antes de que se inicie la supervisión. Véase Salidas supervisadas [→ 58] para más información.
Sólo batería principal	Marque esta casilla si no hay ninguna batería secundaria conectada a la fuente de alimentación.

Cuando se añaden o se borran módulos de expansión:

- Haga clic en **Reconfigurar** para implementar los cambios.

Ver también

- Cableado del sistema [→ 73]
- Atributos de zona [→ 372]
- Tipos de zona [→ 368]

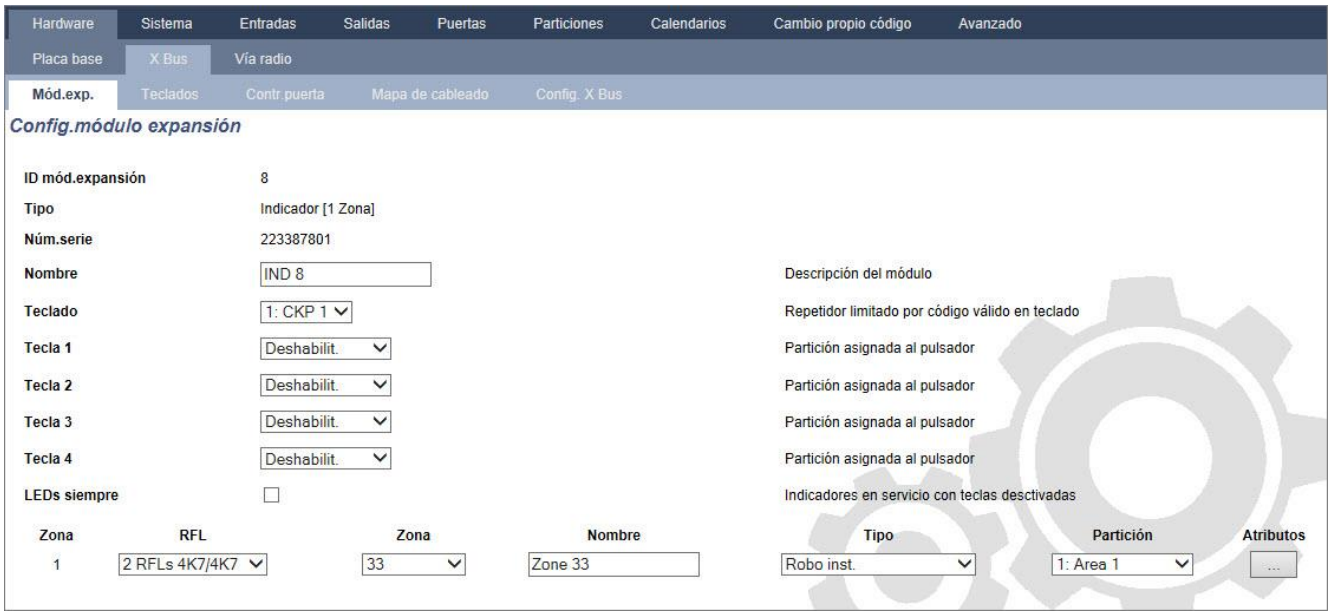
17.9.2.1.1 Configuración de un módulo de expansión de indicador

Hay dos modos de configuración posibles para el módulo de expansión de indicación:

- Modo ligado
- Modo flexible

1. Seleccione **Configuración > Hardware > X-Bus > Mód.exp.**.
2. Haga clic en uno de los parámetros de identificación del indicador.

⇨ La siguiente pantalla se muestra para la configuración de **Modo ligado**.



Modo ligado

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 deberán controlar mediante las cuatro teclas de función.
4. Configure la entrada.

Modo flexible

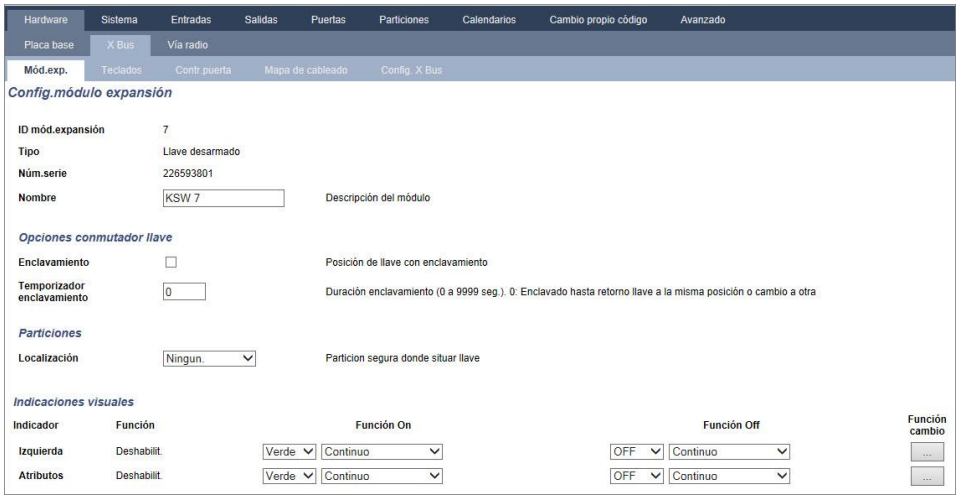
1. Haga clic en el botón **Modo flexible**.
2. Configure los campos tal como se describe en las siguientes tablas.
3. Configure la entrada.

	⚠ ADVERTENCIA Su sistema no cumplirá las normas EN si usted activa una tecla de función para armar el sistema sin que se solicite un PIN válido.

Teclas de función	
Partición	Seleccione la partición que se deberá controlar mediante la tecla de función.
Función	Seleccione la función que deberá realizar esta tecla en esta partición.
Partición	Seleccione una partición si el módulo indicador está situado en una partición segura.
Indicación visual	
Repetidor	Hay 8 indicadores / LED en el lado derecho y otros 8 indicadores / LED en el izquierdo.
Función	La función que está indicada por este LED.
Función On	Seleccione el color y el estado para cada indicador si la función seleccionada está activada.
Función Off	Seleccione el color y el estado para cada indicador si la función seleccionada está desactivada.
Función cambio	Pulse este botón para cambiar la función de este indicador. La función se puede habilitar o utilizar para un sistema, partición, zona o conmutador de llave.
Indicaciones audibles	
Alarmas	Seleccione si las alarmas deben ser audibles.
Robo E/S	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 del indicador debe estar limitado por un calendario.
Actuaciones	Seleccione si el módulo indicador debe estar limitado por una salida de sistema.
Conmutador llave	Seleccione si el módulo indicador debe estar limitado por un conmutador de llave.
Teclado	Seleccione si el módulo indicador debe estar limitado a un PIN válido introducido en un teclado (véase advertencia más arriba).
Lector de tarjetas	Seleccione si el módulo indicador no se debe activar hasta que se presente una tarjeta o un mando válido en el lector de tarjetas integrado.

17.9.2.1.2 Configuración de un módulo de expansión de conmutador de llave

1. Seleccione **Configuración > X-Bus > Módulos expansión**.
2. Haga clic en uno de los parámetros de identificación del conmutador de llave.
   ⇨ Aparecerá el siguiente cuadro de diálogo.



- Configure los campos tal como se describe en las siguientes tablas.

Descripción	Introduzca una descripción para el módulo de expansión de conmutador de llave.
Opciones de llave	
Enclavamiento	Seleccione si la posición de la llave se debe enclavar.
Tiempo enclavamiento	Introduzca la duración del enclavamiento en segundos (0 - 9999, 0 significa que el enclavamiento dura hasta que se gire la llave en sentido contrario).
Particiones	
Localización	Seleccione la partición en la que se encuentra el conmutador de llave.
Indicaciones visuales	
Indicador/LED	Hay 1 indicador/LED en el lado derecho y 1 indicador/LED en el izquierdo.
Función	La función para este indicador / LED.
Función On	Seleccione el color y el estado para cada indicador si la función seleccionada está activada.
Función Off	Seleccione el color y el estado para cada indicador si la función seleccionada está desactivada.
Función cambio	Pulse este botón para cambiar la función de este indicador. La función se puede habilitar o utilizar para un sistema, partición, zona o conmutador de llave.
Desactivación	
Calendario	Seleccione si el módulo de conmutador de llave debe estar limitado por un calendario.
Actuaciones	Seleccione si el módulo de conmutador de llave debe estar limitado por una salida de sistema.
Salida	
Salida *x*	Configure y compruebe las salidas para el conmutador de llave. Consulte Salidas [→ 210] para más información.
Funciones de la llave	
Posiciones Central, Derecha e Izquierda	Seleccione la **Función** que realizará el conmutador de llave en esta posición, y la **Partición** afectada.

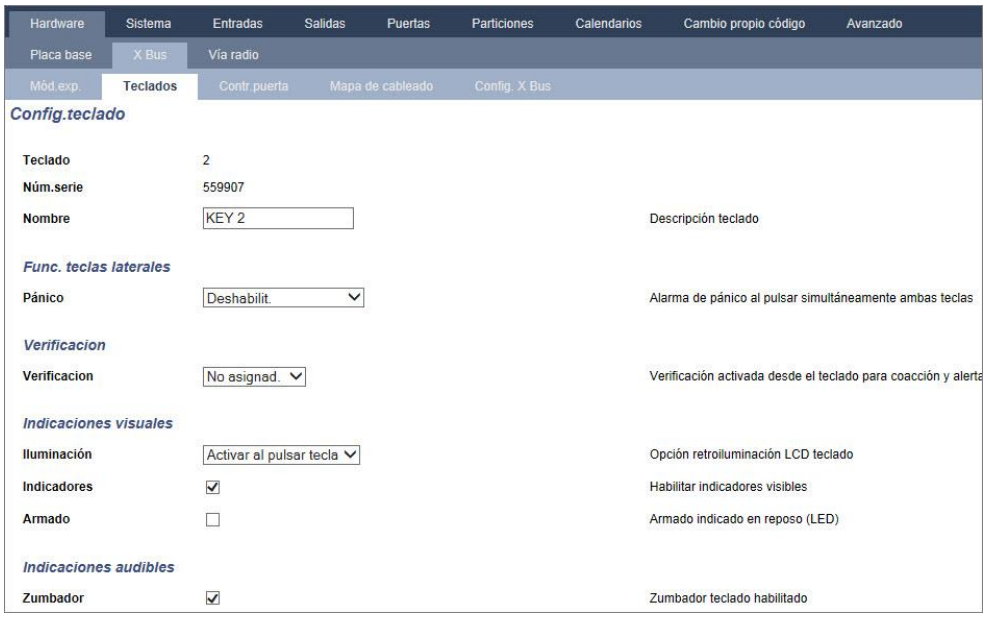
⚠ ADVERTENCIA

Su sistema no cumplirá las normas EN si usted activa una función de conmutador de llave para armar el sistema sin que se solicite un PIN válido.

17.9.2.2 Teclados

17.9.2.2.1 Edición de un teclado estándar

1. Seleccione **Configuración > Hardware > X-Bus > Teclados**.
2. Haga clic en los parámetros de identificación del teclado estándar.
3. Configure los campos tal como se describe en la siguiente tabla.



Descripción	Introduzca una descripción única para identificar el teclado.
Func. teclas laterales	
Pánico	Seleccione Habilitar, Deshabilitar o Habilit.silencio Cuando está habilitada, la alarma de pánico se activa pulsando las dos teclas programables al mismo tiempo.
Verificación	Si asigna una zona de verificación al teclado, cuando se dispare una alarma de pánico al pulsar 2 teclas programables simultáneamente o al introducir un código de coacción, se activarán las incidencias de audio y vídeo.
Indicaciones visuales	
Iluminación	Seleccione cuándo estará encendida la iluminación. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Indicadores	Habilite o deshabilite los LED en el teclado.
Estado de configuración	Seleccione si el estado de configuración se debe indicar en modo inactivo.
Indicaciones audibles	
Zumbador	Habilite o deshabilite el zumbador en el teclado.
Zumb.arm.parcial	Habilite o deshabilite el zumbador durante el tiempo de salida en armado parcial.
Pulsac.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 un calendario. Consulte Calendario [→ 267].
Actuaciones	Seleccione si el teclado debe estar limitado por una salida de sistema.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador de llave.

Entrada CCAA	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay una tarjeta configurada en el teclado.
Particiones	
Localización	Seleccione la partición segura donde se encuentra localizado el teclado.
Particiones	Particiones controladas por el teclado
Opciones	
Retardo arm.total	Seleccione esta opción para configurar un armado retardado en todos los teclados. La ubicación del teclado se ignora, y todas las particiones realizarán una cuenta atrás de tiempo de salida completo.

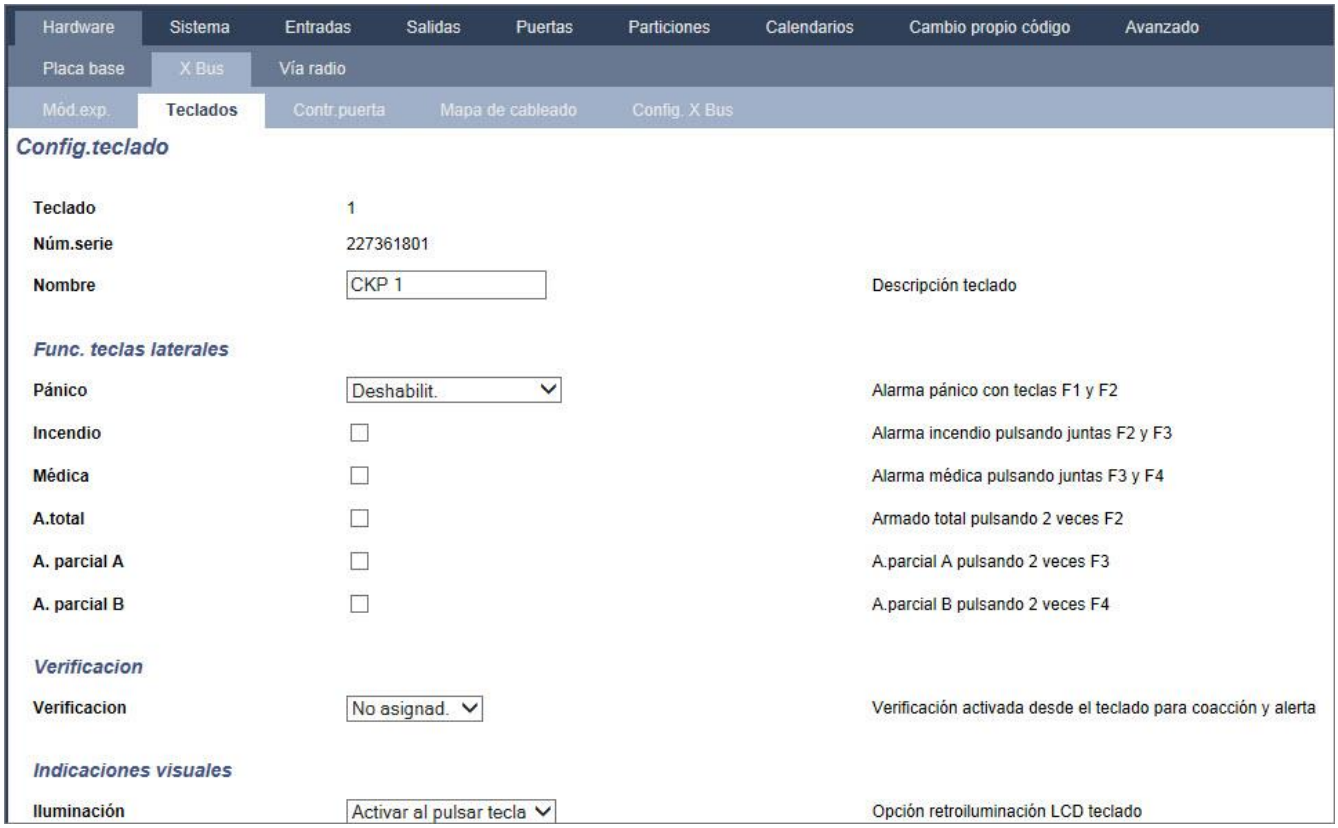
	AVISO
	Solo se debe asignar una partición a un teclado si el teclado se encuentra dentro de la partición asignada, y si se ha definido una ruta de entrada/salida. Si se asigna una partición, cuando se arma o se desarma esa partición en particular, se utilizan los temporizadores de entrada y salida (siempre y cuando estén configurados). También quedan disponibles otras funciones relacionadas con rutas de entrada/salida. Si no hay ninguna partición asignada, la partición se arma o se desarma inmediatamente y otras funciones de entrada/salida dejan de estar disponibles.

Ver también

Calendarios [→ 267]

17.9.2.2.2 Edición de un teclado confort

1. Seleccione **Configuración > Hardware > X-Bus > Teclados**.
2. Haga clic en uno de los parámetros de identificación del teclado confort.
3. Configure los campos tal como se describe en la siguiente tabla.



Descripción	Introduzca una descripción única para identificar el teclado.
Func. teclas laterales	
Pánico	Seleccione Habilitar, Deshabilitar o Habilit.silencio Cuando está habilitada, la alarma de pánico se activa pulsando las teclas programables F1 y F2 al mismo tiempo.
Incendio	Habilite esta opción para permitir que se active la alarma de incendio pulsando las teclas programables F2 y F3 al mismo tiempo.
Alarma médica	Habilite esta opción para permitir que se active la alarma médica pulsando las teclas programables F3 y F4 al mismo tiempo.
Armado total	Habilite esta opción para permitir que se active el armado total pulsando dos veces la tecla F2.
Armado parcial A	Habilite esta opción para permitir que se active el armado parcial A pulsando dos veces la tecla F3.
Armado parcial B	Habilite esta opción para permitir que se active el armado parcial B pulsando dos veces la tecla F4.
Verificación	Si asigna una zona de verificación al teclado de confort, cuando se dispare una Alarma médica, una incidencia de Pánico o de Incendio, o si un usuario introduce un código de coacción, entonces se activarán las incidencias de audio y vídeo.
Indicaciones visuales	
Iluminación	Seleccione cuándo estará encendida la iluminación. Las opciones son: Encendida al presionar una tecla, Siempre encendida y Siempre apagada.
Nivel retroilum.	Seleccione la intensidad de la retroiluminación. Intervalo del 1 al 8 (alta).

Indicadores	Habilite o deshabilite los LED en el teclado.
Estado de configuración	Habilite esta opción si, estando en reposo, se desea indicar el estado de configuración. (LED)
Logo	Habilite esta opción si, estando en reposo, se desea que se vea el logotipo.
Reloj analógico	Seleccione la posición del reloj en caso de verse estando en reposo. Las opciones son: Situado a la izquierda, Alineado centro, Situado a la derecha o Deshabilitado.
Emergencia	Habilite esta opción si desea que las teclas de función Pánico, Incendio y Médico se indiquen en la pantalla LCD.
Armado directo	Habilite esta opción si desea que las teclas de función Armado total y Armado parcial se indiquen en la pantalla LCD.
Indicaciones audibles	
Alarmas	Seleccione el volumen del altavoz para indicaciones de alarma o desactive el sonido.
Entrada/salida	El intervalo es de 0 a 7 (volumen máximo)
Chime	Seleccione el volumen del altavoz para indicaciones de entrada y salida, o desactive el sonido.
Pulsac.tecla	El intervalo es de 0 a 7 (volumen máximo)
Mensajes hablados	Seleccione el volumen del altavoz para la función Chime o desactive el sonido.
Zumb.arm.parcial	El intervalo es de 0 a 7 (volumen máximo)
Desactivación	
Calendario	Seleccione si el teclado debe estar limitado por un calendario. Consulte Calendario.
Actuaciones	Seleccione si el teclado debe estar limitado por una salida de sistema.
Conmutador llave	Seleccione si el teclado debe estar limitado por un conmutador de llave.
Entrada CCAA	Marque esta casilla para deshabilitar las teclas del teclado durante el tiempo de entrada cuando hay una tarjeta configurada en el teclado.
Particiones	
Localización	Seleccione la partición segura donde se encuentra localizado el teclado.
Particiones	Particiones controladas por el teclado
Opciones	
Retardo arm.total	Seleccione esta opción para configurar un armado retardado en todos los teclados. La ubicación del teclado se ignora, y todas las particiones realizarán una cuenta atrás de tiempo de salida completo.

	AVISO
	Solo se debe asignar una partición a un teclado si el teclado se encuentra dentro de la partición asignada, y si se ha definido una ruta de entrada/salida. Si se asigna una partición, cuando se arma o se desarma esa partición en particular, se utilizan los temporizadores de entrada y salida (siempre y cuando estén configurados). También quedan disponibles otras funciones relacionadas con rutas de entrada/salida. Si no hay ninguna partición asignada, la partición se arma o se desarma inmediatamente y otras funciones de entrada/salida dejan de estar disponibles.

17.9.2.3 Controladores de puerta

17.9.2.3.1 Edición de un controlador de puerta

1. Seleccione **Configuración > Hardware > X-Bus > Contr.puerta**.
2. Haga clic en uno de los datos marcados en azul (p. ej. número de serie).
3. Configure los campos tal como se describe en la siguiente tabla.

Para darles nombre e identificarlos:

En una configuración de lazo, cada módulo de expansión se numera de forma consecutiva desde el primero (conectado a 1A 1B en el controlador SPC) al último (conectado a 2A 2B en el controlador).

Ejemplo para SPC63xx: Cuando están numerados del 1 al 63, se asignan zonas a los módulos de expansión (en grupos de 8) en identidades consecutivas de 1 a 512 (el número más alto en la identificación de zona es 512). Por tanto, cualquier módulo de expansión designado o identificado por un número superior a 63 no tiene zonas asignadas.

ID mód. expansión	ID del controlador de puerta configurado con los conmutadores rotativos.
Tipo	Tipo de controlador de puerta.

Nº serie	Número de serie del controlador de puerta.
Descripción	Descripción del controlador de puerta.
E/S puerta 1 E/S puerta 2	● Si hay una puerta 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, la configuración de la puerta se puede modificar haciendo clic en el botón Editar. Es lo mismo que **Configuración > Puertas**. ● Si se selecciona **Zonas / Opciones**, las dos zonas y la única salida se pueden configurar haciendo clic en el botón Editar.
Perfil 1	Para lectores con un LED verde y otro rojo.
Perfil 2	Para lectores de VANDERBILT con un LED amarillo (AR618X).
Perfil 3	El perfil 3 se utiliza con lectores de HID que envían un código al panel como lectura de tarjeta con un código local predefinido (0)
Perfil 4	El perfil 4 se utiliza con lectores de HID que envían un código al panel como lectura de tarjeta con un código local 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.

Edición de zonas/salidas para una E/S de puerta

1. Seleccione una zona/salida para la E/S de puerta.
2. Haga clic en el botón **Editar**.
3. Las dos entradas y la salida pertenecientes a esta E/S de puerta se pueden configurar como entradas y salidas de puerta normales. Consulte la página [→ 261].
4. Para utilizar las entradas, estas deben estar asignadas a un número de zona.

17.9.2.4 Mapa de cableado

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 > Dispositivos X-Bus**.
  - ⇨ Se mostrará la siguiente ventana:

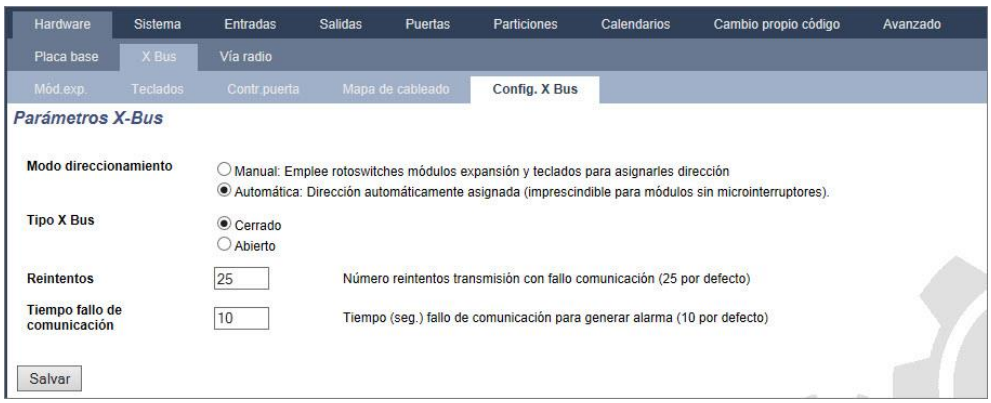
Posición	ID	Estado	Tipo	Núm.serie	Nombre
1	1	Activo	E/S [8 Zona / 2 Salida]	11327907	IO 1
2	2	Activo	Audio [4 Zona]	1434900	AEX 2
3	3	Activo	Audio [4 Zona / 1 Salida]	37070907	AEX 3
4	4	Activo	Vía radio	489907	WIR 4
5	5	Activo	E/S analizada [8 Zona / 2 Salida]	165074801	IOA 5
6	1	Activo	DC-2 [4 Zona / 2 Salida]	195309801	DC2 1
7	6	Activo	E/S [8 Salida]	443907	IO 6
8	7	Activo	Llave desarmado [1 Salida]	226593801	KSW 7
9	8	Activo	Indicador [1 Zona]	223387801	IND 8
10	1	Activo	Teclado Confort	227361801	CKP 1
11	2	Activo	Teclado	559907	KEY 2

Para obtener más detalles sobre el interconexionado de X-BUS, consulte la página [→ 73].

17.9.2.5 Configuración

Para configurar las conexiones de X-BUS:

1. Seleccione **Configuración > Hardware > X-Bus > Config. X Bus**.
   ⇨ Se mostrará la siguiente ventana.
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 X-BUS	Seleccione configuración en lazo o en punta.
Reintentos	El número de veces que el sistema intenta retransmitir datos por la interfaz X-BUS antes de generar un fallo de comunicación. (1 – 99: por defecto, 25)
Tiempo fallo de comunicación	El periodo de tiempo hasta que se registra un fallo de comunicación.

17.9.3 Vía radio

La detección mediante detectores vía radio (868 MHz) en la central SPC se realiza mediante módulos receptores vía radio que pueden venir montados de fábrica en el teclado, o instalando un módulo de expansión vía radio.

1. Seleccionar **Configuración > Hardware > Vía radio > Vía radio**.
2. Consulte la tabla a continuación para obtener más información.

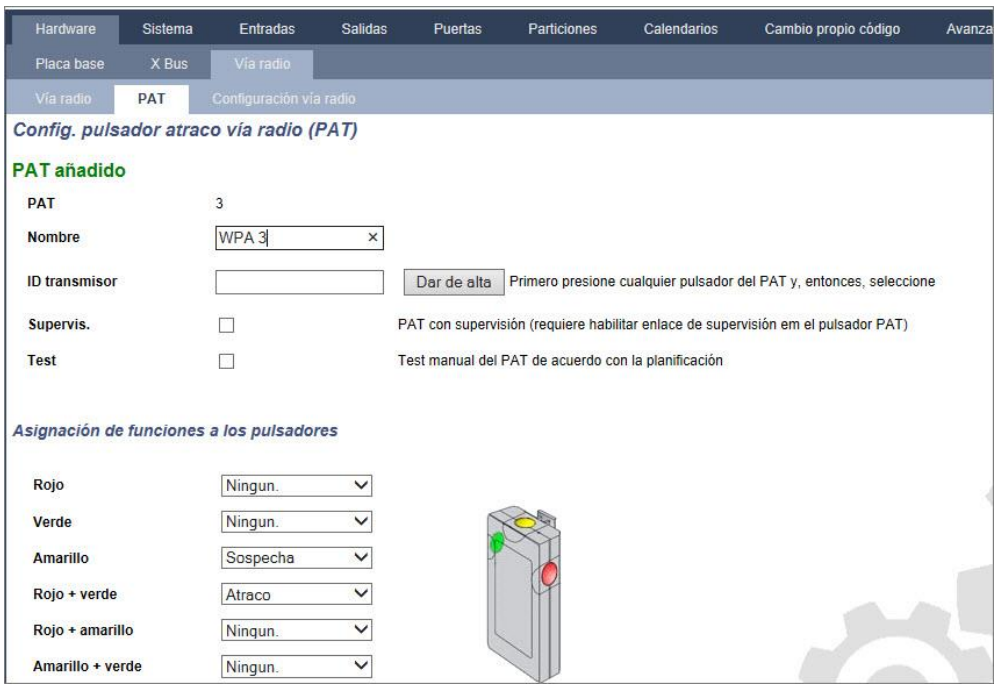
ID detector	Tipo	Recibido	Estado	Receptor	Señal	Dar de alta
58906531	PIR	23/07/2014 15:29:12	Reposo	Vía radio 4	Alto (9)	Dar de alta
26424410	Cont. magn.	23/07/2014 15:28:27	Reposo	Placa base	Alto (9)	Dar de alta
58732159	PIR	23/07/2014 15:28:12	Reposo	Vía radio 4	Alto (8)	Dar de alta
60306033	PIR	23/07/2014 15:28:11	Reposo	Vía radio 4	Alto (9)	Dar de alta
58808327	PIR	23/07/2014 15:27:51	Reposo	Placa base	Alto (9)	Dar de alta
26422359	Cont. magn.	23/07/2014 15:27:33	Reposo	Placa base	Alto (9)	Dar de alta
26661509	Cont. magn.	23/07/2014 15:26:22	Reposo	Vía radio 4	Alto (9)	Dar de alta
26424404	Cont. magn.	23/07/2014 15:26:19	Reposo	Vía radio 4	Alto (9)	Dar de alta
26647859	Cont. magn.	23/07/2014 15:26:07	Reposo	Placa base	Alto (9)	Dar de alta
26663381	Cont. magn.	23/07/2014 15:25:57	Reposo	Placa base	Alto (9)	Dar de alta
58740535	PIR	23/07/2014 15:25:28	Reposo	Vía radio 4	Alto (9)	Dar de alta

Detector	El número del sensor dado de alta en el sistema (1 = primero, 2 = segundo, etc.)
ID	Un número de identificación exclusivo para ese detector.
Tipo	El tipo de detector vía radio detectado (contacto magnético, inercial/de impacto, etc.)
Zona	La zona en la que se ha dado de alta el detector.
Batería	El estado de la batería del detector (si está montada).
Supervisar	El estado de la operación de supervisión (OK = señal de supervisión recibida, No supervisado = 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 pierden la conexión.

Se pueden realizar las siguientes acciones

Registro	Haga clic para ver el registro del detector vía radio. Consulte la página [→ 230].
Dar de alta	Haga clic para abrir la lista de dispositivos vía radio sin estar dados de alta.

1. Seleccione **Estado > Hardware > Vía radio > PAT**.
2. Se muestra la identidad de cada PAT dado de alta así como su estado.



17.9.3.1 Registro: detector vía radio X

Para ver un registro rápido de las incidencias de un detector vía radio:

1. Haga clic en el botón **Registro**.
2. Consulte la tabla a continuación para obtener más información.
3. Cree un fichero de texto del registro haciendo clic en **Fichero de texto**.

Fecha/hora	La fecha y la hora de la incidencia registrada.
Receptor	La ubicación del receptor vía radio, es decir, 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 detector (OK, Fallo).

17.9.3.2 Configuración de un PAT

	AVISO
	La página de configuración y estado de un PAT solo se muestra si hay un módulo vía radio montado en el panel o en alguno de sus módulos de expansión, y si el panel cuenta con licencia para el tipo de módulo(s) instalado(s).

Un PAT no se asigna a un usuario. Normalmente, un PAT es compartido por varias personas, como por ejemplo guardas de seguridad que trabajan por turnos; como alternativa, los PAT pueden estar situados de forma permanente en una

superficie, como por ejemplo debajo de un escritorio o detrás de una caja registradora.

Se permite un máximo de 128 PAT por panel.

Para configurar un PAT desde el navegador:

- Seleccione el modo Técnico total y, a continuación ,seleccione las siguientes opciones **Configuración > Hardware > Vía radio > PAT**.

Desde esta página se pueden comprobar o configurar los siguientes elementos:

- **Estado batería**

  El panel recibe el estado de la batería desde el PAT en cada imagen. El estado de la batería puede ser OK o Bajo.

  Para supervisar la batería se necesita un PAT equipado con la revisión de PCI E-PC138612 o posterior.

- **Estado de supervisión**

  El estado de supervisión puede ser cualquiera de los siguientes:

  – Fallo
  El panel no ha recibido un mensaje de supervisión del PAT en el período configurado en la página de Configuración vía radio.

  – Inhibido
  La supervisión no está configurada.

  – OK
  La supervisión se está transmitiendo normalmente.

- **Estado del test**

  El estado del test puede ser cualquiera de los siguientes:

  – Vencido
  El PAT no ha sido comprobado en el período configurado en la página de Configuración vía radio.

  – Inhibido
  La supervisión no está configurada.

  – OK
  El test PAT es correcto.

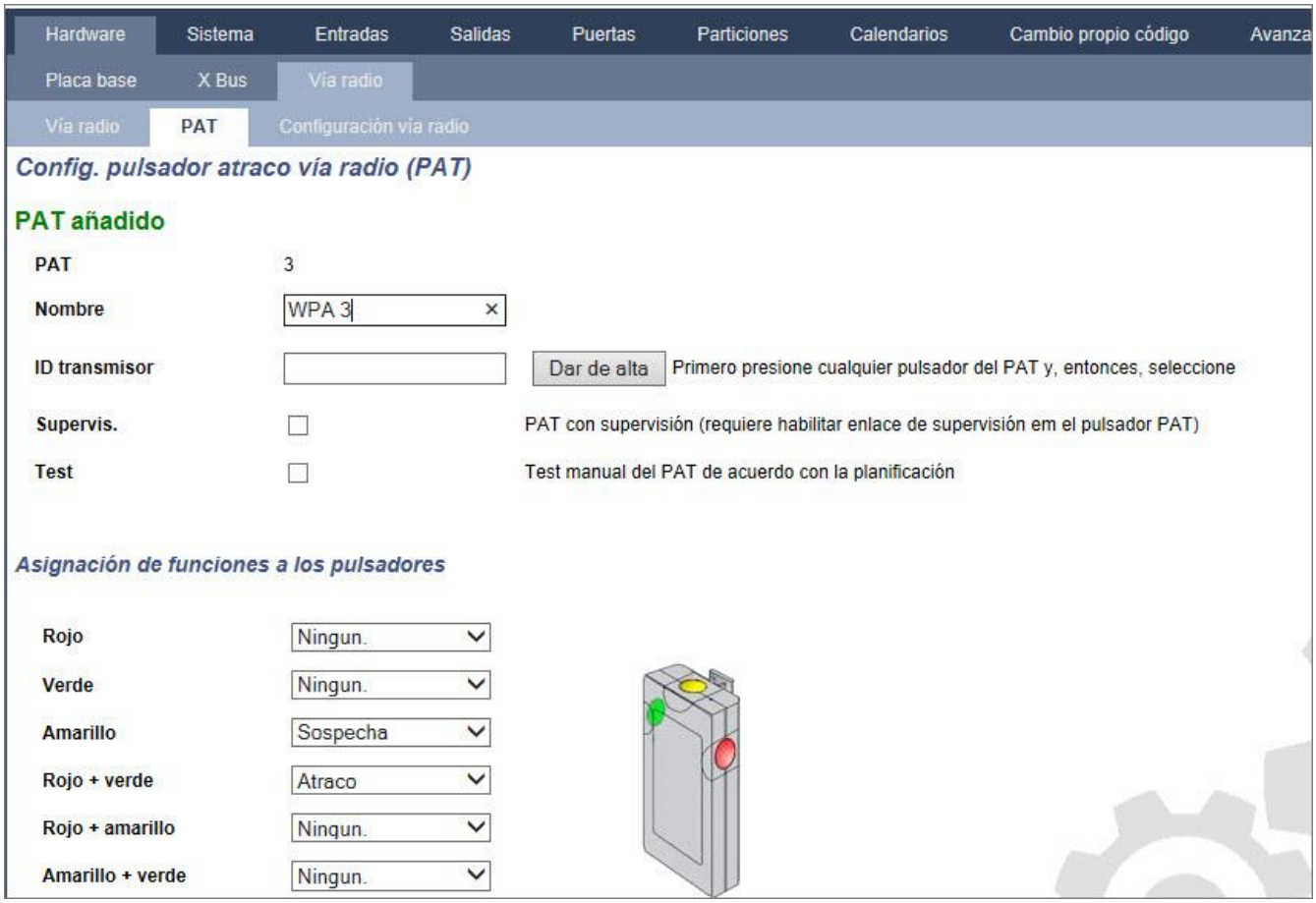
1. Haga clic en el botón **Editar** para editar la configuración del PAT.
2. Haga clic en el botón **Borrar** para eliminar un PAT del sistema.

17.9.3.2.1 Añadir un PAT

Para añadir un PAT al sistema:

- Haga clic en el botón **Añadir** en la página principal de configuración y estado de PAT.

⇨ Aparece la página de configuración de PAT para el nuevo PAT.



- Configure el PAT con los siguientes detalles:

Descripción/Nombre	Introduzca una descripción o un nombre para identificar el PAT de manera inequívoca.
ID transmisor	El ID de transmisor está impreso en la carcasa del PAT y se puede introducir manualmente aquí. También puede identificar el ID de forma remota pulsando cualquier botón del PAT y haciendo clic a continuación sobre el botón **Dar de alta**. El panel introduce automáticamente su ID en este campo, siempre que no haya ningún otro PAT definido actualmente con él.
Supervisar	El dispositivo WPA puede configurarse para que envíe señales de supervisión periódicas. La supervisión se habilita en el PAT mediante un puente. La función de supervisión también se debe habilitar en el panel para ese PAT en concreto para que la supervisión funcione correctamente. Si el panel no recibe una señal de supervisión, se activa una alarma que se indica en el teclado y queda registrada. Si no se activa esta función, cada 24 horas aproximadamente el dispositivo WPA envía un mensaje de supervisión para comunicar al panel el nivel de carga de la pila. Este mensaje también es aleatorio para disminuir las posibilidades de que los envíos coincidan con los de otros PAT. Marque la casilla **Supervisar** si se ha habilitado la supervisión para ese PAT en particular.
Test	Marque la casilla **Test** si se requiere un test de PAT periódico. El intervalo de tiempo para el test periódico está configurado en la página Cambio de configuración vía radio [→ 233].
Asignación de botón	Utilice esta sección para asignar funciones a combinaciones de botones. Las funciones disponibles son Pánico, Pánico silencioso, Atraco, Sospecha, Salida y Alarma médica. Se puede seleccionar más de una combinación

	para una misma función. La pantalla anterior muestra la configuración por defecto para el panel en una instalación financiera: ● 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 una fuente. Consulte Fuentes [→ 270]

- Haga clic en el botón **Salvar** para guardar la configuración.

Ver también

- Cambio de configuración vía radio [→ 233]
- Cambio de configuración vía radio [→ 233]
- Fuentes [→ 270]

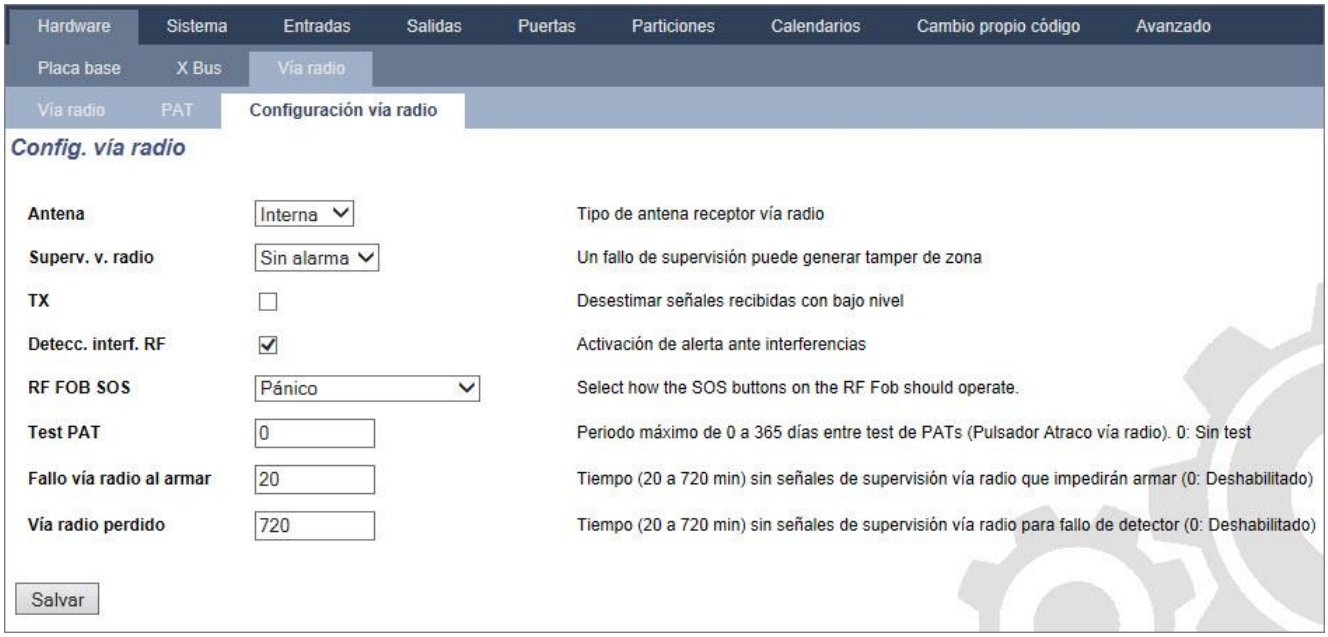
17.9.3.2.2 Edición de un PAT

Para editar un PAT, haga clic en el botón **Editar** en la página principal de configuración y estado de PAT.

La página de **Editar** es muy similar a la de **Añadir**, solo que no tiene el botón "Dar de alta" para introducir automáticamente el ID del PAT.

17.9.3.3 Cambio de configuración vía radio

1. Seleccionar **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) desde el menú desplegable. El tipo de antena que se necesita para

	el módulo vía radio depende del tipo de módulo vía radio montado.
Superv.v.radio	Seleccione si un detector vía radio del que se ha informado como perdido registra una condición de tamper en la central de sello. Se informa de que un detector vía radio está perdido cuando no se ha recibido ninguna señal de supervisión de ese receptor durante un período superior al programado en el temporizador **Vía radio perdido**. Consulte la página [→ 244].
Filtro	Marque esta casilla para filtrar las señales de RF de baja intensidad.
Detectar interf. RF	Marque esta casilla para activar una incidencia si se detecta una interferencia RF.
Test PAT	Seleccione cómo deben funcionar los botones SOS en el mando vía radio: ● Inhibir ● Habilitar ● Habilitado (silencioso) ● Alarma medica usuario ● Atraco usuario ● Salida RF
Config.test del PAT	Introduzca un período máximo (en días) entre tests de PAT.
Fallo vía radio al armar	Introduzca un tiempo en minutos tras el cual, si no hay señales del sensor, se evita un armado para la partición en la que se encuentra la zona vía radio. Esta configuración solamente se aplica para las siguientes zonas de intrusión. ● Robo inst. ● Entrada/salida ● Robo fin salida ● Pánico ● Atraco ● Tamper ● Superv.llave ● Sísmico ● Todo OK ● Autorización de armado ● Elemento bloqueo
Vía radio perdido	Introduzca el número de minutos tras el cual se considerará perdido un dispositivo vía radio (detector o PAT).

17.9.4 Cambio de configuración del sistema

17.9.4.1 Opciones

1. Seleccione **Configuración > Sistema > Opciones sistema**.
2. Configure los campos tal como se describe en la siguiente tabla.

Opciones del sistema

Las opciones que se muestran varían en función del 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. Tras restaurar la alarma, se solicita un código de 6 dígitos. El usuario debe llamar al instalador para que genere un código de restauración con el que podrá restaurar la alarma.
	Tamper sin comunicación	Habilite esta opción para que las zonas de módulos de expansión fuera de línea generen un tamper de zona.
	Reset alarma mando	Si esta opción está habilitada, se habilitará la tecla mando vía radio para restaurar las alertas pulsando el botón Desarmado.
Solo web y SPC Pro	LED módulo audio	Con esta opción habilitada, el módulo de expansión de audio no encenderá el 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.
	Redisparo intimidación	Con esta opción habilitada, la alarma de intimidación se redisparará.
	Redisparo pánico	Con esta opción habilitada, la alarma de pánico se reactivará.
	Anulación LEDs lector	Con esta opción habilitada, el comportamiento de los LED de los lectores será controlado por la central.
	Silencio con verificación audio	Con esta opción habilitada, las sirenas interiores y exteriores (de sistema y de partición), los zumbadores del teclado y los mensajes de anuncio del teclado confort se silenciarán 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.

Restricciones	Opciones del sistema	Descripción
		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 transmitida 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, véase CRAs [→ 309].
	SPCP355	Se habilita la alimentación de VdS. En las instalaciones VdS, esta opción se selecciona automáticamente.
	Sirena con fallo al armar (FTS)	Habilite esta opción para activar la sirena interior si el sistema falla en el armado.
	Flash con fallo al armar (FTS)	Habilite esta opción para activar el flash si el sistema falla en el armado.
⏻	Ocultar puenteo	Si está habilitado, los mensajes de puenteo no se mostrarán más en el teclado.
	Capacidad de la batería	Capacidad total de las baterías en AH, solo para central (3 - 100 Ah). Deberá introducir este valor y el valor de **Máxima corriente** para poder ver el tiempo de batería remanente en el teclado en caso de producirse un fallo de la red de alimentación. Esto se indica en el menú ESTADO - BATERÍA - DURACIÓN BATERÍA
	Máxima corriente	Corriente total extraída de las baterías cuando se produce un fallo de la red de alimentación (30 - 20000 mA). Deberá introducir este valor y el valor de **Capacidad de la batería** para poder ver el tiempo de batería remanente en el teclado en caso de producirse un fallo de la red de alimentación. Esto se indica en el menú ESTADO - BATERÍA - DURACIÓN BATERÍA.
Armado parcial		
	Renombrar armado parcial A	Introduzca un nuevo nombre para el modo ARMADO PARCIAL A (p. ej. Modo noche).
	Renombrar armado parcial B	Introduzca un nuevo nombre para el modo ARMADO PARCIAL B (p. ej. Sólo planta 1).
Alarma		
	Sirena primero	Habilitada para activar las sirenas relevantes en una alarma sin confirmar. Cuando esta opción está deshabilitada, las sirenas relevantes sólo se activan si la alarma está confirmada o si el detector que provocó la alarma no confirmada se vuelve a activar.
	Redisparo sirena	Habilite esta opción para que vuelvan a sonar las sirenas si se detecta una segunda activación de zona (una vez

Restricciones	Opciones del sistema	Descripción
		transcurrido el tiempo de la sirena). Si no está marcada, las sirenas exteriores sólo se activarán una vez.
Solo web	Armado prohibido con alertas	Con esta opción habilitada, un usuario no puede armar una partición con alertas en otras particiones o 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 "Modo libre".
	Reset tras desarmado	Habilite esta opción para que las alertas se borren automáticamente después de 30 segundos en modo Desarmado. **Nota:** Para cumplir la norma PD6662 se debe deshabilitar esta opción.
	Antienmascaramiento con armado	Seleccione el tipo de incidencia notificada resultante de la detección antienmascaramiento cuando la central está armada. Las opciones son Deshabilitar, Tamper, Problema o Alarma. Esta opción solo se puede configurar cuando la central está en modo "Libre". En modo Grado 2 ó 3, el tipo de incidencia notificada cumple las normas de la región seleccionada. ● Irlanda - Alarma ● Todas las demás regiones - Alarma
	Antienmascaramiento con desarmado	Seleccione el tipo de incidencia notificada resultante de la detección de antienmascaramiento cuando la central está desarmada. Las opciones son Deshabilitar, Tamper, Problema o Alarma. Esta opción solo se puede configurar cuando la central está en modo "Libre". En modo Grado 2 ó 3, el tipo de incidencia notificada cumple las normas de la región seleccionada. ● Irlanda - Deshabilitada ● Todas las demás 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. Esta opción solo se puede configurar cuando la central está en modo "Libre". En modo Grado 2 ó 3, el tipo de incidencia notificada cumple las normas 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. Esta opción solo se puede configurar cuando la central está en modo "Libre". En modo Grado 2 ó 3, el tipo de incidencia notificada cumple las normas 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.

Restricciones	Opciones del sistema	Descripción
		Una zona es inestable si no se puede obtener una muestra simple en un plazo de 10 segundos. Esta opción solo se puede configurar cuando la central está en modo "Libre". En modo Grado 2 ó 3, el tipo de incidencia notificada cumple las normas de la región seleccionada. ● Alemania VdS - Tamper ● Resto de regiones - Problema
⏻	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. Esta opción solo se puede configurar cuando la central está en modo "Libre". En modo Grado 2 ó 3, el tipo de incidencia notificada cumple las normas de la región seleccionada. ● Alemania VdS - Tamper ● Resto de regiones - Problema
⏻	Tolerancia RFL	Si esta opción está habilitada, se utilizan bandas anchas de RFL.
	Sospecha audible	Con esta opción habilitada, alarma de sospecha generada por PAT con indicación audible y visual en teclados. (Solo en modo Financiero).
Pro	RFLs (Resist.fin línea)	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.
	Test manual sísmico	Con esta opción habilitada, todos los detectores sísmicos de cualquier partición que se arme serán comprobados antes de que se arme la partición o el sistema. (Solo en modo Financiero).
⏻	Auto reset	Habilite esta función para restaurar automáticamente las alertas del sistema, esto es, cuando se cierra la zona abierta que ha activado una alarma, no se requiere realizar ninguna operación de restauración manual con el teclado o el explorador. Si se deshabilita, impide al usuario restaurar alertas reiniciando la entrada que activó 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**.
Confirmación		
⏻	Confirmación	La variable Confirmación determina cuándo una alarma se considera confirmada. ● BS8243: Impone el cumplimiento de los requisitos de la Policía británica y se trata de una obligación específica para las instalaciones industriales británicas. Esta norma estipula que una alarma sólo se considerará confirmada si cumple la siguiente condición: Que después de activarse una alarma de zona inicial, y antes de que expire 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. (Véase Temporizaciones [→ 244]) Si no se activa una segunda alarma en zona dentro del tiempo de confirmación de alarma, la primera alarma de zona se anulará. 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. Esta norma estipula que una alarma se considerará confirmada en el momento en que se active una segunda alarma de zona en el sistema dentro del período de tiempo configurado para una alarma. La opción de confirmación de 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 requerimiento estipula que una alarma solamente se la considerará como alarma 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 STA[1] en un plazo de 30 minutos (por defecto). - fallo STA seguido por una condición de tamp o de

Restricciones	Opciones del sistema	Descripción
		alarma en un plazo de 30 minutos (por defecto). Si pasan 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 será anulada 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 Esta opción impone el cumplimiento de la norma VdS.
Teclado		
ⓘ	Mostrar siempre el estado (VER ESTADO. SIST.)	Si esta opción está habilitada, el estado de armado del sistema (Armado total/Armado parcial/Desarmado) se muestra permanentemente en la línea inferior de la pantalla del teclado. Si no está marcada, el estado de armado desaparecerá de la pantalla del teclado transcurridos siete segundos.
	Mostrar zonas abiertas	Si esta opción está habilitada, las zonas abiertas se mostrarán en el teclado en modo Desarmado.
	Mensaje TX a CRA	Si esta opción está habilitada, el mensaje a la CRA se mostrará durante 30 segundos después del desarmado, si se ha notificado 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	Con esta opción habilitada, las cámaras fuera de línea serán mostradas en el teclado en modo desarmado.
	Idioma en reposo	Se selecciona el idioma mostrado en estado de 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.
PIN		
	Dígitos PIN	Introduzca el número de dígitos de los códigos PIN de usuario (ocho dígitos como máximo). 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 que sea 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., el código PIN de usuario ya existente 00002134 (8 dígitos) pasará a ser 02134 si los dígitos del código PIN se reducen a 5.

Restricciones	Opciones del sistema	Descripción
		Nota: Esta opción no se puede cambiar si se ha establecido un modo de dígitos de código PIN con SPC Manager. Consulte la página [→ 320] **Nota:** Para cumplir con las normas INCERT, el código de usuario debe tener más de cuatro dígitos.
	Tarjeta + PIN	Si esta opción está habilitada, se solicitan los datos de tarjeta y código.
	Código coacción 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 del 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 [→ 244]. ● 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 [→ 244]. ● 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 [→ 244]. ● Código generado: si esta opción está habilitada, el PIN es generado automáticamente por la central.
Puerta		
	Reset tarjetas	Con esta opción habilitada, diariamente a medianoche se restablecerá el estado de retorno de las tarjetas de CCAA.
	Ignorar código lugar	Si está habilitado, el sistema de acceso ignorará los códigos del lugar. Al ignorar el código del lugar, solamente se añade el número de tarjeta y se aumentan los usuarios de tarjeta del sistema de 100 a 2.500.
	Formatos de tarjeta	Haga clic en el botón **Editar** para seleccionar los formatos de tarjeta que se permitirán en esta central. Para más información sobre los lectores de tarjetas y formatos de tarjetas soportados actualmente, consulte el apéndice del Manual de instalación y configuración de

Restricciones	Opciones del sistema	Descripción
		SPC. **Nota:** Si se selecciona **Wiegand**, se habilitan todos los formatos de tarjeta Wiegand.
Solo web y SPC Pro	Modo de 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**.
Solo web y SPC Pro	Modo de 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**.
Técnico		
⏻	Reset de técnico	(sólo para Reino Unido): Si se habilita esta opción, el técnico deberá restaurar las alarmas confirmadas. Esta opción funciona conjuntamente con la opción "Confirmación".
	Salida técnico	Con esta opción habilitada, el técnico puede salir del modo Técnico total habiendo alertas activas.
⏻	Acceso a técnico	Habilite esta función para asegurarse de que el técnico sólo puede acceder al sistema si el usuario lo permite. Con eta opción deshabilitada, la opción de menú TECN.HABILITADO no estará disponible en el teclado. **Nota**: Solo disponible si el grado de seguridad es "Modo Libre". Para los grados 2/3, el control por parte del usuario del acceso del técnico al sistema siempre está disponible.
⏻	Permitir fabricante	Habilite esta función para asegurarse de que el técnico sólo puede acceder al sistema si el usuario lo permite. Con esta opción deshabilitada, la opción de menú HABILITAR FABRICANTE no estará disponible en el teclado. **Nota**: Solo disponible si el **grado de seguridad** es "Modo Libre". Para los grados 2/3, el control por parte del usuario del acceso del técnico al sistema siempre está disponible si el tipo de usuario es "Maestro".
SMS		
	Autentificación SMS	Seleccione una de las siguientes opciones: ● Sólo código PIN: Se trata de un código de usuario válido. Consulte página. ● 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 SMS sólo estará disponible para ser configurado por el usuario cuando esta opción esté seleccionada. ● Código e identificador llamada ● Sólo PIN SMS. Es un código PIN válido configurado para el usuario diferente del código de acceso del mismo usuario. Los controles SMS sólo estarán disponibles para ser configurados por el usuario cuando esta opción esté seleccionada. ● PIN e ID llamante SMS.
Política		
Solo web	Modo del sistema	Configure, para el sistema, el comportamiento de inicio de sesión de técnico y de notificación de tamper.

Restricciones	Opciones del sistema	Descripción
Solo web	Modo temporizaciones	Se muestra la política de temporizaciones del sistema.
Solo web y SPC Pro	Configuración salidas	Haga clic en el botón **Editar** para configurar los ajustes de salida de enclavamiento y autoarmado [→ 214].
Solo web	Alertas del sistema	Esta opción de programación permite restringir la capacidad de restaurar, inhibir y anular incidencias por parte del usuario y del técnico. También se puede programar la forma en que el sistema reacciona a las incidencias.
Solo web	Alarma de zona	Esta opción le permite seleccionar si el usuario o el técnico pueden restaurar, inhibir o aislar alarmas en zonas concretas.
Solo web	Tamper de zona	Esta opción le permite seleccionar si el usuario o el técnico pueden restaurar, inhibir o aislar tampers en zonas concretas.
Solo web	Modo display teclado	Esta opción le permite seleccionar las incidencias que se mostrarán en el teclado tanto en modo Armado como Desarmado.
Solo web	Modo LEDs teclado	Esta opción le permite seleccionar los LED que se mostrarán en el teclado tanto en modo Armado como Desarmado.
Solo web	Política general sistema	Seleccione, de las opciones abajo indicadas, las correspondientes para gestionar el control remoto del sistema y los ajustes de alarma y sirena: - Sin alarmas confirmadas si armada internamente - Reposición remota bloqueo - Aislamiento remoto bloqueo - Inhibición remota bloqueo - Sin sirena exterior si armada internamente - Retardo TX con entrada activa - Cancelación retardo alarma confirmada
Solo web	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		
	Clave atraco 1	Introduzca la primera clave de atraco que se debe enviar al CMS en caso de evento de Información de Atraco (HD).
	Clave atraco 2	Introduzca la segunda clave de atraco que se debe enviar al CMS en caso de evento de Información de Atraco (HD).
	Teléfono 1	Introduzca el número de teléfono del primer lugar que se debe enviar al CMS en caso de evento de Información de Atraco (HD).
	Teléfono 2	Introduzca el número de teléfono del segundo lugar que se debe enviar al CMS en caso de evento de Información de Atraco (HD).

Ver también

- Añadir/Editar una partición [→ 251]

17.9.4.2 Temporizaciones

Esta ventana proporciona una visión general sobre los valores por defecto de los temporizadores identificados y su 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. Al volver a establecer un grado de seguridad EN 50131 grado 2 ó 3, se sobrescribirá cualquier cambio realizado en esta página.

1. Seleccione **Configuración > Sistema > Temporizadores y retardos**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.

Temporizaciones

Designación de las funciones en el siguiente orden:

- 1.ª fila: Web/SPC Pro
- 2.ª fila: Teclado

Temporizador	Descripción	Por defecto
Audible		
Sirenas interiores Tiempo Sirena interior	Tiempo que sonarán las sirenas interiores cuando la alarma esté activada. (1 – 15 minutos: 0 = nunca))	15 min.
Sirenas exteriores Tiempo Sirena exterior	Retardo activación sirenas exteriores. (1 – 15 minutos: 0 = nunca)	15 min.
Retardo sirena exterior Retardo.sir.ext.	Provocará una activación retardada de la sirena exterior. (0 – 600 segundos)	0 segundos
Chime TEMP.CHIME	Número de segundos que se activará la salida de chime cuando se abra una zona con atributo CHIME. (1 – 10 segundos)	2 segundos
Confirmación		
Confirmar TIEMPO CONFIRM.	● **Nota**: Solo disponible cuando el grado de seguridad es "Libre" y se ha seleccionado "DD243" para la variable "Confirmación". (Consulte Opciones del sistema [→ 234]) Este temporizador se aplica a la función de confirmación de alarma y se define como el tiempo máximo entre alarmas de zonas diferentes no solapadas para generar una alarma confirmada. (30 – 60 minutos)	30 min.
Atraco confirmado	Este temporizador se aplica a la función de atraco confirmado y se define como el tiempo máximo entre alarmas de zonas diferentes no solapadas para generar una alarma confirmada. (480 - 1200 minutos)	480 min.
Retardo TX RETARDO TX	Cuando está programado, el retardo de marcación inicia un período de retardo predefinido (de 0 a 30 segundos) antes de que el sistema llame a un CRA. Esta opción está específicamente diseñada para reducir respuestas sin fiabilidad de CRAs y comisarías de policía. En caso de que salte una zona posterior, el periodo de retardo del marcador se ignora y éste llama inmediatamente. (0 – 30 segundos)	30 segundos
Abortar alarma ABORTAR ALARMA	Tiempo tras transmitirse una alarma en el que se puede transmitir un mensaje de interrupción de alarma. (0 – 999	30 segundos

Temporizador	Descripción	Por defecto
	segundos)	
Armado		
Autorización de armado AUTORIZ. ARMADO	Período durante el cual es válida la autorización de armado. Introduzca un valor entre 10 y 250 segundos.	20 segundos
Fin de salida FIN DE SALIDA	El tiempo de fin de salida es el número de segundos que se retarda el armado después de que una zona programada con el atributo Fin de salida se cierre. (1 – 45 segundos)	7 segundos
Sirena con armado total SIR.ARM.TOTAL	Activa la sirena exterior momentáneamente para indicar un estado totalmente armado. (0 – 10 segundos)	0 segundos
Flash con armado total FLAH.ARM.TOTAL	Activa el flash en la sirena exterior momentáneamente para indicar un estado totalmente armado. (0 – 10 segundos)	0 segundos
Fallo al armar FALLO AL ARMAR	Núm. de seg. para mostrar el mensaje de fallo al armar en teclados (0: Hasta introducir código válido). (0 – 999 segundos)	10 segundos
Alarma		
Doble detección DOBLE DETECCIÓN	Máximo retardo entre activaciones de zonas con doble detección para generar alarma. (1 – 99 segundos)	10 segundos
Pruebas Zonas en pruebas	Número de días en test de zona antes de retornar automáticamente al modo normal. (1 – 99 días)	14 días
Intervalo test sísmico AUTOTEST SÍSMICO	El tiempo medio entre tests automáticos de detector sísmico (12 – 240 horas) **Nota**: Para habilitar la comprobación automática, el atributo **test de detector automático** debe estar habilitado para una zona sísmica.	168 horas.
Duración test sísmico T TEST SÍSMICO	Tiempo máximo de alarma (seg) en respuesta a un test. (3 - 120 segundos)	30 segundos
Bloqueo post-alarma BLOQUEO POST-ALARMA	Tiempo tras alarma en el que el acceso es denegado.	0 minutos
Flash sirena exterior Flash	Tiempo que el flash estará activo cuando se active una alarma. (1 – 15 minutos: 0 = indefinidamente)	15 min.
Incidencias		
Retardo red c. a. RETAR.FALLO C.A.	El tiempo que transcurre desde que se detecta un fallo de corriente antes de que el sistema active una alerta. (0 – 60 minutos)	0 min.
Técnico		
Acceso de técnico ACCESO DE TÉCNICO	El temporizador para el acceso a técnico comienza en cuanto el usuario habilita el acceso al técnico. (0 – 999 minutos. "0" indica que no hay limitación para acceso al sistema).	0 min.
Salida modo técnico automática SAL.AUTO.M.TÉC.	Tiempo de inactividad tras el cual el técnico finalizará la sesión automáticamente	0 minutos
Teclado		
Retorno teclado a normal T.fallo.comunic.teclado	El número de segundos que esperará un RKD la introducción de la clave antes de salir del menú actual (10 – 300 segundos)	30 segundos
Idioma teclado Idioma teclado	Tiempo que espera el teclado en reposo antes de pasar al idioma por defecto (0 - 9999 segundos; 0 = nunca).	10 segundos
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. (1 – 999 segundos)	30 segundos

Temporizador	Descripción	Por defecto
	Véase Edición de una zona [→ 251].	
Reconocimiento alarma incendio RECONOCIMIENTO ALARMA INCENDIO	Tiempo adicional que se debe esperar antes de notificar una alarma de incendio para zonas con los atributos "Prealarma incendio" y "Reconocimiento alarma incendio" seleccionados. (1 – 999 segundos). Véase Edición de una zona [→ 251].	120 segundos
PIN		
PIN válido PIN VÁLIDO	Periodo en el que el PIN es válido en días (1 - 330)	30 días
Límite cambios de PIN LÍMITE CAMBIOS DE PIN	Número de cambios dentro de un periodo válido (1 - 50)	5
Aviso PIN AVISO EXP. PIN	Tiempo para expiración del PIN mostrado mediante aviso en display (1 - 14)	5 días
Configuración general		
Tiempo salida RF SALIDA RF	Tiempo en que permanece activa la salida RF del sistema (0 – 999 segundos)	0 segundos
Límite tiempo sincronismo LÍMITE TIEMPO SINCRONISMO	Límite de tiempo durante el cual no se notificará ninguna incidencia. (0 – 999 s) La sincronización de tiempo solo se produce si la hora del sistema y la hora de actualización están fuera de este límite.	0 segundos
T. fallo link T.ENLAC.EXC.	Tiempo de espera para fallo de Link Ethernet (0 = Deshabilitado) (0 - 250)	0 segundos
Cámara fuera de línea CAM.NO EN LÍNEA	Tiempo para cámara fuera de línea (10 - 9999)	10 segundos
Retardo técnico RETARDO TÉCNICO	Número de segundos de retardo para zonas técnicas con el atributo "retardo técnico". (0 – 9999 segundos)	0 segundos
Supervisada SUPERVISADA (!)	Este atributo sólo se aplica al Mantenimiento remoto. El número de horas que una zona debe abrirse por dentro si la zona está programada con el atributo **Uso frecuente**. (1 – 9999 horas)	336 horas (2 semanas)
Coacción silenciosa	Tiempo durante el cual la coacción permanecerá silenciosa y sin poderse restaurar desde el teclado (0 - 999).	0 minutos
Silencio con atraco/pánico	Número de minutos que un atraco/pánico permanecerá en silencio y sin poderse restaurar desde el teclado (0 - 999).	0 minutos

Los tiempos por defecto dependen de la configuración del técnico. Los tiempos por defecto indicados pueden permitirse o no y dependen de la configuración que realice el técnico.

17.9.4.3 Identificación

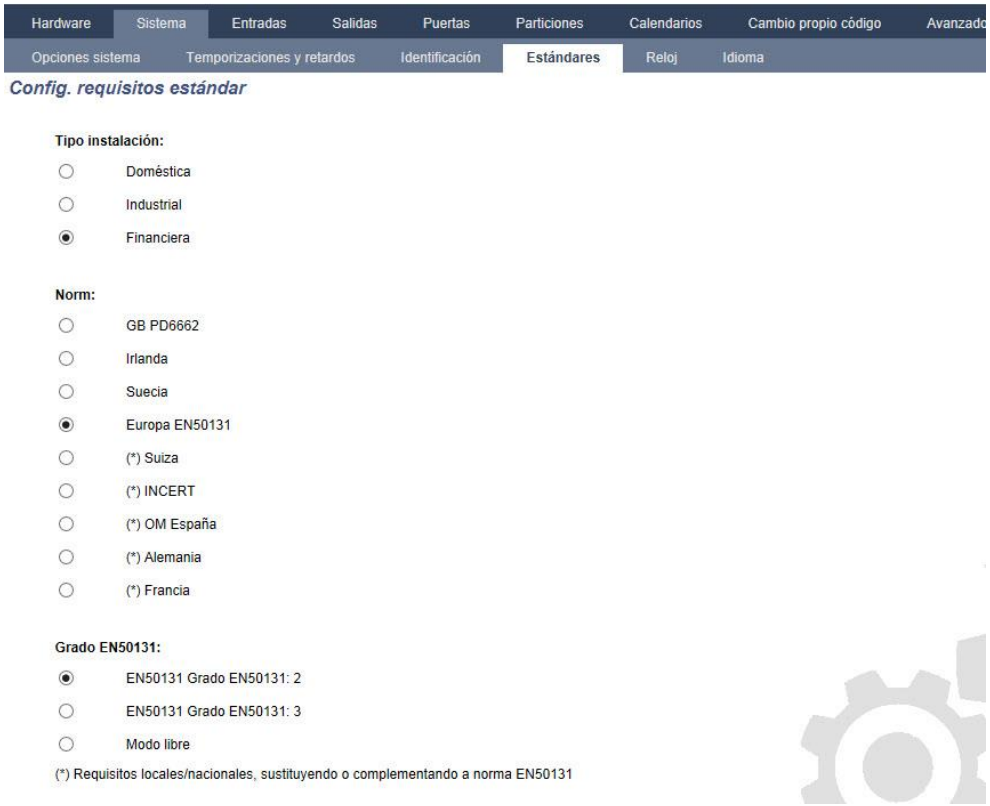
1. Seleccione **Configuración > Sistema > Identificación**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.

ID instalación	Introduzca un número exclusivo para cada instalación. Dicho número identifica la instalación (1–999999).
Nombre instalación	Introduzca el nombre de la instalación. Se debe introducir el nombre de una instalación antes de que la instalación se guarde en el sistema. La instalación se puede ver desde el teclado.
Fecha instalación	Seleccione en el menú desplegable la fecha en la que finalizó la instalación.
Nombre instalador	Introduzca el nombre de la persona que instaló el sistema (para consultas y avisos).
Teléfono instalador	Introduzca el teléfono de contacto de la persona que instaló el sistema (para consultas y avisos).
Detalles instalador	Marque esta casilla para mostrar los detalles de la instalación en el teclado conectado a la central cuando esté en estado de inactividad.
Bloqueo técnico	Marque esta casilla para solicitar el uso del PIN de bloqueo del técnico y restituir la central a su configuración por defecto.
Cód.bloqueo técnico	Introduzca valor para el 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 cuenta con unos requisitos de seguridad específicos para su aplicación en el mercado/país en el que se va a instalar el sistema de alarma.

1. Seleccione **Configuración > Sistema > Estándares**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.



Tipo instalación	Seleccione el tipo de instalación. Las opciones son Doméstica, Industrial o Financiera.
Región	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 en la que se realizará la instalación y los requisitos regionales que debe cumplir. Las opciones son GB, Irlanda, Suecia, Europa, Suiza, Bélgica (INCERT), España y Alemania (VDS).
Grado	Seleccione el grado de seguridad que se aplica a la instalación. ● Irlanda y Europa: – EN50131 Grado 2 – EN50131 Grado 3 – Modo libre ● Reino Unido: – PD6662 (basada en EN50131 Grado 2) – PD6662 (basada en EN50131 Grado 3) – Modo libre ● Suecia: – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Modo libre ● Bélgica: – TO-14 (basada en EN50131 Grado 2) – TO-14 (basada en EN50131 Grado 3) – Modo libre ● Suiza: – SES EN-CH-Grado 2 – SES EN-CH-Grado 3 – Modo libre ● España – EN50131 Grado 2

	– EN50131 Grado 3 ● Alemania – VdS Clase A – VdS Clase C – Modo libre ● Francia – NF&A2P - Grado 2 – NF&A2P - Grado 3 – Modo libre

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. El modo libre permite a un técnico personalizar la instalación, modificando las opciones de política de seguridad, y configurar opciones adicionales que no cumplan con las normas regionales de seguridad seleccionadas.

Las opciones de configuración en modo libre aparecen indicadas en el presente documento mediante el siguiente símbolo: ⓘ

Consulte Opciones del sistema para más información sobre la configuración de políticas del sistema.

17.9.4.5 Reloj

Esta ventana 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 analógico**.
   ⇨ Se mostrará la siguiente ventana.

2. Seleccione la **Hora** y la **Fecha** en los menús desplegables.
3. Configure los siguientes campos:

Cambio automático del horario verano/invierno	Si se selecciona, el sistema cambiará automáticamente al horario de verano.
Sincronización de la hora con la	Si se selecciona, el reloj en tiempo real (RTC) se sincroniza con

red de CA	la onda sinusoidal de la línea de alimentación eléctrica.

La fecha y hora seleccionadas se mostrarán en el teclado, la interfaz Web y el registro de incidencias.

17.9.4.6 Idioma

- Seleccione **Configuración > Sistema > Idioma**.
  - ⇨ Aparecerá la siguiente ventana:

- 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.
- Para la opción **Idioma por defecto**, seleccione "Emplee idioma por defecto" o "Último usado".
- ⇨ El idioma por defecto determina qué idioma se mostrará en los teclados cuando la central esté en reposo. Si se selecciona "Último usado", se mostrará el idioma asociado al último inicio de sesión realizado por un 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.

Ver también

Idioma [→ 250]
OPCIONES [→ 115]

17.9.5 Configuración de zonas, puertas y particiones

17.9.5.1 Edición de una zona

Las acciones del técnico y usuario incluyen Registro, Inhibir/Restaurar y Pruebas/Normal para cada zona según permiten los Grados de seguridad EN 50131 grados 2 y 3.

1. Seleccionar **Configuración >Entradas > Todas las zonas**.
   ⇨ Se mostrará la siguiente ventana.

Puede seleccionar **Configuración > Entradas > Zonas X-Bus** para configurar solamente las zonas cableadas o **Configuración > Entradas > Zonas vía radio** para configurar solamente las zonas inalámbricas.

2. Configure los campos tal como se describe en la siguiente tabla.

Zona	El número se presenta para referencia y no se puede programar.
Descripción	Introduzca un texto (máx. 16 caracteres) que sirva para identificar la zona de forma exclusiva.
Zona	La entrada física se muestra como referencia y no se puede programar.
Tipo	Seleccione un tipo de zona en el menú desplegable (consulte la página [→ 368]).
Partición	Sólo si está activado **Particiones** (múltiples). Seleccione en el menú desplegable la partición a la que se haya asignado la zona.
Calendario Pro !	Si es necesario, seleccione el calendario deseado (consulte la página [→ 267]). En el grado de seguridad 2/3, los calendarios sólo se pueden asignar a zonas del tipo Salida terminador, Técnica, Armado clave, Anul. ligada y Anul. siguiente. Para el grado de seguridad Libre, cualquier tipo de zona se puede asociar con un calendario.
Atributos	Marque la casilla de verificación relevante de la zona. Sólo se mostrarán los atributos relativos a dicho tipo de zona (consulte Atributos de zona [→ 372])

17.9.5.2 Añadir/Editar una partición

▷ Sólo si está activado **Particiones** (múltiples).

1. Seleccionar **Configuración >Particiones > Particiones**.
   ⇨ Se mostrará la siguiente ventana:

2. Pulse **Editar** para editar una partición ya existente.
3. Pulse **Añadir** para añadir una nueva partición. Si el tipo de instalación es *Doméstica* o *Comercial*, se añade automáticamente una partición y se muestra la ventana "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 ventana, y la partición se deberá añadir manualmente.

4. Introduzca una descripción para la nueva partición y seleccione un tipo de partición de entre las siguientes opciones:
   - Estándar - adecuado para la mayoría de particiones.
   - Cajero automático - proporciona configuración y ajustes predeterminados relevantes para cajeros automáticos.
   - Cámara acorazada - proporciona configuración y ajustes predeterminados relevantes para cámaras acorazadas
   - Avanzado - proporciona configuración para 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 como se indica en las siguientes secciones:

17.9.5.2.1 Entrada/salida

Configure los siguientes ajustes de entrada/salida:

Tiempo de entrada	Es el periodo de tiempo (en segundos) que se concede al usuario para DESARMAR la alarma después de 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 tiempo (en segundos) permitido para que un usuario salga de una partición protegida antes de que se complete el armado. El tiempo de salida se contará hacia atrás en el teclado cuando suene el zumbador para indicar al usuario que el sistema se armará cuando el temporizador 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 temporizador de salida y el armado se activa por zona "Robo fin salida" o zona "Robo E/S" con el atributo "Fin de salida". Consulte Temporizaciones [→ 244].
Des.t.ent.c.remoto	El mando vía radio solo desarmará cuando el temporizador de entrada esté en funcionamiento. Por defecto está activado.
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 [→ 244].

17.9.5.2.2 Opciones de armado parcial

Configure el funcionamiento de zonas en particular para los modos Armado parcial A y Armado parcial B tal como se detalla a continuación:

A.parcial habilitado	Habilite el armado parcial para A y B según sea necesario.
Armado parc. temporizado:	Marque la casilla de verificación correspondiente (Armado parcial A o B) para aplicar el temporizador de salida al modo Armado parcial A o B.
Acceso armado parcial:	Marque la casilla de verificación correspondiente para convertir las zonas de acceso en zonas del tipo entrada/salida para el funcionamiento de Armado parcial A o B. Esta función es útil para las instalaciones domésticas en las que un detector de infrarrojos pasivo (PIR) se encuentra en el vestíbulo. Si el usuario arma parcialmente el sistema por la noche y baja en algún momento de la noche, es

	posible que active sin querer el detector PIR del vestíbulo y active la alarma. Al definir la opción de acceso a armado parcial, el zumbador sonará durante el periodo del tiempo de entrada cuando el detector PIR se active, advirtiendo así al usuario de que se activará la alarma si no se realiza ninguna acción.
E/S en armado parcial:	Marque la casilla de verificación correspondiente para convertir el comportamiento de las zonas de entrada/salida en zonas de alarma cuando se encuentre en modo Armado parcial A o B. Esta función es útil para las instalaciones domésticas cuando el sistema se ha ajustado en modo Armado parcial. Si el usuario activa el sistema por la noche, es posible que desee que la alarma se active de inmediato si la puerta principal o la trasera se abren durante la noche.
Armado parcial local:	Marque la casilla de verificación correspondiente para limitar los informes de alarmas en modo Armado parcial a únicamente informes locales (sin informes remotos).
Sin sirenas	Si se marca esta opción, no habrá sirenas activadas para armado parcial A o B.

17.9.5.2.3 Particiones ligadas

Esta sección le permite ligar particiones para operaciones de armado y desarmado:

Armado total	Armado total de esta partición, cuando todas las particiones ligadas estén en Armado total.
Todo arm.total	Armado total de todas las particiones cuanto esta partición esté en Armado total.
Impedir a.total	Impedir armado total de esta partición si todas las particiones ligadas están en armado total.
Imped.a.tot.todas	Impedir armado total de todas las particiones ligadas, si esta partición no está en armado total.
Desarmado	Desarmado de esta partición, cuando todas las particiones ligadas están desarmadas.
Todo desarmado	Desarmado de todas las particiones cuanto esta partición está desarmada.
Impedir desarm.	Impedir desarmado de esta partición si alguna de las particiones ligadas está en Armado total.
Imped.des.todas	Impedir desarmado de todas las particiones ligadas, si esta partición no es desarmada.
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 desee ligar a esta partición.

17.9.5.2.4 Automatización armado/desarmado

Configure la planificación con los siguientes ajustes:

Calendario	Seleccione un calendario para controlar la planificación.
Desarmado	Seleccione si la partición se debería desarmar automáticamente en función del

	tiempo especificado en el calendario seleccionado.
Armado total	Seleccione esta opción para poner la partición en Armado total según el tiempo especificado en el calendario seleccionado. La partición también se armará cuando haya transcurrido el tiempo de duración de desarmado o el intervalo de retraso (consulte la sección Armados y desarmados [→ 257]). Si la duración de desarmado se superpone con el tiempo planificado, la partición utilizará la configuración del calendario.
Bloqueo de tiempo	Seleccione esta opción para bloquear temporalmente la partición según el calendario seleccionado. (Partición de tipo Cámara acorazada solo en modo Financiero)
Temp.acc.cám.acorz.	Introduzca el número de minutos (0 – 120) para activar este temporizador al final de un periodo de desarmado con bloqueo de tiempo. Si la partición no es desarmada al expirar este tiempo, ya no puede ser desarmada hasta el inicio del siguiente periodo de desarmado con bloqueo de tiempo. (Partición de tipo Cámara acorazada solo en modo Financiero)

17.9.5.2.5 Transmisión

Los ajustes de la configuración de transmisión solo son aplicables a particiones estándar en instalaciones comerciales y financieras, y solo son relevantes si se ha seleccionado un calendario. (Consulte la sección Automatización armado/desarmado [→ 254])

Esta configuración permite enviar una transmisión al centro de control o al personal responsable si el panel está armado o desarmado fuera de las horas del calendario planificado.

Arm. prematuro	Permite enviar una transmisión si el panel se ha puesto en Armado total manualmente antes de un armado programado, y antes del número de minutos introducidos en el campo Temporizador.
Armado tarde	Permite enviar una transmisión si el panel se ha puesto en Armado total manualmente después de un armado programado, y después del número de minutos introducidos en el campo Temporizador.
Desarm.prematuro	Permite enviar una transmisión si el panel se ha puesto en Desarmado manualmente antes de un desarmado programado, y antes del número de minutos introducidos en el campo Temporizador.
Desarmado tarde	Permite enviar una transmisión si el panel se ha puesto en Desarmado manualmente antes de un desarmado programado, y antes del número de minutos introducidos en el campo Temporizador.

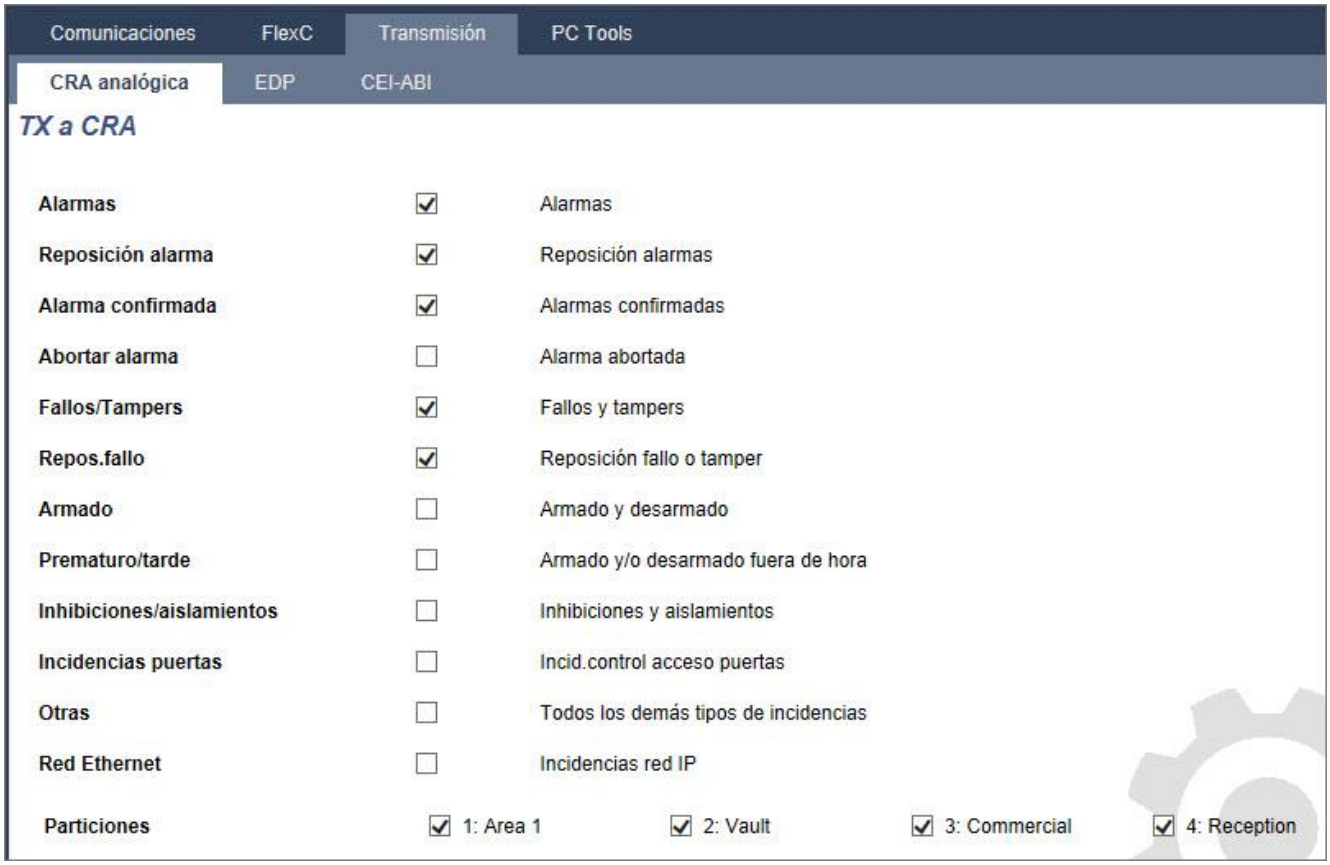
La transmisión se realiza por SMS, o bien se envía a la CRA a través de SIA e ID de contacto. Las incidencias también se guardan en el registro del sistema.

Solo se transmitirán las incidencias configuradas para transmisión tardía o prematura correspondientes a la partición.

La transmisión de incidencias también debe estar habilitada para una CRA o SMS, tal como se describe en las siguientes secciones.

Habilitación de transmisión de armado/desarmado irregular para una CRA

Para configurar la transmisión de incidencias para una CRA configurada para comunicarse mediante SIA o CID, seleccione **Comunicaciones > Transmisión > CRA analógica > Editar >Filtro** para mostrar la página de TX a CRA.

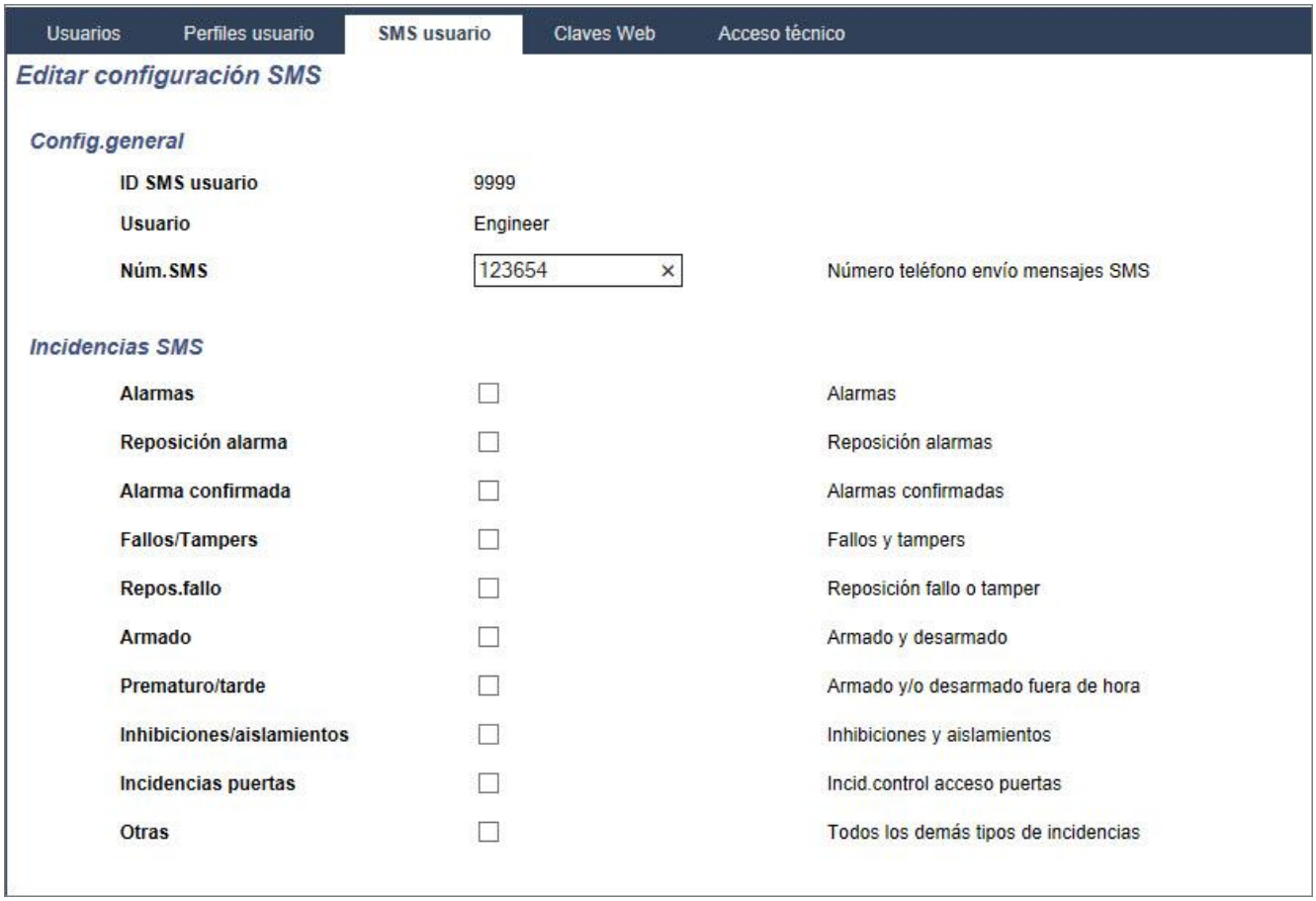


El parámetro **Prematuro/tarde** está habilitado para transmitir cualquier armado o desarmado que difiera de la planificación.

Habilitación de transmisión de armado/desarmado irregular para SMS

Las incidencias por SMS se pueden configurar con las páginas de configuración de técnico y de usuario.

Para la configuración de Acceso Técnico, seleccione **Usuarios > SMS usuario > SMS Técnico > Editar**:



Habilite Prematuro/tarde para transmitir cualquier armado o desarmado que difiera de la planificación.

17.9.5.2.6 Armado/Desarmado

Los siguientes parámetros (a excepción del parámetro Interrelacionado) solo son relevantes en los siguientes casos:

- Hay un calendario seleccionado (consulte Automatización armado/desarmado [→ 254]), o
- Está habilitada la opción **Duración desarm.** (tiene un valor mayor de cero), o
- Se cumplen las dos condiciones indicadas.

Aviso autoarmado	Introduzca el número en minutos de aviso antes del armado automático. (0 - 30) Tenga en cuenta que la central se arma a la hora programada o bien a la hora definida por el parámetro Retard. desarmado. La primera advertencia se muestra a la hora configurada antes de la hora programada. Hay más advertencias que empiezan un minuto antes de la hora de armado.
Canc.arm.auto.	Permite al usuario cancelar el armado automático introduciendo un código en el teclado.
Retard.autoarm.	Permite al usuario retrasar el armado automático introduciendo un código en el

	teclado.
Conmutador llave	Permite retrasar el armado automático mediante el módulo de expansión de conmutador de llave.
Interv.retardo	Introduzca el número de minutos que se retrasa el armado automático. (1 - 300)
Contador retraso	Introduzca el número de veces que se puede retrasar el armado automático. (0 - 99) 0 = ilimitado)
Retardo desarmado	Introduzca el número de minutos que se retrasa un desarmado. (0 = sin retraso)
No activo	Seleccione un grupo de particiones interrelacionadas para asignar a esta partición. La interrelación solo permite que se desarme una partición del grupo cada vez. Se utiliza normalmente en particiones de cajero automático.
Duración des.	Si la partición permanece desarmada durante más tiempo que el aquí indicado, se armará automáticamente. (Intervalo de 0 a 120 min.: 0 = no activo).
Doble código	Si esta opción está habilitada, se requieren dos códigos para armar o desarmar la partición con el teclado. Los dos códigos deben pertenecer a usuarios que cuenten con el derecho de usuario necesario para realizar la operación (armado o desarmado). Si el segundo código no se introduce en un plazo de 30 segundos, o si es incorrecto, la partición no se podrá armar ni desarmar.

Soporte para trabajo fuera de horario

Un ejemplo del uso de parámetros de armado y desarmado se da en situaciones en las hay que trabajar hasta más tarde del horario habitual, cuando se ha configurado un calendario para el armado automático de instalaciones a una hora concreta pero es posible que una parte del personal tenga que trabajar más allá del horario y el armado automático tenga que retrasarse.

Cada retardo se determina por la cantidad configurada en el parámetro **Interv.retardo**, y el parámetro **Contador retraso** determina el número de veces que se puede retrasar ese armado. Un usuario necesita el valor correcto en **Retard.autoarm.** para utilizar esta función.

Hay tres formas de retrasar el armado:

1. Introduciendo el código en el teclado.
   En el teclado estándar hay una opción de menú llamada RETARDO. La función de retardo se maneja con los botones que hay en la parte superior del teclado confort.
2. Mediante el conmutador de llave.
   Si se gira la llave a la derecha, el armado del sistema se retrasa durante el tiempo que esté configurado, siempre y cuando no se haya sobrepasado el número máximo de veces que se puede retrasar el armado (**Contador retraso**).
   Si se gira la llave a la izquierda, se establece un retardo de tres minutos (no configurable). Esto se puede hacer independientemente de cuántas veces se haya retrasado el armado.

3. Utilizando un mando vía radio, un PAT o un botón que active el disparador de **Retardo autoarmado**. (Consulte la página 172).

Desarmado temporal

Para permitir que el sistema se desarme temporalmente durante un período de tiempo especificado por un calendario, se deben configurar los tres parámetros siguientes:

1. **Calendario**
   Debe haber un calendario configurado y seleccionado para esta partición.
2. **Bloqueo tiempo**
   Esta casilla debe estar marcada para que la partición se pueda desarmar solo cuando el calendario configurado lo permita.
3. **Duración desarm.**
   Este parámetro se debe ajustar con un valor mayor de cero para establecer un límite superior para el tiempo que estará desarmada la partición.

La siguiente pantalla muestra estos parámetros configurados con los ajustes correspondientes:

17.9.5.2.7 Todo OK

Todo OK requerido	Si se selecciona esta opción, el usuario deberá confirmar que se ha generado la entrada "Todo OK" o la alarma silenciosa. Consulte Edición de una zona [→ 251] para más información sobre la configuración de una entrada de zona "Todo OK".
Temp.'Todo OK'	Tiempo (en segundos) en el que "Todo OK" debe ser confirmado para evitar que se genere una alarma silenciosa. (Intervalo de 1 a 999 segundos)
Incid.'Todo OK'	Seleccione el tipo de incidencia que se deberá enviar cuando expire el temporizador "Todo OK". Las opciones son Pánico (silencioso), Pánico y Coacción.

17.9.5.2.8 Salida RF

Tiempo salida RF	Introduzca el número de segundos durante los cuales la salida RF permanecerá activa. Si se selecciona 0 segundos, la salida alternará entre activa e inactiva,

El resto de opciones se describen en Entrada/salida [→ 252] para SPC Pro.

17.9.5.2.9 Ruta salida emergencia incendio

Ruta salida emergencia incendio	Seleccione las puertas que se abrirán cuando se produzca un incendio en esta partición. Esta opción no se muestra en modo Doméstica.

17.9.5.2.10 Fuentes partición

La sección Fuentes solo se muestra si las fuentes han sido definidas previamente. (Consulte la sección sobre fuentes).

Haga clic en el botón **Editar** para añadir, editar o eliminar condiciones de fuente para la partición. Aparecerá la siguiente página:

Configure la fuente para la partición mediante los siguientes parámetros:

Activación	Seleccione una fuente de la lista desplegable.
Activación	La fuente se puede activar desde el borde positivo o negativo de la señal de activación.
Acción	Esta es la acción que deberá llevarse a cabo cuando se accione la fuente. Las opciones son: ● Desarmado ● Armado parcial A ● Armado parcial B ● Armado total ● Retardo autoarmado Esta acción retrasará el armado de la alarma cuando el temporizador de autoarmado esté en marcha. La fuente solo añadirá tiempo si no se ha sobrepasado el límite de retardo y cada activación de una fuente retrasará el armado el tiempo definido en el intervalo de retardo (consulte la sección Armado/desarmado automáticos [→ 257]). ● Restaurar alarmas Esta acción borrará todas las alarmas en la zona configurada.

Nota: las fuentes no se pueden configurar desde un teclado.

Ver también

Fuentes [→ 270]

17.9.5.3 Edición de 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 predefinida. Estas dos entradas, el sensor de posición de la puerta y el interruptor de liberación de la puerta se pueden configurar.

Nombre	Descripción
Zona	El interruptor de liberación de la puerta también se puede utilizar para la parte de intrusión. Si la entrada del sensor de posición de la puerta también se utiliza para la parte de intrusión, se debe seleccionar el número de zona que tiene asignado. Si el sensor de posición de la puerta se utiliza únicamente para la parte de acceso, se debe seleccionar la opción "SIN ASIGNAR". Si el sensor de posición de la puerta está asignado a una zona de intrusión, se puede configurar como una zona normal pero sólo con funcionalidad limitada (p. ej. no se pueden seleccionar todos los tipos de zona). Si una partición o el sistema están armados con el lector de tarjetas, la entrada del sensor de posición de la puerta se debe asignar a un número de zona y a la partición o al sistema que se deben armar.
Descripción (Solo web y SPC Pro)	Descripción de la zona a la que está asignado el sensor de posición de la puerta.
Tipo de zona (Solo web y SPC Pro)	Tipo de zona de la zona a la que está asignado el sensor de posición de la puerta (no todos los tipos de zonas están disponibles).
Atributos de zona (Solo web y SPC Pro)	Los atributos de la zona a la que está asignado el sensor de posición de la puerta se pueden modificar.
Partición (Solo web y SPC Pro)	La partición a la que están asignados la zona y el lector de tarjetas. (Si el lector de tarjetas se usa para armar y desarmar, esta partición se armará o desarmará).
Posición de puerta (web) RFL posic.puerta (teclados) RFL posición puerta (SPC Pro)	La resistencia usada con el sensor de posición de la puerta. Elija el valor / la combinación de la resistencia usada.
DPS Normalmente abierto	Seleccione si el interruptor de liberación de la puerta debe ser una entrada normalmente abierta o normalmente cerrada.
Liberar puerta (web) RFL LIBER.PUERTA (teclados) RFL posición puerta (SPC Pro)	La resistencia usada con el interruptor de liberación de la puerta. Elija el valor / la combinación de la resistencia usada.
Liberación puerta NA	Seleccione si el interruptor de liberación de la puerta es una entrada normalmente abierta o no.

Nombre	Descripción
Sin DRS (Solo web y SPC Pro)	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) (Solo web y SPC Pro)	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 (no disponible en SPC Pro).

Todos los números de zona libres se pueden asignar 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 desplazará al siguiente número de zona libre. La configuración se adaptará consecuentemente.

Atributos de puerta

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

Atributo	Descripción
Nulo	La tarjeta está bloqueada temporalmente.
Grupo de puerta	Se utiliza cuando hay múltiples puertas asignadas a la misma partición y/o se requiere la funcionalidad antirretorno, responsable o interbloqueo.
Tarj. y código	Se requiere tarjeta y código PIN para entrar.
Sólo código	Se requiere el código PIN. No se acepta ninguna tarjeta.
Código o tarjeta	Se requiere código o tarjeta para entrar
Código para salir	Se requiere código en lector de salida. Se requiere puerta con lector de entrada y salida.
Código para desarmar	Se requiere código para armar y desarmar la partición vinculada. La tarjeta se debe presentar antes de introducir el código.
Desarmado desde exterior (navegador) Desarmado en lector de entrada (SPCPro)	Desarmado central/partición al presentar tarjeta en lector acceso.
Desarmado desde interior (navegador) Desarmado en lector de salida (SPCPro)	Desarmado central/partición al presentar tarjeta en lector salida.
Inhibir alarma	Se garantiza el seguimiento si hay una partición armada y la puerta es un tipo de zona de alarma o de entrada.
Armado total desde exterior	Armado total central/partición al presentar 2 veces

Atributo	Descripción
(navegador) Armado total en lector de entrada (SPCPro)	tarjeta en lector acceso.
Armado total desde interior Armado total en lector de salida (SPCPro)	Armado total central/partición al presentar 2 veces tarjeta en lector salida.
Forzar armado total	Si el usuario tiene permisos, puede forzar el armado desde el lector de entrada.
Emergencia	El bloqueo de la puerta se abre si se detecta una alarma de incendio dentro de la partición asignada.
Cualquier emergencia	Un incendio en cualquier partición desbloqueará la puerta.
Visita	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 el "atributo de acompañante" 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 la atribución de Visita se puede configurar individualmente para cada puerta.
Evitar retorno*	Se debe imponer el antirretorno 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 tarjetas deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta ha presentado su tarjeta de acceso para entrar en un grupo de puertas y no la ha presentado para salir de él, dicho titular habrá violado las normas antirretorno. La próxima vez que el titular de tarjeta intente entrar en el mismo grupo de puertas se activará una alarma Hard antirretorno y no se le permitirá entrar en el grupo de puertas.
Registr.retorno*	Las violaciones del antirretorno solamente quedan registradas. 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 tarjetas deben usar su tarjeta de acceso para entrar y salir de un grupo de puertas definido. Si un titular de tarjeta ha presentado su tarjeta de acceso para entrar en un grupo de puertas y no la ha presentado para salir de él, dicho titular habrá violado las normas antirretorno. La próxima vez que un titular de tarjeta intente entrar en el mismo grupo de puertas se activará una alarma Soft de antirretorno. No obstante, al titular de la tarjeta se le seguirá permitiendo la entrada al grupo de puertas.
Responsable*	La función de responsable permite al titular de una tarjeta con atributo de responsable (el responsable de custodia) proporcionar acceso a otros titulares de tarjetas (no responsables de custodia). El responsable debe ser el primero en entrar en la estancia. Sólo podrán entrar personas no responsables de custodia si el responsable de custodia está en la estancia. El responsable de custodia no podrá salir hasta que todas las personas no responsables de custodia hayan salido de la

Atributo	Descripción
	estancia.
Sirena puerta	La sirena montada en la placa del controlador de puerta suena cuando se producen alarmas en puertas.
Forzado ignorado	La puerta abierta de forma forzada no se procesa.
Interrelacionada* (navegador) Límite acceso a puerta interrelacionada (SPCPro)	Solo se permite una puerta abierta al mismo tiempo en una partición. Se requiere un grupo de puertas.
Configurando prefijo	Autorización con prefijo de clave (A,B,* o #) para armar el sistema.
* Se requiere un grupo de puertas	

Temporizadores puerta

Temporizador	Mín.	Máx.	Descripción
Autorización acceso	1 s	255 s	El tiempo que el bloqueo permanecerá abierto tras la autorización de acceso.
Acceso denegado	1 s	255 s	Temporización para que el controlador esté listo para leer la siguiente incidencia tras una denegación de acceso.
Apertura puerta	1 s	255 s	Temporización para cerrar la puerta y evitar alarma de "Puerta abierta demasiado tiempo".
Puerta dejada abierta	1 min	180 min	Temporización para cerrar la puerta y evitar alarma de "Puerta dejada abierta".
Extendido	1 s	255 s	Tiempo adicional tras acceso autorizado a tarjeta con atributo "Extendido"
Visita	1 s	30 s	Período de tiempo tras presentarse una tarjeta con atributo de acompañante en el que un usuario sin atributo de acompañante puede acceder a la puerta.

Calendario de puerta

Puerta bloqueada	Seleccione un calendario que debería bloquear la puerta durante el período configurado. Durante este tiempo no se aceptará ninguna tarjeta / código.
Puerta bloqueada	Seleccione un calendario que debería desbloquear la puerta. Durante el tiempo configurado, la puerta estará desbloqueada.

Actuaciones puerta

Activación	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.

Activación	Descripción
Activación para bloqueo de puerta	Si la activación asignada está activada, la puerta se bloqueará. No se aceptará ninguna tarjeta / código.
Activación para desbloqueo de puerta	Si la activación asignada está activada, la puerta se desbloqueará. No se necesitará ninguna tarjeta / código para abrir la puerta.
Activación que configura la puerta como normal	Si la activación asignada está activada, la puerta volverá al funcionamiento normal. Sirve para deshacer el bloqueo/desbloqueo de la puerta. Se necesitará una tarjeta / código para abrir la puerta.

17.9.5.3.1 Interbloqueo de puertas

La función de interbloqueo de puertas impide que las puertas restantes de un grupo interrelacionado se abran si alguna puerta del grupo está abierta.

A continuación vemos algunos ejemplos de cómo se utiliza esta función:

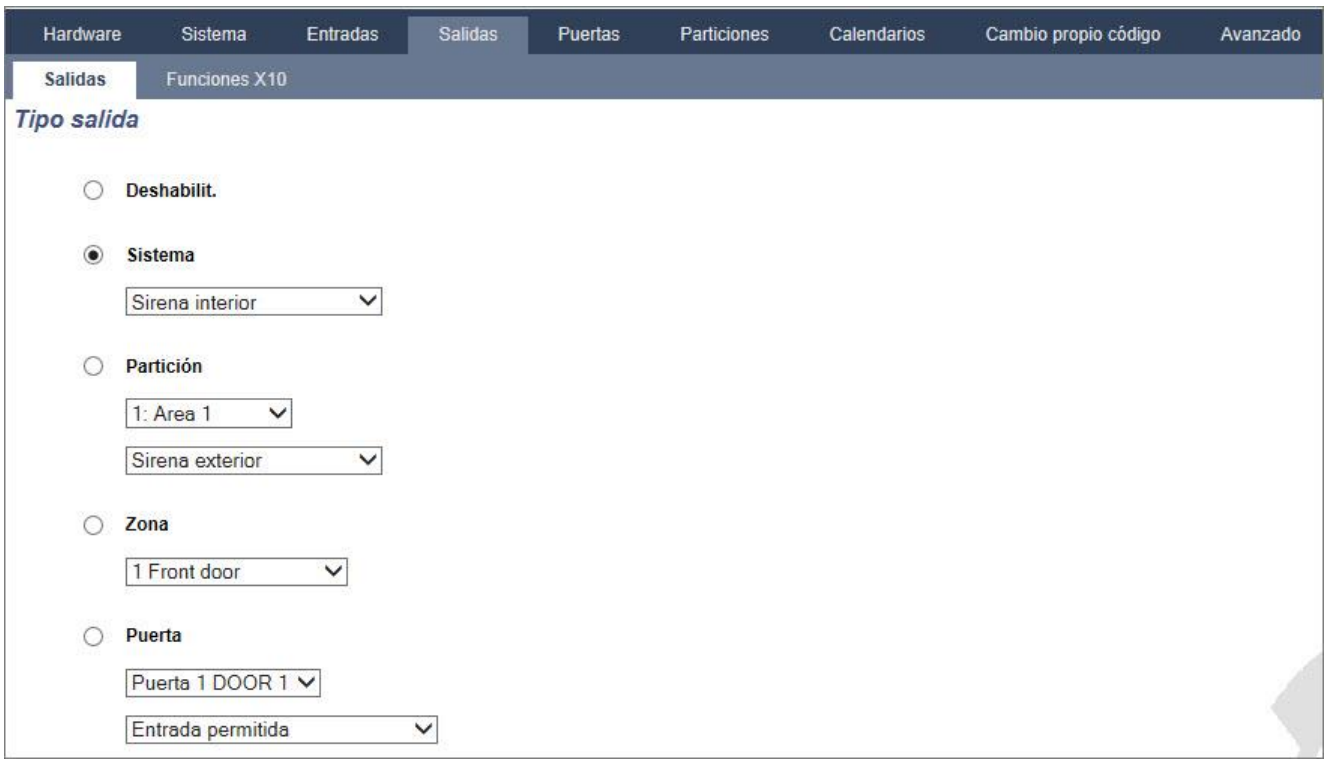
- En sistemas de entrada de dos puertas como las que se emplean en bancos y otros edificios. Normalmente se pulsan botones o se utilizan tarjetas para entrar, y unos LED rojos y verdes indican si la puerta se puede abrir o no.
- En puertas de acceso a particiones técnicas de cajero automático. Normalmente, todas las puertas de cajeros automáticos, además de la puerta que da acceso a la partición, estarían interbloqueadas.

Para crear un bloqueo de puerta:

1. Crear un grupo de puertas. Véase Edición de una puerta [→ 261].
2. Ajuste el atributo **Interbloqueo** para las puertas requeridas en el grupo. Véase Edición de una puerta [→ 261].
3. Configure una salida de puerta para el funcionamiento del interbloqueo de puertas. Esta salida estará activa para todas las puertas del grupo interrelacionado cada vez que una puerta perteneciente al grupo esté abierta, incluyendo la propia puerta abierta.
   Esta salida podría estar conectada, por ejemplo, a un LED o una luz roja para indicar que la puerta no se ha podido abrir y, si se invierte, se podría conectar a un LED o una luz verde.

Para configurar una salida para interbloqueo de puertas.

1. En el Modo Técnico, seleccione **Configuración > Hardware > X-BUS > Mód.exp.**.
2. En la página de **Configuración de módulo de expansión**, haga clic en el botón **Cambiar tipo** para la salida requerida.
3. Seleccione **Puerta** como el tipo de salida.
4. Seleccione la puerta que desee, e **Interrelacionado** como tipo de salida.



17.9.5.4 Añadir un grupo de particiones

Puede utilizar grupos de particiones para configurar varias particiones. Así pues, no es necesario realizar la configuración para cada partición.

▷ Sólo si está activada la opción **Particiones** (múltiples).

- Seleccione **Configuración > Particiones > Grupos particiones**.

1. Haga clic en el botón **Añadir**.
2. Introduzca una descripción para el grupo.
3. Seleccione las particiones que desee asignar a este grupo.
4. Haga clic en **Añadir**.

	AVISO
	Para utilizar los grupos de particiones para el teclado confort, active todas las particiones del campo **Particiones** en **Configuración > Hardware > X-BUS > Teclados > Tipo: Teclado confort**.

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 fuentes, habilitación de usuarios, zonas, salidas físicas, etc.

En cualquier momento, cualquier programación dentro del calendario puede estar "activa" si se cumplen sus condiciones temporales.

Se asigna un número ordinal a cada semana del año. Según la disposición de los días en un mes, puede haber 52 o 53 semanas en un año. La implementación del calendario del SPC cumple con el estándar internacional ISO 8601.

Configuración de calendarios

- Seleccionar **Configuración > Calendarios**.
  - ⇨ Se muestra una lista de calendarios configurados:

Se pueden realizar las siguientes acciones

Añadir	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, activación, 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

- Seleccionar **Configuración > Calendarios > Añadir**.
  - ⇨ Se mostrará la siguiente ventana:

- Indique un **Nombre** para el calendario (máx. 16 caracteres).

Copiar un calendario

Para realizar una copia de esta estructura de 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 todas las semanas tienen por qué tener un Tipo de semana (por ejemplo, el tipo de semana puede ser "Ninguno"). El número máximo del sistema es 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 activadores. Utilice las directrices sobre tiempo para Armado/desarmado automático de particiones (véase página [→ 269]), o para Armado/desarmado automático de otras operaciones en la central (véase página [→ 270]).

   ⇨ 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**.

Ver también

🗎 Armado/desarmado automático de particiones [→ 269]
🗎 Armado/desarmado automático de otras operaciones en la central [→ 270]

17.9.6.1.1 Excepciones

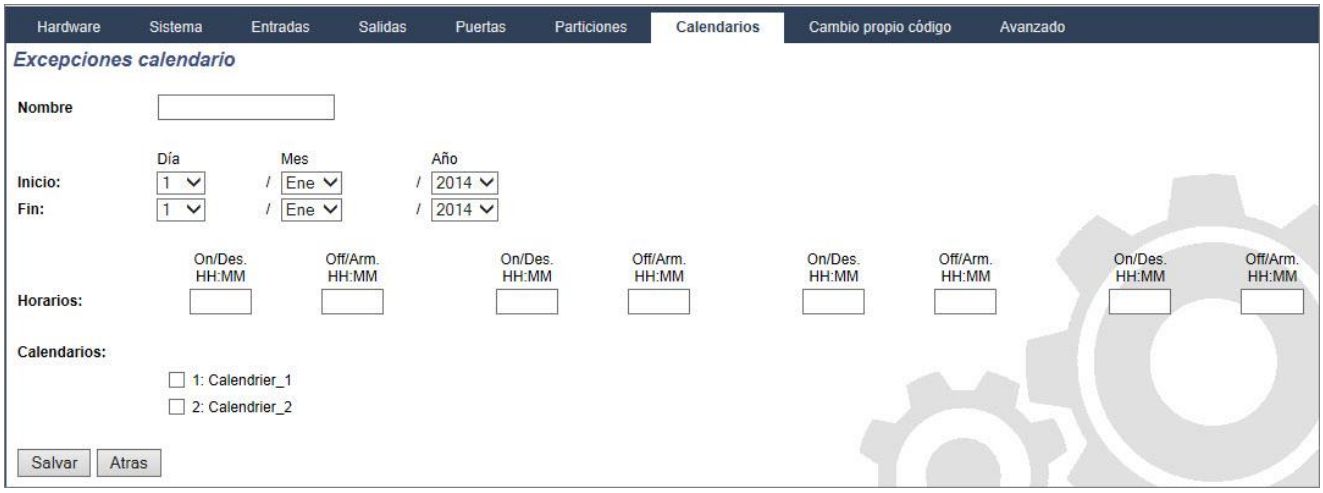
Las excepciones, o días especiales, sirven para configurar programaciones automáticas para circunstancias excepcionales fuera de las programaciones semanales normales definidas en los calendarios. Las excepciones se definen con

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. Seleccionar **Configuración > Calendarios > Excepciones > Añadir**.
   ⇨ Se mostrará la siguiente ventana.
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 finalización.
En hora / Fuera de hora	Seleccione las horas deseadas para armado/desarmado o para fuentes. Utilice las directrices sobre tiempo para Armado/desarmado automático de particiones (véase página [→ 269]), o para Armado/desarmado automático de otras operaciones en la central (véase página [→ 270]).
Calendarios asignados a	Seleccione el/los calendario(s) que desee para que surta efecto.

!	*AVISO*
	Los días especiales 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

Un calendario se puede configurar para armar o desarmar automáticamente una partición.

Para un día cualquiera de la semana, una configuración puede tener un máximo de cuatro horas de Armado y cuatro de Desarmado. Las horas que se configuran utilizan el formato de 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. Las horas configuradas activan la partición a Armado o Desarmado (si se cumplen todas las condiciones). Las horas que se introducen no se consideran una duración temporal, ya que representan el momento en que dichas acciones (Armado/Desarmado) tendrán lugar. Si el controlador se enciende o se reinicia, el estado de Armado/Desarmado se mantiene y las horas de armado o desarmado suceden según 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. Las horas que se configuran utilizan el formato de 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 Cambio propio código

Para cambiar un código PIN , consulte Cambio de código de técnico y de clave web [→ 206].

17.9.8 Configuración de ajustes avanzados

17.9.8.1 Fuentes

Una macro es un estado del sistema (p. ej. cierre de zona / tiempo / incidencia del sistema (alarma), etc.) que se puede utilizar como entradas de Causa & Efecto. Las macros se pueden asignar lógicamente de forma conjunta empleando los operadores lógicos And / Or para crear salidas de usuario. El sistema admite un máximo de 1024 macros por todo su sistema de Causa & Efecto.

1. Seleccione **Configuración > Avanzado > Fuentes**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.

Activación	Número generado por el sistema para una nueva macro. Para que una macro se active, debe configurarse uno de los dos pasos opcionales (limitación de calendario/tiempo).
Descripción	Introduzca una descripción de texto para la macro.
Calendario	Seleccione un calendario si es necesario. Si hay un calendario seleccionado, la macro sólo funcionará durante este periodo de tiempo. Consulte la página [→ 267].
Hora/temporización activa	Introduzca el número de segundos durante el cual las condiciones de la macro deben ser ciertas antes de que ésta se active.
Calendario	Seleccione el único período de tiempo, entre 00:00 y 24:00, durante el cual funcionará la macro. La hora de inicio queda incluida, mientras que la hora de finalización queda excluida. **Nota**: Este parámetro sólo retarda la transición de una macro cuando es de ON a OFF; de OFF a ON es inmediata.
Condiciones fuente	La macro está activada si se cumplen las siguientes condiciones (p. ej. se realiza una operación AND lógica): **Zona** – la macro está activada si la zona configurada se encuentra en alguno de los siguientes estados: abierta, cerrada, cortocircuitada o desconectada. **Puerta** – la macro está activada si está configurada alguna de las siguientes opciones para la puerta: Entrada autorizada, Entrada denegada, Salida autorizada, Salida denegada, Tiempo excedido apertura puerta, Puerta dejada abierta, Puerta forzada, Puerta normal, Puerta bloqueada, Puerta desbloqueada **Sistema** - la macro está activada si la salida del sistema se encuentra en el estado configurado, que puede ser activada o desactivada. Algunas de las posibles salidas del sistema son "Sirena exterior", "Alarma", etc. **Partición** - la macro está activada si la salida de partición está activada o desactivada. Algunas de las posibles salidas de partición son "Sirena exterior", "Alarma", etc. **Mando vía radio** - esta condición se puede configurar para un usuario particular o para cualquier usuario. Con esta configuración, si el usuario configurado (o cualquier usuario) pulsa la tecla '*' en el mando, provocará un impulso instantáneo ACT/DES/ACT. Esto sólo es aplicable a mandos que han sido registrados con el sistema. **Pulsador pánico vía radio** - esta condición se puede configurar para un usuario 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 impulso instantáneo ACT/DES/ACT. Esto sólo es aplicable a pulsadores de pánico vía radio que hayan sido registrados con el sistema. **PAT** – la fuente se activa si se pulsa un botón o una combinación de botones. Es posible asignar una condición de fuente a todos los PAT o solo a un PAT específico. Cuando se define una fuente con una condición de fuente PAT, se puede asignar a una salida de sistema para múltiples fines, como armar un sistema, encender luces o abrir una puerta.

	Código de teclado válido - 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. **Conmutador de llave** – la macro se puede configurar para una posición específica de la llave en el conmutador de llave. **Tiempo condiciones** – la macro se activa a la hora específica introducida en el cuadro proporcionado, en formato hh:mm.

	⚠ ADVERTENCIA
	Su sistema no cumplirá las normas EN si usted activa una macro para armar el sistema sin que se solicite un PIN válido.

17.9.8.2 Actuaciones

Las macros se utilizan con salidas de sistema, que son salidas virtuales definidas por el usuario que pueden asignarse a una salida física. Puede haber un máximo de 512 salidas de sistema.

En cuanto a las salidas continuas, cuando la macro es un código de usuario válido, ambos estados deben ser iguales, ya sean negativos o positivos.

1. Seleccione **Configuración > Avanzado > Actuaciones**.
   ⇨ Se mostrará la siguiente ventana.

2. Introduzca un **nombre** para la puerta. Esto es importante porque en la página de usuario **Salidas** para activar y desactivar las salidas no se indica el número de puerta, solo el nombre.
3. Marque la casilla **Protegido** si no desea permitir a los usuarios activar y desactivar esta puerta, aunque tengan derecho a hacerlo. Si la puerta está protegida, no aparecerá en la página de configuración **Salidas** para los usuarios.
4. Seleccione la **tecla rápida** que desee.
   Una tecla rápida es una "#" seguida de un único dígito del teclado. Si se configura y se pulsa un acceso directo en el teclado, se solicitará al usuario que active o desactive la salida.

Puede haber muchas salidas activadas por un acceso directo, tanto X-10 como salidas del sistema.

5. Añada una **temporización** para la puerta. La cantidad de tiempo empleada es 1/10 de segundo.
6. Haga clic en el botón **Fuentes** paraconfigurar fuentes para la activación y desactivación de la salida. En ambos casos debe definirse un flanco positivo o negativo de la macro. Consulte Fuentes [→ 270] para más información sobre la configuración de fuentes.
7. Haga clic en **Añadir** para añadir una nueva puerta o **Salvar** para guardar la nueva configuración para una puerta existente.

Ver también

Fuentes [→ 270]

17.9.8.3 Verificación de audio/vídeo

Para configurar una verificación audio/vídeo en un sistema SPC:

1. Instale y configure módulo(s) de expansión de audio.
2. Instale y configure cámara(s) de vídeo.
3. Instale y configure un equipo de audio.
4. Configure zona(s) de verificación.
5. Compruebe la reproducción de audio de zonas de verificación.
6. Asigne zona(s) de verificación a zona(s) físicas.
7. Configure los ajustes de verificación.
8. Vea imágenes de zonas de verificación en el navegador web o en SPC Pro.

!	*AVISO*
	Los teclados y el control de acceso se pueden deshabilitar durante varios minutos mientras se envía un fichero de audio a la central, dependiendo del tamaño del fichero.

17.9.8.3.1 Configuración de vídeo

Visión general

Las cámaras se utilizan 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.

i	*AVISO*
	Las cámaras no se deben compartir con otras aplicaciones de CCTV.

Las cámaras solo se pueden configurar con el navegador web o con SPC Pro. No se admite la configuración con el teclado. SPC Pro proporciona un método más sencillo de configuración y es la opción más recomendable.

La central admite dos resoluciones de cámara:

- 320X240
  (Esta configuración se recomienda 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 en color VGA 1/4”)
- Vanderbilt CFMC1315 (cámara IP Domo en color para interior de 1/3" y 1,3 MP)

Hay un flujo de comandos disponible por defecto para acceder directamente a los detalles de configuración de las cámaras anteriormente indicadas. Otras cámaras IP genéricas requieren la introducción manual de un flujo de comandos.

Añadir una cámara

1. Seleccione **Configuración > Avanzado > Verificación > Vídeo**.
   ⇨ Se muestra una lista de todas las cámaras previamente configuradas y su estado en línea o fuera de línea. Una cámara está en línea si ha proporcionado una imagen en los últimos 10 segundos.

2. Haga clic en el botón **Añadir** para añadir una nueva cámara, o en el botón **Editar** para editar una cámara ya existente.
   ⇨ Aparecerá la siguiente pantalla.

3. Configure la cámara con los siguientes parámetros:

ID cámara	ID de cámara generado automáticamente.
Descripción	Introduzca una descripción para identificar esta cámara.
Tipo	Seleccione uno de los siguientes tipos de cámara: ● Genérico ● Vanderbilt CCIC410 ● Vanderbilt CFMC1315
IP cámara	Introduzca la dirección IP de la cámara.
Puerto cámara	Introduzca el puerto TCP que escuchará la cámara. Por defecto es 80.

	Nota: 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 para iniciar sesión en la cámara que se añadirá al flujo de comandos que figura abajo cuando se pulse el botón **Actualizar línea CMD** .
Clave	Solo cámaras Vanderbilt CCIC1410 y CFMC1315. Introduzca una clave para la cámara que se añadirá al flujo de comandos que figura abajo cuando se pulse el botón **Actualizar línea CMD** .
Flujo de comandos	Introduzca el flujo de comandos que se enviará al servidor HTTP de la cámara para obtener imágenes. Esta secuencia debe incluir el nombre de usuario y la contraseña para la cámara. Consulte la documentación de la cámara para la secuencia específica que se necesita para el tipo de cámara seleccionada. SPC Pro puede configurarla automáticamente si está conectado a una cámara Vanderbilt CCIC1410 o CFMC1315 a través de una red LAN. El flujo de comandos por defecto para una cámara Vanderbilt CCIC1410 o CFMC1315 sin clave es "/cgi-bin/stilljpeg".
Imágenes previas	Introduzca el número de imágenes previas a una incidencia que desee grabar (0 - 16). Por defecto es 8.
Intervalo previo	Introduzca el intervalo de tiempo, en segundos, entre imágenes previas a una incidencia (1 - 10). Por defecto, 1 segundo.
Imágenes posteriores	Introduzca el número de imágenes posteriores a una incidencia que desee grabar (0 - 16). Por defecto es 8.
Intervalo posterior	Introduzca el intervalo de tiempo, en segundos, entre imágenes posteriores a una incidencia (1 - 10). Por defecto, 1 segundo.

17.9.8.3.2 Configuración de zonas de verificación

Para crear una zona de verificación

1. Vaya a **Configuración > Avanzado > Verificación> Zonas deverificación**.
   ⇨ Se muestra una lista de todas las zonas de verificación existentes.

2. Haga clic en el botón **Añadir**.
3. Introduzca un **Nombre** para la zona.
4. Seleccione un módulo de expansión de **audio** de la lista desplegable.
5. Seleccione un **vídeo** de la lista desplegable.
6. Haga clic en el botón **Salvar**.
7. Asigne esta zona de verificación a una zona física en el sistema SPC. (Véase Edición de una zona [→ 251])

La entrada y salida de audio para la zona de verificación solo pueden ser comprobadas por el técnico en SPC Pro.

Ver también

- Edición de una zona [→ 251]

17.9.8.3.3 Configuración de ajustes de verificación

Nota: los siguientes ajustes son aplicables a todas las zonas de verificación [→ 275].

1. Seleccione **Configuración > Avanzado > Verificación > Audio**.
   ⇨ Aparecerá la siguiente pantalla.

2. Configure los siguientes ajustes.

Registro incid. previas	Introduzca la duración requerida de una grabación de audio previa a una incidencia, en segundos (0 - 120). (por defecto, 10)
Registro incidenc.poster.	Introduzca la duración requerida de una grabación de audio posterior a una incidencia, en segundos (0 - 120). Por defecto es 30.

17.9.8.3.4 Visualización de imágenes de vídeo

Las imágenes de vídeo de las cámaras configuradas se pueden ver en el navegador web, en los modos Técnico total o Modo normal. Esta funcionalidad también está disponible para los usuarios que tienen en su perfil la autorización de Ver vídeo. (Véase Configuración de derechos de usuario [→ 194]) Para esta funcionalidad también debe estar habilitado el derecho de Acceso web.

La autorización de Ver vídeo también se puede configurar en el teclado y en SPC Pro (configuración "Vídeo en navegador").

Para ver imágenes vaya a **SPC Home > Vídeo**. Véase Visualización de vídeos [→ 175].

Ver también

- Añadir/editar un usuario [→ 194]
- Configuración de vídeo [→ 273]

17.9.8.4 Actualización de licencias de SPC

La función de **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 > Avanzado > Licencia**.

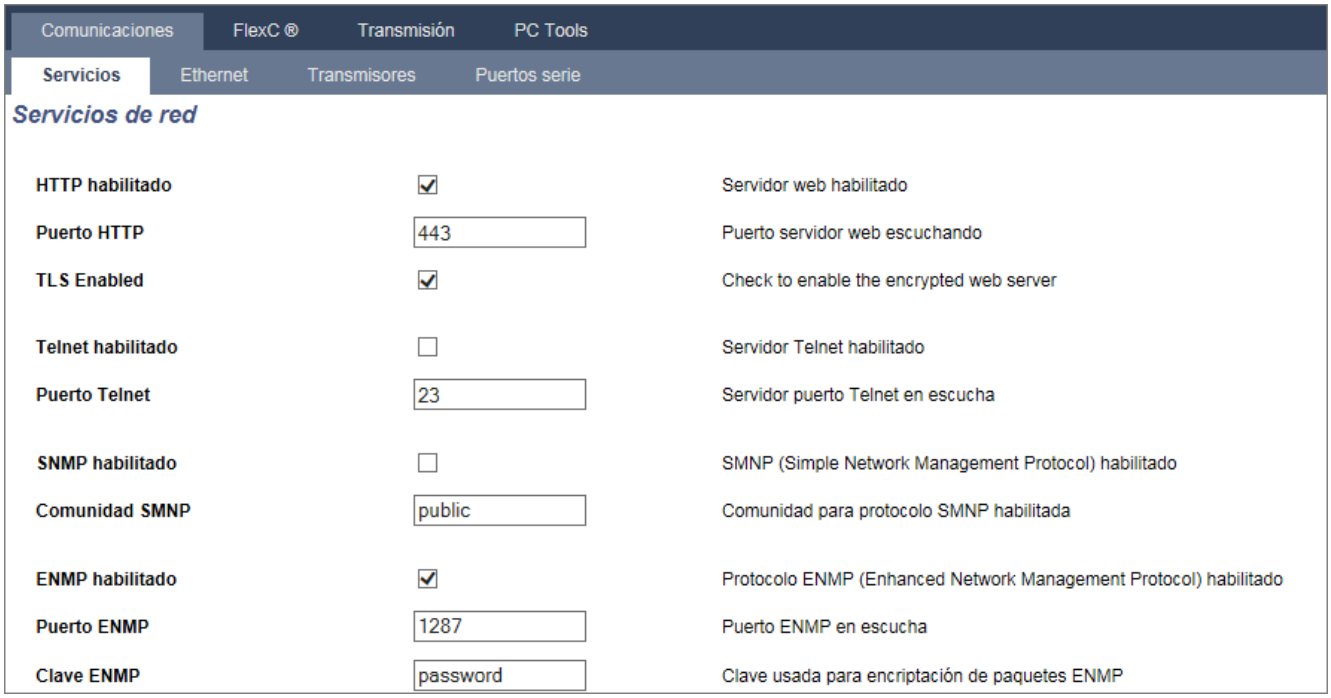
2. Póngase en contacto con el servicio de asistencia técnica con la funcionalidad solicitada indicando la clave de licencia actual tal como se ve.
   ⇨ Si se aprueba su solicitud, se emitirá una nueva clave de licencia.
3. Introduzca la nueva clave en el campo correspondiente.

17.10 Configuración de las comunicaciones

17.10.1 Configuración de comunicaciones

17.10.1.1 Configuración de los servicios de red de la central

1. Seleccione **Comunicaciones > Comunicaciones > Servicios**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.



HTTP habilitado	Marque esta casilla para habilitar el servidor web incorporado en la central.
Puerto HTTP	Introduzca el número de puerto en el que el servidor web está "escuchando". Por defecto, estará fijado en 443.
TLS habilitado	Marque esta casilla para habilitar el funcionamiento de la encriptación en el servidor web incorporado. Por defecto, está habilitada. Con TLS habilitado,

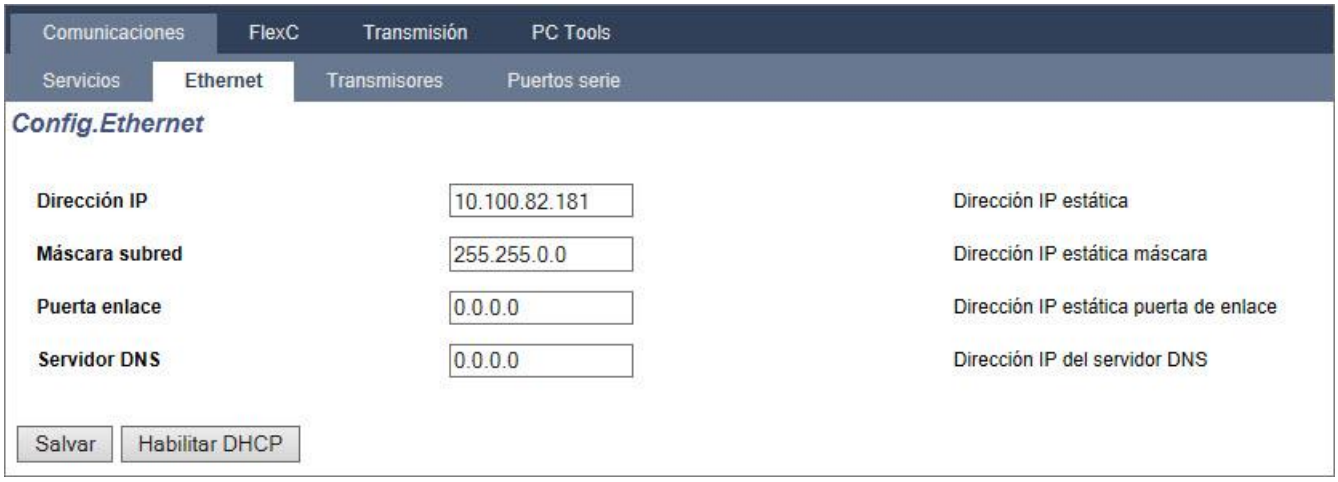
	sólo se puede acceder a las páginas web utilizando el prefijo "https://" antes de escribir la dirección IP.
Telnet habilitado	Marque esta casilla para habilitar el servidor Telnet. (Por defecto: Habilitado) **Nota**: Si se utiliza Telnet sin tener un conocimiento exhaustivo, la configuración del controlador puede resultar dañada; sólo se debe utilizar si se tienen los conocimientos suficientes o si se está recibiendo una instrucción de alguien que tenga dichos conocimientos.
Puerto Telnet	Introduzca el número del puerto Telnet.
SNMP habilitado	Marque esta casilla para habilitar el Protocolo Sencillo de Administración de Redes (SNMP). (Por defecto: Deshabilitado)
Comunidad SMNP	Introduzca el ID de clave para el protocolo SNMP. (Por defecto: Público)
ENMP habilitado	Marque esta casilla para habilitar el Protocolo Mejorado de Administración de Redes (ENMP). (Por defecto: Deshabilitado)
Puerto ENMP	Introduzca el número de puerto ENMP (por defecto: **1287**).
Clave ENMP	Introduzca la clave para el protocolo ENMP.
Cambio ENMP habilitado	Marque esta casilla para habilitar los cambios que se van a hacer en la red con el protocolo ENMP.

17.10.1.2 Ethernet

IP

El puerto Ethernet del controlador puede configurarse tanto desde la interfaz del navegador como desde la del teclado. Se puede establecer una conexión Ethernet con el controlador SPC de forma directa o con LAN.

1. Seleccione **Comunicaciones > Comunicaciones > Ethernet**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.



Dirección IP	Introduzca la dirección IP de la central.
Máscara subred	Introduzca la máscara de subred que define el tipo de estructura de direcciones de red implementada en la red de área local (LAN).
Puerta enlace	Introduzca la dirección IP de la puerta de enlace IP si existe alguna. Es la dirección IP a través de la cual se transmitirán los paquetes al acceder 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 Transmisores

La central SPC proporciona dos conectores de interfaz de módem incorporados (principal y backup) que le permiten instalar un módem RTB o GMS en el sistema.

Tras un retorno a la configuración predeterminada de fábrica, durante el proceso de configuración inicial del sistema con el teclado, el panel detecta si hay un módem principal o de reserva instalado y, en ese caso, muestra el tipo de módem y lo(s) habilita automáticamente con la configuración por defecto. En esta fase no se permite ninguna otra configuración de módem.

Para programar el/los módem(s):

Nota: Se debe instalar e identificar un módem. (Consulte la sección Instalación de módulos complementarios [→ 90])

1. Seleccione **Comunicaciones > Comunicaciones > Transmisores**.
2. Haga clic en **Habilitar** y en **Configurar**.

La detección y configuración de SMS no está disponible a menos que los módems estén configurados y habilitados.

17.10.1.3.1 Test de SMS

Una vez activada la función SIM para el módem, se puede realizar un test con el número del receptor que se desee incluyendo un mensaje escrito.

1. Introduzca el número de teléfono móvil (incluido el prefijo nacional de tres dígitos) en el campo del número y un mensaje corto de texto en el cuadro del mensaje.
2. Haga clic en **Enviar SMS** y compruebe que el mensaje se haya recibido en el teléfono móvil.

El test de SMS se realiza únicamente con el fin de asegurarse de que la función SMS funciona correctamente. Debe utilizarse un mensaje corto de texto con caracteres alfanuméricos (A-Z) para probar 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 con 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 proveedores de servicios sólo permiten los SMS a un teléfono registrado en el mismo país (esto se debe a problemas derivados de la facturación).

17.10.1.3.2 Función SMS

El controlador SPC permite la mensajería remota (SMS) en sistemas que tengan un módem instalado. Una vez instalado el módem, se necesitan las siguientes configuraciones para la función SMS:

- Módem habilitado para SMS. Consulte la página.
- Autentificación SMS. Consulte la página.
- Control SMS técnico. Consulte la página.
- Control SMS usuario. Consulte la página.

Dependiendo de las configuraciones, las funciones incluyen estas posibilidades de SMS:

- Notificación de incidencias. Consulte la página.
- Comandos remotos (los usuarios deben asignarse seleccionando comandos remotos). Consulte la página.

17.10.1.3.3 Opciones del sistema para SMS

Una vez instalado un módem y habilitada la función SMS, el sistema SPC debe utilizar la autentificación de SMS para las operaciones con SMS.

1. Seleccione **Configuración > Sistema > Opciones sistema**.
2. Seleccione la opción deseada del menú desplegable **Autentificación SMS**:

- **Sólo código**: Se trata de un código de usuario válido. Consulte la página [→ 109].
- **Sólo identificación de llamada**: Es el número de teléfono (incluyendo el prefijo nacional de tres dígitos) configurado para el control de SMS por parte del usuario. El Control de SMS sólo estará disponible para ser configurado por el usuario cuando esta opción esté seleccionada.
- **Código e identificador llamada**
- **Sólo código PIN el SMS**: Es un código PIN válido configurado para el usuario diferente del código de acceso de dicho usuario. Consulte la página. El Control SMS sólo estará disponible para ser configurado por el usuario cuando esta opción esté seleccionada.
- **Sólo código SMS e identificación de llamada**

17.10.1.3.4 Comandos de SMS

Una vez finalizada la configuración de SMS, pueden activarse sus funciones. Los comandos, en función de la configuración de SMS, se envían utilizando un código o el ID de quien llama. El tipo de código depende de lo establecido en cuanto a la

autentificación de SMS. Para más información sobre la autentificación de SMS, consulte la página [· 136]).

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 utilicen un código, el formato del texto es el código seguido de un espacio o punto. Donde **** es el código y "comando" es el comando: ****.comando o **** comando.

Por ejemplo, el comando "AYUDA" tiene el texto: **** AYUDA o ****.AYUDA

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 (Armado total) ****.ATOT	ATOT	Armado total alarma	Hora/fecha de armado del sistema. Si fuera aplicable, responde con zonas abiertas o de armado forzado
****APA (Armado parcial A) ****.APA		Permite armado parcial A de alarma por SMS	
**** APB (Armado parcial B) ****.APB			
**** DESM ****.DESM	DESM	Desarmar alarma	Desarmado sistema
**** ESTD (Estado) ****.ESTD	ESTD	Se muestra el estado	Estado del sistema y particiones aplicables
**** 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
**** ENG.ON ****.ENG.ON	ENG.ON	Habilitar acceso de técnico	Estado de técnico
**** ENG.OFF ****.ENG.OFF	ENG.OFF	Deshabilita el acceso del técnico	Estado de técnico
**** AFAB.ON ****.AFAB.ON		Habilita el acceso de fabricante	Estado de fabricante
**** MAN.Off ****.MAN.Off		Deshabilita el acceso de fabricante	Estado de fabricante
**** ABT.5.ON		Cuando la salida se identifica	Estado de "ABT.5"

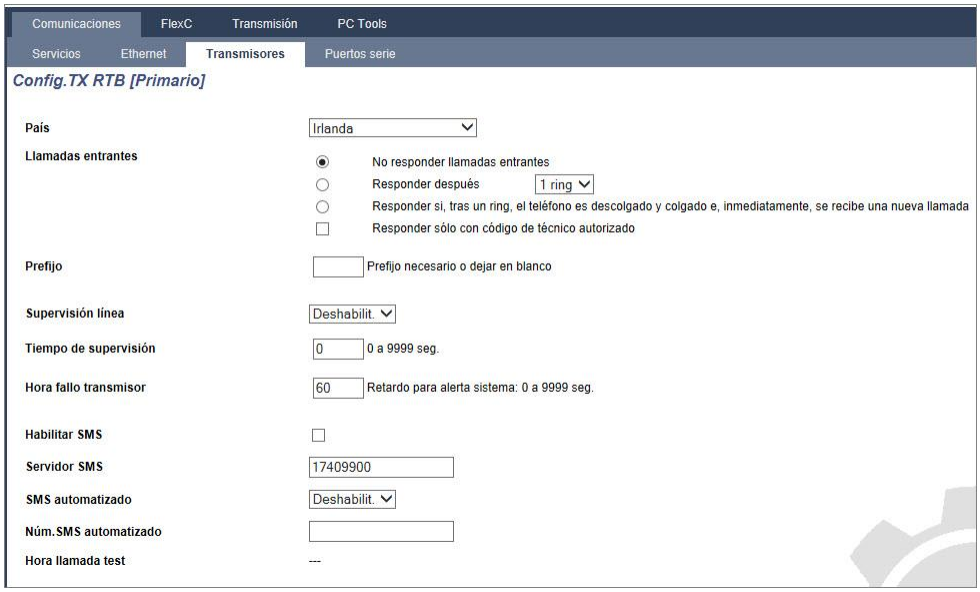
****.ABT.5.On		como "O5", está activado	
**** ABT.5.OFF ****.ABT.5.Off		Cuando la salida se identifica como "O5", está desactivado	Estado de "ABT.5"

Para el reconocimiento de SMS, la identificación de la salida utiliza el formato ONNN, donde O se refiere a la salida y NNN son los espacios numéricos, de los cuales no todos son necesarios. 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.

17.10.1.3.5 Módem RTB

1. Seleccione **Comunicaciones > Comunicaciones > Transmisores > Configuración**.
2. Configure los campos tal como se describe en la siguiente tabla.



Configuración módem

País	Seleccione el país en que está instalado el SPC.
Código de SIM	Sólo para GSM. Introduzca el código PIN para la tarjeta SIM instalada en el módulo GSM.
Permitir roaming	Seleccione esta opción para habilitar el roaming con GSM. **Nota**: Al cambiarse este ajuste se reinicia el módem. **Nota:** Soportado en módems GSM v3.08 o superior.
Llamadas entrantes	El módem se puede programar para responder a las llamadas en función de las siguientes condiciones: ● No responder llamadas: El módem nunca responde a las llamadas ● Descolgar tras "n" tonos de llamada: Seleccione el número de tonos tras los que el módem responderá a la llamada entrante. ● Responde después de que alguien llame al módem: cuelgue después de escuchar un único tono e, inmediatamente después, vuelva a llamar al módem. El sistema SPC sabe cómo responder a la llamada automáticamente.

	● Responder sólo con código de técnico autorizado.
Prefijo	Introduzca el número que se necesita para acceder a una línea (p. ej. si está conectada a PBX)
Supervisión línea	**Módem RTB:** Habilite esta función para controlar el voltaje de la línea conectada al módem. **Módem GSM:** Habilite esta característica para supervisar el nivel de señal de la antena GSM conectada 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 activada. (Consulte Opciones del sistema [→ 234]).
Controlar temporizador	Seleccione el periodo (en segundos) que el voltaje de la línea debe parecer incorrecto antes de que el SPC considere que la línea presenta fallos.
Hora fallo transmisor	Tiempo de retardo para una alerta del sistema (0 - 9999 segundos). Por defecto 60 segundos.
Habilitar SMS	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 con 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 proveedores de servicios sólo permiten los SMS a un teléfono registrado en el mismo país (esto se debe a problemas derivados de la 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 servidor SMS	Sólo 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 el tiempo para los mensajes SMS automáticos.
Núm.SMS automatizado	Indique el número de SMS para la recepción de mensajes SMS automáticos.
Tiempo llamada test	Muestra el tiempo de la última llamada de test por SMS.
Versión de chip GSM	Muestra el número de versión de GSM WISMO. Si no hay ningún número de versión disponible, se muestra "---".
Nombre punto acceso GPRS	Sólo para GSM. El proveedor de servicios debe proporcionar detalles sobre el punto de acceso.
Usuario GPRS	Sólo para GSM. El proveedor de servicios debe proporcionar detalles sobre el punto de acceso.
Clave GPRS	Sólo para GSM. El proveedor de servicios debe proporcionar detalles sobre el punto de acceso.

Haga clic en el botón **Test SMS** para enviar un mensaje corto de texto con el fin de probar el sistema.

Nota: El test de SMS se realiza únicamente con el fin de asegurarse de que la función SMS funciona correctamente. Debe utilizarse un mensaje corto de texto con caracteres alfanuméricos (A-Z) para probar esta función.

El test de SMS se realiza únicamente con el fin de asegurarse de que la función SMS funciona correctamente. Debe utilizarse un mensaje corto de texto con caracteres alfanuméricos (A-Z) para probar esta función.

Cuando se utiliza la opción de mensaje SMS en 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 activarse la identidad de la línea llamante en la línea RTB para que este parámetro funcione. Cada país contará con su propio proveedor de servicios SMS con un número de teléfono exclusivo.

Esta función no está disponible en todos los países. Póngase en contacto con su proveedor local para más información (apoyo de función, proveedor de servicios recomendado).

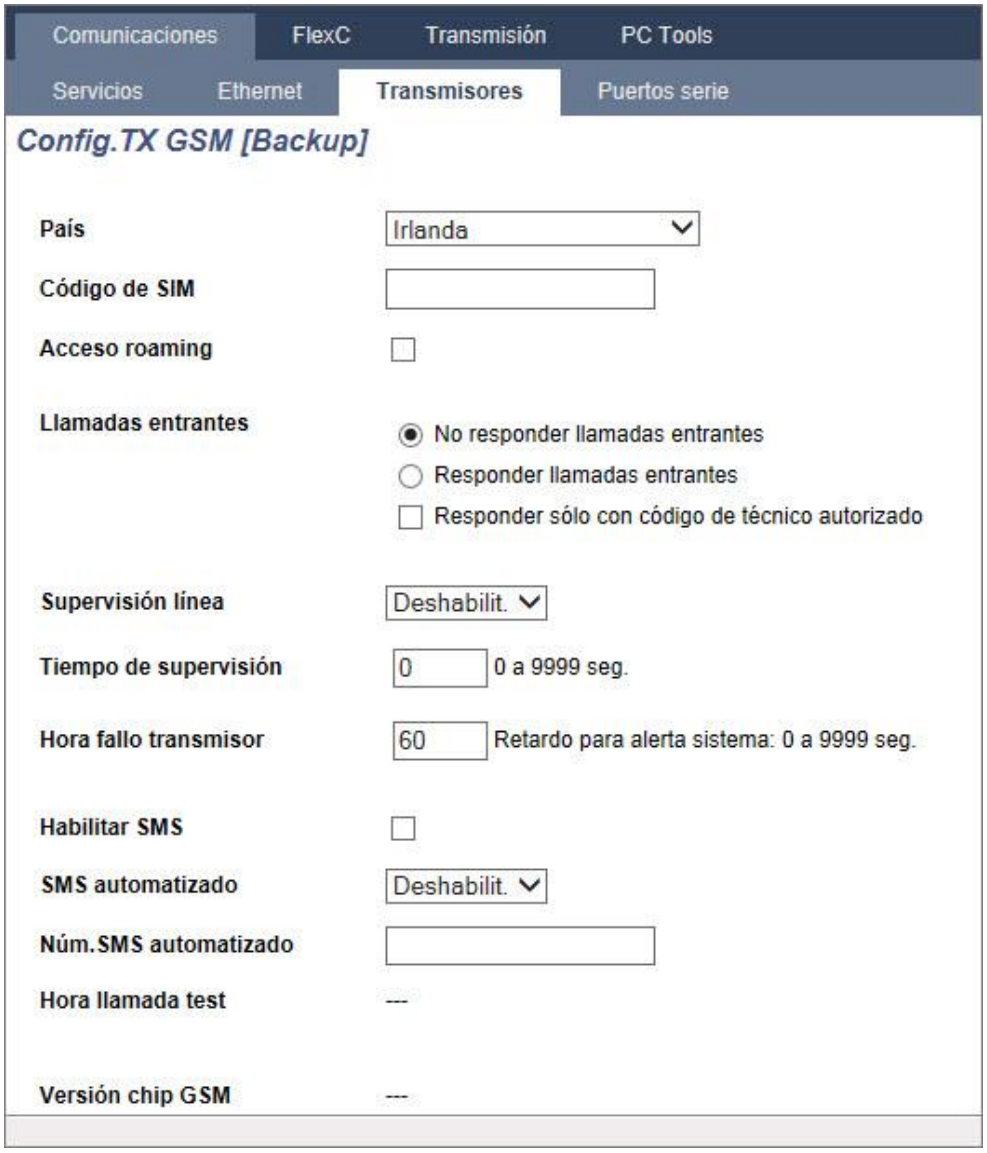
Compruebe con los proveedores de servicios específicos del país la disponibilidad del servicio y el número de servidor SMS.
Algunos servidores SMS pueden contar con requisitos técnicos adicionales necesarios para un funcionamiento correcto del servicio. Verifique estos requisitos en profundidad con su proveedor de servicios SMS local.

17.10.1.3.6 Módem GSM

▷ Debe haber un módem GSM instalado y funcionando correctamente.

1. Seleccione **Comunicaciones > Comunicaciones > Transmisores > Configuración**.

   ⇨ Se mostrará la siguiente ventana:



2. Configure los siguientes campos:

Configuración módem

País	Seleccione el país en que está instalado el SPC.
Código de SIM	Sólo para GSM. Introduzca el código PIN para la tarjeta SIM instalada en el módulo GSM.
Permitir roaming	Seleccione esta opción para habilitar el roaming con GSM. **Nota**: Al cambiarse este ajuste se reinicia el módem. **Nota:** Soportado en módems GSM v3.08 o superior.
Llamadas entrantes	El módem se puede programar para responder a las llamadas en función de las siguientes condiciones: ● No responder llamadas: El módem nunca responde a las llamadas ● Descolgar tras "n" tonos de llamada: Seleccione el número de tonos tras los que el módem responderá a la llamada entrante. ● Responde después de que alguien llame al módem: cuelgue después de escuchar un único tono e, inmediatamente después, vuelva a llamar al módem. El sistema SPC sabe cómo responder a la llamada automáticamente. ● Responder sólo con código de técnico autorizado.
Prefijo	Introduzca el número que se necesita para acceder a una línea (p. ej. si

	está conectada a PBX)
Supervisión línea	**Módem RTB:** Habilite esta función para controlar el voltaje de la línea conectada al módem. **Módem GSM:** Habilite esta característica para supervisar el nivel de señal de la antena GSM conectada 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 activada. (Consulte Opciones del sistema [→ 234]).
Controlar temporizador	Seleccione el periodo (en segundos) que el voltaje de la línea debe parecer incorrecto antes de que el SPC considere que la línea presenta fallos.
Hora fallo transmisor	Tiempo de retardo para una alerta del sistema (0 - 9999 segundos). Por defecto 60 segundos.
Habilitar SMS	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 con 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 proveedores de servicios sólo permiten los SMS a un teléfono registrado en el mismo país (esto se debe a problemas derivados de la 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 servidor SMS	Sólo 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 el tiempo para los mensajes SMS automáticos.
Núm.SMS automatizado	Indique el número de SMS para la recepción de mensajes SMS automáticos.
Tiempo llamada test	Muestra el tiempo de la última llamada de test por SMS.
Versión de chip GSM	Muestra el número de versión de GSM WISMO. Si no hay ningún número de versión disponible, se muestra "---".
Nombre punto acceso GPRS	Sólo para GSM. El proveedor de servicios debe proporcionar detalles sobre el punto de acceso.
Usuario GPRS	Sólo para GSM. El proveedor de servicios debe proporcionar detalles sobre el punto de acceso.
Clave GPRS	Sólo para GSM. El proveedor de servicios debe proporcionar detalles sobre el punto de acceso.

Haga clic en el botón **Test SMS** para enviar un mensaje corto de texto con el fin de probar el sistema.

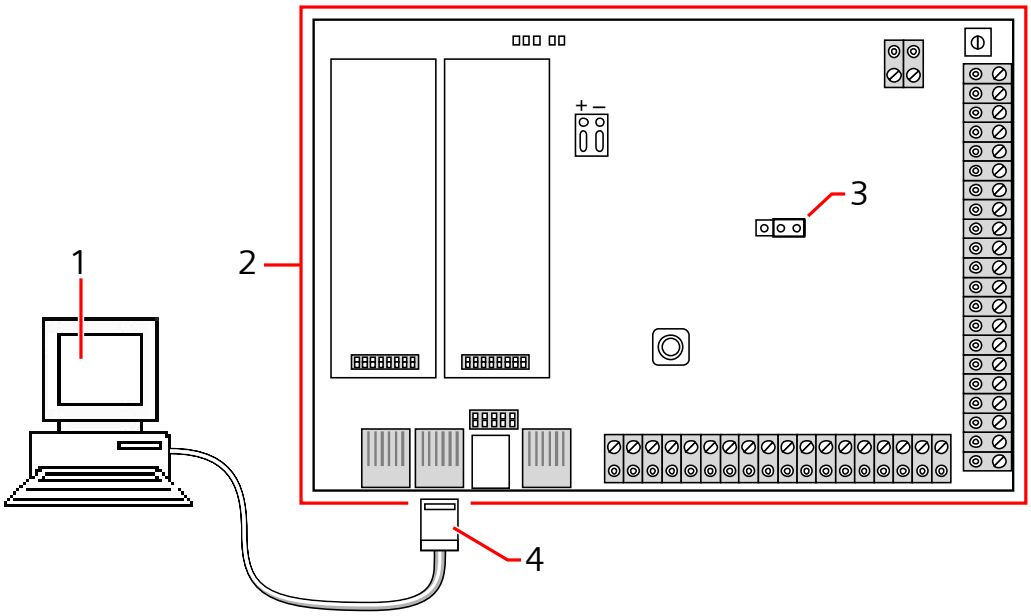
Nota: El test de SMS se realiza únicamente con el fin de asegurarse de que la función SMS funciona correctamente. Debe utilizarse un mensaje corto de texto con caracteres alfanuméricos (A-Z) para probar esta función.

El test de SMS se realiza únicamente con el fin de asegurarse de que la función SMS funciona correctamente. Debe utilizarse un mensaje corto de texto con caracteres alfanuméricos (A-Z) para probar esta función.

17.10.1.4 Puertos serie

El controlador SPC ofrece 2 puertos de serie (RS232) que proporcionan la siguiente funcionalidad:

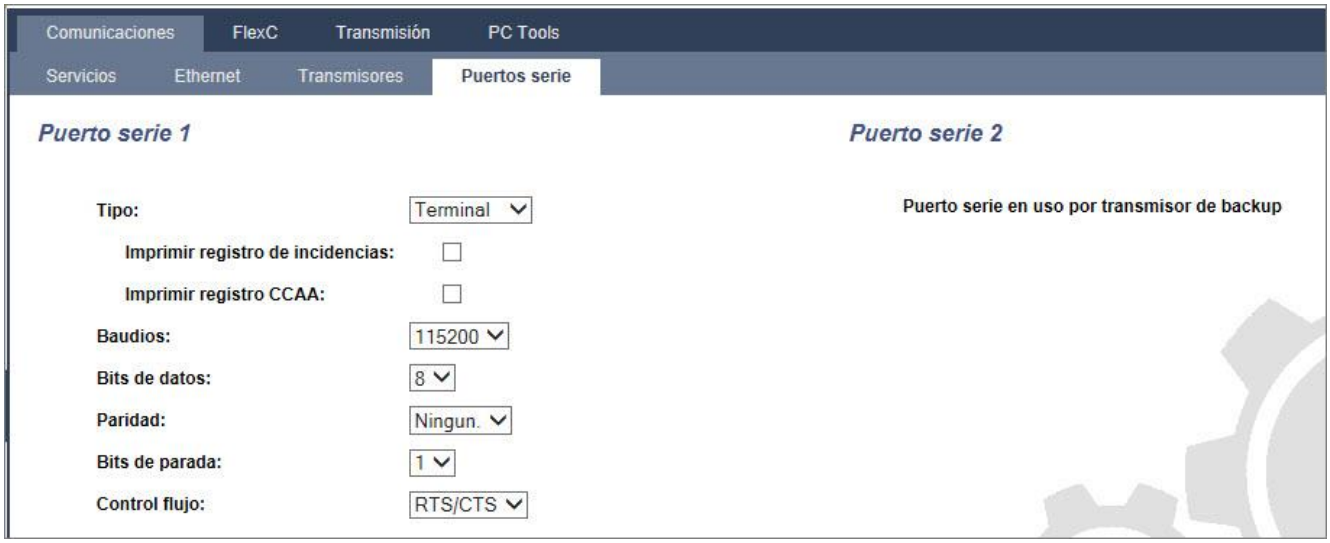
- **X10:** el Puerto serie 1 es una interfaz dedicada compatible con el protocolo X10. Este protocolo permite el uso de los cables de alimentación existentes de un edificio para transmitir información de control a dispositivos X10, ofreciendo la posibilidad de activar y controlar estos dispositivos a través de la interfaz de programación del controlador SPC.
- **Registro de incidencias:** la interfaz del Puerto serie 2 ofrece la posibilidad de 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 proporciona una interfaz a través de un programa del terminal que permite la ejecución de una serie de comandos para preguntar al controlador sobre información específica del sistema. Esta ventaja sólo está disponible como herramienta para fines de depuración e información y sólo deben utilizarla instaladores experimentados.



1	PC con Puerto serie que ejecute un hiperterminal
2	Controlador SPC
3	JP9 4000
4	RS232

Para configurar puertos serie:

- Seleccione **Comunicaciones > Comunicaciones > Puertos serie**.
  - ⇨ Se mostrará la siguiente ventana:



La configuración mostrada dependerá del tipo de conexión para la que se utilicen los puertos. La configuración se describe en las siguientes secciones:

17.10.1.5 Registro en el portal SPC

IP

El portal SPC ofrece la posibilidad de conectarse de forma remota a través de Internet al servidor web incorporado en el controlador SPC sin necesidad de conocer la dirección IP WAN de la unidad SPC. El servidor del portal SPC es un servidor externo con una dirección IP fija que tiene la capacidad de escuchar o "rastrear" en busca de controladores SPC en números de puerto especificados. El número de puerto por defecto en el que el servidor del portal escucha es el 80 y el puerto WAN por defecto (la dirección del puerto del SPC tal como se ve desde la red externa) es el 443.

1. Seleccione **Comunicaciones > Comunicaciones > Portal**.
2. Configure los campos tal como se describe en la siguiente tabla.

Habilitado	Marque esta casilla para habilitar el funcionamiento del portal.
Puerto del Portal	Introduzca el número de puerto en el que el servidor del portal está "escuchando" (por defecto: 80).
Dirección IP portal	Introduzca la dirección IP fija del servicio del portal SPC (**87.192.253.140**; póngase en contacto con Vanderbilt para confirmar esta información). La dirección IP del servidor del portal también se puede especificar como un nombre DNS en lugar de un formato IP numérico. Tenga en cuenta que para ello se debe configurar un servidor DNS en la configuración de Ethernet.
Dirección IP WAN	Si su ISP ha asignado una dirección IP fija para su conexión a Internet, introdúzcala aquí. Si no tiene una dirección IP fija, deje este campo en blanco.
Puerto WAN	Deje este número en su valor por defecto (443), a menos que el administrador de la red le indique que lo cambie.
Intervalo actualización	Introduzca el intervalo de tiempo para registrar la configuración del portal.

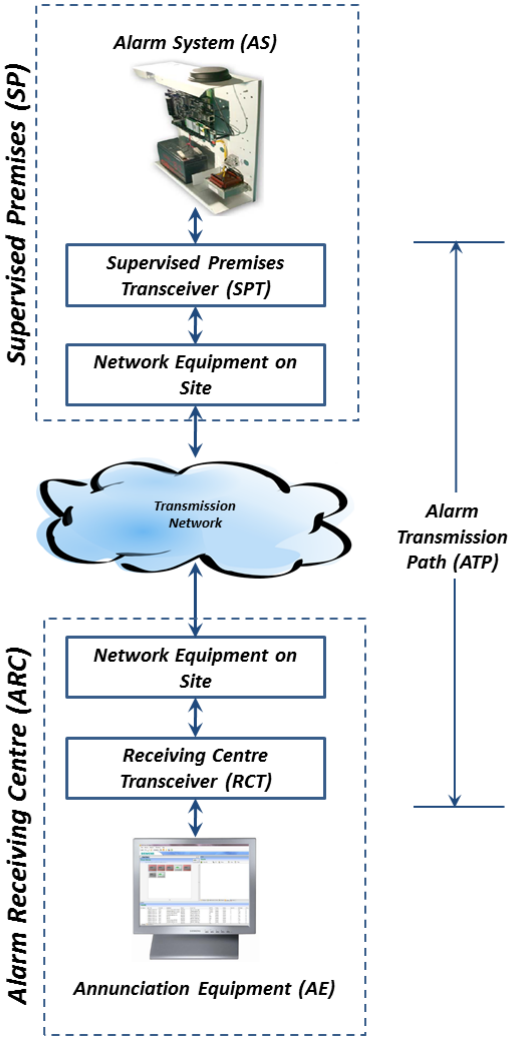
17.10.2 FlexC®

El protocolo de comunicaciones SPC Flexible Secure (FlexC) permite la comunicación de un sistema de transmisión de alarmas (ATS) de una o múltiples rutas basado en un protocolo de internet (IP). Un ATS es un enlace de comunicación fiable entre un transceptor de instalaciones supervisadas (SPT por ejemplo Ethernet integrado en la central SPC) y un transceptor del centro de recepción (RCT por ejemplo SPC Com XT). Un ATS FlexC consiste en una ruta primaria de transmisión de alarmas (ATP) y en hasta nueve rutas de backup de transmisión de alarmas (ATPs). Permite:

- Transferencia bidireccional de los datos entre el ATE, por ejemplo la central SPC por Ethernet y el RCT, por ejemplo, el servidor SPC Com XT.
- Supervisión de la comunicación de un ATS completo y de las ATPs individuales.

Las centrales de intrusión SPC soportan FlexC sobre IP con cualquier de las siguientes interfaces:

- Ethernet
- Módem GSM habilitado con GPRS
- Módem RTB



Ver también

- Configuración de la ATP de inicio rápido para el ATS EN50136. [→ 290]
- Configuración de perfiles de incidencias [→ 302]
- Definición excepción incidencia [→ 305]
- Configuración de perfiles de comando [→ 307]
- Estado FlexC [→ 189]
- Configuración de un ATS EN50136-1 o ATS Personalizado [→ 292]

17.10.2.1 Modo de Operación.

El sistema utiliza el método de almacenamiento y retransmisióncuando comunica eventos.

El sistema de alarma SPC envía eventos al SPC COM XT y requiere su reconocimiento por parte del SPC COM XT antes de que el sistema de alarma SPC considere que el evento ha sido transmitido con éxito. SPC COM XT solo reconoce el evento una vez que ha sido escrito como tal dentro de la base de datos SQL. Es entonces cuando SPC COM XT retransmite el evento al Cliente de SPC COM XT y a los interfaces Sur-Gard.

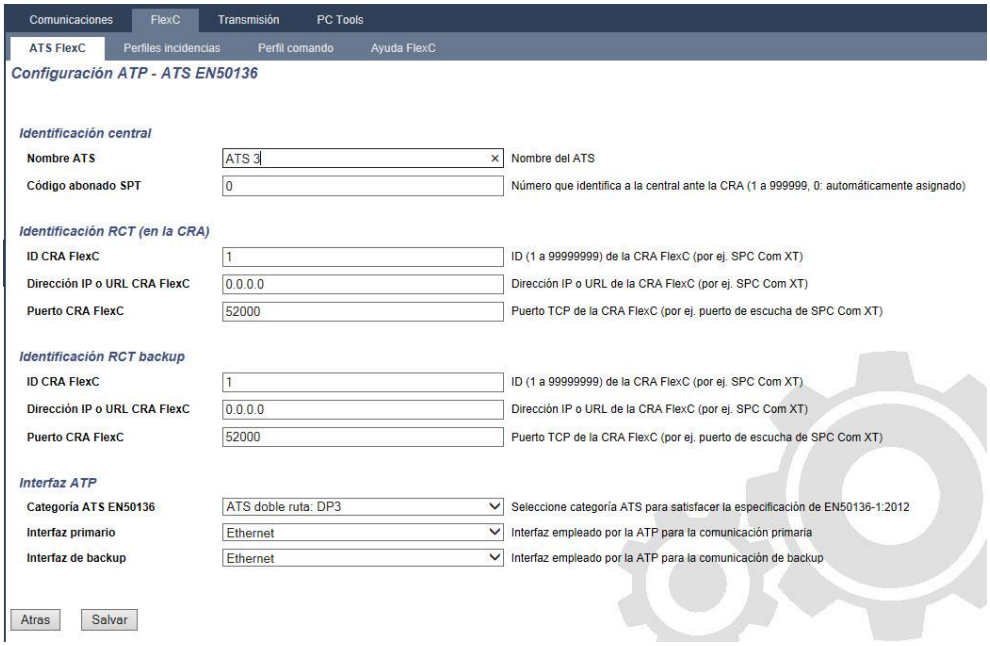
17.10.2.2 Configuración de la ATP de inicio rápido para el ATS EN50136.

FlexC ofrece las novedosas características siguientes que le permitirán poner en marcha FlexC con rapidez:

- Pantalla de configuración de inicio rápido para un **ATS con ruta simple** según EN50136, **ATS de doble ruta** y **ATS doble ruta y doble servidor**
- Perfil incidencia por defecto
- Perfil comando por defecto (este no soporta verificación de audio y vídeo)
- **FlexC Nombre usuario comando** por defecto (FlexC) y **Clave de comando** (FlexC) para el control de la central desde el RCT (p. ej. SPC Com XT)
- Encriptación automática sin clave

1. Para configurar rápidamente una conexión FlexC entre una central y un RCT (p. ej. SPC Com XT), vaya a **Comunicaciones - FlexC - ATS FlexC**.
2. En **Nuevo ATS EN50136-1**, seleccione una de las siguientes opciones para mostrar la pantalla **Configuración ATP**:

- **Nuevo ATS con ruta simple** - solo ATP primaria
- **Nuevo ATS doble ruta** - ATPs primaria y de backup
- **Nuevo ATS doble ruta y doble servidor** - ATPs primaria y de backup, servidores primario y de backup



1. Complete los campos de la pantalla **Configuración ATP - ATS EN50136** que se muestran en la tabla de abajo. Como mínimo, deberá completar el campo **Dirección IP o URL CRA FlexC** para poder guardar. Si no introduce un **Código abonado SPT**, puede poner en servicio la central utilizando el **ID registro ATS** el cual se genera automáticamente cuando se pulsa Salvar. El operador del RCT deberá introducir este **ID registro ATS**, por ejemplo, en SPC Com XT.
2. Haga clic en **Salvar**. La pantalla **Configuración ATS** muestra el **ID registro ATS** y la ATP primaria o bien las ATP primario y de backup configuradas en la **Tabla secuencia incidencias**.
3. En la pantalla **Configuración ATS**, haga clic en **Salvar** para aceptar la configuración por defecto, por ejemplo el **Perfil incidencia por defecto**, el **Perfil comando por defecto** (incluyendo el **Nombre usuario comando** FlexC y la **Clave comando** FlexC), y la **Encriptación automática** sin clave. Para cambiar la configuración, véase Configuración de un ATS EN50136-1 o ATS Personalizado [→ 292].
4. Haga clic en **Atrás**. El ATS se muestra en la tabla **ATS configurado**.

Identificación central	
Nombre ATS	Introduzca el nombre del ATS Si no se introduce ningún valor, el ATS adoptará por defecto el nombre ATS 1, ATS 2, etc.
Código abonado SPT	Número que identifica inequívocamente a la central ante el RCT. Introduzca 0 si no tiene el Código abonado SPT. En este caso, puede poner en funcionamiento la central utilizando el **ID registro ATS**. En el caso de un ATS EN50136, el **ID registro ATS** se genera automáticamente cuando se pulsa **Salvar**. El RCT puede enviar el **Código abonado SPT** a la central cuando está disponible.
Identificación RCT (en la CRA) e Identificación RCT backup (solo doble ruta y doble servidor)	
ID CRA FlexC	Introduzca el **ID CRA FlexC** que identifique inequívocamente la RCT (p. ej. SPC Com XT) en la central. Este debe coincidir con el valor introducido en la herramienta del

	gestor de configuración del servidor SPC Com XT en el campo **ID CRA FlexC Servidor** de la pestaña **Detalles del servidor** . Consulte el *Manual de instalación y configuración del SPC Com XT*.
Dirección IP o URL CRA FlexC	Introduzca la **Dirección IP o URL CRA FlexC** para la ubicación del servidor RCT (p. ej. Servidor SPC Com XT).
Puerto CRA FlexC	Introduzca el puerto TCP de del RCT (p. ej. SPC Com XT). Este valor debe coincidir con el introducido en el capo **Puerto servidor FlexC** en el gestor de configuración del servidor SPC Com XT.
Interfaz ATP	
Categoría ATS EN50136	Seleccione la categoría ATS EN50136 Category (SP1-SP6, DP1-DP4). Para una descripción de las categorías, véase Tiempos de categoría ATS [→ 384].
Interfaz primario	Seleccione la **Interfaz primario** que se va a aplicar a la ruta de comunicaciones primaras de entre las siguientes opciones: ● Ethernet ● GPRS Transmisor 1 ● GPRS Transmisor 2 ● Comunicación WAN Transmisor 1 ● Comunicación WAN Transmisor 2
Interfaz de backup	Para una **ATS doble ruta**, seleccione la **Interfaz de backup** que se va a utilizar para la ruta de comunicaciones de backup de entre las siguientes opciones: ● Ethernet ● GPRS Transmisor 1 ● GPRS Transmisor 2 ● Comunicación WAN Transmisor 1 ● Comunicación WAN Transmisor 2

17.10.2.3 Configuración de un ATS EN50136-1 o ATS Personalizado

Un ATS está compuesto por una central de alarmas, por rutas de red y por un RCT (p. ej. SPC Com XT). Combina una o múltiples rutas entre una central SPC y un RCT. Puede añadir hasta 10 ATPs a un ATS.

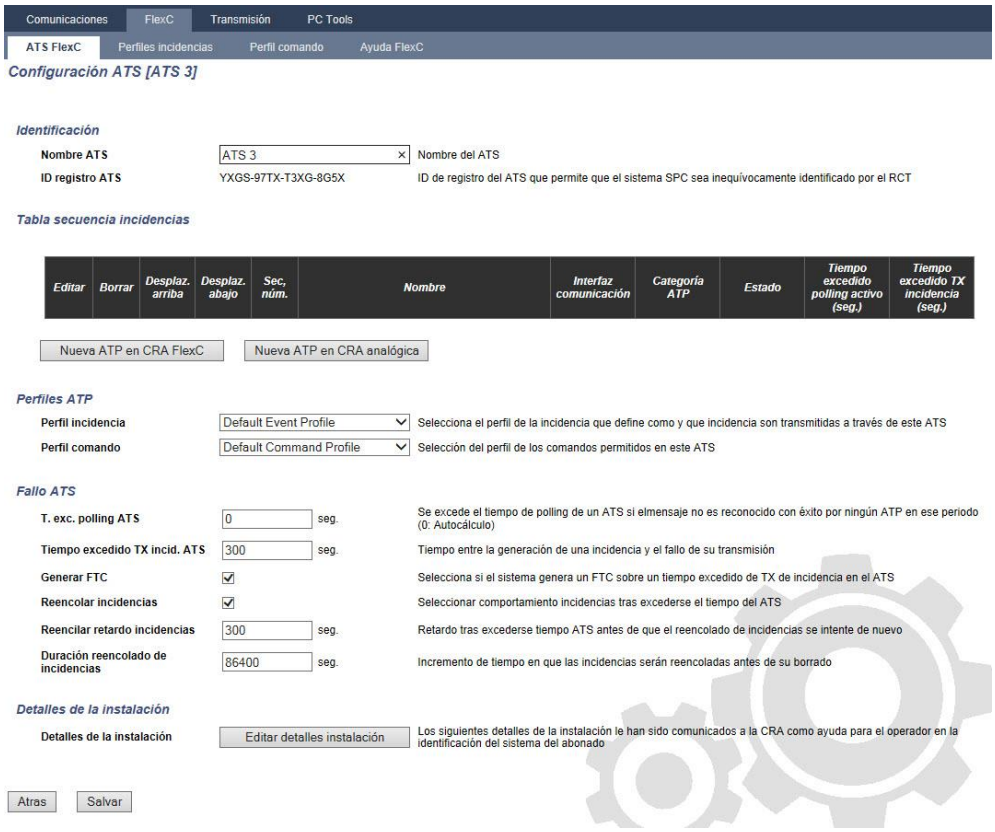
!	*AVISO*
	Para un ATS EN50136-1, la secuencia de la configuración del ATS comienza con la configuración de una ATP para un ATS. Esto le ofrece una función de configuración rápida. Consulte Configuración de la ATP de inicio rápido para el ATS EN50136. [→ 290].

1. Para configurar un ATS, vaya a **Comunicación - FlexC - ATS FlexC**.
2. Elija una de las siguientes opciones:

- **Nuevo ATS con ruta simple**
- **Nuevo ATS doble ruta**
- **Nuevo ATS doble ruta y doble servidor**

- **Nuevo ATS a medida**.

1. Para un ATS EN50136, debe configurar primero los ajustes de la pantalla **Configuración ATP - ATS EN50136**. Consulte Configuración de la ATP de inicio rápido para el ATS EN50136. [→ 290].
2. La pantalla **Configuración ATS** muestra. Un ATS EN50136-1 ATS mostrará una ATP primaria o una ATP primaria y de backup en la **Tabla secuencia incidencias**.



1. Introduzca un **Nombre ATS** para identificar el ATS. Si no se introduce ningún valor, el ATS adoptará por defecto el nombre ATS 1, ATS 2, etc.
2. Para añadir 1 ATP primaria y hasta 9 ATP de backup a una ATS, haga clic en **Nueva ATP en CRA FlexC**, consulte Nueva ATP en CRA FlexC [→ 294], o haga clic en **Nueva ATP en CRA analógica**, consulteNueva ATP en CRA analógica [→ 299].
3. Seccione un **Perfil incidencia** del menú desplegable. Para personalizar cómo se transmiten las incidencias en un ATS, consulte Configuración de perfiles de incidencias [→ 302].
4. Seleccione un **Perfil comando** del menú desplegable. Para personalizar los comandos habilitados para que un RCT controle una central, consulte Configuración de perfiles de comando [→ 307].
5. Complete los campos de **Fallo ATS** tal como se muestran en la tabla de abajo.
6. Haga clic en el botón **Editar detalles instalación** para completar los ajustes que identifican la central al operador del RCT. Consulte Editar detalles de la instalación [→ 300].
7. Haga clic en **Salvar** y en **Atrás** para regresar a la página **Configuración ATS**. El nuevo ATS se muestra en la tabla **ATS configurado**.
8. En el caso de contar con múltiples ATPs, puede emplear las flechas arriba y abajo de la **Tabla secuencia incidencias** para reordenar la secuencia de las ATP.

!	*AVISO*
	Para un ATS, el **ID registro ATS se genera automáticamente. Este** identifica inequívocamente a la central ante el RCT. Si no conoce el **Código abonado SPT**, puede poner en servicio la central empleando este **ID registro ATS**. El operador del CMS también deberá introducir este **ID registro ATS** en el RCT (p. ej. SPC Com XT. Consulte el *Manual de instalación y configuración del SPC Com XT*).

T. exc. polling ATS	Este campo se calcula automáticamente añadiendo los valores de la columna **Tiempo excedido polling activo** de la Tabla secuencia incidencias; es decir, para todas las APS de un ATS. Puede sobrescribir este campo manualmente. Por ejemplo, CAT 2 [Módem] posee un **Tiempo excedido polling activo** de 24 horas 10 minutos (87000 segundos). Para permitir que el tiempo de reacción sea más corto, introduzca un valor más bajo.
Tiempo excedido TX incid. ATS	Periodo de tiempo desde que se ha producido una incidencia sin que se haya transmitido con éxito antes de que el ATS abandone. Por defecto: 300 segundos.
Generar FTC	Seleccione si el sistema debe generar un DTC al excederse el tiempo de incidencia de ATS.
Reencolar incidencias	Seleccione esta opción para reencolar incidencias tras alcanzar el tiempo excedido de ATS.
Reencolar retardo incidencias	Retardo tras excederse tiempo ATS antes de que el reencolado de incidencias se intente de nuevo Por defecto: 300 segundos.
Duración reencolado de incidencias	Incremento de tiempo en que las incidencias serán reencoladas antes de su borrado. Por defecto: 86400 segundos.

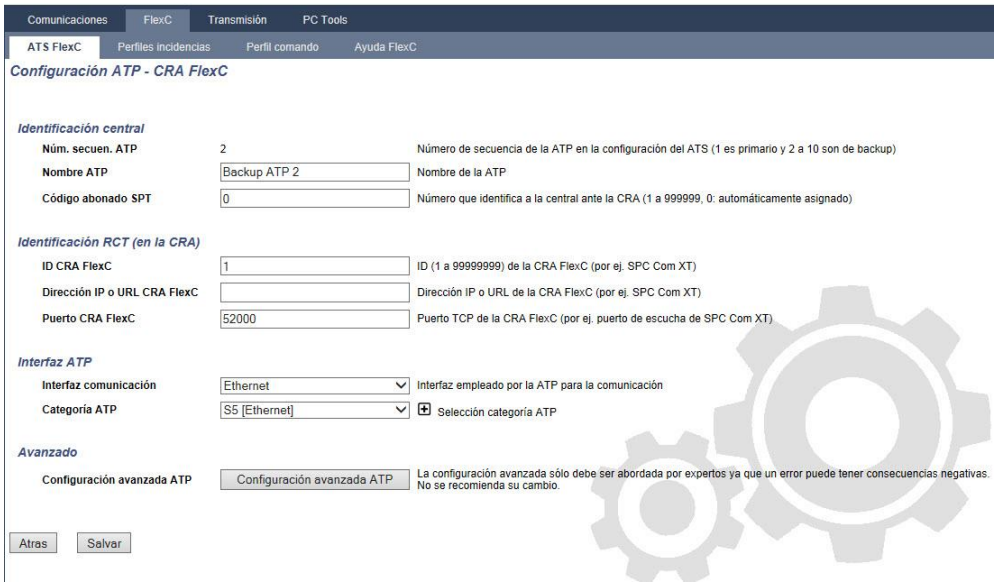
Ver también

Tiempos de categoría ATS [→ 384]

17.10.2.2.1 Nueva ATP en CRA FlexC

Nueva ATP en CRA FlexC le permite configurar una ATP entre la central SPC y la CRA (p. ej. SPC Com XT) Puede configurar hasta 10 ATPs para cada ATS.

1. Haga clic en el botón **Nueva ATP en CRA FlexC**.



1. Complete los campos de la ATP descritos en la tabla de abajo.
2. En caso necesario haga clic en **Configuración avanzada ATP**, por ejemplo, si está utilizando encriptación automática, puede opcionalmente introducir una clave en el campo **Clave encriptación**. Consulte Configuración avanzada ATP. [→ 296].
3. Haga clic en **Salvar**.

	⚠ ADVERTENCIA No se recomienda cambiar la **Configuración avanzada ATP**. Cualquier cambio solamente debe ser realizado por usuarios expertos.

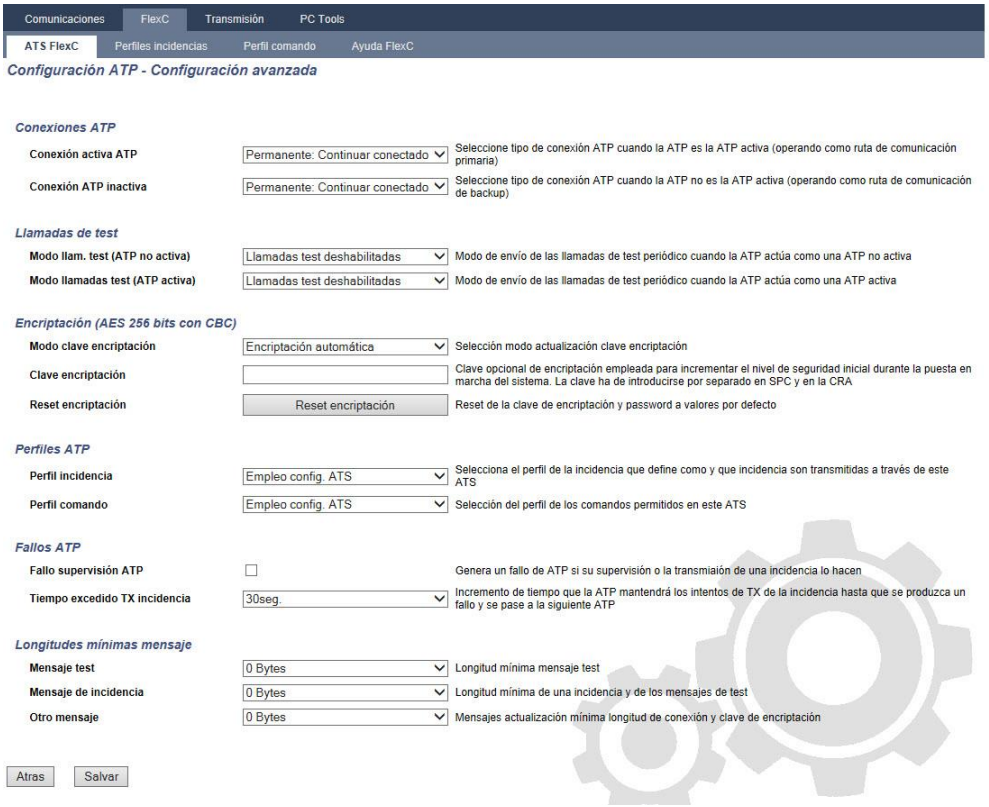
Identificación central	
Núm. secuen. ATP	Este campo muestra el número de secuencia de la ATP en la configuración ATS. La número 1 es la primaria, los números del 2 al 10 son las de backup.
ID ATP	Cuando se guarda una ATP, el sistema asigna un ID único a una ATP. Este es el ID exclusivo de la ATP, de manera que puede ser reconocida por el RCT.
Nombre ATP	Introduzca un nombre para la ATP.
Código abonado SPT	Introduzca un número para identificar de manera inequívoca la central ante el RCT.
Identificación RCT (en la CRA)	
ID CRA FlexC	Introduzca el número que identifica al RCT (por ejemplo, SPC Com XT) de manera inequívoca ante la central. Este debe coincidir con el número introducido en el campo **ID CRA FlexC Servidor** del gestor de configuración del servidor SPC Com XT.
Dirección IP o URL CRA FlexC	Introduzca la URL o la dirección IP de la CRA (por ejemplo, SPC Com XT).
Puerto CRA FlexC	Introduzca el puerto TCP que el RCT (p. ej. SPC Com XT) está escuchando. Por defecto es el 52000. Este debe coincidir con el valor del campo **Puerto FlexC Servidor** del gestor de configuración del servidor. Consulte el *Manual de instalación y*

	configuración del SPC Com XT.
Interfaz ATP	
Interfaz de comunicaciones	Del menú desplegable, seleccione la interfaz que emplea esta ATP para la comunicación. ● Ethernet ● GPRS Transmisor 1 ● GPRS Transmisor 2 ● Comunicación WAN Transmisor 1 ● Comunicación WAN Transmisor 2
Categoría ATP	Seleccione la categoría a aplicar a esta ATP. Para más información sobre las categorías ATP, consulte Tiempos categoría ATP [→ 385].
Avanzado	
Configuración avanzada ATP	No se recomienda cambiar la configuración avanzada. Cualquier cambio solamente debe ser realizado por usuarios expertos.

17.10.2.2.1.1 Configuración avanzada ATP.

	⚠ ADVERTENCIA
	No se recomienda cambiar la Configuración avanzada ATP. Cualquier cambio solamente debe ser realizado por usuarios expertos.

1. Haga clic en el botón **Configuración avanzada ATP**.



1. Configure los campos tal como se describe en la siguiente tabla.

2. Haga clic en **Salvar**.

Conexiones ATP	
Conexión activa ATP	Seleccione el tipo de conexión ATP cuando la ATP funciona como la ruta de comunicación primaria. ● Permanente: Continuar conectado ● Temporal: Fin TX 1 seg. ● Temporal: Fin TX 20 seg. ● Temporal: Fin TX 80 seg. ● Temporal: Fin TX 3 minutos ● Temporal: Fin TX 10 minutos ● Temporal: Fin TX 30 minutos
Conexión ATP inactiva	Seleccione el tipo de conexión ATP cuando la ATP funciona como ruta de comunicación de backup. ● Permanente: Continuar conectado ● Temporal: Fin TX 1 seg. ● Temporal: Fin TX 20 seg. ● Temporal: Fin TX 80 seg. ● Temporal: Fin TX 3 minutos ● Temporal: Fin TX 10 minutos ● Temporal: Fin TX 30 minutos
Llamadas de test	
Modo llam. test (ATP no activa)	Seleccione el modo para el envío de llamadas de test cuando la ATP es la ATP no activa. ● Llamadas test deshabilitadas ● Llamada test cada 10 minutos ● Llamada test cada hora ● Llamada test cada 4 horas ● Llamada test cada 24 horas ● Llamada test cada 48 horas ● Llamada test cada 7 días ● Llamada test cada 30 días
Modo llamadas test (ATP activa)	Seleccione el modo para el envío de llamadas de test cuando la ATP es la ATP activa. ● Llamadas test deshabilitadas ● Llamada test cada 10 minutos ● Llamada test cada hora ● Llamada test cada 4 horas ● Llamada test cada 24 horas ● Llamada test cada 48 horas ● Llamada test cada 7 días Llamada test cada 30 días
Encriptación (AES 256 bits con CBC))	
Modo clave encriptación	Seleccionar el modo de actualización de la clave de encriptación. ● Encriptación automática ● Encriptación automática con actualizaciones ● Encriptación fija

	Nota: La encriptación automática utiliza la clave po17.6.4r defecto y la actualiza una vez. La encriptación automática cambia la clave de encriptación cada 50 000 mensajes o una vez a la semana, lo primero que se produzca.
Clave encriptación	Clave de encriptación empleada para incrementar el nivel de seguridad inicial durante la puesta en marcha de la ATP. La clave ha de introducirse por separado en el SPT o en la RCT.
Reset encriptación	Reset de la clave de encriptación y contraseña a los valores por defecto.
Perfiles ATP	
Perfil incidencia	Seleccione el perfil de la incidencia que define cómo y qué incidencia son transmitidas a través de este ATS ● Empleo config. ATS ● Perfil incidencia por defecto ● Todas las incidencias
Perfil comando	Seleccione el perfil de los comandos permitidos en este ATS. ● Empleo config. ATS ● Perfil comando por defecto ● Perfil comando a medida
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.
T.reint.TX IP	Incremento de tiempo que la ATP mantendrá los intentos de TX de la incidencia hasta que se produzca un fallo y se pase a la siguiente ATP. ● 30 seg. ● 60 seg. ● 90 seg. ● 2 minutos ● 3 minutos ● 5 minutos ● 10 minutos
Longitudes mínimas mensaje	
Mensaje test	Longitud mínima mensaje test. ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes
Mensaje de incidencia	Longitud mínima de una incidencia y de los mensajes de test. ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes

Otro mensaje	Mensajes actualización mínima longitud de conexión y clave de encriptación. ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes

17.10.2.2.2 Nueva ATP en CRA analógica

Si falla una conexión entre la central SPC y la CRA (p. ej. SPC Com XT), FlexC tiene la capacidad de conmutar a una conexión de ATP de backup entre la central SPC y la CRA analógica. Se puede configurar hasta 10 ATP para cada ATS.

1. Para configurar una ATP entre una central SPC y una CRA analógica, haga clic en el botón **Nueva ATP en CRA analógica**.
2. Complete los campos de la ATP descritos en la tabla de abajo.
3. Haga clic en **Salvar**.

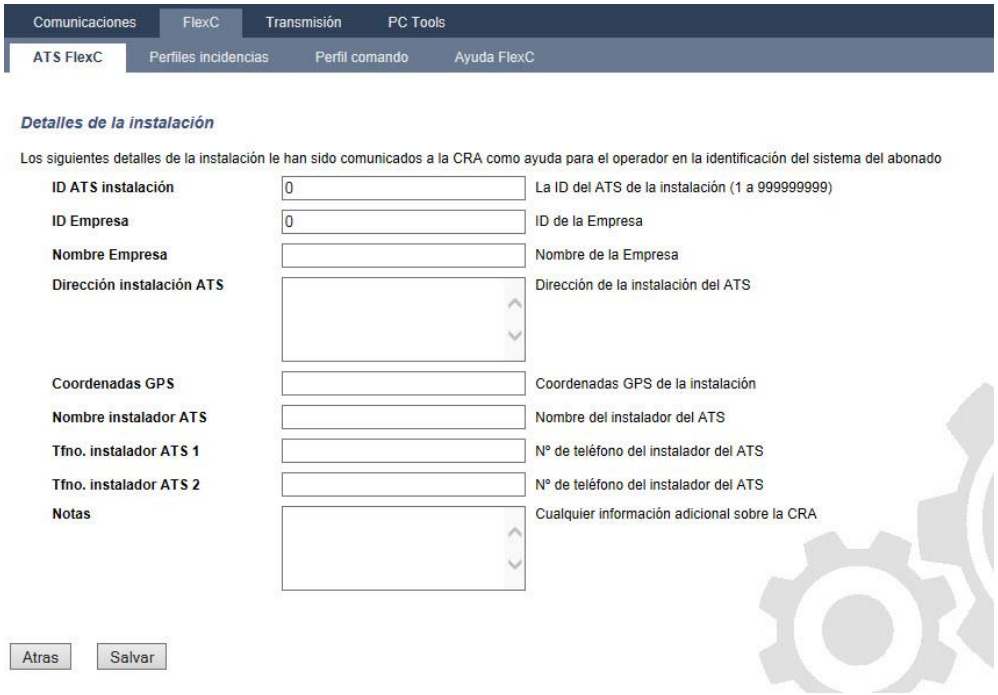
Identificación central	
Núm. secuen. ATP	Este campo muestra el número de secuencia de la ATP en la configuración ATS. La número 1 es la primaria, los números del 2 al 10 son las de backup.
ID ATP	Este ID identifica la ATP de manera inequívoca ante la CRA
Nombre ATP	Introduzca un nombre para la ATP.
Código abonado SPT	Introduzca un número para identificar de manera inequívoca la central ante la CRA (1 - 999999)
Conexión CRA	
Número 1	Número teléfono 1
Número 2	Número de teléfono 2
Seleccionar transmisor	Selección del transmisor a usar ● Transmisor 1 ● Transmisor 2
Llamadas de test	
Modo llam. test (ATP no activa)	Seleccione el modo de envío de llamadas de test cuando la ATP se encuentra en modo no activa. Por defecto: 24 horas. ● Llamadas test deshabilitadas ● Llamada test cada 10 minutos ● Llamada test cada hora ● Llamada test cada 24 horas ● Llamada test cada 48 horas ● Llamada test cada 7 días ● Llamada test cada 30 días.
Modo llamadas test (ATP activa)	Seleccione el modo para el envío de llamadas de test cuando la ATP es una ATP activa. Por defecto: 24 horas. ● Llamadas test deshabilitadas ● Llamada test cada 10 minutos ● Llamada test cada hora ● Llamada test cada 24 horas ● Llamada test cada 48 horas

	● Llamada test cada 7 días ● Llamada test cada 30 días.
Hora primera llamada de test	Hora de la primera llamadade test tras un reset o inicialización del ATS. ● Envío inmediato (predeterminado) ● o bien ● Seleccione un intervalo de media hora entre 00:00 y 23:30
Protocolo incidencia	
Protocolo	Protocolo usado en comunicación ● SIA ● SIA extendido 1 ● SIA extendido 2 ● Contact ID
Perfil incidencia	Seleccione el perfil de la incidencia que define cómo y qué incidencia son transmitidas a través de este ATS ● Empleo config. ATS ● Perfil incidencia por defecto ● Perfil incidencia portal por defecto ● Todas las incidencias ● Perfil incidencia 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.
T.reint.TX IP	Incremento de tiempo que la ATP mantendrá los intentos de TX de la incidencia hasta que se produzca un fallo y se pase a la siguiente ATP. Por defecto: 2 minutos ● 30 seg. ● 60 seg. ● 90 seg. ● 2 minutos ● 3 minutos ● 5 minutos ● 10 minutos

17.10.2.2.3 Editar detalles de la instalación

Los detalles de la instalación se pasan al RCT para ayudar al operador a identificar la central.

1. Haga clic en el botón **Editar detalles Instalación**.



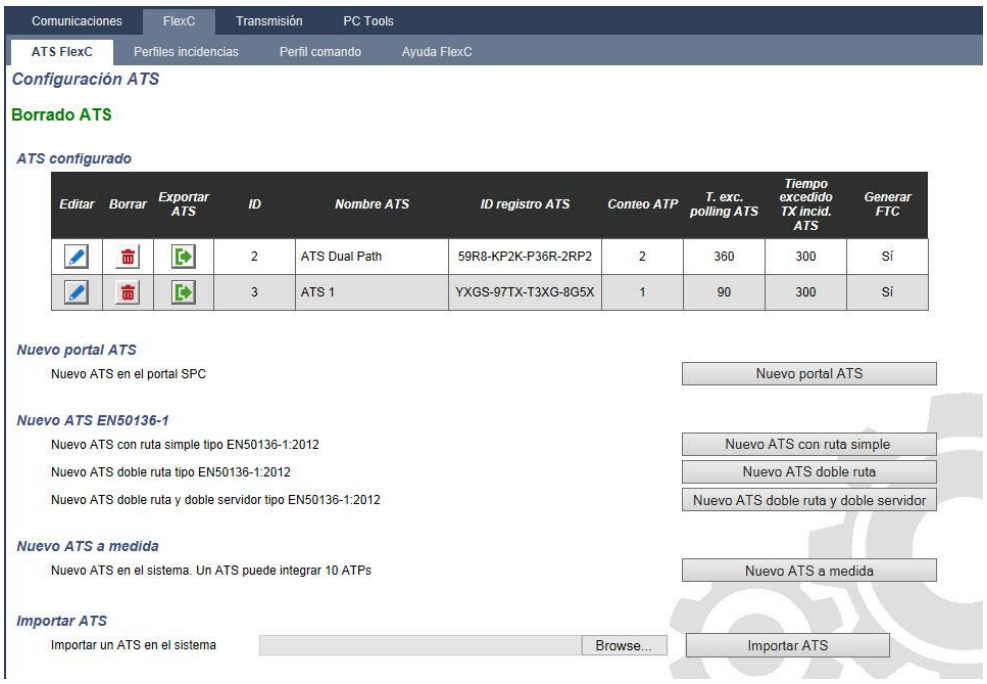
1. Complete los campos de la tabla inferior.
2. Haga clic en **Salvar**.

ID ATS instalación	La ID del ATS de la instalación (1 a 999999999).
ID de la compañía	ID de la compañía (1 - 99999999).
Nombre Empresa	Nombre de la empresa.
Dirección instalación ATS	La dirección de la instalación ATS.
Coordenadas GPS	Las coordenadas GPS de la instalación.
Nombre instalador ATS	El nombre del instalador del ATS.
Tfno. instalador número 1	Nº de teléfono del instalador del ATS.
Tfno. instalador número 2	Nº de teléfono del instalador del ATS.
Notas	Cualquier información adicional sobre el RCT.

17.10.2.4 Exportación e importación de un ATS

Los archivos ATS poseen una extensión .cxml. Deberá crear un ATS en el navegador SPC y exportarlo antes de poderlo importar a un sistema.

1. Para exportar un ATS, vaya a **Comunicaciones- FlexC - ATS FlexC**.
2. En la tabla **ATS configurado**, localice el ATS que se desea exportar y haga clic en el botón **Exportar ATS** (flecha verde).



3. Guarde 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 en el sistema, vaya a **Comunicaciones - FlexC - ATS FlexC**.
6. Bajar hasta **Importar ATS**.
7. Haga clic en el botón **Browse** y seleccione un ATS para importar (extensión de archivo .cxml).
8. Haga clic en **Importar ATS**.

⇨ El ATS se muestra en la tabla **ATS configurado** con el siguiente ID disponible.

!	Cuando se exporta un ATS, el Código abonado SPT cambia a 0. Con esto se evita que un ATS sea exportado y después importado replicando cualquier ATS existente.

17.10.2.5 Configuración de perfiles de incidencias

El perfil de incidencia define qué incidencias serán transmitidas a un ATS, el estado de informe para una incidencia y las excepciones de incidencia. Las excepciones de incidencia le permiten modificar los valores por defecto de las incidencias por otros valores personalizados. Para obtener más información, consulte Definición excepción incidencia [→ 305].

!	*AVISO*
	Para ver una lista con todas las incidencias, vaya a **Comunicaciones - FlexC - Perfiles incidencias.** Haga clic en **Editar** (lápiz azul) para un perfil de incidencia. Desplácese hasta el final de la pantalla y haga clic en **Ver tabla completa incid.**.

!	*AVISO*
	Para crear rápidamente un nuevo perfil de incidencia, vaya a **Comunicaciones- FlexC - Perfiles de incidencia**. En la tabla **Perfiles incidencias** seleccione un perfil de incidencia y haga clic en el botón editar (lápiz azul). Desplácese hasta la parte inferior de la pantalla y haga clic en **Copiar.** Ahora puede hacer los cambios que requiera.

1. Para configurar los perfiles de incidencias FlexC paso a paso, vaya a **Comunicaciones- FlexC - Perfiles incidencias**.
2. Haga clic en **Añadir**. La ventana **Perfiles incidencias** muestra.

1. Introduzca un **Nombre** para identificar el perfil de incidencia.
2. Seleccione los grupos de filtro de incidencia con los que se van a crear los informes para este perfil marcando las casillas **TX incidencia**.
3. Para evitar informar de ciertas incidencias o de direcciones dentro de una incidencia, seleccione la incidencia de la correspondiente lista desplegable **Nueva excepción incidencias**.
4. Haga clic en **Añadir** para visualizar la pantalla **Definición excepción incidencia**. Véase Definición excepción incidencia [→ 305].
5. Para aplicar un perfil de incidencia a una partición, seleccione la partición en **Filtro partición**.

6. Haga clic en **Salvar** y **Atrás**. El nuevo perfil se muestra en la tabla **Perfiles incidencias** .

Puede ver una lista de todas las excepciones de incidencia para un perfil de incidencia en **Excepciones incidencia**, en la pantalla **Perfiles incidencias**.

	AVISO
	No puede borrar el **perfil incidencia por defecto, el perfil incidencia portal por defecto** ni cualquier perfil de incidencia que esté asignado a un ATS. Si intenta borrar un perfil de incidencia que esté en uso, se le mostrará un mensaje de error.

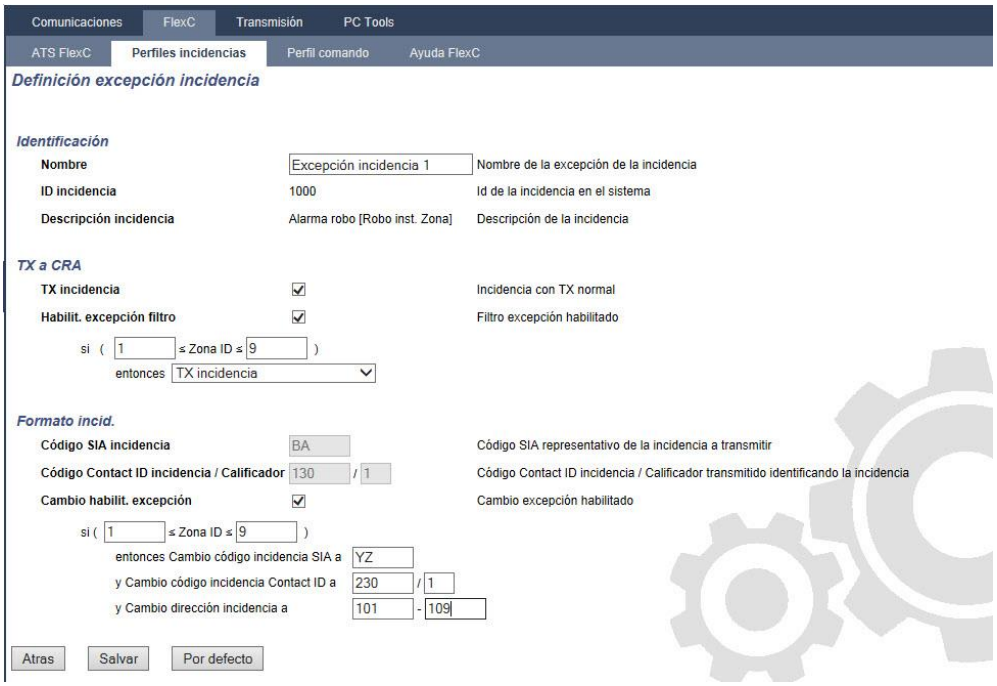
17.10.2.4.1 Definición excepción incidencia

Las excepciones de incidencia le permiten modificar la siguiente configuración para un rango de direcciones dentro de una incidencia:

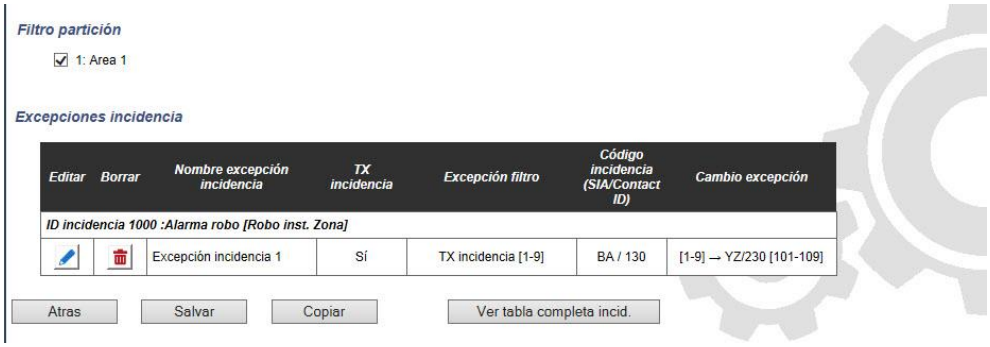
- TX incidencia
- Código SIA
- Código CID
- Dirección incidencia (p. ej. IDs de zona, IDs de partición, IDs de usuario)

Por ejemplo, en el Grupo filtro **Alarmas intrusión** puede definir una excepción de incidencia para un rango de IDs de zona en la incidencia Alarma robo (BA) de la siguiente manera:

- No informe de incidencias BA para la ID de zona 1 a 9
- Modifique el código SIA desde BA hasta YZ
- Modifique el CID desde 130 / 1 hasta 230 / 1
- Modifique el ID zona 1 - 9 a ID zona 101 - 109



1. Para configurar una **Definición excepción incidencia**, complete los campos descritos en la tabla de abajo.
2. Haga clic en **Salvar**.
3. Haga clic en **Atrás** para regresar a la pantalla **Perfiles incidencias**.
   ⇨ El nombre de cada excepción se muestra en la tabla **Excepciones incidencia** en la parte inferior de la pantalla. La tabla muestra los ajustes para los campos **TX incidencia**, **Excepción filtro**, **Código incidencia (SIA/Contact ID)** y **Cambio excepción** de la incidencia.



1. Haga clic en el icono de **Editar** para realizar cambios o en el icono **Borrar** para eliminar una **Excepción incidencia**.
2. Para aplicar el perfil de incidencia a una partición, marque la casilla de la partición.
3. Haga clic en **Salvar** para guardar el perfil de incidencia.
4. Haga clic en **Atrás** para ver el perfil en la tabla **Perfiles incidencias**.

Identificación	
Nombre	Introduzca el nombre de la excepción de incidencia.
ID incidencia	ID de la incidencia en el sistema Esta solamente se visualiza.
Descripción incidencia	Descripción de la incidencia. Esta solamente se visualiza.
TX a CRA	
TX incidencia	Seleccionar para informar de la incidencia Esto prevalece sobre el valor de informe ajustado para el Grupo filtro de incidencia. Por ejemplo, si el Grupo filtro **Alarmas intrusión** se configura para informar, puede excluir la incidencia BA deshabilitando este ajuste.
Habilit. excepción filtro	Seleccionar para excluir un rango de direcciones, por ejemplo IDs de zona, del campo **TX incidencia**.
si (0 ≤ *ID zona* ≤ 9999) entonces TX incidencia/No comunicar incidencia	Introduzca un rango de direcciones para excluirlas de la configuración **TX incidencia**. Por ejemplo, si decide informar sobre el tipo de evento BA, puede elegir no informar sobre las *ID de zona 1 - 9* para dicho evento. Alternativamente, si decide no informar sobre el tipo de incidencia BA, puede elegir informar la *ID de zona 1- 9* para dicha incidencia.
Formato incid.	
Código SIA incidencia	Código SIA de incidencia por defecto que se transmite para representar la incidencia. Este campo solo se puede visualizar.

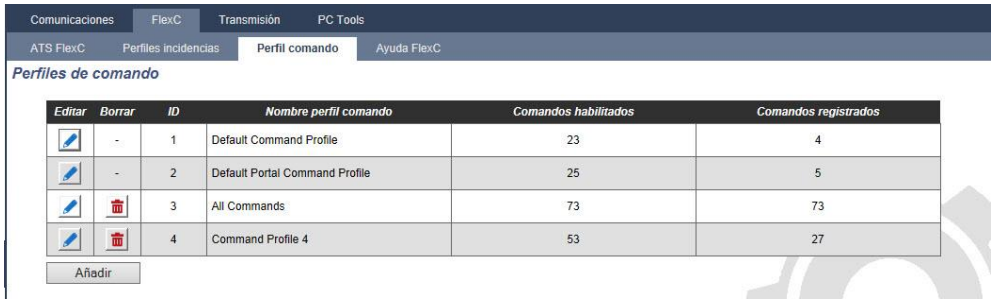
Código Contact ID incidencia / Calificador	Código Contact ID incidencia / Calificador transmitido identificando la incidencia predeterminado. Este campo solo se puede visualizar.
Cambio habilit. excepción	Seleccione para cambiar el SIA por defecto, código CID/calificador y la dirección de evento para modificar a medida los valores, por ejemplo, para cambiar *ID zona 1 - 9* a *ID zona 101 - 109*. Si está habilitado, los campos de abajo muestran.
si (0 ≤ *ID zona* ≤ 9999)	Introduzca el rango de direcciones a cambiar para una incidencia, por ejemplo, si desea cambiar *ID zona 1 - 9* a *ID zona 101 - 109*, introduzca *1* y *9*. La cantidad de direcciones del rango debe ser la misma que la cantidad de direcciones definidas en el campo mostrado abajo**Cambio dirección incidencia a**.
entonces, Cambio código incidencia SIA a BA	Cambie el código SIA por defecto a un código SIA personalizado.
y Cambio código incidencia Contact ID a	Cambie el Código Contact ID incidencia/calificador por defecto a un Código Contact ID incidencia/cualificador a medida.
y Cambio dirección incidencia a	Introduzca el nuevo rango de direcciones, por ejemplo, si está cambiando *ID zona 1 - 9* a *ID zona 101 - 109*, introduzca *101 y 109*.

17.10.2.6 Configuración de perfiles de comando

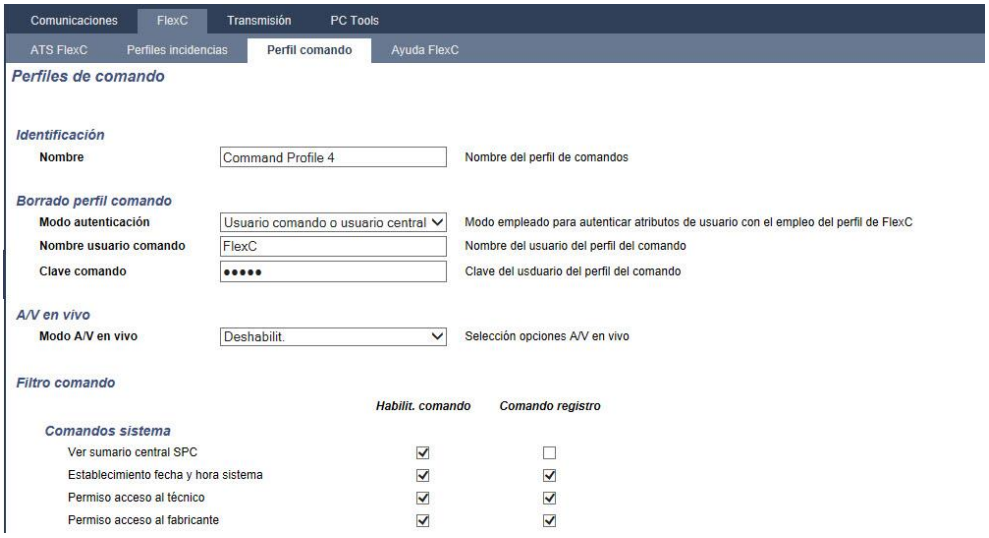
El perfil de comando define los comandos que están permitidos en un ATS. Este perfil determina cómo un CMS puede controlar una central. El perfil de comando no es compatible con la verificación de vídeo.

!	*AVISO*
	Para crear rápidamente un nuevo perfil de comando, vaya a **Comunicaciones-FlexC - Perfiles de comando**. En la tabla **Perfiles de comando**, seleccione un perfil de comando y haga clic en el botón editar (lápiz azul), desplácese hasta la parte inferior de la pantalla y haga clic en **Copiar**. Ahora puede hacer los cambios que requiera.

- Para añadir un perfil de comando paso a paso, vaya a **Comunicaciones - FlexC - Perfiles de comando**.



- Haga clic en **Añadir**.



1. Introduzca un **Nombre** para identificar el perfil de comando.
2. Seleccione un **Modo autenticación** (Usuario comando o usuario central, Sólo usuario comando, o Cualquier usuario sistema) del menú desplegable.

!	*AVISO*
	El **Nombre usuario comando** por defecto proporciona un usuario que, con rapidez y facilidad, habilita el control de la central desde el SPC Com XT. Ofrece un amplio rango de comandos. Por ejemplo, el usuario de comando por defecto puede ajustar todas las particiones o controlar todas las zonas. Para un control más estricto, por ejemplo para permitir solamente el ajuste de ciertas áreas, puede ajustar un perfil de comando personalizado con un juego de permisos definido. No puede borrar el **Perfil comando por defecto**,el **Perfil comando portal por defecto** ni un perfil de comando que esté asignado a un ATS.

3. Introduzca el nombre el usuario del perfil de comando en el campo **Nombre usuario comando**. Este debe coincidir con el campo **Nombre usuario autenticación** del SPC Com XT.
4. Introduzca la clave del usuario de perfil de comando en el campo **Clave comando**. Esta debe coincidir con el campo de **Código de usuario o contraseña de** autenticación en SPC Com XT.
5. Seleccione **Modo A/V en vivo** (Deshabilitar, Sólo tras incidencia de alarma, siempre disponible, Sistema en armado total) para determinar las opciones de privacidad del flujo. **Siempre disponible** genera el mayor volumen de datos.
6. En **Filtro comando**, seleccione los comandos para habilitar. Para una lista completa de comandos, véase Comandos FlexC [→ 383].
7. Seleccione los comandos a registrar.
8. Haga clic en **Salvar**.
9. Haga clic en **Atrás** para visualizar el perfil de comando en la tabla **Perfiles de comando**.
10. Para cambiar un perfil de comando haga clic en el botón **editar** (icono del lápiz) próximo a un perfil de comando.

17.10.3 Transmisión

17.10.3.1 CRAs

La central SPC ofrece la posibilidad de comunicar información a una estación receptora remota cuando tiene lugar una incidencia de alarma específica.

Estas CRAs se deben configurar en la central para permitir el funcionamiento de esta comunicación remota.

17.10.3.1.1 Añadir/editar una CRA utilizando SIA o CID

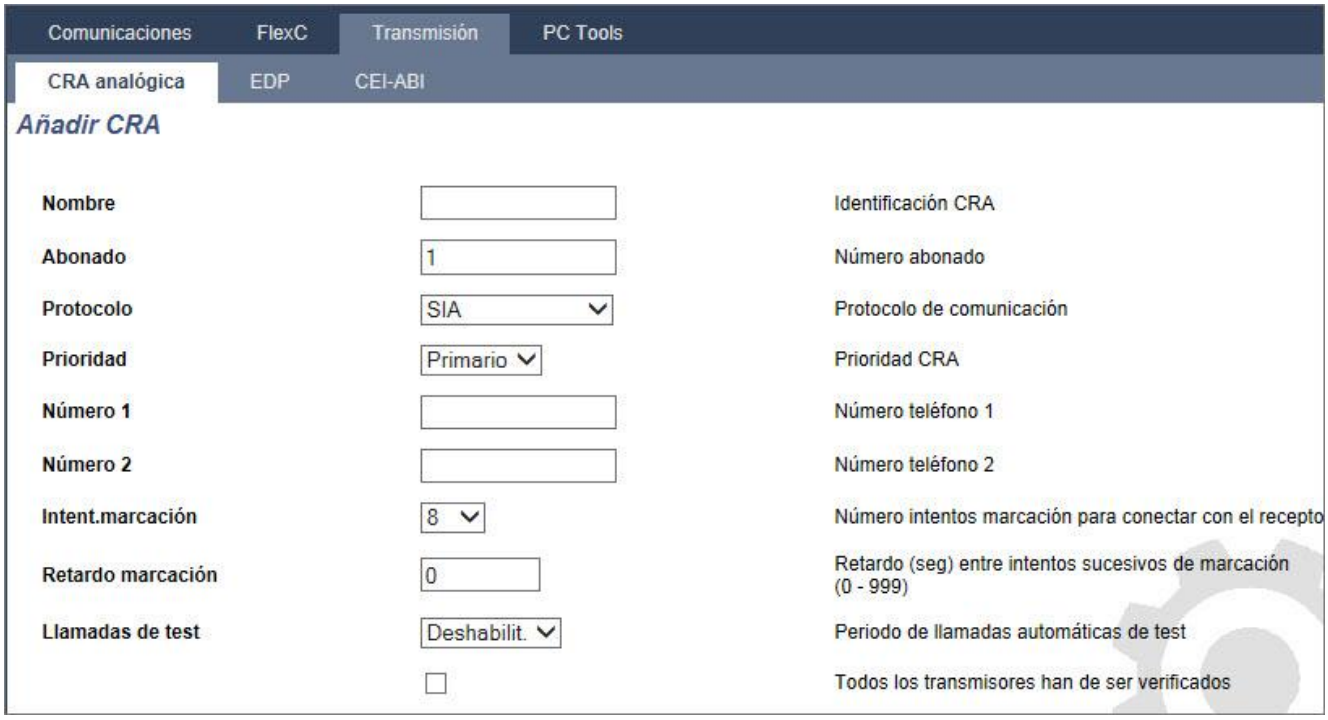
▷ Debe haber un módem RTB o GSM instalado y funcionando correctamente.

1. Seleccione **Comunicaciones > Transmisión > CRA analógica**.

   ⇨ Se mostrará la siguiente ventana:

2. Haga clic en el botón **Transm. 1/2** para hacer una llamada de test a la CRA desde el módem 1 o desde el módem 2.
3. Haga clic en el botón **Reg** para recibir un archivo de registro. Se mostrará una ventana 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 en **Editar**.

   ⇨ Se mostrará la siguiente ventana.
5. Configure los campos tal como se describe en la siguiente tabla.



Descripción	Introduzca una descripción de la CRA remota.
Abonado	Introduzca su número de abonado. Esta información debería estar disponible desde la estación receptora y se utiliza para identificarle cada vez que realiza una llamada a la CRA. Para una cuenta de Contact ID se permite un máximo de 6 caracteres.
Protocolo	Introduzca el protocolo de comunicación que se utilizará (SIA, SIA Extendido, Contact ID, Formato rápido). Nota: El SPC es compatible con el protocolo SIA extendido. Seleccione este protocolo para poder ver descripciones de texto adicionales de las incidencias SIA que se estén enviando a la CRA.
Prioridad	Seleccione la prioridad para la CRA en términos de informes principales o de copia de seguridad.
Número 1	Introduzca el primer número que se debe marcar para contactar con la CRA. El sistema siempre intentará contactar con la CRA en este número antes de probar con otro número.
Número 2	Introduzca el segundo número que se debe marcar para contactar con la CRA. El sistema sólo intentará contactar con la CRA en este número si el primer número de contacto no pudo establecer con éxito una llamada.
Intentos de marcación	Introduzca el número de veces que el sistema intentará realizar una llamada al receptor. (por defecto, 8)
Retardo marcación RTPC	Retardo en segundos entre intentos de marcación fallidos (0 - 999)
Intervalo marcación	Introduzca el número de segundos entre intentos de marcación fallidos. (0 - 999)
Llamadas de test	Habilite la llamada de test eligiendo un intervalo de tiempo. De esta forma, se enviará una llamada automática de prueba desde el módem 1 a la CRA primaria.
Comprobar TX	Marque esta casilla si desea iniciar también una llamada automática de test desde el módem 2 a la CRA de backup.

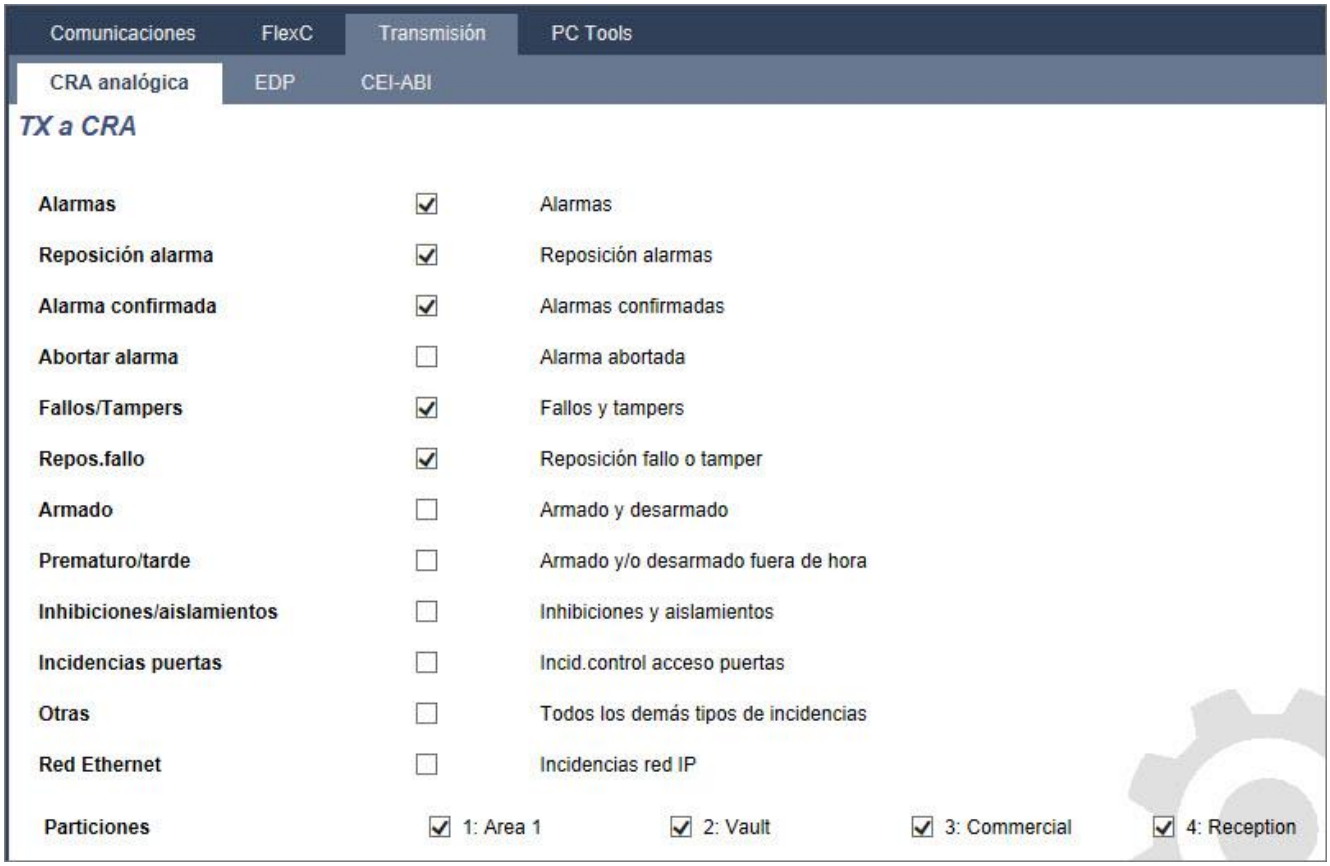
- Haga clic en el botón **Añadir** para introducir estos detalles en el sistema.
  - ⇨ Se mostrará una lista de los abonados de la CRA configurados en la pantalla del navegador junto con la información del abonado, descripción,

protocolo, estado de marcación y fecha y hora de la última llamada a la CRA.

17.10.3.1.2 Edición de un filtro CRA utilizando SIA o CID

Para configurar las incidencias del SPC que activará la llamada a la CRA:

1. Seleccione **Comunicaciones- Transmisión - CRA analógica - Editar - Filtro**.
   ⇨ Se mostrará la siguiente ventana:



2. Configure los siguientes campos:

Marque alguna de las siguientes casillas si desea iniciar una llamada remota a la CRA para notificarle una incidencia en particular.

Alarmas	Las alarmas están activadas.
Repos.alarma	Las alarmas del sistema están restauradas.
Alarmas confirmadas	Alarmas confirmadas
Abortar alarma	Incidencias de Alarma abortada. Las alarmas se abortan tras introducir un código de usuario válido a través del teclado tras una alarma confirmada o sin confirmar.
Fallos	Los fallos y tampers están activados.
Reposiciones de fallos	Se han restaurado las alarmas de fallo o tamper.
Configuración	El sistema está armado y desarmado.
Prem./tarde	Armado y desarmado no programados del sistema.
Inhib./Aisl.	Se ejecutan operaciones de inhibición y aislamiento en el sistema.
Incidencias puerta	Las incidencias de puertas están activadas. Sólo funciona con protocolo SIA.
Otras	Todos los demás tipos de incidencias se detectan en el sistema.

Red	Incidencias red IP
Particiones	Seleccione particiones específicas para las que son aplicables las incidencias arriba indicadas.

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.

17.10.3.1.3 Edición de un filtro de CRA utilizando el formato rápido

Para configurar las incidencias en el SPC que ejecutarán la llamada a la CRA cuando el protocolo seleccionado es **Formato rápido**:

- Seleccione **Comunicaciones- Transmisión - CRA analógica - Editar - Filtro**.

1. Se muestra una lista de los ocho canales junto con las condiciones de alarma que se pueden programar para cada canal. Seleccione para cada canal las condiciones de alarma según se requiera. Para ver una descripción de cada una de ellas, consulte Tipos de salida y puertos de salida [→ 211].
2. En el menú desplegable **Vista** seleccione **Sistema** o un área específica para aplicar su configuración seleccionada.
3. Haga clic en el botón **Test** próximo al primer canal para probar la activación de alarma.
   ⇨ Se enciende el icono de la bombilla.
4. Espere aproximadamente cinco segundos y haga clic de nuevo en el botón **Test** del mismo canal. Esto envía una señal de restauración de canal a la CRA y el icono de la bombilla se apaga.
5. Prosiga probando los demás canales.

17.10.3.2 Configuración EDP

IP

El sistema ofrece la posibilidad de transmitir información al servidor Com del SPC de forma remota utilizando el propio protocolo de Vanderbilt, el Protocolo de datagrama mejorado (EDP - **E**nhanced **D**atagram **P**rotocol). Configurando correctamente el receptor EDP en el sistema, puede programarse para realizar llamadas de datos automáticamente al servidor Com del SPC 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 al servidor remoto a través de las rutas siguientes:

- **RTB** (se necesita un modem RTB)
- **GSM** (se necesita un módem GSM)
- **Internet** (interfaz Ethernet)

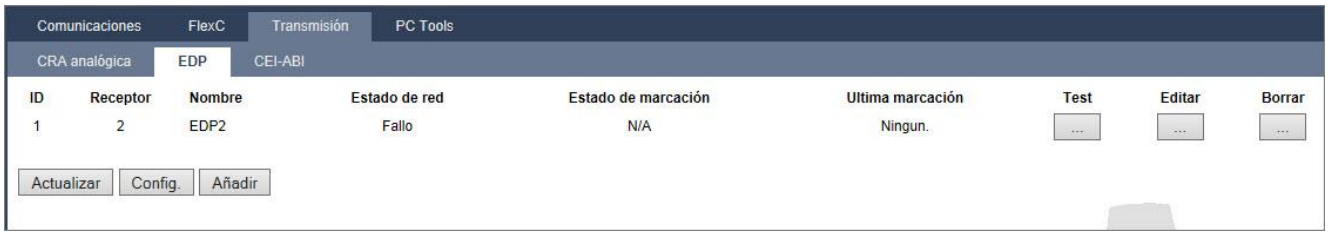
Si utiliza una red RTB, asegúrese de que el módem RTB esté instalado de forma adecuada y funcione correctamente, y de que haya una línea RTB conectada a los terminales A y B en el módem RTB.

Si utiliza una red GSM, asegúrese de que haya un módulo GSM instalado de forma adecuada y funcionando correctamente. Se puede establecer una conexión IP en Internet con un servidor mediante una dirección IP fija pública.

Si se necesita una conexión IP, asegúrese de que la interfaz Ethernet esté configurada correctamente (consulte la página [→ 169]) y de que el acceso a Internet esté habilitado en el router.

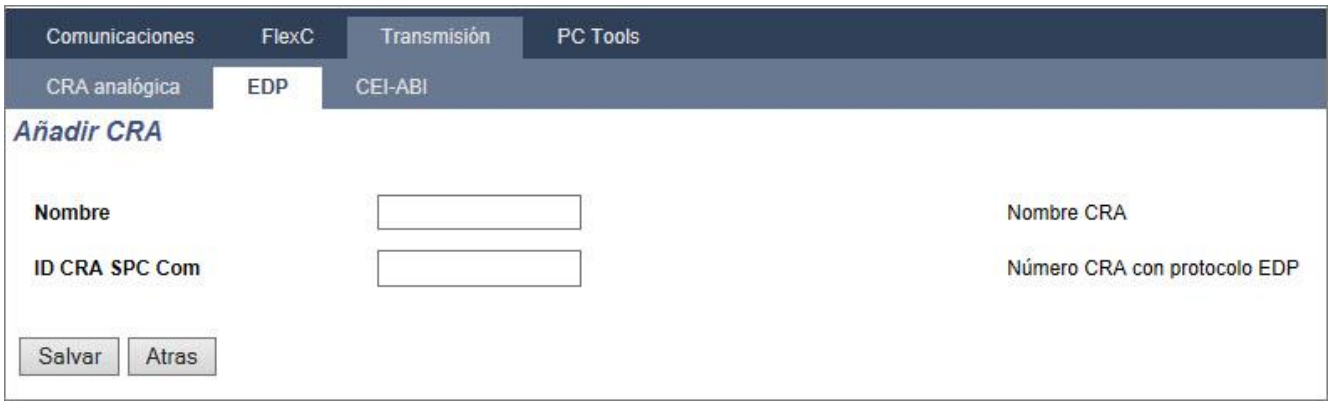
17.10.3.2.1 Agregar un receptor EDP

1. Seleccione **Comunicaciones > Transmisión > EDP**.
   ⇨ Se mostrará la siguiente ventana:



Máx. 8 receptores pueden agregarse al sistema SPC.

2. Haga clic en el botón **Añadir**.
   ⇨ Se mostrará la siguiente ventana.
3. Consulte la tabla a continuación para obtener más información.



Descripción	Introduzca una descripción de texto de la CRA.
ID CRA	Introduzca un número exclusivo que utilizará el EDP para identificar a la CRA.

Ver también

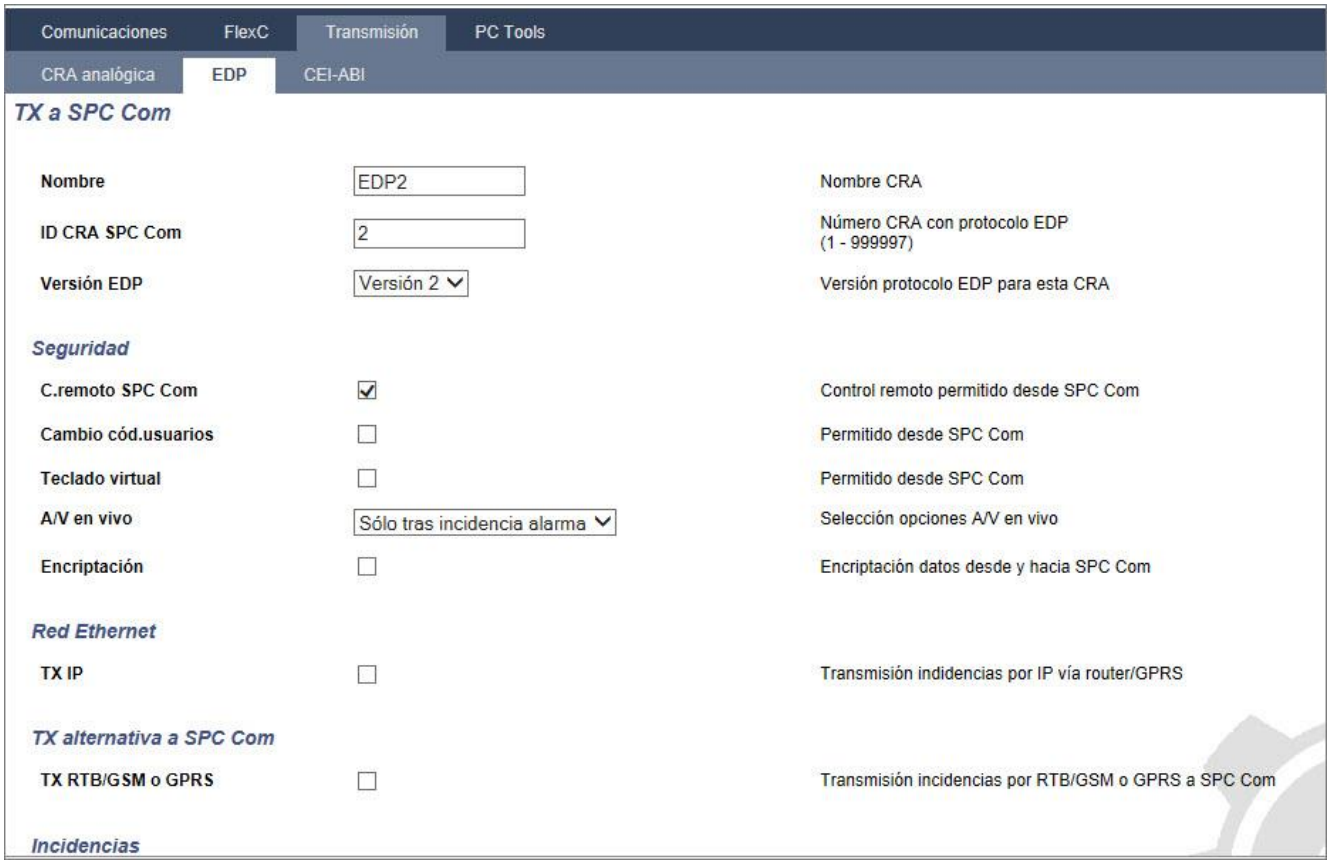
Editar config. CRA EDP [→ 313]

17.10.3.2.2 Editar config. CRA EDP

1. Seleccione **Comunicaciones > Transmisión> EDP > Editar**.

⇨ Se mostrará la siguiente ventana.

2. Configure los campos tal como se describe en la siguiente tabla.



Descripción	Edite el nombre del receptor EDP. Utilice 16 caracteres como máximo.
ID CRA SPC Com	Edite el ID CRA SPC Com del EDP. El rango va del 1 al 999997 (999998 y 999999 están reservados para fines especiales).
Versión EDP	Seleccione la versión de protocolo EDP para utilizar con este receptor EDP. Las opciones son Versión 1 o Versión 2. Se recomienda la versión 2, siempre que sea compatible con el receptor, pues 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 el receptor acepte comandos.
Cambio Cód.usuarios	Marque esta casilla para permitir cambiar los códigos de usuario desde una ubicación remota. Esta función solo es aplicable si los

	comandos están habilitados desde el receptor.
Encriptación	Marque esta casilla para habilitar la encriptación de datos hacia y desde el receptor.
Clave encriptación	Introduzca una clave hexadecimal (máx. 32 dígitos) que se utilizará para encriptar los datos. **Nota**: Será necesario utilizar la misma clave en el receptor.
Teclado virtual	Habilita el acceso al panel con un teclado virtual, es decir, un módulo de software con el aspecto de teclado SPC y que se comporta como tal. Está disponible con el cliente SPC Com.
Transmisión en vivo / modo de transmisión	Especifica cuándo está disponible la transmisión en vivo de audio y vídeo. Las opciones son Nunca, Siempre y Solo tras alarma. Por defecto, la opción habilitada es "Solo tras alarma". **Nota**: Esta configuración tiene implicaciones obvias sobre la privacidad, por lo que solo se debe habilitar donde corresponda, y siempre respetando 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. Se recomienda el TCP si es admitido por el receptor.
Dirección ID CRA SPC Com	Introduzca la dirección IP de la CRA.
Puerto IP	Introduzca el puerto IP que el receptor EDP está escuchando.
Siempre conectado	Si está habilitado, el panel mantendrá una conexión permanente con el receptor. Si está deshabilitado, el panel solo se conectará con el receptor tras una incidencia de alarma.
Intervalo test	Si está habilitado, el panel es maestro de mensajes de test. 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.
TX alternativa a SPC Com (aplicable sólo a la conexión de un módem GPRS)	
TX RTB/GSM o GPRS	Marque esta casilla para informar de incidencias a través de una conexión de marcación.
Vía alternativa	Seleccione tipo de comunicación cuando está habilitada la función TX alternativa a SPC Com. Seleccione GPRS.
Protocolo GPRS	Seleccione el protocolo de capa de transporte utilizado en 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 conexiones GPRS. Solo aplicable si el tipo de llamada es GPRS.
Puerto GPRS	Introduzca el puerto que esté escuchando el receptor EDP para conexiones GPRS. Las opciones son UDP o TCP. Solo aplicable si el tipo de llamada es GPRS. Por defecto, 50000.
Tiempo fin GPRS	Introduzca el tiempo en segundos tras el cual se colgará la llamada GPRS. (0 = permanece conectada hasta que la conexión IP está activa)
Autoconexión GPRS	Marque esta casilla para activar automáticamente una llamada GPRS al servidor si se produce un fallo de red IP.
TX alternativa a SPC	Marque esta casilla para informar de fallos de red en una llamada

Com tras fallo de red	de test de TX alternativa a SPC Com.
Intervalo de TX alternativa a SPC Com 1*	Introduzca el número de minutos entre llamadas de test de marcación cuando un enlace de red esté activado.
Intervalo de TX alternativa a SPC Com 2*	Introduzca el número de minutos entre llamadas de test de marcación cuando un enlace de red esté desactivado.
Dirección de red*	Introduzca la dirección IP de la CRA. Sólo es necesario si la conexión con la CRA del EDP se realiza a través de la interfaz Ethernet. Si utiliza uno de los módems incorporados, deje este campo en blanco.
Número de teléfono*	Introduzca el primer número de teléfono que marca el/los módem(s) para contactar con la CRA.
Número de teléfono 2*	Introduzca el segundo número de teléfono que marcará(n) el/los módem(s) en caso de que no se consiga establecer con éxito una llamada con el primer número de teléfono marcado.
Incidencias	
Receptora primaria	Marque esta casilla para indicar que este es el receptor principal. Si no se marca, este será el receptor de reserva.
Incidencias en cola	Marque esta casilla si las incidencias de las que no se informó deben volver a ponerse en cola para la transmisión
Verificación	Marque esta casilla si la verificación de audio/vídeo se debe enviar a este receptor.
TX Incidencias	Haga clic en este botón para editar las incidencias de filtros que activarán una llamada de EDP. Consulte Edición de la configuración de filtros de incidencias [→ 316].

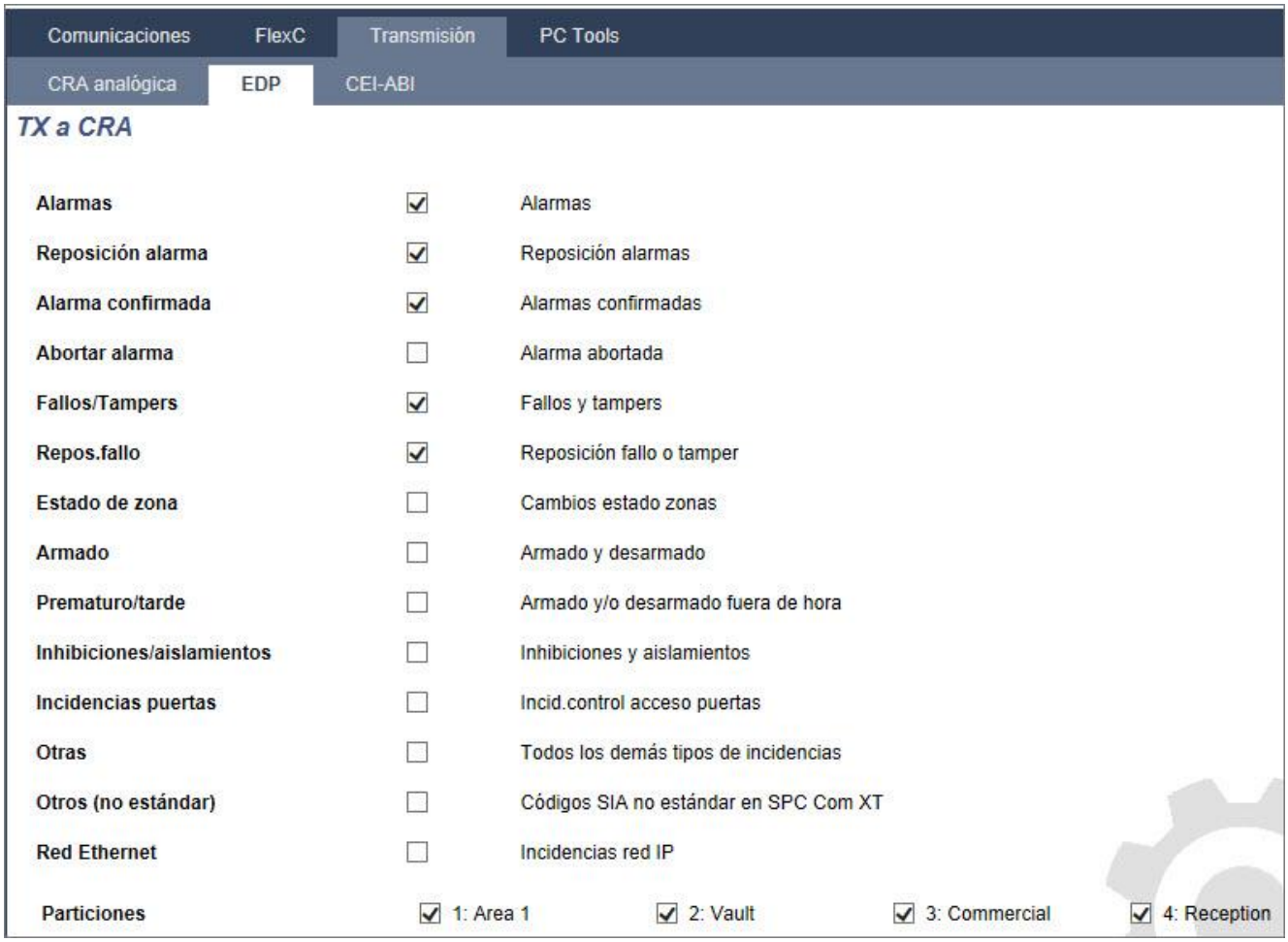
* La marcación de EDP a través de RTB no está admitida en esta versión.

Ver también

- Configuración de SMS [→ 201]

17.10.3.2.3 Edición de la configuración de filtros de incidencias

1. Seleccione **Comunicaciones > Transmisión> EDP > Editar** > **Filtro**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.

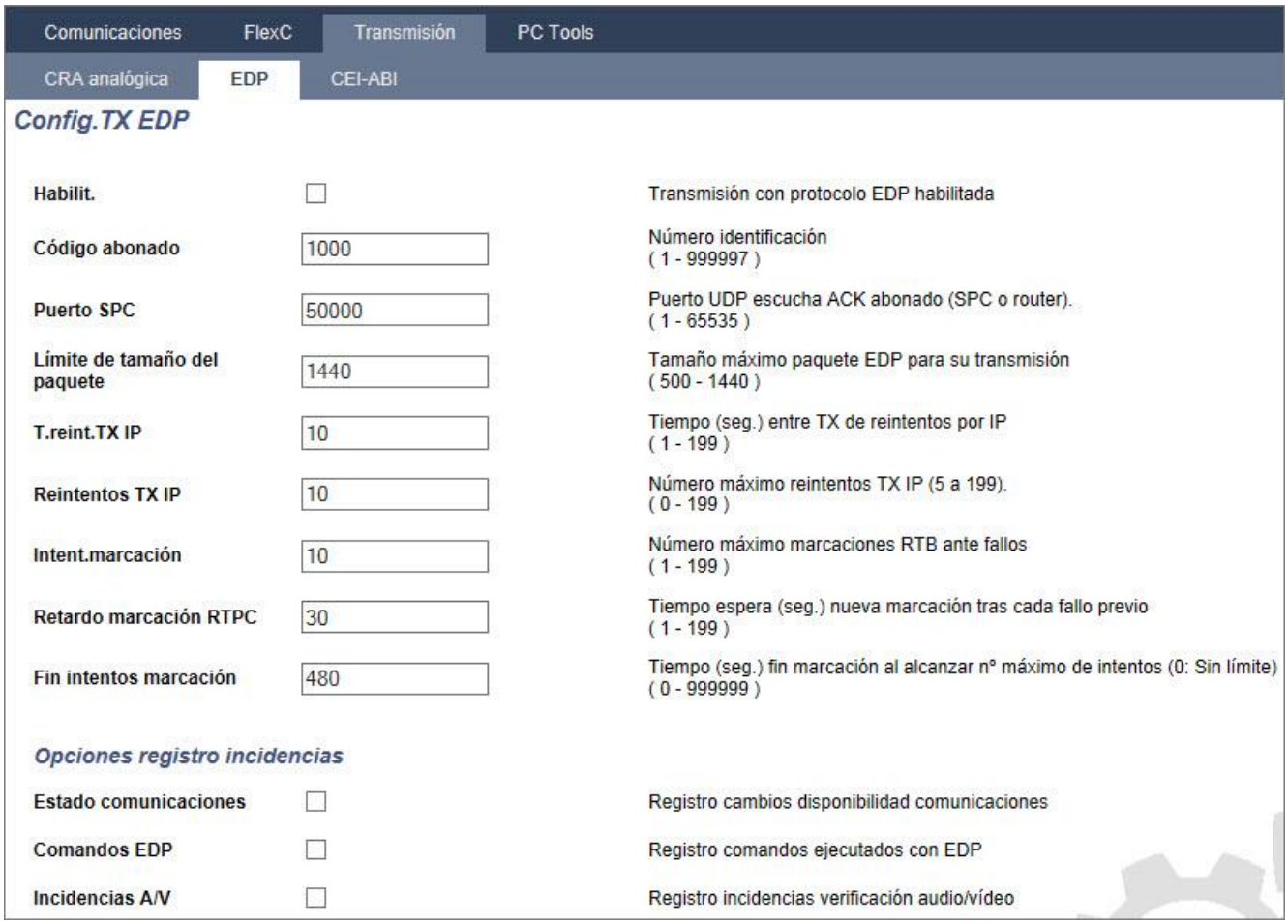


Marque alguna de las siguientes casillas si desea iniciar una llamada remota a un receptor EDP para notificarle una incidencia en particular.

Alarmas	Las alarmas están activadas.
Repos.alarma	Las alarmas del sistema están restauradas.
Alarmas confirmadas	Alarmas confirmadas
Abortar alarma	Incidencias de Alarma abortada. Las alarmas se abortan tras introducir un código de usuario válido a través del teclado tras una alarma confirmada o sin confirmar.
Fallos	Los fallos y tampers están activados.
Reposiciones de fallos	Se han restaurado las alarmas de fallo o tamper.
Estado de zona	Transmitir todos los cambios de estado de entrada de zona.
Configuración	El sistema está armado y desarmado.
Prem./tarde	Armado y desarmado no programados del sistema.
Inhib./Aisl.	Se ejecutan operaciones de inhibición y aislamiento en el sistema.
Incidencias puerta	Las incidencias de puertas están activadas. Sólo funciona con protocolo SIA.
Otras	Todos los demás tipos de incidencias se detectan en el sistema.
Otros (no estándar)	Códigos SIA no admitidos empleados con SPC COM XT, incluyendo incidencias de cámara en línea / fuera de línea.
Red	Incidencias red IP
Particiones	Seleccione particiones específicas para las que son aplicables las incidencias arriba indicadas.

17.10.3.2.4 Edición de la configuración de EDP

1. Seleccione **Comunicaciones > Transmisión> EDP > Config.**.
   ⇨ Se mostrará la siguiente ventana.
2. Configure los campos tal como se describe en la siguiente tabla.



Habilitar	Marque esta casilla para habilitar el funcionamiento de EDP en el sistema.
Código abonado	Introduzca un identificador numérico utilizado por el receptor EDP para identificar la central de forma exclusiva.
Puerto UDP abonado	Seleccione el puerto IP para recibir paquetes de IP. Por defecto, 50000.
Límite de tamaño del paquete	Introduzca el tamaño máximo de paquete EDP para su transmisión.
Timeout incidencia	Introduzca el límite de tiempo (en segundos) entre las retransmisiones de incidencias no reconocidas.
Reintentos TX IP	Introduzca el número máximo de retransmisiones de incidencias permitidas por el sistema.
Intentos de marcación	Introduzca el número máximo de intentos de marcación fallidos que acepta el sistema antes de que el módem se bloquee (se evita que realice más intentos de marcación). El periodo de bloqueo se define en la opción Finalización marcación.
Retardo marcación RTPC	Introduzca el periodo de tiempo (en segundos) que esperará el sistema antes de volver a marcar tras un intento de marcación fallido.

Fin intentos marcación	Introduzca el periodo de tiempo (en segundos) que el sistema suspenderá la marcación cuando se haya alcanzado un número máximo de intentos de marcación fallidos. Para intentar marcar de forma continua, introduzca el valor "0".

Opciones registro incidencias

Estado comunicaciones	Registro de toda la disponibilidad de comunicaciones.
Comandos EDP	Registro comandos ejecutados con EDP
Incidencias A/V	Registro incidencias verificación audio/vídeo
Flujo señal A/V	Registro inicio flujo señal audio/vídeo
Uso teclado	Registro activación teclado remoto

17.10.4 PC Tools

17.10.4.1 SPC Pro / SPC Safe

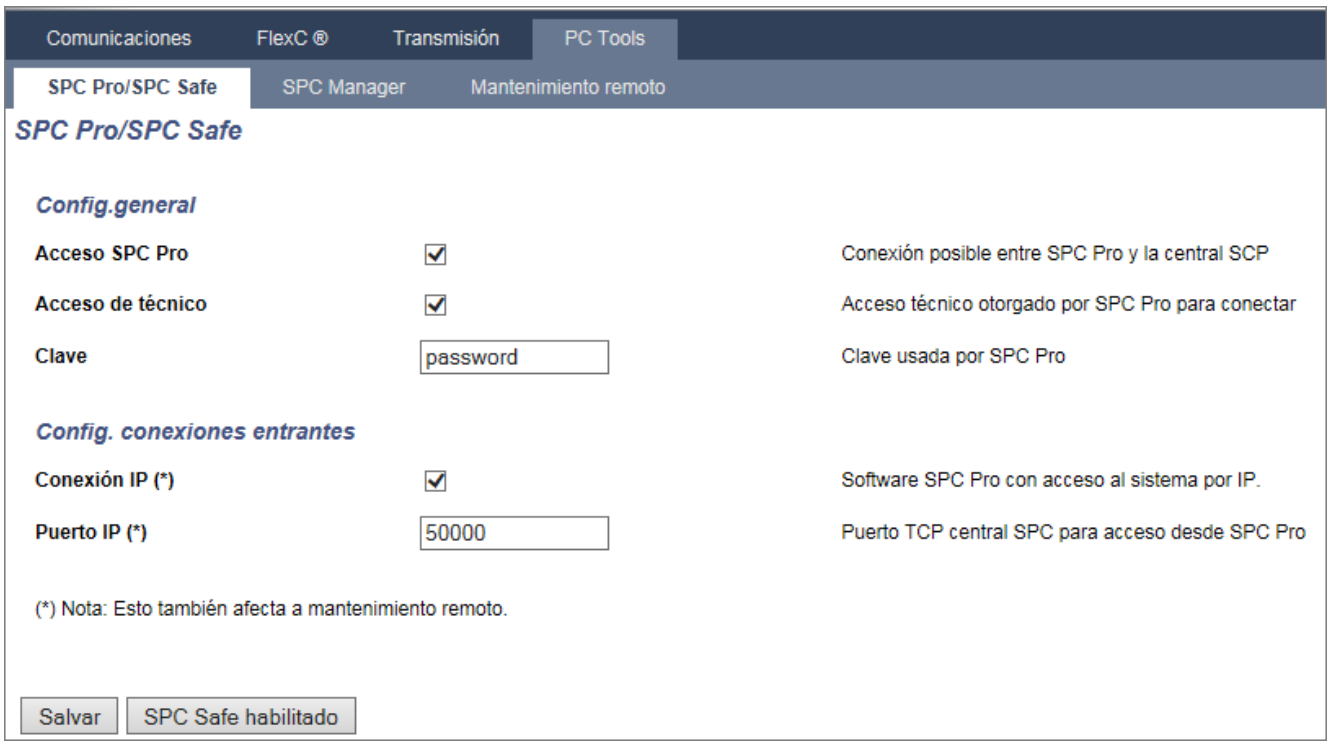
1. Seleccione **Comunicaciones > PC Tools > SPC Pro/SPC Safe**.
2. Configure los campos tal como se describe en la siguiente tabla.

Habilitar	Marque esta casilla para permitir que el SPC Pro se conecte a la central.
Acceso de técnico	Marque esta casilla si debe permitirse el acceso del técnico para que el SPC Pro se conecte a la central
Clave	Introduzca la clave para la conexión del SPC Pro. La central comprueba la clave cada vez que el SPC Pro intenta conectarse a ella. Si la clave programada en este campo coincide con la programada en la central, se permitirá la conexión (por defecto:).
Conexión IP	Marque esta casilla para permitir que se realice una conexión con la central utilizando el Protocolo Internet (IP).
Puerto IP	Seleccione el puerto IP que el SPC Pro utilizará para conectarse a la central.

SPC Safe

Para más información sobre la configuración de SPC Safe, consulte el *Manual de instalación y configuración de SPCS410.*

1. Haga clic en el botón **Habilitar SPC Safe**.
2. Configure los campos tal como se describe en la siguiente tabla.



Habilitar	Marque esta casilla para permitir que el Pro se conecte a la central.
Acceso de técnico	Marque esta casilla si debe permitirse el acceso del técnico para que el Pro se conecte a la central.
Clave	Introduzca la clave para la conexión del Pro. La central comprueba la clave cada vez que el Pro intenta conectarse a ella. Si la clave programada en este campo coincide con la programada en la central, se permitirá la conexión (por defecto:).
ID instalación	Introduzca la identificación numérica de esta instalación (también se puede configurar en la página de identificación del sistema).
Habilitar informe	Contacto entre sistema y servidor SPC Safe tras cambio de configuración
Temporiz.informe	Introduzca los minutos que debe tardar la central en comunicarse con el servidor tras el último cambio de configuración para informar sobre la misma (mín.: 1, máx.: 120).
Conexión IP	Marque esta casilla para permitir que se realice una conexión con la central utilizando el Protocolo Internet (IP).
Puerto TCP/IP	Introduzca el puerto IP que el SPC Safe utilizará para conectarse a la central (el puerto IP de la central).
Dirección servidor	Introduzca nombre Host, URL o dirección IP del servidor SPC Safe (p. ej. la dirección IP de su PC).
Puerto TCP/IP del servidor	Introduzca el puerto TCP del servidor SPC (p. ej. el puerto IP de su PC).

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, admite 1.000 usuarios globales

Modo51: código PIN de 5 dígitos, admite 10.000 usuarios globales

Modo61: código PIN de 6 dígitos, admite 100.000 usuarios globales

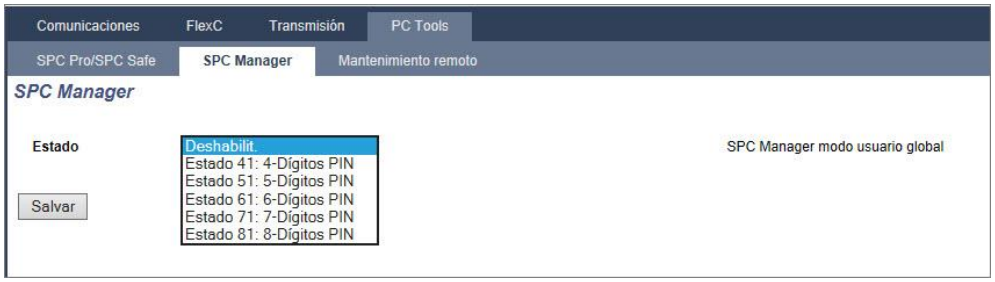
Modo71: código PIN de 7 dígitos, admite 1.000.000 de usuarios globales

Modo81: código PIN de 8 dígitos, admite 10.000.000 de usuarios globales

Cuando se configura un modo de SPC Manager, se añaden ceros adicionales delante de los códigos de usuario de 4 o 5 dígitos ya existentes, modificándose así el código PIN para uso global. Por ejemplo, si se utiliza el **Modo71: Se selecciona un código PIN de 7 dígitos**, se añaden 3 ceros a los códigos PIN de 4 dígitos; así el 2222 se convertirá en el 0002222.

Para configurar el modo SPC Manager:

1. Seleccione **Comunicaciones > PC Tools > SPC Manager**.



2. Seleccione el modo de usuario global de SPC Manager en la lista desplegable.
3. Haga clic en el botón **Salvar**.
   ⇨ Este modo no se puede guardar si hay un conflicto entre un código de usuario local ya existente y otro código 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 guardar el modo nuevo, o modifique el código PIN sustituyéndolo por el nuevo PIN generado aleatoriamente que se muestra ahora y, a continuación, guarde el modo nuevo.

i	*AVISO*
	Los modos SPC Manager no pueden modificarse si existen usuarios globales en el sistema.

17.10.4.3 Mantenimiento remoto

Para más información, consulte el manual de configuración del mantenimiento remoto.

17.10.4.3.1 Informe de mantenimiento remoto

El SPC Pro puede obtener directamente de la central un informe de mantenimiento remoto.

▷ El SPC Pro debe estar en línea con la central.

▷ **Mantenimiento remoto** debe estar habilitado.

1. Haga clic en el menú **Avanzado**.
2. Seleccione la opción de menú **Solicitar informe mantenim. central**.

Para más detalles sobre el Mantenimiento remoto, consulte el manual de Mantenimiento remoto del SPC.

17.11 Operaciones con ficheros

Para realizar operaciones en los ficheros y en la configuración de la central:

- Seleccione **Fichero**.
  - ⇨ Se muestran las siguientes pestañas.

Actualiz.firmware	Opciones para actualizar el firmware del controlador y de los periféricos, así como el idioma en la central. Consulte Operaciones para la actualización de ficheros [→ 322].
Gestión fichero	Opciones para gestionar el archivo de configuración del sistema y para cargar y descargar los datos de los usuarios desde y hacia la central. Consulte Operaciones de gestión de ficheros [→ 327].
Gestión página Web	Seleccione el diseño que desea aplicar a las páginas web del navegador del SPC. Escoja entre **Azul moderno** o **Menús agrupados** y haga clic en **Salvar**.
Audio	Cargue un archivo de audio en el SPC. El archivo se debe haber creado con el SPC Pro Audio Manager. Haga clic en **Browse** y después en **Program.** para añadir el archivo de audio al SPC. Tras realizar la carga, haga clic en el botón **Test** para validar el archivo de audio.
Programador rápido	Operaciones rápidas de fichero de programación. Consulte Uso del Programador rápido [→ 328].
Por defecto	Se restaura el sistema SPC a la configuración por defecto de fábrica. **¡AVISO! La dirección IP se mantiene para conectar a la interfaz web tras una configuración inicial de fábrica desde la página web.**
Reset	Se reinicia la central.
Política de textos	Esta pestaña resume la configuración de los ajustes de su producto SPC basándose en la **Región**, **Grado** y **Tipo** seleccionado.

17.11.1 Operaciones para la actualización de ficheros

Para actualizar el firmware y los idiomas en el sistema:

- Seleccione **Fichero > Actualiz.firmware**.
  - ⇨ Aparecerá la siguiente página:

Ver también

- Opciones [→ 234]
- Uso del Programador rápido [→ 328]

17.11.1.1 Actualización de firmware

i	*AVISO*
	Para realizar operaciones de actualización de firmware es necesario el acceso como fabricante y, cuando está habilitado, se pueden completar las actualizaciones de firmware tanto del controlador como de los periféricos. Consulte Opciones del sistema [→ 234].

El firmware del SPC se encuentra en dos ficheros separados:

- Fichero de firmware del controlador
  Solamente contiene el firmware para las CPU del controlador. El fichero tiene la extensión *.fw.
- Fichero de firmware de periféricos
  Contiene el firmware para los nodos X-BUS, más los módems RTB y GSM. El fichero tiene la extensión *.pfw.

Los dos ficheros se actualizan por separado.

!	*AVISO*
	Se recomienda actualizar el firmware de todos los periféricos tras actualizarse el firmware de un nuevo controlador.

Nota: El firmware también se puede actualizar mediante el teclado, el SPC Pro y el programador rápido.

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 pantalla de confirmación.

3. Haga clic en el botón **Confirmar** para confirmar la actualización a la nueva versión de firmware de la placa base.

⇨ Cuando el firmware de la placa base esté actualizado, se mostrará un mensaje indicando que el sistema se está reiniciando. Deberá volver a iniciar sesión en el sistema para continuar con la operación.

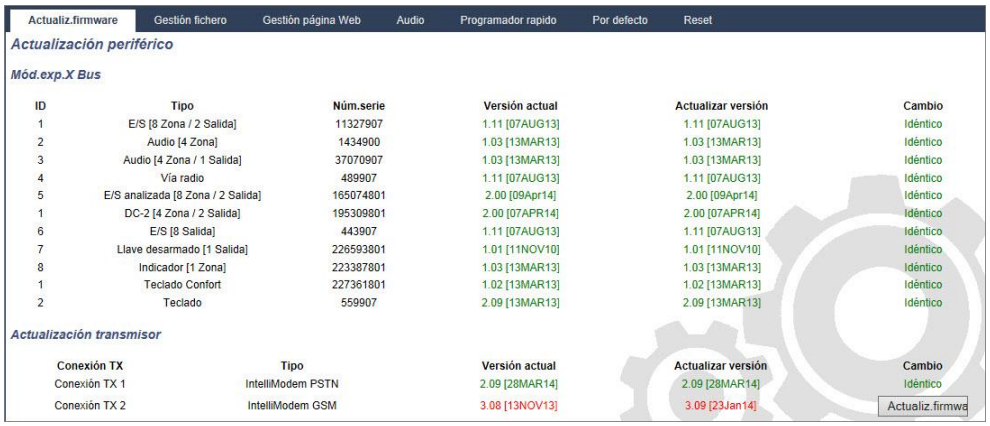
	⚠ ADVERTENCIA Si instala una versión anterior del firmware del controlador, el sistema restablecerá toda la configuración por defecto. Asimismo, cuando se instala una versión anterior de firmware, es importante instalar la versión anterior correspondiente del firmware de los periféricos; de lo contrario, 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 usuario, no se asignará ningún perfil (véase Perfiles de usuario [→ 196]). Por favor, 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 fichero de firmware de los periféricos solo se almacena temporalmente en el sistema de ficheros. Cuando se actualiza un nuevo fichero de firmware de periféricos, las versiones actual y nueva del firmware para cada periférico y módem se muestran de la siguiente manera:



ID	Tipo	Núm.serie	Versión actual	Actualizar versión	Cambio
1	E/S [8 Zona / 2 Salida]	11327907	1.11 [07AUG13]	1.11 [07AUG13]	Idéntico
2	Audio [4 Zona]	1434900	1.03 [13MAR13]	1.03 [13MAR13]	Idéntico
3	Audio [4 Zona / 1 Salida]	37070907	1.03 [13MAR13]	1.03 [13MAR13]	Idéntico
4	Vía radio	489907	1.11 [07AUG13]	1.11 [07AUG13]	Idéntico
5	E/S analizada [8 Zona / 2 Salida]	165074801	2.00 [09Apr14]	2.00 [09Apr14]	Idéntico
1	DC-2 [4 Zona / 2 Salida]	195309801	2.00 [07APR14]	2.00 [07APR14]	Idéntico
6	E/S [8 Salida]	443907	1.11 [07AUG13]	1.11 [07AUG13]	Idéntico
7	Llave desarmado [1 Salida]	226593801	1.01 [11NOV10]	1.01 [11NOV10]	Idéntico
8	Indicador [1 Zona]	223387801	1.03 [13MAR13]	1.03 [13MAR13]	Idéntico
1	Teclado Confort	227361801	1.02 [13MAR13]	1.02 [13MAR13]	Idéntico
2	Teclado	559907	2.09 [13MAR13]	2.09 [13MAR13]	Idéntico

Conexión TX	Tipo	Versión actual	Actualizar versión	Cambio
Conexión TX 1	IntelliModem PSTN	2.09 [28MAR14]	2.09 [28MAR14]	Idéntico
Conexión TX 2	IntelliModem GSM	3.08 [13NOV13]	3.09 [23Jan14]	

- Haga clic en el botón **Actualizado** para los periféricos que requieran actualización, o haga clic en el botón **Actualizar todo** para actualizar todos los periféricos.

⇨ Si el firmware para un dispositivo periférico del fichero pfw es más antiguo que el firmware instalado en ese dispositivo, se habilitará el botón de **Lectura** para cambiar a la versión anterior.

Durante la actualización, el panel comprueba si el firmware del fichero para periféricos admite las correspondientes versiones de hardware de los periféricos instalados, y no permite la actualización de aquellos periféricos que no sean compatibles.

Si la versión del fichero pfw es diferente de la versión del controlador, se mostrará un mensaje de advertencia.

Si el número de la versión principal del firmware disponible para un dispositivo es diferente del número principal existente de un dispositivo, también se mostrará un mensaje de advertencia.

El firmware de los periféricos también se puede actualizar con SPC Pro o mediante el Programador rápido [→ 328].

Actualización de firmware de la fuente de alimentación inteligente SPCP355

Para actualizar la fuente de alimentación inteligente SPCP355, debe comprobar lo siguiente:

El firmware de la fuente de alimentación inteligente SPCP355 solo se puede actualizar a través del navegador. No se puede actualizar mediante SPCPro.

- La alimentación eléctrica debe estar conectada.

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.

Ver también

🗎 Añadir/Editar perfiles de usuario [→ 196]

17.11.1.2 Actualización de idiomas

Se puede cargar un fichero de idioma personalizado (*.clng) en la central. Este fichero solo es aplicable al firmware de la central, y no está disponible para SPC Pro ni para SPC Safe.

!	*AVISO*
	La central debe contar con licencia para el uso de idiomas personalizados, así como con otros idiomas.

Para actualizar los idiomas en el sistema:

1. Seleccione **Fichero** > **Actualiz.firmware**.

⇨ Se muestra 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.

Idioma	ID	Tamaño (bytes)	Líneas perdidas	Versión actual	Actualizar versión	Actualiz.firmwa
Inglés	0	N/A	0	3.6.0	3.6.0	☑
Danés	9	41338	-	---	3.6.0	☐
Holandés	13	40637	-	---	3.6.0	☐
Finlandés	4	43580	-	---	3.6.0	☐
Flamenco	17	40637	-	---	3.6.0	☐
Francés	2	44567	6	3.6.0	3.6.0	☑
Alemán	15	44533	6	3.6.0	3.6.0	☑
Italiano	3	42863	6	3.6.0	3.6.0	☑
Noruego	8	39819	-	---	3.6.0	☐
Polaco	11	44085	-	---	3.6.0	☐
Castellano	1	36553	6	3.6.0	3.6.0	☑
Sueco	7	40418	-	---	3.6.0	☐

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 pantalla **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:

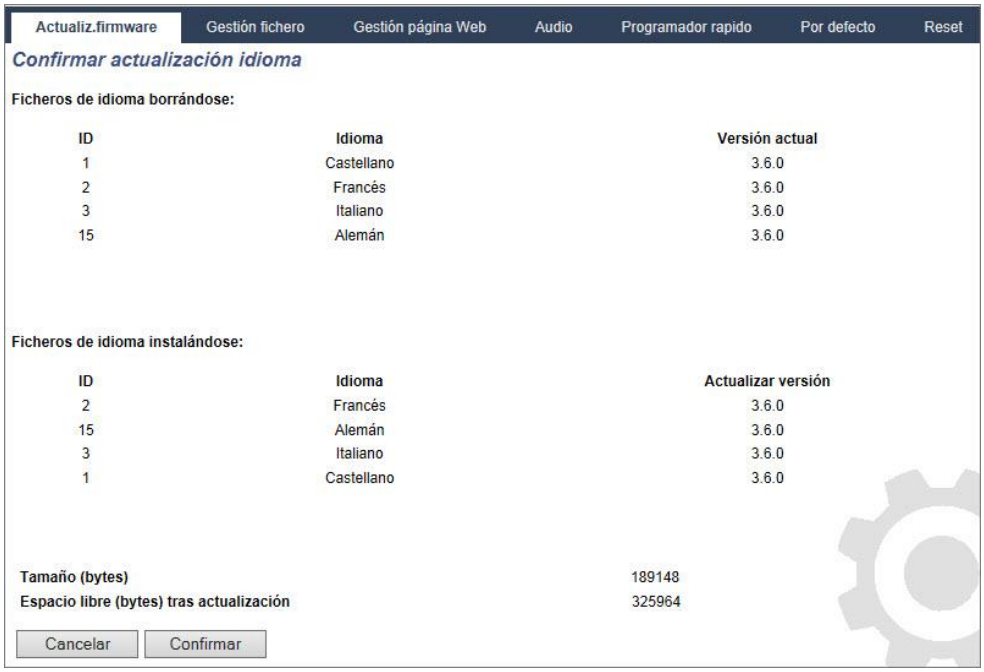
1. Seleccione el fichero de idioma que desee actualizar haciendo clic en el botón **Browse** (examinar) para elegir la opción **Actualización de fichero de idioma**, seleccionando a continuación el fichero de idioma necesario, y haciendo clic en el botón de **Actualizado** correspondiente.

   ⇨ 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 pantalla **Confirmar actualización idioma**. Cuando se borra un idioma, la central borra todos los idiomas y reinstala solo los idiomas requeridos. En el siguiente ejemplo, se borra el idioma Flamenco.



4. Haga clic en el botón **Confirmar** para confirmar el idioma que se borrará.

Los ficheros de idiomas también se pueden importar mediante el Programador rápido [→ 328].

Consulte Idioma [→ 250] para más información sobre cómo seleccionar en el navegador los idiomas del panel para "Sistema" y "En reposo".

Consulte OPCIONES [→ 115] para más información sobre cómo seleccionar en el teclado los idiomas del panel para "Sistema" y "En reposo".

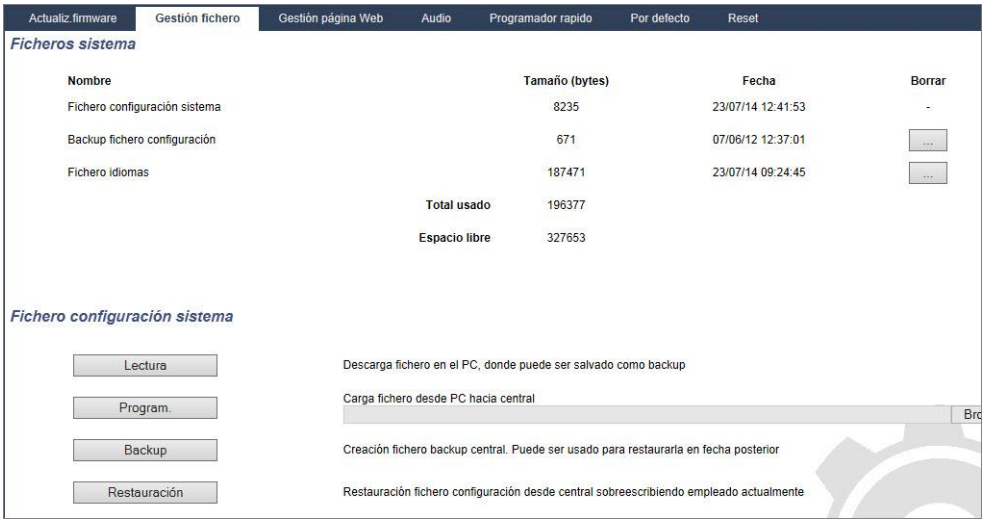
Ver también

🗎 Idioma [→ 250]

17.11.2 Operaciones de gestión de ficheros

- Seleccione **Fichero -> Gestión fichero**.

  ⇨ Se muestra una pantalla que muestra los detalles de la configuración del sistema, del idioma y de los ficheros de trazado.



Fichero de configuración del sistema

Para gestionar el fichero de configuración del sistema están disponibles las siguientes opciones:

Lectura	Descarga un fichero de configuración desde el controlador. **Nota**: Si aparece un mensaje de error tras hacer clic sobre el botón de Leer configuración, proceda de la siguiente manera: 1. Seleccione **Opciones de Internet** en el menú Herramientas. 2. Seleccione la pestaña **Avanzadas**. 3. Marque la casilla **No guardar páginas encriptadas en disco**. 4. Haga clic en **Aplicar.** 5. Haga clic en **Aceptar**. 6. Vuelva a hacer clic en **Lectura**. Al descargar un fichero de configuración, los parámetros de configuración se guardan en un fichero **.cfg**. Este fichero se puede cargar entonces en otros controladores para evitar los largos procedimientos de programación.
Programar	Carga un fichero de configuración en el controlador.
Backup	Guarda una copia de seguridad de la configuración actual en la memoria flash.
Restaurar	Restaura una copia de seguridad de la configuración actual desde la memoria flash.

Datos de los usuarios

Se dispone de las siguientes opciones para gestionar los datos de los usuarios:

Lectura	Haga clic en el botón para la **Lectura** de los datos de los usuarios de la central. Un cuadro de diálogo le preguntará dónde le gustaría guardar el fichero **users.csv**.
Programar	Haga clic en el botón **Browse** para **Programar** los datos de los usuarios en la central. Este debe ser un fichero con extensión .csv.

17.12 Uso del Programador rápido

El Programador rápido del SPC es un dispositivo de almacenamiento portátil que ofrece al técnico la posibilidad de cargar y descargar ficheros de configuración de forma rápida y eficaz. El Programador rápido tiene dos interfaces ubicadas en los extremos opuestos del dispositivo:

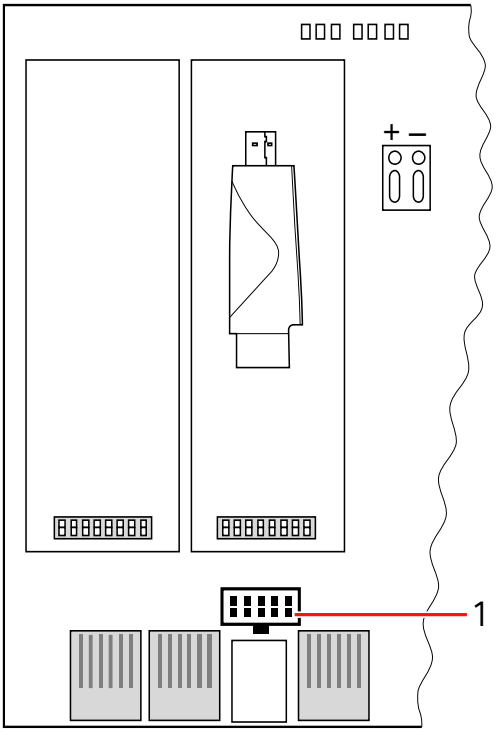
Interfaz del controlador SPC

Esta interfaz de serie de 10 clavijas se encuentra situada en la parte superior del Programador rápido y se conecta directamente a la interfaz del Programador rápido en la placa del controlador. Una vez conectada, el técnico puede cargar y descargar ficheros directamente desde el Programador rápido a través de las herramientas de programación del navegador y del teclado.

Interfaz USB del PC

Esta interfaz USB está ubicada en la parte inferior del Programador rápido y se conecta directamente a la interfaz USB del PC. El fichero de configuración y otros ficheros solo se pueden copiar entre el PC y el Programador rápido mediante la herramienta de programación SPC Pro.

17.12.1 Conexión del programador rápido a la placa base



Interfaz del programador rápido

1	Interfaz del programador rápido

Para conectar el programador rápido del SPC al controlador:

1. Abra la caja del controlador SPC y localice la interfaz del programador rápido.
   ¡AVISO! No desconecte el controlador.
2. Alinee el programador rápido, sobre la interfaz para el programador rápido de la placa del controlador SPC, con la interfaz serie de 10 clavijas hacia abajo.
3. Asegúrese de que las clavijas encajen correctamente en los agujeros de la ranura y presione firmemente, pero con cuidado, hasta colocarlo.

⇨ El LED del programador rápido parpadea momentáneamente al acceder a los datos.
¡ATENCIÓN! NO retire el programador rápido mientras el LED esté parpadeando.

⇨ El programador rápido está ahora conectado al controlador.

Para retirar el programador rápido, tire suavemente del dispositivo hacia fuera de la interfaz del programador rápido.

17.12.2 Instalación del Programador rápido en un PC

Para Windows XP

▷ SPCPro debe estar instalado en el PC con Windows XP.

1. Conecte el programador rápido a una interfaz USB del PC.
   ⇨ Se muestra el asistente de **Nuevo hardware encontrado**.
2. Pulse **Siguiente**.
3. Haga clic en **Continuar de todas formas**.
   ⇨ Al final del proceso de instalación, una ventana indica que éste ha terminado.
4. Haga clic en **Finalizar**.

Para Windows 7

▷ Tiene privilegios de administrador.

▷ SPCPro debe estar instalado en el PC con Windows 7.

- Conecte el programador rápido a una interfaz USB del PC.

⇨ Las unidades se instalan automáticamente

Véase Programador rápido SPC.

- Abra el menú de Windows **Inicio > Panel de control > Sistema > Administrador de dispositivos**.

⇨ El controlador del Programador rápido aparecerá en el directorio Puertos (COM & LPT) como Programador rápido SPC **USB (COM X)** (X = número de puerto com).

17.12.3 Operaciones con archivos del Programador rápido

Las actualizaciones de firmware de la placa base y de los periféricos, y las importaciones de idiomas personalizados, se pueden realizar mediante el Programador rápido y el SPC Pro.

17.12.3.1 Acceso al programador rápido mediante el teclado

1. Entre en modo técnico total y desplácese a VARIOS > PROGRAMADOR RÁPIDO.
2. Pulse SELECC.
3. Desplácese y seleccione la opción que desee:

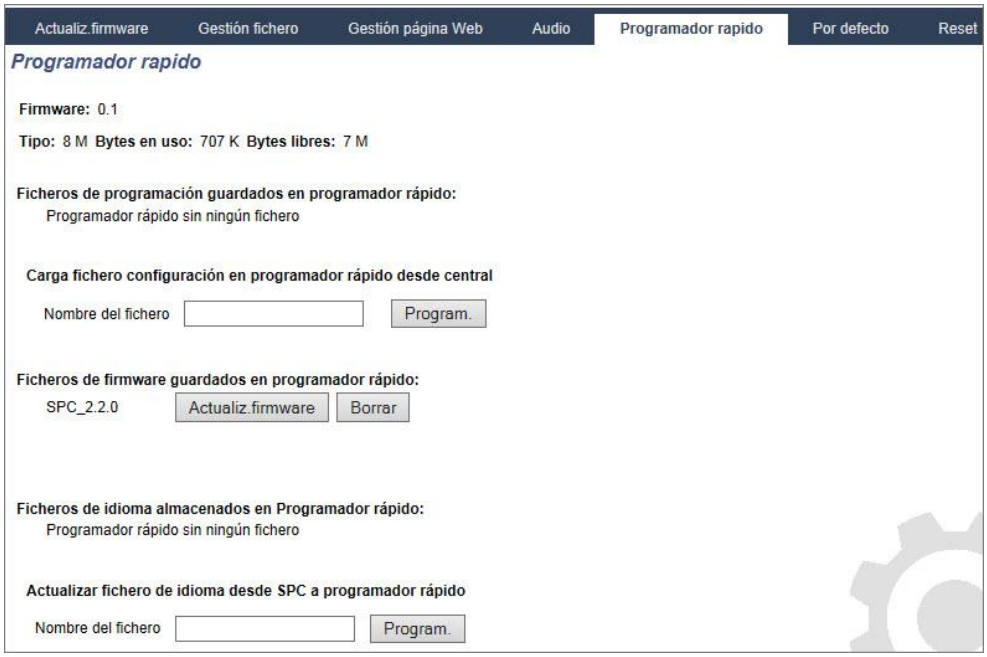
CENTRAL - PROGR.	Seleccione el fichero que desee de la lista.
PROGR. - CENTRAL	Seleccione el fichero que desee de la lista.

BORRAR FICHEROS	Seleccione el fichero que desee de la lista.
ACTUALIZACION FIRMWARE	El panel busca un fichero de firmware de controlador válido. Una vez que lo encuentra, el usuario puede seleccionar y actualizar la central.
ACTUALIZACIÓN PERIFÉRICO	La central busca un fichero de firmware de periféricos válido. Una vez que lo encuentra, el usuario puede seleccionar y actualizar la central.
ACTUALIZACIÓN IDIOMA	Se muestra una lista de los ficheros de idiomas disponibles en el Programador rápido. Seleccione el idioma requerido y pulse SELECC para importar el fichero.

17.12.3.2 Acceso al programador rápido mediante el navegador

1. Introduzca Técnico total en la programación del navegador y seleccione la página de programación **Fichero**.
2. Haga clic en **Programador rápido**.

⇨ Se muestran las opciones para cargar y descargar ficheros.



Descarga de ficheros de configuración en el panel

Aparece una lista de los ficheros de configuración almacenados en el programador rápido junto con las opciones para descargarlos o borrarlos.

Carga de ficheros de configuración en el Programador rápido

Cuando se cargan ficheros del SPC al Programador rápido, se le solicitará que borre el fichero existente en el programador antes de que se pueda guardar el nuevo fichero.

Para cargar un fichero de configuración del programador rápido al SPC, introduzca el nombre del fichero en el cuadro de nombre de fichero y haga clic en **Program.**.

Para una información más detallada sobre el uso del Programador rápido con SPC Pro, consulte el *Manual de configuración de SPC Pro*.

Actualización de firmware

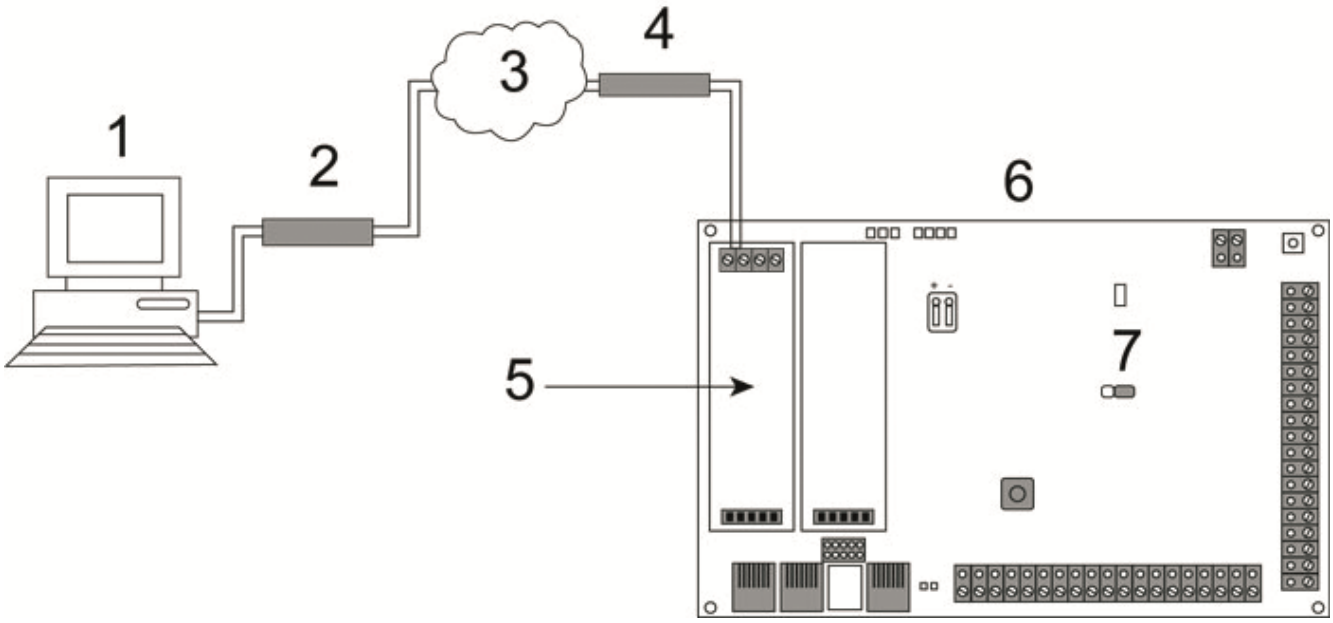
!	*AVISO*
	Para las operaciones de firmware se requiere el Acceso de fabricante.

Se muestra una lista de los ficheros de firmware guardados en el Programador rápido.

Para actualizar el firmware, haga clic en el botón **Actualiz.firmware** que aparece junto al fichero de firmware requerido.

18 Acceso al servidor web de forma remota

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~~

Se puede acceder al servidor web del controlador a través de una conexión remota desde una línea telefónica RTB. Deben conectarse un módulo RTB y una línea RTB al controlador, tal como se muestra anteriormente, para proporcionar acceso remoto al controlador.

En la parte remota de la conexión, el usuario debe tener un módem RTB instalado en un PC con acceso a una línea RTB.

Para conectarse de forma remota al controlador:

1. Instale un módem RTB en el controlador (consulte las instrucciones de instalación correspondientes).
2. Conecte la línea telefónica a los terminales roscados A/B del conector situado en la parte superior del módem.
3. Entre en la programación de técnico desde el teclado y configure el módem (primario o de copia de seguridad) para responder a una llamada entrante.
4. En el teclado, desplácese a **Modo técnico total > Coms. > Módems**.
5. Seleccione la siguiente configuración:

- **Habilitar módem:** Configurado en Habilitado
- **Tipo**: Muestra el tipo de módem (RTB)
- **Código del país:** Seleccione el código del país que proceda (Irlanda, R. U., Europa).
- **Modo de respuesta:** Seleccione tonos numerados; de este modo se indica al módem que espere un número de tonos antes de responder a una llamada entrante.
- **Rings TX:** Seleccione el número de tonos permitidos antes de responder a la llamada (máx. 8 tonos).

6. Cree una conexión telefónica en el PC remoto utilizando el número de teléfono de la línea telefónica conectada al módulo RTB del controlador. Las instrucciones para hacerlo en el sistema operativo Windows XP se indican más abajo:

En Windows XP:

1. Abra el Asistente de nueva conexión desplazándose a **Panel de control> Conexiones de red> Crear una conexión nueva** (en la ventana Tareas de red).
2. En la ventana **Tipo de conexión de red**, seleccione **Conectarse a Internet**.
3. En la ventana **Preparándose**, elija **Establecer mi conexión manualmente**.
4. En la ventana **Conexión de Internet**, elija **Conectarse usando un 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 que desea marcar**, introduzca el número de teléfono de la línea RTB conectada al módem RTB.
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
   - Contraseña: password (por defecto)
   - Confirmar contraseña: password
   ⇨ Aparece la ventana **Finalización del Asistente para conexión nueva**.
9. Haga clic en **Finalizar** para guardar la conexión telefónica al PC.

El código por defecto debe cambiarse y anotarse adecuadamente ya que Vanderbilt

no puede recuperar este nuevo código. Si se olvida un código, la única solución es restaurar el sistema a la configuración inicial de fábrica, lo que provoca una pérdida de la programación. La programación se puede recuperar si hay una copia de seguridad disponible.

Para activar esta conexión telefónica:

- Haga clic en el icono situado en la ventana **Panel de control > Conexiones de red**.

- ⇨ El PC realizará una llamada de datos a la línea PSTN conectada al módulo PSTN del SPC.
- ⇨ El módulo PSTN 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.

En algunos sistemas operativos de Windows aparece 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 del ratón en el icono Acceso telefónico.
2. Haga clic en la pestaña **Propiedades**.

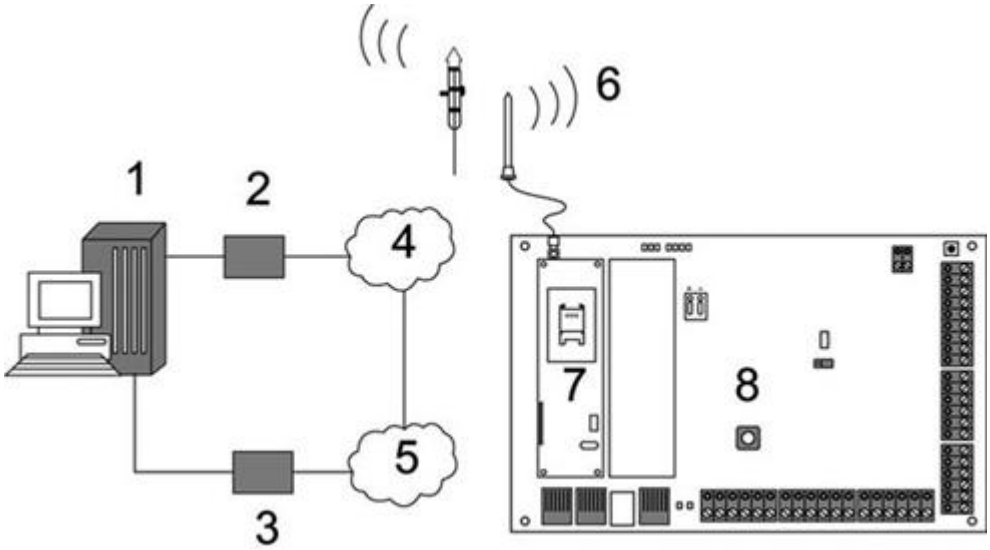
⇨ Se muestra la dirección IP como dirección IP del servidor.

1. Introduzca esta dirección IP en la barra de direcciones del navegador y haga clic.
2. Cuando se muestre el icono de Acceso telefónico en la barra de tareas del PC, abra el navegador e introduzca la dirección IP del SPC.

⇨ Se mostrará la pantalla de inicio del navegador.

Para establecer una conexión telefónica en otro sistema operativo, consulte el menú de ayuda del mismo.

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

Se puede acceder al servidor web del controlador a través de una conexión remota desde la red GSM. Debe instalarse un módulo GSM (con tarjeta SIM) en el controlador como se muestra anteriormente para ofrecer un acceso remoto al SPC. Se debe activar la opción de datos de la tarjeta SIM y usarse el número de datos.

En la parte remota de la conexión, el usuario debe tener un módem RTB o GSM instalado en un PC con navegador. Si hay instalado un módem RTB, debe estar conectado a una línea RTB en funcionamiento.

Para conectarse de forma remota al controlador:

1. Instale un módem GSM en el controlador (consulte las instrucciones de instalación correspondientes).
2. Entre en la programación de técnico total desde el teclado y configure el módem (primario o de backup) para responder a una llamada entrante.
3. En el teclado, desplácese al menú siguiente: TÉCNICO TOTAL > COMUNICACIÓN > MÓDEMS y seleccione los parámetros listados:

Habilitar módem	Configurar en TX habilitado.
Tipo	Muestra el tipo de módem (GSM).
Código del país	Seleccione el código del país correspondiente.
Modo respuesta	Seleccione tonos numerados; de este modo se indica al módem que espere un número de tonos antes de responder a una llamada entrante.
Rings TX	Seleccione el número de tonos permitidos antes de responder a la llamada (máx. 8 tonos).

En Windows XP:

1. Abra el Asistente de nueva conexión desplazándose a **Panel de control> Conexiones de red> Crear una conexión nueva** (en la ventana Tareas de red).
2. En la ventana **Tipo de conexión de red**, seleccione **Conectarse a Internet**.
3. En la ventana **Preparándose**, elija **Establecer mi conexión manualmente**.
4. En la ventana **Conexión de Internet**, elija **Conectarse usando un 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 que desea marcar**, introduzca el número de teléfono de la línea RTB conectada al módem RTB.
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
- Contraseña: password (por defecto)
- Confirmar contraseña: password

⇨ Aparece la ventana **Finalización del Asistente para conexión nueva**.

9. Haga clic en **Finalizar** para guardar la conexión telefónica al PC.

El código por defecto debe cambiarse y anotarse adecuadamente ya que Vanderbilt

no puede recuperar este nuevo código. Si se olvida un código, la única solución es restaurar el sistema a la configuración inicial de fábrica, lo que provoca una pérdida de la programación. La programación se puede recuperar si hay una copia de seguridad disponible.

Para activar esta conexión telefónica:

- Haga clic en el icono situado en la ventana **Panel de control > Conexiones de red**.
  - ⇨ El PC realizará una llamada de datos a la línea PSTN conectada al módulo PSTN del SPC.
  - ⇨ El módulo PSTN 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.

En algunos sistemas operativos de Windows aparece 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 del ratón en el icono Acceso telefónico.
2. Haga clic en la pestaña **Propiedades**.

⇨ Se muestra la dirección IP como dirección IP del servidor.

1. Introduzca esta dirección IP en la barra de direcciones del navegador y haga clic.
2. Cuando se muestre el icono de Acceso telefónico en la barra de tareas del PC, abra el navegador e introduzca la dirección IP del SPC.

⇨ Se mostrará la pantalla de inicio del navegador.

Para establecer una conexión telefónica en otro sistema operativo, consulte el menú de ayuda del mismo.

19 Funcionalidad de alarma de intrusión

El sistema SPC puede funcionar con 3 modos distintos de operaciones de la alarma de intrusión, **Financiero**, **Comercial** o **Doméstico**, y todos admiten varias particiones.

A su vez, cada partición admite 4 modos de alarma diferentes. Los modos Comercial y Financiero presentan más tipos de alarma programable que el Doméstico. Los parámetros de nombre y tipo de zona por defecto para cada modo se encuentran listados en la página [→ 357].

19.1 Funcionamiento en modo Financiero

El modo Financiero es adecuado para bancos e instituciones financieras con particiones de seguridad especial, como cámaras acorazadas y cajeros automáticos.

Cada partición definida en el sistema admite los modos de alarma que se indican más abajo.

Modo de alarma	Descripción
Desarmado	La partición esta desarmada y sólo las zonas de alarma clasificadas como de 24 horas activarán la alarma.
ARMADO PARCIAL A	Este modo ofrece protección del perímetro de un edificio, a la vez que permite el movimiento libre por la salida y las áreas 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 seleccionarse este modo). Es posible aplicar un tiempo de salida a este modo habilitando la variable Armado parcial A por control horario.
ARMADO PARCIAL B	Este modo de configuración ofrece 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 seleccionarse este modo). Es posible aplicar un tiempo de salida a este modo habilitando la variable Armado parcial B por control horario.
ARMADO TOTAL	La partición está totalmente armada; 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 instalaciones empresariales con varias particiones y un número elevado de zonas de alarma. Cada partición definida en el sistema admite los modos de alarma que se indican más abajo.

Modo de alarma	Descripción
Desarmado	La partición esta desarmada y sólo las zonas de alarma clasificadas como de 24 horas activarán la alarma.
ARMADO PARCIAL A	Este modo ofrece protección del perímetro de un edificio, a la vez que permite el movimiento libre por la salida y las áreas 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 seleccionarse este modo). Es posible aplicar un tiempo de salida a este modo habilitando la variable Armado parcial A por control horario.
ARMADO PARCIAL B	Este modo de configuración ofrece 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 seleccionarse este modo). Es posible aplicar un tiempo de salida a este modo habilitando la variable Armado parcial B por control horario.

Modo de alarma	Descripción
ARMADO TOTAL	La partición está totalmente armada; 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 instalaciones de residencias con una o más particiones y un número de zonas de alarma de pequeño a moderado. Cada partición definida en el sistema admite los modos de alarma que se indican más abajo.

Modo de alarma	Descripción
Desarmado	La partición esta desarmada y sólo las zonas de alarma clasificadas como de 24 horas activarán la alarma.
ARMADO PARCIAL A	Este modo ofrece protección del perímetro de un edificio, a la vez que permite el movimiento libre por la salida y las áreas de acceso (por ejemplo, la puerta delantera y el vestíbulo) Las zonas que se han clasificado como Excl.A.parc.A continúan sin protección en este modo. No hay tiempos de salida asociados a este modo, y la protección se aplica instantáneamente al seleccionarlo.
ARMADO PARCIAL B	Este modo de configuración ofrece 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 seleccionarse este modo). Es posible aplicar un tiempo de salida a este modo habilitando la variable Armado parcial B por control horario.
ARMADO TOTAL	La partición está totalmente armada y la apertura de una zona de Entrada/Salida inicia el temporizador de entrada. Si la alarma no se ha desarmado antes de que termine el tiempo de entrada, la alarma se activa.

19.4 Alarmas completa y local

El tipo de alarmas generadas por el sistema SPC puede variar en función del tipo de zona que produjo la activación de la alarma. La gran mayoría de las alarmas requieren una indicación visual (flash) y acústica (sirena) al producirse una intrusión en las instalaciones o el edificio.

Por defecto, las 3 primeras salidas físicas del controlador SPC están asignadas a la sirena exterior, a la sirena interior y al flash de sirena exterior. Al activarse, estas 3 salidas juntas proporcionan un aviso suficiente de una condición de alarma a las personas que se encuentren dentro o en las inmediaciones del edificio o de las instalaciones donde ha tenido lugar la intrusión.

Las alarmas completa y local 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 más detalles sobre cómo cablear las sirenas y el flash, consulte la página [→ 73].

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 situaciones del sistema

20.1 Cuándo utilizar una partición común

Las particiones comunes representan una forma práctica de configurar varias particiones en una sola instalación. Un usuario asignado a una partición común tiene la posibilidad de ARMAR TODAS las particiones dentro de dicha partición común (incluso para aquellas particiones que no hayan sido asignadas a ese usuario). Sin embargo, los usuarios sólo pueden DESARMAR particiones que les estén asignadas.

Las particiones comunes sólo deben utilizarse cuando hay un único teclado instalado en la ubicación de acceso principal y lo comparten todos los usuarios en el edificio (no se recomienda definir una partición común en un sistema con varios teclados en particiones diferentes).

Situación: dos departamentos de una empresa (Contabilidad y Ventas) comparten un punto de acceso común (la puerta delantera).

En este caso, se crearían 3 particiones en el sistema (Área común, Contabilidad 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, como mínimo, 2 usuarios en el sistema, uno para cada departamento, y asigne los usuarios tanto a sus particiones respectivas como a la partición común.

Operación: armado del sistema

El Jefe de contabilidad sale de la oficina a las 5 de la tarde. Cuando introduce su código en el teclado, la opción ARMADO TOTAL presenta los 3 submenús siguientes:

- 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 de la puerta delantera indica al usuario que abandone el 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 sale del edificio, cierra todas las puertas y ventanas de la PARTICIÓN 3 e introduce su código en el teclado. La opción ARMADO TOTAL presenta los 3 submenús siguientes:

- 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 de la puerta delantera indica al usuario que abandone el 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.

Operación: desarmado del sistema

Cuando el Jefe de contabilidad vuelve a abrir el edificio e introduce su código en el teclado; la opción DESARMADO presenta los 3 submenús siguientes:

- 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: los empleados de Contabilidad no pueden DESARMAR la partición de Ventas.
- COMÚN: desarma SÓLO la partición común (Recepción). Ofrece la opción de desarmar la partición de recepción sólo cuando se sale de las oficinas de Contabilidad y Ventas.
- CONTABILIDAD: desarma la partición de Contabilidad y la partición común (Recepción). En este caso, la partición de Ventas sigue armada mientras que aún se permite el acceso por la puerta delantera.

Uso de particiones comunes:

- Zona llave A/D

Si la ruta de entrada/salida en la partición común está programada como zona llave A/D, cuando se active se ARMARÁN todas las particiones de la partición común. Al desactivar la zona de llave A/D, se DESARMAN todas las particiones en las particiones comunes.

- Múltiples teclados

Si las particiones asignadas a la partición común tienen sus propios teclados para entrada/salida, es importante que los tiempos de salida asociados a dichas particiones dejen tiempo suficiente para permitir que el usuario llegue a la salida de la partición común. Esto tiene lugar en el caso de que la partición que se está armando sea la última partición desarmada del sistema y, por tanto, activará el armado de toda la partición común.

Como regla general, es recomendable utilizar particiones comunes en las instalaciones que tengan un sólo teclado ubicado en el punto de acceso común, p. ej. la puerta de acceso delantera de todo el edificio.

21 Detectores sísmicos

Los detectores de vibración, también llamados detectores sísmicos, sirven para detectar intentos de intrusión por medios mecánicos, p. ej. taladrando o haciendo agujeros en paredes o cajas fuertes.

El soporte para detectores sísmicos solo está disponible si la instalación de la central es de tipo "Financiera".

Hay varias formas de comprobar los detectores sísmicos. La forma más sencilla de comprobar los detectores sísmicos es golpeando una pared o caja fuerte, y ver si la zona se abre durante un test de intrusión. Esta forma de comprobación está disponible con todos los tipos de detectores sísmicos.

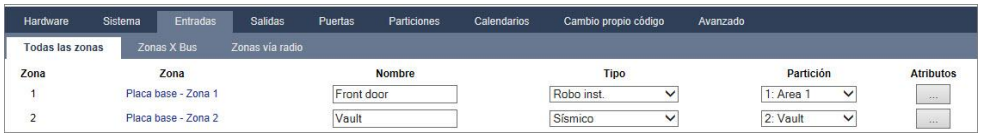
Si el detector sísmico se instala con un transmisor de prueba, estarán disponibles las siguientes opciones de comprobación:

- Comprobación manual iniciada en el teclado o con SPC Pro (no admitido por el navegador);
- Comprobación automática periódica o cuando la central se configura mediante el teclado.

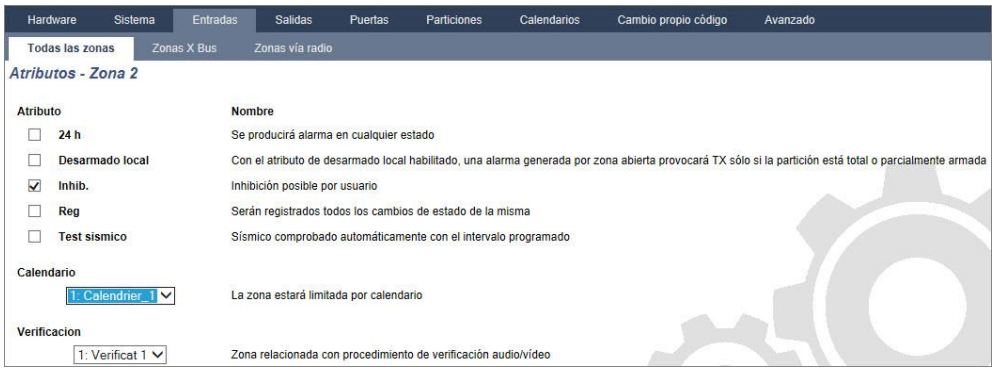
El transmisor de prueba es un pequeño vibrador de alta frecuencia que se instala en la misma pared que el detector, a una corta distancia de él. El transmisor de prueba se conecta mediante un cable a una salida en la central o en un módulo de expansión.

Configuración de detectores sísmicos en la central

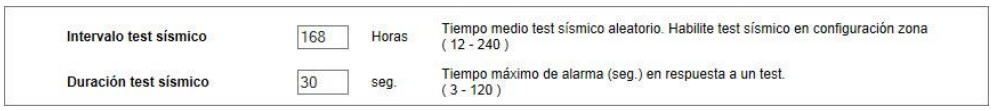
1. Configure una zona sísmica. Los detectores sísmicos se deben asignar a una zona. (Véase Edición de una zona [→ 251])



2. Configure los atributos para la zona.



3. Habilite la comprobación automática del detector 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 7 días) y la duración de los tests. (el atributo de zona Test sísmico automático debe estar activado). (Consulte Temporizaciones [→ 244]).



7. Configure una salida para comprobar una zona sísmica. (Véase Tipos de salida y puertos de salida [→ 211])
   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 se debe asignar al sistema si la central no utiliza particiones.

Mediante el teclado

1. Seleccione **MODO TÉCNICO->ZONAS->(seleccione una zona)->TIPO DE ZONA->SÍSMICO**
2. Seleccione **MODO TÉCNICO->ZONAS->(seleccione una zona)->ATRIBUTOS->AUTOTEST SÍSMICO**

Ver también

- Temporizaciones [→ 244]
- Tipos de salida y puertos de salida [→ 211]
- Edición de una zona [→ 251]

21.1 Comprobación de detectores sísmicos

Las zonas sísmicas se deben configurar de modo que estén disponibles tanto los tests manuales como los automáticos. Los resultados de los tests, tanto manuales como automáticos, se almacenan en el registro de incidencias del sistema.

Durante un test sísmico se comprueban una o varias zonas sísmicas. Cuando se comprueba una zona sísmica, todas las demás zonas de la misma partición se deshabilitan temporalmente, pues solo hay una salida de test sísmico por cada partición.

21.1.1 Proceso de comprobación manual y automática

Una comprobación manual o automática funciona de la siguiente manera:

1. La central activa la salida de test sísmico para la partición o las particiones correspondientes en las que se debe(n) comprobar la(s) zona(s) sísmica(s).
2. A continuación, la central espera a que se abran las zonas sísmicas sometidas al test, y verifica que todos los detectores sísmicos de la partición entren en estado de alarma dentro del tiempo configurado para **"Duración test sísmico"**. Si alguna zona no se abre dentro del período máximo, se considerará que no ha pasado el test.

3. Cuando todas las zonas sísmicas de la partición estén abiertas o se haya alcanzado la duración máxima del test sísmico (lo que ocurra primero), la central borrará la salida de test sísmico para esa partición.
4. La central espera un tiempo determinado a que todos los detectores sísmicos de la partición se cierren. Si alguna zona no se cierra, se considerará que no ha pasado el test.
5. A continuación, la central espera otro intervalo de tiempo determinado antes de informar sobre el resultado del test. El resultado del test, tanto manual como automático, se almacena en el registro de incidencias del sistema.

La salida sísmica es normalmente alta, y va bajando durante los tests (esto es, cuando está activa). Si esta señal no es adecuada para un detector en particular, la salida física se puede configurar para que se pueda invertir.

21.1.2 Comprobación automática de detectores

Los detectores sísmicos se comprueban periódicamente o después de configurarse el sistema mediante el teclado.

Comprobación automática periódica

Los test automáticos periódicos se realizan en todas las zonas sísmicas para las que están habilitados los test automáticos.

Los test automáticos son aleatorios dentro del período de test configurado, y se realizan de manera independiente para cada partición.

Todas las zonas sísmicas en una misma partición (para la que estén habilitados los tests sísmicos) se comprueban simultáneamente.

La opción de configuración **Intervalo test sísmico** en el menú Temporizaciones [→ 244] determina el período de comprobación medio para tests automáticos de detectores sísmicos. El valor por defecto es 168 horas (7 días), y los valores permitidos se encuentran en un rango de entre 12 y 240 horas.

El tiempo de comprobación es aleatorio dentro del rango especificado ±15%. Por ejemplo, si hay un test programado cada 24 horas, se puede realizar un test entre 20,4 y 27,6 horas después del último test.

Un test sísmico se realiza después de un reinicio si están habilitados los tests automáticos. Si la central estaba en modo técnico antes del reinicio, el test solo se realizará después de que la central haya salido del modo técnico tras un reinicio.

Si un test sísmico resulta fallido, se notifica una incidencia de Problema (código SIA "BT"). También hay una incidencia de Restauración correspondiente (código SIA "BJ").

Test automático en Armado

La opción **Test manual sísmico** se puede configurar en el menú Opciones del sistema [→ 234]. Si está habilitada, todas las zonas sísmicas que se deben armar se comprueban antes de la secuencia de armado habitual. Esto solo es aplicable al funcionamiento con teclado.

Mientras se está realizando el test, en el teclado se indica "AUTOTEST SÍSMICO". Si el test sísmico es satisfactorio, el armado continúa normalmente.

Si se seleccionan todas las particiones, un grupo de particiones o una única partición para armar, y un test sísmico falla, se indicará "FALLO SÍSMICO". Si se pulsa la tecla de **Retorno** se muestra una lista de las zonas con fallos, por la que es posible desplazarse con las teclas de flecha hacia arriba y hacia abajo.

Dependiendo de la configuración de **Inhibición** para las zonas sísmicas con fallo y de su perfil de usuario, puede ocurrir lo siguiente:

- Si todas las zonas sísmicas que no han pasado el test tienen establecido el atributo **Inhibida**, y su perfil de usuario está configurado con la atribución **Inhibir**:

1. Pulse la tecla de **Retorno** en alguna de las zonas con fallo.
   ⇨ Se muestra el mensaje "¿Forzar A. todo?".
2. Vuelva a pulsar la tecla de **Retorno** para anular todas las zonas sísmicas que no hayan pasado el test. (Como alternativa, vuelva al menú anterior).
   ⇨ El armado continúa normalmente.

- Si alguna de las zonas sísmicas que no han pasado el test no tienen establecido el atributo **Inhibida**, y su perfil de usuario no cuenta con la atribución **Inhibir**:
- Pulse la tecla de **Retorno**.
  ⇨ Se mostrará el mensaje "FALLO AL ARMAR" y no se armará ninguna partición.

No hay test sísmico automático para las particiones que están autoarmadas por algún motivo (por ejemplo, particiones activadas por un calendario o una fuente). Asimismo, tampoco hay test sísmico automático cuando el sistema se arma con SPC Com, con SPC Pro o con el navegador. Sin embargo, hay test sísmico automático cuando se utiliza un teclado virtual con SPC Com o SPC Pro.

No se notifica ninguna incidencia si falla el test sísmico armado.

El temporizador de test de sistema automático periódico se reinicia tras realizarse un test después del armado.

21.1.3 Comprobación manual de detectores

Para comprobar manualmente los detectores, seleccione la opción TEST>TEST SÍSMICO en el menú TEST del teclado.

El test sísmico manual con el teclado puede ser realizado por el técnico en Modo técnico, y también por un usuario de tipo Maestro o de tipo Estándar:

- Un técnico puede comprobar todos los detectores en todas las particiones configuradas en el sistema mediante cualquier teclado.
- Un usuario solo puede comprobar los detectores en particiones que estén asignadas a él y al teclado en particular que esté utilizando.

Para realizar un test sísmico en Modo técnico, seleccione MODO TÉCNICO ⇒ TEST ⇒ TEST SÍSMICO

Para realizar un test sísmico en modo Usuario, seleccione MENÚS ⇒ TEST ⇒ TEST SÍSMICO

Nota: Las siguientes instrucciones son aplicables a los modos Técnico y Usuario, pero tenga en cuenta que es posible que para un usuario solo estén disponibles un pequeño conjunto de opciones.

En el menú TEST SÍSMICO están disponibles las siguientes opciones:

- TEST TODAS PART.
  Se comprueban todas las zonas sísmicas en todas las particiones disponibles si hay 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 de esta partición si hay más de una zona sísmica.
- *NOMBRE DE ZONA*
  Se listan los nombres de todas las zonas sísmicas, y 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".

Las entradas se graban en el registro de incidencias con los siguientes detalles:

- usuario que inició el test
- resultado (OK o FALLO)
- número y nombre de partición y de zona.

No se notifica ninguna incidencia para 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.

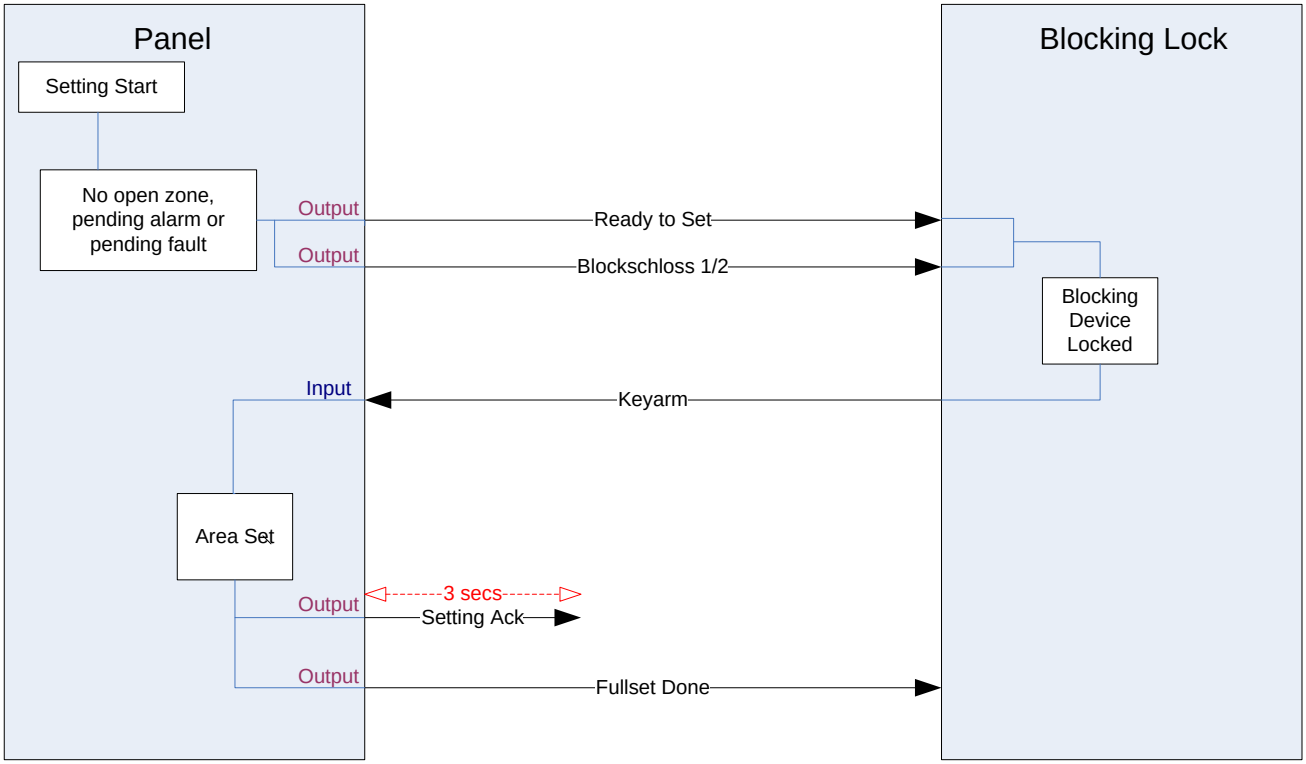
22.1 Cierre de bloqueo

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 está disponible la señal Listo para armar en 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
  - Config. ACK
  - Arm. total hecho
  - Blockschloss 1/2
- Entradas
  - Llave A/D

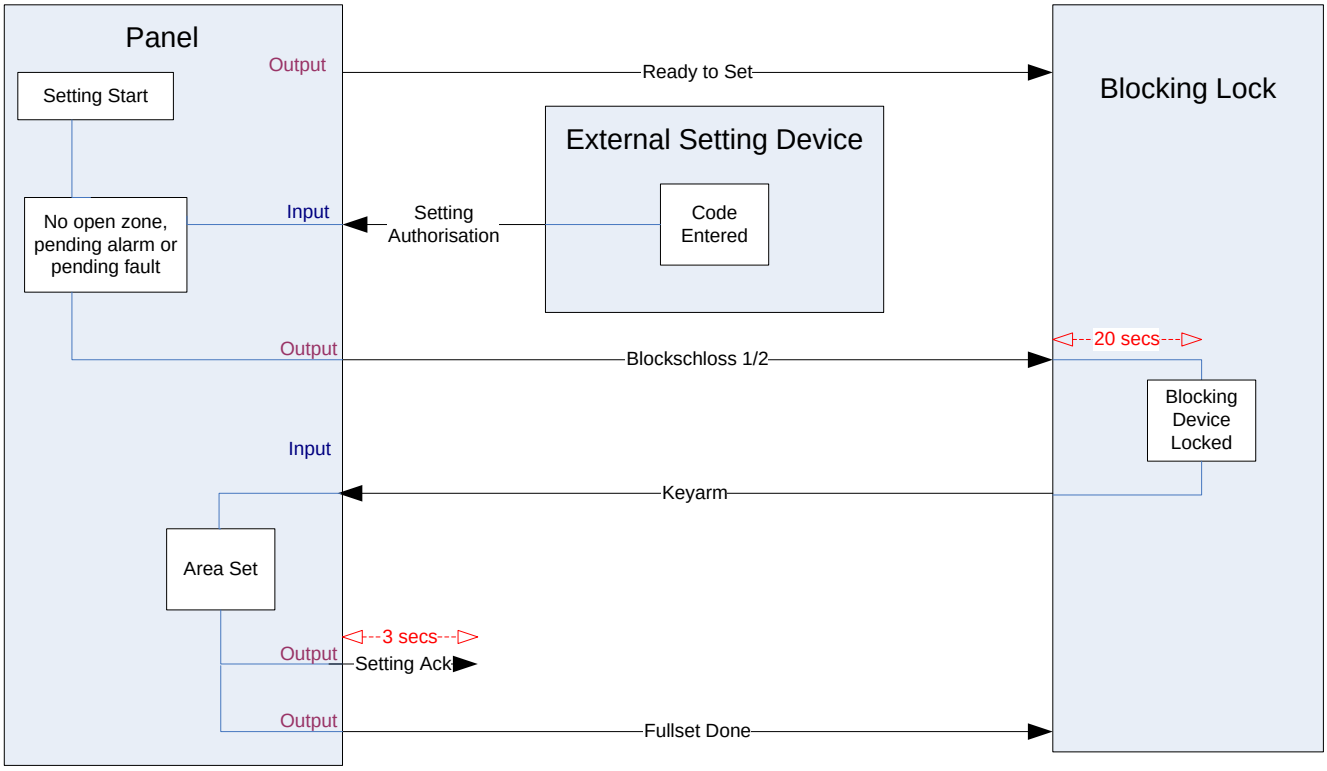
22.2 Armado autorizado del cierre de bloqueo

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
  - Config. ACK
  - Arm. total hecho
- Entradas
  - Llave A/D

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 - Desbloqueada**. 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

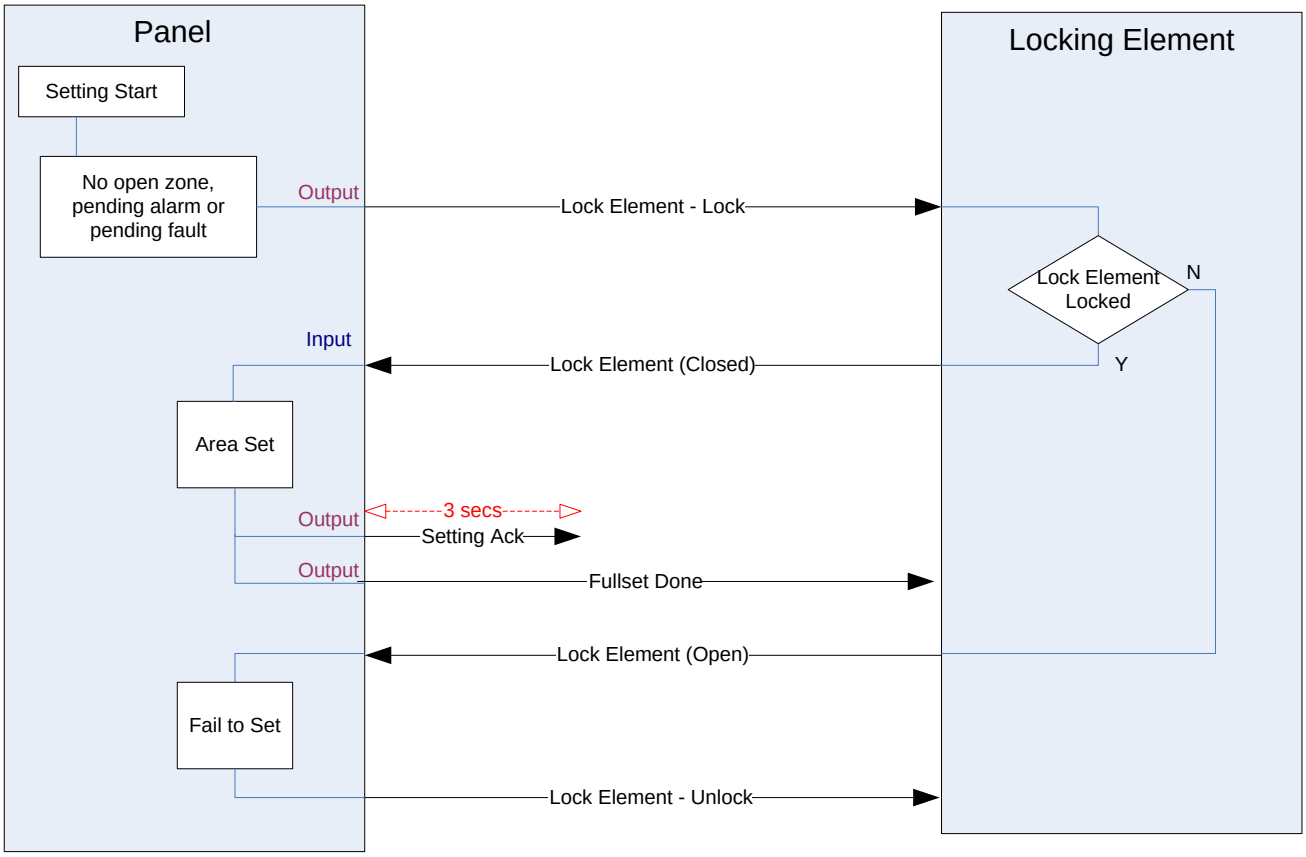
termine el temporizador de salida, la entrada del elemento de bloqueo debe estar cerrada, y entonces se arma el sistema.

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 del elemento de bloqueo (si está configurado) no está cerrada cuando finaliza el temporizador de salida, el sistema no se armará y se emitirá una señal de Fallo al armar. Se activará la salida Elemento bloqueo – Desbloqueada.



Los requisitos de configuración para el elemento de bloqueo son los siguientes:

- Salidas:
  - Elemento bloqueo - Bloqueo
  - Elemento bloqueo - Desbloqueada
- Entradas
  - Elemento bloqueo

23 Apéndice

23.1 Conexiones de cable de red

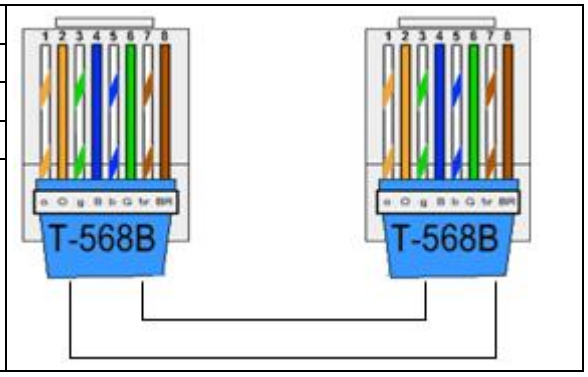
IP

Puede conectarse un PC directamente a la interfaz Ethernet del controlador SPC o a través de una conexión LAN. Las tablas siguientes muestran las 2 configuraciones de conexión posibles.

- 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.

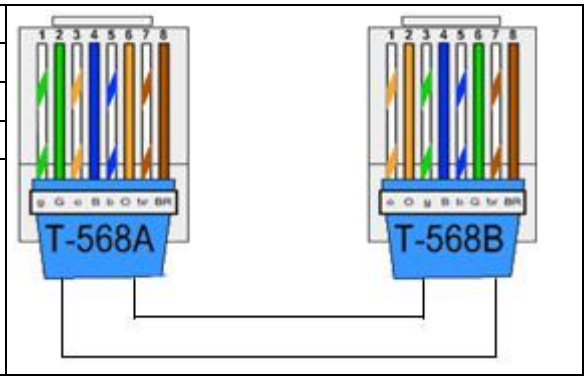
Utilice el cable directo para conectar el controlador SPC a un PC a través de un concentrador.

CONTACTO RJ45	CONTACTO 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 a un PC.

CONTACTO RJ45	CONTACTO RJ45
1 (RX +)	3 (TX+)
2 (RX -)	6 (TX-)
3 (TX+)	1 (RX +)
6 (TX-)	2 (RX -)



23.2 Los 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 de la 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 red ENCENDIDO: fallo de la red c. a. APAGADO: red de c. a. OK.
LED 4	Estado de X-BUS ENCENDIDO: La configuración de X-BUS es una configuración en lazo APAGADO: la configuración de X-BUS es una configuración en punta PARPADEANDO: detecta módulos de expansión RFL o rupturas en el cableado.
LED 5	Fallo del sistema ENCENDIDO: se ha detectado un fallo de hardware en la placa. APAGADO: no se ha detectado ningún fallo de hardware
LED 6	Escritura en memoria flash ENCENDIDO: el sistema está escribiendo en la memoria flash. APAGADO: el sistema no está escribiendo en la memoria flash.
LED 7	Telegrama de vida PARPADEANDO: el sistema está funcionando con normalidad.

ENCENDIDO	APAGADO	PARPADEANTE

23.3 Alimentación de módulos de expansión desde los terminales de alimentación auxiliares

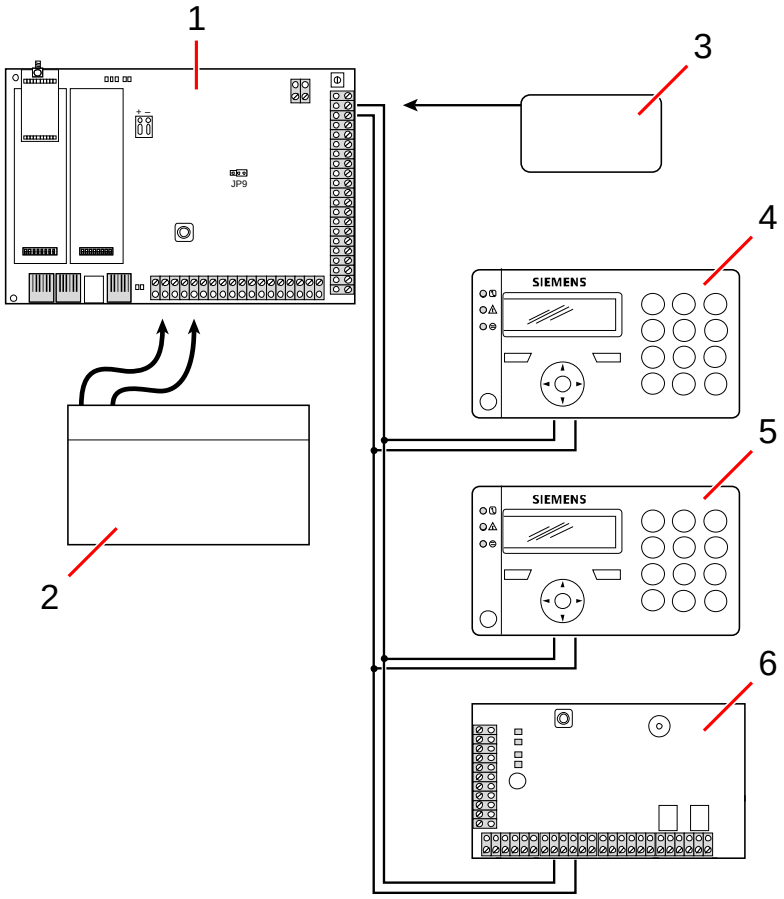
Para calcular el número de módulos de expansión y de teclados que pueden encenderse con seguridad desde los terminales de alimentación auxiliares de 12 V C.C., sume la corriente máxima total de todos los módulos de expansión y de los teclados que se deben alimentar, y determine si el total es inferior a la alimentación auxiliar especificada de 12 V C.C.

Véase Datos técnicos para consultar la corriente auxiliar específica, y las instrucciones de instalación correspondientes o la hoja de datos sobre el consumo de corriente de 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 a dispositivos externos, la alimentación suministrada a estos dispositivos deberá restarse de la alimentación auxiliar de 12 V C.C. 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.



Alimentación de módulos de expansión desde los terminales de alimentación auxiliares

1	Controlador SPC
2	Batería
3	Terminales de alimentación de 12 V auxiliares
4	Teclado
5	Teclado
6	Mód.exp.E/S

23.4 Cálculo de los requisitos de alimentación de la batería

Es importante que haya una fuente de alimentación en espera disponible para abastecer a todos los dispositivos en caso de que se produzca un fallo en el suministro de red. Para asegurarse de que hay suficiente alimentación disponible, conecte siempre la batería de apoyo y la unidad de fuente de alimentación apropiadas.

La tabla siguiente indica, de forma aproximada, la corriente de carga máxima que puede extraerse de cada tipo de batería en los períodos de espera determinados.

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.

0,85 x tamaño de la batería (Ah)	-	(I cont. + I sirena)	=	I máx.
Tiempo (horas)				

Tamaño de la batería = capacidad, en Ah, dependiendo de la carcasa de SPC elegida

Tiempo = tiempo de reserva, en horas, dependiendo del grado de seguridad

I cont. = Corriente de reposo (en A) para el controlador SPC

I sirena = Corriente de reposo (en A) para las sirenas exteriores e interiores conectadas

I máx. = 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.	Ninguna	RTB	GSM	RTB+GSM
Tiempo en espera				
12 h	356 mA	331 mA	226 mA	201 mA
30 h	58 mA	33 mA	N/A	N/A

Cantidad de corriente de la salida auxiliar utilizando una batería de 17 Ah (SPC523x)

Comunic.	Ninguna	RTB	GSM	RTB+GSM
Tiempo en espera				
12 h	750 mA	750 mA	750 mA	750 mA
30 h	342 mA	317 mA	212 mA	187 mA

Cantidad de corriente de la salida auxiliar utilizando una batería de 7 Ah (SPC432x/532x)

Comunic.	Ninguna	RTB	GSM	RTB+GSM
Tiempo en espera				
12 h	326 mA	301 mA	196 mA	171 mA
30 h	28 mA	N/A	N/A	N/A

Cantidad de corriente de la salida auxiliar utilizando una batería de 17 Ah (SPC533x/633x)

Comunic.	Ninguna	RTB	GSM	RTB+GSM
Tiempo en espera	mA	mA	mA	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.d. indican que la batería seleccionada no tiene capacidad para alimentar la carga mínima únicamente desde el controlador SPC para el tiempo de espera indicado. Consulte la página [→ 354] para ver la carga máxima de los dispositivos y módulos.

Sólo deben utilizarse tipos de batería de célula sellada reguladas por válvula.

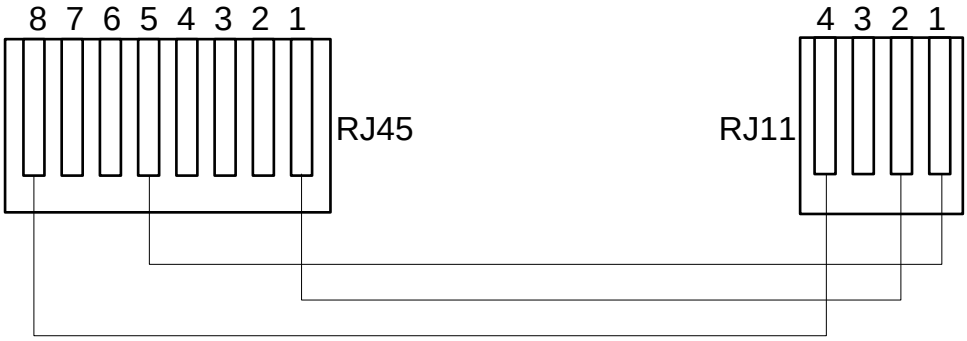
Para cumplir con los estándares EN, la batería debe suministrar corriente durante el periodo de espera necesario.

23.5 Configuración por defecto de modos doméstico, comercial y financiero

Esta tabla indica los nombres y tipos de zona por defecto del controlador para cada modo de funcionamiento. Todas las zonas de los módulos de expansión conectados se clasifican como sin uso hasta que el técnico instalador las configure explícitamente.

Función	Modo doméstico	Modo comercial	Modo financiero
Nombres de zona			
Controlador - Zona 1	Puerta entrada	Puerta entrada	Puerta entrada
Controlador - Zona 2	Salon	Ventana 1	Ventana 1
Controlador - Zona 3	Cocina	Ventana 2	Ventana 2
Controlador - Zona 4	Escalera delant.	PIR 1	PIR 1
Controlador - Zona 5	Escalera trasera	PIR 2	PIR 2
Controlador - Zona 6	PIR del vestíbulo	Salida incendio	Salida incendio
Controlador - Zona 7	PIR del rellano	Alarma incendio	Alarma incendio
Controlador - Zona 8	Pulsador de pánico	Pulsador de pánico	Pulsador de pánico
Tipos de zona			
Controlador - Zona 1	E/S	E/S	E/S
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 X-10



Cableado del X-10 al controlador

Código	RJ45	RJ11
TX	8	4
GND	5	1
RX	1	2

23.7 Códigos SIA

DESCRIPCIÓN	CÓDIGO
REPOSICIÓN RED CA	AR
FALLO RED C.A	AT
ALARMA ROBO	BA
ANULACIÓN ROBO	BB
CANCELACIÓN ROBO	BC
AVERÍA SWINGER	BD
REPOSICIÓN AVERÍA SWINGER	BE
REPOSICIÓN AVERÍA ROBO	BJ
REPOSICIÓN ROBO	BR
AVERÍA ROBO	BT
ROBO SIN ANULAR	BU
ROBO VERIFICADO	BV
TEST ROBO	BX
ARMADO TOTAL	CD
ARMADO TOTAL FORZADO	CF
PARTICIÓN EN ARMADO TOTAL	CG
FALLO DE ARMADO TOTAL	CI
TEMPRANO PARA ARMAR	CK
COMUNICACIÓN DE ARMADO TOTAL	CE
ARMADO TOTAL AUTOMÁTICO	CP
ARMADO TOTAL REMOTO	CQ
LLAVE DE ARMADO TOTAL	CS

DESCRIPCIÓN	CÓDIGO
TARDE PARA DESARMAR	CT
SEGUIMIENTO	DC
ACCESO DENEGADO	DD
PUERTA FORZADA	DF
ACCES.AUTORIZADO	DG
RETORNO DE ACCESO DENEGADO	DI
PUERTA DEJADA ABIERTA	DN
ACCESO ABIERTO	DO
REPOSICIÓN DE PUERTA	DR
SOLICITUD DE SALIDA	DX
ALARMA AL SALIR	EA
REPOSICIÓN TAMPER MÓDULO EXPANSIÓN	EJ
MÓDULO PERDIDO	EM
PÉRDIDA SOLUCIONADA MÓDULO EXPANSIÓN	ES
REPOSICIÓN MÓDULO EXPANSIÓN	ER
TAMPER MÓDULO EXPANSIÓN	ES
PROBLEMA DE EXPANSIÓN	ET
ALARMA INCENDIO	FA
INCENDIO ANULADO	FB
CANCELACIÓN INCENDIO	FC
REPOSICIÓN PROBLEMA INCENDIO	FJ
REPOSICIÓN INCENDIO	FR
PROBLEMA INCENDIO	FT
INCENDIO NO ANULADO	FU
ALARMA DE ATRACO	HA
ATRACO ANULADO	HB
REPOSICIÓN PROBLEMA ATRACO	HJ
REPOSICIÓN ATRACO	HR
PROBLEMA ATRACO	HT
ATRACO NO ANULADO	HU
ATRACO CONFIRMADO	HV
CÓDIGO TAMPER USUARIO ¦WEB o ¦XBUS	JA
HORA CAMBIADA	JT
PROGRAMACIÓN LOCAL	LB
RESTAURACIÓN DE MÓDEM ¦ 1 o 2	LR
PROBLEMA DE MÓDEM ¦ 1 o 2	LT
FIN PROGRAMACIÓN LOCAL	LX
ALARMA MÉDICA	MA
ALARMA MÉDICA ANULADA	MB

DESCRIPCIÓN	CÓDIGO
REPOSICIÓN PROBLEMA ALARMA MÉDICA	MJ
REPOSICIÓN ALARMA MÉDICA	MR
PROBLEMA ALARMA MÉDICA	MT
ALARMA MÉDICA NO ANULADA	MU
PERÍMETRO ARMADO	NL
RESTAURACIÓN IP ENLACE RED	NR
RESTAURACIÓN GPRS ENLACE RED	NR
FALLO IP ENLACE RED	NT
FALLO GPRS ENLACE RED	NT
DESARMADO AUTOMÁTICO	OA
PARTICIÓN DESARMADA	OG
DESARMADO PREMATURO	OK
COMUNICACIÓN DESARMADO	Ab
LLAVE DESARMADO	OS
ARMADO TARDE	OT
DESARMADO REMOTO	OQ
DESARMADO CON ALARMA	OR
ALARMA DE PÁNICO	PA
PÁNICO ANULADO	PB
REPOSICIÓN PROBLEMA PÁNICO	PJ
REPOSICIÓN PÁNICO	PR
PROBLEMA PÁNICO	PT
PÁNICO NO ANULADO	PU
CIERRE RELÉ	RC
RESET REMOTO	RN
APERTURA RELÉ	RO
TEST AUTOMÁTICO	RP
ENCENDIDO	RR
ÉXITO PROGRAMACIÓN REMOTA	RS
PÉRDIDA DATOS	RT
TEST MANUAL	RX
TAMPER	TA
TAMPER ANULADO	TB
REPOSICIÓN TAMPER	TR
TAMPER NO ANULADO	TU
LLAMADA DE TEST	TX
ALARMA INDETERMINADA	UA
ALARMA INDETERMINADA ANULADA	UB
REPOSICIÓN PROBLEMA INDETERMINADO	UJ

DESCRIPCIÓN	CÓDIGO
REPOSICIÓN ALARMA INDETERMINADA	UR
PROBLEMA INDETERMINADO	UT
ALARMA INDETERMINADA NO ANULADA	UU
FALLO SIRENA	YA
REPOSICIÓN INTERF.RF	XH
REPOSICIÓN TAMPER RF	XJ
LECTOR BLOQUEADO	RL
LECTOR DESBLOQUEADO	RG
TECLADO DESBLOQUEADO	KG
FALLO INTER. RF	XQ
TAMPER RF	XS
FALLO COMUNICACIÓN	YC
FALLO CHEKCSUM	YF
REPOSICIÓN SIRENA	YH
REPOSICIÓN COMUNICACIÓN	YK
PÉRDIDA BATERÍA	YM
PROBLEMA FUENTE ALIMENTACIÓN	YP
REPOSICIÓN FUENTE ALIMENTACIÓN	YQ
REPOSICIÓN BATERÍA	YR
PROBLEMA COMUNICACIÓN	YS
PROBLEMA BATERÍA	YT
RESET WATCHDOG	YW
SERVICIO REQUERIDO	YX
SERVICIO COMPLETADO	YZ
INCIDENCIAS SIA ESPECIALES	
CÓDIGO COACCIÓN	HA
REPOSICIÓN CÓDIGO COACCIÓN	HR
ENET ALARMA PÁNICO	PA
REPOSICIÓN ALARMA PÁNICO	PR
ALARMA PÁNICO USUARIO	PA
ENET ALARMA INCENDIO	FA
ENET REPOSICIÓN INCENDIO	FR
ENET ALARMA MÉDICA	MA
ENET REPOSICIÓN ALARMA MÉDICA	MR
PÁNICO HCD	PA
TILT HCD	MA
CLIP CINTURÓN HCD	HA
REPOSICIÓN PÁNICO HCD	PR
REPOSICIÓN TILT HCD	MR
REPOSICIÓN CLIP CINTURÓN HCD	HR
PÁNICO RPA	PA

DESCRIPCIÓN	CÓDIGO
REPOSICIÓN PÁNICO RPA	PR
Atraco RPA	HA
REPOSICIÓN 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
ZONA CORTA	ZX
ZONA DESCON.	ZD
ZONA ENMASCARADA	ZM
ZONA INTRUSIÓN	TP
INICIO TEST INTRUSIÓN	ZK
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 (V)	XD
RESTAURACIÓN DE BAJO VOLTAJE	XG
CARGA PROFUNDA	XK
Desbloqueada	WW

23.8 Códigos CID

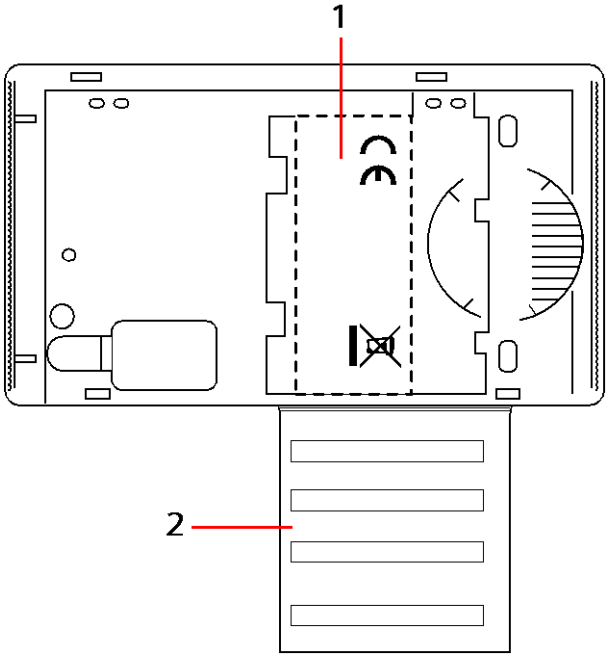
CÓDIGO	INCIDENCIA CID	DESCRIPCIÓN
100	MÉDICA	Alarma médica y de hombre caído y reposición
110	INCENDIO	
120	PÁNICO	
121	CÓDIGO COACCIÓN	
129	ATRACO CONFIRMADO	Consulte Requisitos de configuración para el cumplimento de la norma PD 6662:2010.

		[→ 26]
130	ROBO	
134	ENTRADA/SALIDA	
137	TAMPER	Fallo y reposición caja y tamper auxiliar
139	VERIFICADO	Alarma confirmada.
144	DETECTOR TAMPER	Fallo y reposición tamper de zona.
150	NO ROBO	
300	PROBLEMA DE SISTEMA	Fallo y reposición de fuente de alimentación.
301	PÉRDIDA CA	Fallo y reposición red eléctrica fuente de alimentación.
302	BAJA BATERÍA	
305	RESET	Restablecimiento del sistema
311	FALLO BATERÍA	Fallo y reposición batería fuente de alimentación.
312	SOBRECORRIENTE FUENTE DE ALIMENTACIÓN	Fallo y reposición fusible interno, externo y auxiliar de fuente de alimentación.
320	SIRENA	Fallo y reposición tamper de sirena.
330	PROBLEMA PERIFÉRICO DE SISTEMA	Fallo y reposición de fuente de alimentación.
333	FALLO EXP.	Fallo y reposición de comunicaciones de cable y nodo X-Bus.
338	BAT. EXP.	Fallo y reposición de batería de nodo X-Bus.
341	TAMPER EXP	Alarma y reposición de tamper de X-Bus y tamper de antena RF.
342	C.A. EXP	Fallo y reposición de red de nodo X-Bus.
344	Int.R.F.	Fallo y reposición de interferencias RF.
351	TELCO 1	Fallo y reposición de módem principal.
352	TELCO 2	Fallo y reposición de módem secundario.
376	PROBLEMA ATRACO	
380	PROBLEMA DETECTOR	
401	ABIERTO/CERRADO	Desarmado, post-alarma y armado total.
406	ABORTAR ALARMA	Cancelar alarma
451	ABIERTO/CERRADO PREMATURO	
452	ABIERTO/CERRADO TARDE	
453	FALLO DE DESARMADO	Desarmado tarde.
454	FALLO DE ARMADO TOTAL	Tarde para armar.
456	ARMADO PARCIAL INCIDENCIA	Armado parcial A y B.
461	COD.TMP.	Tamper de código de usuario.
466	SERVICIO	Modo técnico habilitado y deshabilitado.
570	ANULADO	Zona anulada y desanulada, zona aislada y desaislada.
601	TEST MANUAL	Test manual módem.
602	AUTO TEST	Test automático módem.
607	TEST INTRUSIÓN	

613	ZONA INTRUSIÓN	
614	INCENDIO ZONA INTRUSIÓN	
615	PÁNICO ZONA INTRUSIÓN	
625	REINICIO TIEMPO	Tiempo establecido.

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 PIN de usuario

El sistema admite códigos PIN de 4, 5, 6, 7 u 8 dígitos para cada usuario (códigos de usuario o de técnico) El número máximo de combinaciones/variaciones lógicas para cada número de dígitos de un código se puede ver en la siguiente tabla.

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:

$10^{\text{Nº de dígitos}}$ = Número de variaciones (incluyendo código 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. Para más información, consulte Códigos de técnico [→ 106].

23.11 Códigos 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 - 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 (p. ej. 2906, 2907), ya que al introducir este código desde el teclado se activaría una incidencia de coacción.

Una vez que se ha configurado el sistema para PIN +1 o PIN +2 en Opciones sistema [→ 234] y se han habilitado usuarios específicos para coacción (véase Usuarios [→ 193]), no se debe cambiar a no ser que se borren todos los usuarios y se reasignen nuevos códigos PIN de usuario.

23.12 Anulaciones automáticas

El sistema permite realizar anulaciones automáticas en los siguientes casos.

23.12.1 Zonas

Cuando se seleccionan GB e industrial (véase Estándares [→ 247]), el sistema proporcionará la funcionalidad DD243. En este caso, el sistema anulará zonas en las siguientes circunstancias:

- La zona de entrada no provocará una señal de alarma en la estación central, y no puede formar parte de una alarma confirmada, por lo que se anulará de forma efectiva tal como lo requiere DD243.
- Si se activa una única zona, y otra zona no se activa en el tiempo de confirmación (30 min. por defecto), pero la primera zona sigue activada, dicha primera zona se anulará automáticamente y no se activarán más alarmas desde esta zona durante el período configurado.

23.12.2 Códigos de acceso

Para sistemas de grado 2: Tras 10 intentos sin éxito con un código incorrecto, el teclado o navegador se deshabilitarán durante 90 s, y tras otros 10 intentos con un código incorrecto, el teclado o navegador se deshabilitarán durante otros 90 s. Cuando se haya introducido un código correcto, el contador volverá a cero, permitiendo realizar 10 intentos más antes de deshabilitarse.

Para sistemas de grado 3: Tras 10 intentos sin éxito con un código incorrecto, el teclado o navegador se deshabilitará durante 90 s, y tras cada nuevo intento con un código incorrecto, el teclado o navegador se deshabilitará durante otros 90 s. Cuando se haya introducido un código correcto, el contador volverá a cero, permitiendo realizar 10 intentos más antes de deshabilitarse.

23.12.3 Acceso de técnico

Un técnico solo puede acceder al sistema si lo permite un usuario tipo "Maestro" (véase el atributo "Técnico" en Derechos de usuario), y solo por un tiempo determinado (véase "Acceso técnico" en Temporizaciones [→ 244]).

23.12.4 Cierre de sesión de usuario de teclado

Si no se pulsa ninguna tecla del teclado durante un tiempo determinado (véase "Retorno teclado a normal' en Temporizaciones [→ 244]), la sesión del usuario se cierra automáticamente.

23.13 Cableado del cable de alimentación al controlador

Requisitos:

Se debe incorporar al cableado de la instalación del edificio un dispositivo de desconexión aprobado y de fácil acceso. Este dispositivo debe desconectar ambas fases al mismo tiempo. Los dispositivos que se aceptan son interruptores, disyuntores o similares.

- La sección mínima de conductor utilizada para conectar los cables es de 1,5 mm².
- Los interruptores automáticos deberán tener un poder de corte de 16 A.

El cable de alimentación se fija en el soporte metálico con forma de V de la placa base, mediante una abrazadera, de forma que el soporte metálico quede entre el cable y la abrazadera. Asegúrese de que se coloca la abrazadera para aislamiento adicional del cable de alimentación, es decir, el manguito exterior de PVC del cable. La abrazadera se deberá apretar firmemente de tal manera que el cable quede sujeto sin holgura alguna respecto a la abrazadera.

El conductor de toma de tierra para protección se debe fijar al bloque de terminales de tal modo que, si el cable de alimentación se sale de su anclaje provocando un tirón en los conductores, el conductor de toma de tierra para protección será el último elemento en sufrir el tirón.

El cable de alimentación debe ser de un tipo aprobado y marcado como HO5 VV-F o HO5 VVH2-F2.

La abrazadera de plástico debe tener un índice de inflamabilidad de V-1.

23.14 Controlador de mantenimiento

El servicio técnico del sistema debería realizarse de acuerdo con el calendario de mantenimiento vigente en el lugar. Las únicas piezas reemplazables en el controlador son el fusible de red, la batería en espera y la batería de fecha y hora (montada en la placa).

Se recomenda que, durante el servicio técnico, se compruebe lo siguiente:

- El registro de incidencias, para comprobar si algún test de batería en espera ha fallado desde el último servicio técnico; si ha fallado algún test de batería en espera, se debería comprobar la batería en espera.
- La batería en espera se debería reemplazar conforme al programa de servicio técnico para garantizar que posee la suficiente capacidad como para mantener el sistema en funcionamiento durante el tiempo definido en el diseño del sistema. La batería se debería inspeccionar físicamente para detectar cualquier posible deformación de la carcasa o cualquier indicio de fuga; si se da alguna de estas condiciones, la batería se deberá reemplazar inmediatamente.

i	*AVISO*
	La nueva batería deberá tener una capacidad igual o mayor (hasta el máximo admitido para el sistema).

- Si salta el fusible de red, se debería comprobar el sistema para detectar las posibles causas. El fusible se debería reemplazar por otro con el mismo amperaje. El amperaje se indica en la etiqueta del sistema, situada en la parte trasera de la caja.
- La batería de fecha y hora incorporada en la placa, de litio, únicamente se utiliza cuando el sistema se queda sin alimentación; en este estado, la batería tiene un tiempo de vida de aproximadamente 5 años. La batería se debe inspeccionar visualmente una vez al año, y desconectarse la alimentación del sistema por completo para comprobar si mantiene la fecha y la hora. Si el sistema no mantiene la fecha y la hora, la batería se deberá reemplazar por una nueva del tipo célula de litio CR1216.
- Se deberían inspeccionar todas las conexiones eléctricas para comprobar que cuentan con aislamiento y no hay riesgo de cortocircuitos o desconexiones.
- También se recomienda comprobar cualquier nota de actualización de firmware por si existe alguna actualización adicional que pueda mejorar la seguridad del sistema.
- Compruebe que todos los montajes físicos estén intactos. Cualquier montaje defectuoso se deberá reemplazar con las mismas piezas.

23.15 Fuente de alimentación inteligente para

mantenimiento

El servicio técnico del sistema debería realizarse de acuerdo con el calendario de mantenimiento vigente en el lugar. Las únicas piezas reemplazables en la fuente de alimentación inteligente son el fusible de red y la batería en espera.

Se recomienda que, durante el servicio técnico, se compruebe lo siguiente:

- El registro de incidencias del controlador, para comprobar si algún test de batería en espera ha fallado desde el último servicio técnico; si ha fallado algún test de batería en espera, se debería comprobar la batería en espera.
- La batería en espera se debería reemplazar conforme al programa de servicio técnico para garantizar que posee la suficiente capacidad como para mantener el sistema en funcionamiento durante el tiempo definido en el diseño del sistema. La batería se debería inspeccionar físicamente para detectar cualquier posible deformación de la carcasa o cualquier indicio de fuga; si se da alguna de estas condiciones, la batería se deberá reemplazar inmediatamente.

	AVISO
	La nueva batería deberá tener una capacidad igual o mayor (hasta el máximo admitido para el sistema).

- Compruebe que los LED del panel de control de la fuente de alimentación estén en el estado esperado. Consulte la documentación de la fuente de alimentación inteligente para conocer más detalles sobre los LED.
- Si salta el fusible de red, se debería comprobar el sistema para detectar las posibles causas. El fusible se debería reemplazar por otro con el mismo amperaje. El amperaje se indica en la etiqueta del sistema, situada en la parte trasera de la caja.
- Se deberían inspeccionar todas las conexiones eléctricas para comprobar que cuentan con aislamiento y no hay riesgo de cortocircuitos o desconexiones.
- También se recomienda comprobar cualquier nota de actualización de firmware por si existe alguna actualización adicional que pueda mejorar la seguridad del sistema.
- Compruebe que todos los montajes físicos estén intactos. Cualquier montaje defectuoso se deberá reemplazar con las mismas piezas.

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 exclusivo (una marca o indicador interno) que puede conectarse o asignarse a una salida física para la activación de un dispositivo específico si fuera necesario.

Tipo de zona	Procesando categoría	Descripción
Alarma	Intruso	Este tipo de zona es la configuración de tipo de zona por defecto y, además, es el tipo de zona que se usa con más frecuencia en las instalaciones estándar. La activación, en cualquier modo, de Abierta, Desconectada o Tamper (excepto en Desarmado) provoca una alarma total inmediata. En el modo Desarmado, se registran las condiciones de Tamper, produciéndose el mensaje de alerta TAMPER ZONA y activándose una

		alarma local. En los modos A.parc.A, A.parc.B y A.total se registran todas las actividades.
E/S	Intruso	Este tipo de zona debe asignarse a todas las zonas dentro de una ruta de entrada y salida (por ejemplo, una puerta delantera u otra partición de acceso al edificio o a las instalaciones). Este tipo de zona proporciona un retardo temporal a la entrada y a la salida. El temporizador de entrada controla este retardo. Cuando el sistema se está armando totalmente, este tipo de zona proporciona un retardo de salida que deja tiempo para que se vacíe la partición. El temporizador de salida controla este retardo. En el modo A.parc.A, este tipo de zona permanece inactiva.
TERMINADOR DE SALIDA	Intruso	Este tipo de zona se utiliza junto con un botón en una ruta de salida y actúa como un terminador de salida, es decir, proporciona un periodo de retardo de salida infinito y no permite que el sistema se arme hasta que se pulse dicho botón.
INCENDIO	Atraco	Las zonas de incendio son zonas con control de incendios durante las 24 horas y su respuesta es independiente del modo de funcionamiento de la central. Cuando se abre una zona de incendio, se genera una alarma total y se activa el tipo de salida INCENDIO. Si se configura el atributo "Sólo TX", sólo se informará de la activación a la estación central y no se generará una Alarma total.
SALIDA INCENDIO	Atraco	Se trata de un tipo especial de zona de 24 horas para uso con puertas de salida de incendios que nunca se deberían abrir. En modo Desarmado, si se activa esta zona se activará la salida Inc.X, provocando mensajes de alerta.
Línea	Fallo	Entrada de control de la línea de telemetría. Suele utilizarse junto con una salida de línea de teléfono correcta desde un marcador digital externo o un sistema de comunicación de línea directa. Cuando se activa, produce una alarma local en modo Desarmado y una alarma total en los demás modos.
ALARMA DE PÁNICO	Atraco	Este tipo de zona se mantiene activa 24 horas al día, y se activa mediante un botón de pánico. Cuando se activa una zona de pánico, ésta informa de una incidencia de pánico independientemente del modo de armado de la central. Si el atributo de registro está activado, se registrará y se informará de todas las activaciones. Si está establecido el atributo SILENCIO, la alarma será silenciosa (se informa de la activación a la CRA). De lo contrario, generará una alarma total.
ALARMA DE ATRACO	Atraco	Este tipo de zona se mantiene activa 24 horas al día, y se activa mediante 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 el modo Desarmado, se generará una alarma local, pero no se activará ninguna sirena exterior. Si el sistema está en modo Armado total, se genera una alarma total. Si el Grado de seguridad del sistema se ha configurado con el Grado 3, se necesitará un código de técnico para restaurar la alarma.
ALARMA TÉCNICA	Intruso	La zona técnica controla una salida de zona técnica dedicada. Cuando una zona técnica cambia de estado, la salida de la misma también lo hace. Es decir: ● Cuando la zona técnica se abre, se activa la salida de la misma ● Cuando la zona técnica se cierra, su salida se apaga Si se ha asignado más de una zona técnica, la salida de la zona técnica seguirá activada hasta que se cierren todas las zonas técnicas.
MÉDICA	Atraco	Este tipo de zona se utiliza conjuntamente con interruptores médicos vía radio o cableados. La activación en cualquier modo: ● activará la salida del comunicador digital médico (a menos que el atributo Local esté configurado).

		● Provocará que suene el zumbador del panel (a menos que esté establecido el atributo Silencio). ● Mostrará el mensaje Alarma médica.
Llave armado	Intruso	Este tipo de zona suele utilizarse junto con un mecanismo de bloqueo de teclas. Una zona de Llave de armado ARMARÁ el sistema / la partición / las particiones comunes cuando se ABRA, y DESARMARÁ el sistema / la partición / las particiones comunes cuando se CIERRE. ● Si la zona con el tipo de zona Llave armado está asignada en un sistema sin particiones, el funcionamiento de Llave armado ARMARÁ o DESARMARÁ el sistema. ● Si la zona con el tipo de zona Llave armado está asignada a una partición, el funcionamiento de Llave armado ARMARÁ o DESARMARÁ la partición. ● Si la zona con el tipo de zona Llave armado está asignada a una partición común, el funcionamiento de Llave armado ARMARÁ o DESARMARÁ todas las particiones en la partición común. ● Si está establecido el atributo "Sólo abrir", el estado de armado del sistema, de la partición, o de las particiones comunes cambiará cada vez que se abra el desbloqueo de las teclas. (P. ej. abra una vez para ARMAR el sistema, cierre y abra de nuevo para DESARMAR). ● Si está establecido el atributo "Habilit.a.total", la activación de la zona sólo armará totalmente el sistema. ● Si está establecido el atributo "Habilit.desarm.", la activación de la zona sólo desarmará el sistema. El uso de Llave armado armará de forma forzada el sistema o la partición y autoanulará cualquier zona abierta o condición de fallo. **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.**
Silenciosa	Intruso	Este tipo de zona sólo está disponible en el modo de funcionamiento Comercial. Aunque el tipo de zona de alarma de anulación ligada se puede configurar en modo de funcionamiento Doméstico, no tiene ningún efecto. Este tipo de zona, al abrirse, anula todas las zonas que tienen establecido el atributo de Anulación ligada. Esta operación es válida tanto para el modo ARMADO como para el DESARMADO. En cuanto se cierra la zona de Anulación ligada, las zonas que tengan el atributo Anulación ligada activado dejarán de estar anuladas.
Anul.siguie.	Intruso	Este tipo de zona sólo está disponible en el modo de funcionamiento Comercial. Una zona programada con el tipo de zona Anulación siguiente anula la siguiente zona consecutiva del sistema cuando se abre. Esta operación es válida tanto para el modo ARMADO como para el DESARMADO. En el momento en que se cierra la zona de tipo Anulación siguiente, la siguiente zona deja de estar anulada.
FALLO DE DETECTOR	Fallo	Las zonas de fallo de detector son zonas de 24 horas aplicables a un dispositivo detector, por ejemplo un PIR. El tipo de zona de fallo activa la 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.
XShunt	Intruso	Sólo disponible en modo Comercial. Sirve para supervisar un bloqueo de puerta. El sistema se puede programar para que no se arme a no ser que la puerta esté bloqueada.
SÍSMICO	Intruso	Solo disponible si la central está en modo de funcionamiento Financiero. Los detectores de vibración, también llamados detectores sísmicos, sirven para detectar intentos de intrusión por medios mecánicos, p. ej. taladrando o haciendo agujeros en paredes o cajas fuertes.
Todo OK	Intruso	Este tipo de zona habilita la implantación de un procedimiento de entrada especial mediante un código de usuario y una entrada de "Todo OK". Si no se pulsa un botón de Todo OK dentro de un tiempo configurable después de introducirse un código de usuario, se genera

		una alarma silenciosa. (Véase Particiones [→ 251] para más información sobre la configuración de "Todo OK"). La función "Todo OK" utiliza dos salidas, Estado entrada (LED verde) y Estado aviso (LED rojo), para indicar un estado de entrada mediante los LED del teclado.
Sin utilizar	Intruso	Permite que una zona se deshabilite sin necesidad de que cada zona tenga resistencias RFL instaladas. Se ignorará cualquier activación en la zona.
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 activa la 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 notificará los mensajes SIA, HT (Problema atraco) y HJ (Reposición problema atraco) y para CID, se producirá una incidencia de problema de sensor (380).
FALLO DE ADVERTENCIA	Fallo	Las zonas de fallo de advertencia son zonas de 24 horas aplicables a un dispositivo señalizador de advertencia, por ejemplo una sirena interna o externa. El tipo de zona de fallo activa la 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 notificará los mensajes SIA, YA (Fallo sirena) y YH (Reposición sirena) y para CID, se producirá una incidencia de problema de sensor (380). **Nota:** En un sistema de grado 2, un fallo de cable provoca un fallo y no una alarma.
AUTORIZACIÓN DE ARMADO.	Intruso	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	Intruso	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.
ROTURA DE CRISTAL	Intruso	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.

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 se establece el atributo "Seguimiento" en una zona, al abrirla no se generará una alarma si el temporizador de entrada o el de salida están funcionando. Cuando el sistema está en modo Armado total, el atributo Seguimiento no estará activo y, al abrirse una zona, se iniciará una alarma total. El atributo "Seguimiento" se utiliza principalmente para detectores PIR ubicados cerca de una zona de E/S. Permite al usuario moverse libremente dentro del área de acceso mientras el temporizador de entrada o de salida realiza su cuenta atrás. El atributo "Seguimiento" sólo es válido para tipos de zona de Alarma. Todos los dispositivos conectados (sirenas interiores y exteriores, zumbadores, flashes) están activados. NOTA: Una zona de alarma con el atributo Seguimiento puede cambiarse automáticamente a una zona de E/S en el modo Armado parcial si está establecida la opción Acceso en armado parcial.
Excl.A.parc.A	Si está establecido el atributo "Excl.A.Parc.A" en una zona, no se generará una alarma con la apertura de dicha zona mientras la central se encuentre en modo Armado parcial A. El atributo "Excl.A.Parc.A" es válido sólo para los tipos de zona de Alarma y las zonas de E/S. Se genera una alarma TOTAL si se abre una zona con el atributo Excl.A.Parc.A cuando el sistema está en modo ARMADO TOTAL o en modo A.Parc.B (sirenas interiores y exteriores, flash).
Excl.A.parc.B	Cuando se establece el atributo "Excl.A.parc.B", la apertura de la zona no generará una alarma mientras la central se encuentre en modo A.parc.B. El atributo "Excl.A.parc.B" es válido sólo para los tipos de zona Alarma y las zonas de entrada/salida. Se genera una alarma TOTAL si se abre una zona con el atributo Excl.A.parc.B cuando el sistema está en modo ARMADO TOTAL o Excl.A.parc.A (sirenas interiores y exteriores, flash).
24 horas	Si se asigna el atributo "24 horas" a una zona, éste estará activo en todo momento y provocará una alarma total si se abre en cualquier modo. Este atributo sólo se puede asignar al tipo de zona ALARMA. Genera una alarma TOTAL en los modos DESARMADO, ARMADO y ARMADO PARCIAL. NOTA: El atributo 24 horas anula la configuración de cualquier otro atributo para una zona de alarma concreta.
Local	Cuando se establece el atributo "Local", la alarma generada por la apertura de una zona no provocará un informe externo de la incidencia. El atributo "Local" es válido para los tipos de zona Alarma, E/S, Incendio, Salida incendio y Alarma médica.
Desarmado local	Con este atributo, una alarma generada por la apertura de la zona cuando la partición esté total o parcialmente armada se notificará del modo habitual. Sin embargo, si la partición está desarmada, solo habrá una alarma local, es decir, zumbador de teclado, parpadeo de LED y visualización de zona. Este atributo solo es aplicable a zonas de Alarma, Incendio y Sísmicas.
Doble detección	Utilice este atributo para resolver los problemas que presenten los detectores. (P. ej. algunos detectores pueden generar señales de activación falsas y, como consecuencia, pueden disparar, inadvertidamente, alarmas de activación en el sistema). Si la misma zona de doble detección se activa dos veces durante el período de doble detección, se generará una alarma. El tiempo de doble detección se establece en segundos (consulte la página [→ 244]). Tener dos acciones abiertas durante dicho periodo de tiempo generará una alarma. Cuando el sistema está armado, se registran todas las zonas de doble detección abiertas.
Chime	Cuando está establecido el atributo "Chime" para una zona, cualquier apertura de la zona durante el modo Desarmado provocará que se activen

	los zumbadores internos durante un breve periodo (2 segundos aprox.). El atributo Chime es válido para los tipos de zona Alarma, E/S y Técnica.
Inhibir	Cuando el atributo "Anulación" está configurado, un usuario puede anular esta zona. La operación de anulación deshabilitará dicho fallo o zona solo durante un periodo 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 se establece el atributo "Silenciosa", no habrá indicaciones sonoras ni visuales de la Alarma. La activación de la alarma se enviará a la estación del receptor. Si el sistema está desarmado, se mostrará un mensaje de advertencia en la pantalla.
Registro	Si este atributo está activado, se registrarán todos los cambios de estado de zona.
Salida abierta	Si está seleccionado, se indicará la zona si se encuentra abierta durante el armado.
Supervisada	Este atributo sólo se aplica al Mantenimiento remoto*. Si una zona tiene configurado este atributo, dicha zona debe abrirse para fines de funcionamiento remoto durante el periodo de tiempo frecuente definido.
RFL	El atributo Fin de línea (RFL) proporciona al sistema un número de configuraciones de cableado de zona de entrada.
Analz.	El atributo Analz. debe establecerse en una zona si ésta se encuentra conectada con un sensor inercial. Los valores Conteo impulsos y Ataque serio deben programarse para cada sensor inercial del sistema de acuerdo con los resultados de una calibración sencilla del dispositivo.
Conteo impulsos	Nivel de disparo por conteo de impulsos para detectores inerciales analizados.
Ataque serio	Nivel de disparo de ataque grave para detectores inerciales analizados.
Fin de salida	El atributo Fin de salida sólo puede asignarse a una zona de tipo Entrada/salida. Utilice este atributo para anular el proceso estándar de cuenta atrás del temporizador de salida cuando el sistema esté en modo Armado total. Cuando todas las demás rutas de E/S de las instalaciones estén cerradas, arme totalmente el sistema y cierre la zona de salida/entrada final. En cuanto se cierre la puerta, el tiempo de Fin de salida empezará a avanzar para armar el sistema.
Anulación ligada	Una zona que tenga establecido el atributo Anul.ligada se anulará siempre que una zona de tipo Anul.ligada esté abierta. Esto ofrece un mecanismo para agrupar la anulación de zonas con la apertura de una zona de tipo Anul.ligada.
Sólo TX	Este atributo sólo se aplica a las zonas de tipo INCENDIO. Si este atributo está establecido, la activación de la zona de Incendio sólo será informará a la estación central. No se generarán alarmas in situ.
Sólo abrir	Este atributo sólo se aplica a las zonas de tipo LLAVE ARMADO. Si se habilita, el estado de armado del edificio se activará sólo con las aperturas.
Habilt.a.total	Este atributo sólo se aplica a las zonas de tipo LLAVE ARMADO. Si se establece este atributo, la activación de zona armará totalmente el sistema o la partición. Utilice este atributo si pretende que el usuario tenga sólo la posibilidad de ARMAR TOTALMENTE el sistema desde una zona de Llave armado.
Desarmado	Este atributo sólo se aplica a las zonas de tipo LLAVE ARMADO. Si se establece, la activación de zona desarmará el sistema o la partición. Utilice este atributo si pretende que el usuario sólo pueda tener la posibilidad de DESARMAR el sistema desde una zona de Llave armado.
Informe zona técnica	Permite que una zona, al abrirse, con independencia del modo, envíe una alarma a la CRA en FF, CID, SIA y SIA extendido. Cuando se seleccionan particiones, sólo se enviará la alarma a la CRA a la que se haya asignado la partición. Si se selecciona SIA extendido, esta será una Alarma desconocida

	seguida del número de zona y un texto. También enviará un SMS al usuario final y al técnico si se ha escogido esta opción cuando se seleccione el filtro de alarma no confirmada.
Pantalla zona técnica	Permite que se muestre una zona de apertura en el teclado del sistema. También debe activarse el LED de alerta. Cuando se seleccionan particiones, este sólo se mostrará en el teclado que esté asignado a la partición en la que se ha seleccionado la zona. La alerta sólo se puede mostrar en el teclado cuando la partición esté en modo Desarmado y no en los modos A.P.A, A.P.B y Armado.
Audible 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 zona técnica	Permite a la zona disponer de un retardo programable. El retardo puede variar entre 0 y 9999 segundos y se aplicará a todas las zonas técnicas. El funcionamiento es el mismo que el del temporizador Retardo red c. a.; si la zona se cierra durante el tiempo de retardo, no se envía alarma a la CRA, ni SMS al usuario, y la salida técnica no se activará. NOTA: La salida técnica no se activará hasta que haya finalizado el temporizador de retardo.
Sólo TX armado	Sólo se informa de las aperturas en modo Armado.
Prealarma incendio	Si está habilitado cuando se produce un incendio, se pone en marcha un temporizador de prealarma de incendio y se activan las sirenas interiores y los zumbadores. (Consulte Temporizaciones [→ 244]). Si la alarma no se cancela durante la duración del temporizador, la alarma de incendio se confirma, las sirenas interiores y exteriores se activan, y se envía una incidencia a la CRA.
Reconocimiento alarma incendio	Si esta opción está habilitada, se activa un temporizador de reconocimiento de alarma de incendio que añade tiempo adicional al temporizador de prealarma de incendio hasta que se notifica una alarma de incendio para la zona. Consulte Temporizaciones [→ 244].
Test sísmico / Test de detector automático	Un tipo de zona sísmica se puede comprobar manual o automáticamente. Este atributo permite habilitar la comprobación automática. Consulte la sección temporizaciones [→ 244] para 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 por defecto para el temporizador es de 7 días.
Timed	El atributo "retraso" sirve para que las zonas de Llave armado retrasen el armado de una partición. El retraso sigue al temporizador de salida para la partición con la que está asociada el armado con llave.
Verificación	Seleccione la zona de verificación configurada que se debe asignar a esta zona para activar la verificación de audio/vídeo.
Armado forzado	Si está habilitado, el dispositivo de llave armado puede armar el sistema inhibiendo todas las zonas abiertas.

23.18 Atributos aplicables a tipos de zona

La tabla siguiente muestra los atributos que se pueden aplicar 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	√																							√
Exclude A	√	√																					√	√
Exclude B	√	√																					√	√
24 Hour	√																	√						√
Local	√	√		√	√						√					√				√	√		√	√
Unset Local	√			√														√						√
Double Knock	√																							√
Chime	√	√								√												√		√
Inhibit	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√		√	√
Normal Open	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√		√	√	√	√	√	√
Silent	√						√	√																√
Log	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√
Shunt	√	√			√																			√
Frequent *	√	√	√							√		√		√	√									√
Analyzed	√	√			√																			
Pulse Count	√	√			√																			
Gross attack	√	√			√																			
Calendar	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√
Verification	√	√		√	√		√	√		√	√							√						√
Exit Open		√																						
Seismic Test																		√						
Timed												√												
Report Only				√																				
Open Only												√										√		
Final Exit		√																					√	
Fullset enable												√												
Unset enable												√												
Shunt	√	√			√																			√
Report (Tech)										√														
Display(Tech)										√														
Audible (Tech)										√														
Delay (Tech)										√														
Report When Set										√														
Fire Pre-alarm				√	√																			
Fire Recognition				√	√																			
Force set												√												

Sólo disponible en modo Comercial.

** Sólo en combinación con el Mantenimiento remoto.*

*** Sólo disponible en modo Financiero*

23.19 Niveles y especificaciones de atenuación del STA

Niveles del STA (Sistema de Transmisión de Alarmas)

En la siguiente tabla se muestra una lista de los niveles del STA necesarios para el panel a la hora de comunicar a través de:

- GSM a Central de Recepción de Alarmas (CRA)
- RTB a Central de Recepción de Alarmas (CRA)
- Ethernet a software receptor SPC Comm
- GPRS a software receptor SPC Comm

	GSM CRA	RTB CRA	Ethernet	Conectado
Nivel de STA	STA 2	STA 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 Cat5 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 -95 dB. Por debajo de este nivel, el módem notificará al panel un fallo de señal débil. Este fallo se tratará del mismo modo que otros fallos en el sistema.

Supervisión y vigilancia de RTB (SPCN110) y GSM (SPCN310)

Un fallo de la interfaz entre el módem RTB y el panel se detectará al cabo de 30 segundos, tiempo tras el cual se producirá un fallo del STA.

Un fallo de la interfaz entre el módem GSM y el panel se detectará al cabo de 30 segundos, tiempo tras el cual se producirá un fallo del STA.

23.20 Lectores de tarjeta y formatos de tarjeta admitidos

El sistema SPC admite los siguientes lectores de tarjeta y formatos de tarjeta:

Lector	Formato tarjeta
HD500-EM PR500-EM SP500-EM PM500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-RX AR6182-RX	IB41-EM IB42-EM IB44-EM IB45-EM

Lector	Formato tarjeta
	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
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

Formato del lector	Código local disponible	Restricciones
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 x 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 más información, véase MODO DE DIRECCIONAMIENTO [→ 134].

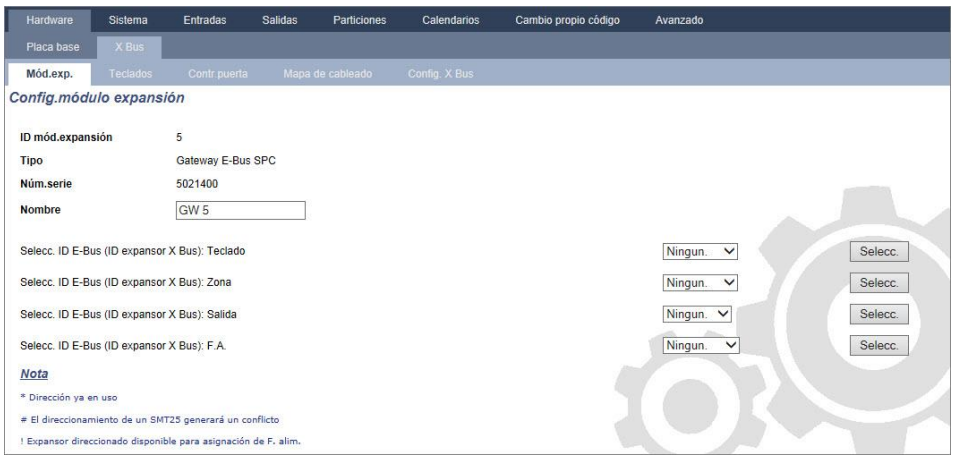
!	*AVISO*
	Vanderbilt recomienda leer el documento **Migración del sistema Sintony** antes de configurar dispositivos E-Bus.

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
- 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 de expansión**.
   ⇨ Se muestra una lista de **Módulos de expansión configurados**.
2. Seleccione un **Gateway E-Bus SPC**.
3. En la pantalla **Configuración de módulo de expansión**, introduzca una **Descripción** para el **Gateway E-Bus SPC**. Para más información sobre la configuración de módulos de expansión, véase Módulos de expansión [→ 217].



4. Para direccionar un dispositivo E-Bus, seleccione un ID del menú desplegable correspondiente descrito en la tabla de abajo. 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**.
   - ⇨ `Dirección en progreso.....Será necesaria la reconfiguración de X-Bus` se muestra en la parte superior de la pantalla.
   - ⇨ 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**.
   - ⇨ `Reconfiguración completada.` se muestra en la parte superior de la pantalla. Las entradas y las salidas de E-Bus se muestran en la lista de los **Módulos expansión configurados.** Si un transpondedor de entrada posee una fuente de alimentación asociada, el tipo de fuente de alimentación se mostrará en la columna **F.A.**. 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**, véase Direccionamiento de transpondedores para SAP 8, SAP 14 y SAP 20 [→ 380].
10. Si el X-BUS posee conflictos de direccionamiento, se mostrará la advertencia `ID duplicada o no válida para 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.
Fuente de 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.

Ver también

MODO DE DIRECCIONAMIENTO [→ 134]

23.21.1.1 Direccionamiento de transpondedores para SAP 8, SAP 14 y SAP 20

Tras asignar un ID de fuente de alimentación a un SAP 8, SAP 14 o SAP 20 (véase Configuración y direccionamiento de dispositivos E-Bus [→ 378]), debe asignar un transpondedor de entrada a la fuente de alimentación. 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 pantalla **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 [→ 378]. Se aplica la fórmula `2n - 1`, siendo `n` 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 fuentes 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

Acrónimo	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 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 instalaría en una CRA.
AS	**Sistema de alarma** Instalación eléctrica capaz de reaccionar de forma manual o automático ante la presencia de un riesgo. El AS (sistema de alarma) no es parte del ATS (sistema de transmisión de alarma)	Central SPC
ATR	**Equipo de transmisión de alarma** Término que describe el STP (transmisor bidireccional o transceptor supervisado de la	-

	instalación) y el RCT (receptor o transceptor de la CRA).	
ATP	**Ruta de transmisión de alarma** Ruta por la que se transfiere un mensaje de alarma entre un AS (sistema de alarma individual) y un AE (equipo de aviso al operador de la CRA de la recepción de este mensaje). La ATP comienza en el interfaz entre el AS (sistema de alarma) y su SPT (TX bidi de la instalación) y finaliza en el interfaz entre RCT (RX de la CRA) y el AE. Para verificación y vigilancia puede usarse el sentido inverso (bidireccionalidad).	Ruta definida entre la central SPC y la aplicación SPC Com XT o equivalente. Por ejemplo, un sistema con Ethernet o una VPN como ruta primaria y GPRS (dentro de Internet o de la VPN) como ruta de backup se consideran 2 ATPs separadas dentro de un ATS.
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 varias rutas de comunicación entre la central SPC y la aplicación SPC Com XT o equivalente.
RCT	**Receptor situado en la CRA** ATE en la CRA que incluye el interfaz con uno o más AEs y el interfaz con una o más redes de transmisión, siendo parte de uno o más ATPS. 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 sobre RTB analógica.

FlexC también emplea los siguientes acrónimos.

Acrónimo	Descripción
ASP	**Protocolos analógicos de seguridad** Protocolos analógicos de seguridad tradicionalmente utilizados para transmisión de alarmas por línea telefónica analógica, p.ej. SIA, Contact ID, etc.

23.23 Comandos FlexC

La siguiente tabla muestra los comandos que se pueden habilitar para un perfil de comando. El perfil de comando que se asigna a un ATS define cómo se puede controlar una central desde SPC Com XT.

Filtro comando	Comandos
Comandos sistema	Ver sumario central SPC
	Establecimiento fecha y hora sistema
	Permiso acceso al técnico
	Permiso acceso al fabricante
Comandos intrusión	Ver estados partición
	Ver estado cambio modo partición
	Cambio de modo (armado/desarmado) de una partición
	Ver estados de alertas de central
	Ejecución acciones ante alertas
	Silenciar sirenas
	Ver estados zona
	Control estado de una zona
	Ver registro del sistema
	Ver el registro de una zona
	Ver registro detect. vía radio
Comandos salida	Ver estados macros
	Control macros
Comandos usuario	Verificar usuario en central SPC
	Ver configuración usuario
	Creación nuevo usuario
	Edición usuario existente
	Borrado usuario
	Ver configuración perfiles usuario
	Añadir un perfil de usuario
	Edición perfil usuario existente
	Borrado perfil usuario
	Cambio del propio PIN del usuario
Comandos calendario	Leer configuración calendario
	Creación nuevo calendario
	Edición calendario
	Edición semana calendario
	Borrado calendario
	Creación día especial calendario
	Edición día especial calendario
	Borrado día especial calendario
Comandos comunicación	Ver estado red Ethernet
	Ver estado transmisor
	Ver registro transmisor
	Ver registro del receptor de la CRA
Comandos FlexC	Ver estado del ATS FlexC
	Ver registro red ATS FlexC
	Ver registro incidencias ATS FlexC

	Ver registro ATP FlexC
	Ver registro red ATP FlexC
	Exportar fichero configuración ATS FlexC
	Importar fichero configuración ATS FlexC
	Borrado ATS FlexC
	Borrado ATP FlexC
	Borrado perfil incidencias FlexC
	Borrar perfil comandos FlexC
	Solicitar llamada test ATP FlexC
Comandos control de accesos	Ver configuración puerta
	Ver estado puerta
	Control puerta
	Ver registro control de accesos
Comandos de verificación	Ver imagen cámara
	Ver estado zona verificación
	Ver datos zona verificación
	Envío datos a zona verificación
Comandos teclado virtual	Teclado de control
Comandos fichero	Actualizar firmware central SPC
	Actualizar firmware periféricos
	Programación fichero configuración en central SPC
	Lectura fichero configuración de central SPC
	Salvado configuración central SPC
	Reset central SPC
Comandos derivados	Ver información central SPC
	Ver estado central SPC
	Ver cabeceras ficheros configuración
	Ver configuración idioma
	Ver configuración intrusión
	Ver estado dispositivos X Bus
	Ver configuración partición

23.24 Tiempos de categoría ATS

Esta tabla describe los tiempos de las categorías ATS Category (SP1-SP6, DP1-DP4) según EN50136-1 establecidos en la norma y cómo la implementación FlexC cumple con esta norma.

		Requisitos temporizaciones categoría ATS EN50136-1				Implementación en FlexC de los requisitos de temporización según categoría ATS			
Categoría ATS	Interfaces por defecto	T.reint.TX IP	Tiempo excedido polling primario	T. exc. polling ATP backup (primario OK)	T. exc. polling ATP backup (primario en fallo)	T.reint.TX IP	Tiempo excedido polling primario	T. exc. polling ATP backup (primario OK)	T. exc. polling ATP backup (primario en fallo)
SP1	S1 [Ethernet]	8 min	32 días	-	-	2 min	30 días	-	-

SP2	S2 [Ethernet]	2 min	25 horas	-	-	2 min	24 horas	-	-
SP3	S3 [Ethernet]	60 s	30 min.	-	-	60 s	30 min.	-	-
SP4	S4 [Ethernet]	60 s	3 min	-	-	60 s	3 min	-	-
SP5	S5 [Ethernet]	30 s	90 s	-	-	30 s	90 s	-	-
SP6	S6 [Ethernet]	30 s	20 s	-	-	30 s	20 s	-	-
DP1	S2 [Ethernet] S2 [TX RTB]	2 min	25 horas	50 horas	25 horas	2 min	24 horas	24 horas 30 min	24 horas 10 min
DP2	S3 [Ethernet] S3 [TX RTB]	60 s	30 min.	25 horas	30 min.	60 s	30 min.	24 horas 30 min	30 min.
DP3	S4 [Ethernet] S4 [TX RTB]	60 s	3 min	25 horas	3 min	60 s	3 min	24 horas 30 min	3 min
DP4	S5 [Ethernet] S5 [TX RTB]	30 s	90 s	5 horas	90 s	30 s	90 s	4 horas 10 min	90 s

23.25 Tiempos categoría ATP

La siguiente tabla muestra la configuración aplicada para los tiempos excedidos de incidencia, intervalos de test (activos y no activos) y tiempos excedidos de test (activos y no activos) para cada categoría ATP. Para la finalidad de Ethernet, el intervalo de test y el intervalo de reintento son idénticos. Para reducir los costes relacionados con las llamadas GPRS, el intervalo y el intervalo de reintento de las rutas GPRS son diferentes, por ejemplo, S3 [TX RTB] realiza un test una vez cada 25 minutos y después, realiza un test cada 60 s durante 5 minutos hasta que excede el tiempo tras 30 minutos. Para poder ver un resumen del intervalo de test configurado, vaya a **Estado - FlexC - Registro red**.

!

Si una ATP se encuentra arriba y activa y, posteriormente falla, permanecerá dentro de los índices de test como activa durante dos ciclos de test más antes de pasar a los intervalos de test de **ATP en fallo**.

Categorías ATP WAN	Test con ATP activa	Test con ATP inactiva	Test con ATP en fallo

Categoría ATP	Tiempo excedido TX incidencia	Intervalo test	Intervalo reintentos	Tiempo excedido test	Intervalo test	Intervalo reintentos	Tiempo excedido test	Test Intervalo	Tiempo excedido
S6 [Ethernet]	30 s	8 s	30 s	20 s	8 s	30 s	20 s	30 s	30 s
S5 [Ethernet]	30 s	10 s	30 s	90 s	10 s	30 s	90 s	30 s	30 s
S4 [Ethernet]	60 s	30 s	30 s	3 min	30 s	30 s	3 min	30 s	30 s
S3 [Ethernet]	60 s	60 s	60 s	30 min.	60 s	60 s	30 min.	60 s	30 s
S5 [Ethernet]	2 min	2 min	2 min	4 horas	2 min	2 min	4 horas	2 min	30 s
S2 [Ethernet]	2 min	2 min	2 min	24 horas	2 min	2 min	24 horas	2 min	30 s
S1 [Ethernet]	2 min	2 min	2 min	30 días	2 min	2 min	30 días	2 min	30 s
Categoría TX ATP									
S5 [TX RTB]	30 s	10 s	30 s	90 s	4 horas	2 min	4 horas 10 min	10 min	90 s
S4A [TX RTB]	60 s	60 s	60 s	3 min	4 horas	2 min	4 horas 10 min	30 min.	90 s
S4 [TX RTB]	60 s	60 s	60 s	3 min	24 horas	2 min	24 horas 30 min	1 hora	90 s
S3 [TX RTB]	60 s	25 min	60 s	30 min.	24 horas	2 min	24 horas 30 min	4 horas	90 s
S2A [TX RTB]	2 min	4 horas	2 min	4 horas 10 min	24 horas	2 min	24 horas 30 min	4 horas	90 s
S2 [TX RTB]	2 min	24 horas	2 min	24 horas 10 min	24 horas	2 min	24 horas 30 min	24 horas	90 s
S1 [TX RTB]	2 min	24 horas	10 min	25 horas	30 días	10 min	30 días 1 hora	7 días	90 s

Editado por
Vanderbilt
I

Clonshaugh Business and Technology Park
Clonshaugh
Dublin
D17 KV84
www.service.vanderbiltindustries.com

© 2016 Copyright Vanderbilt
Reservadas las posibilidades de suministro y modificaciones técnicas.

Documento ID A6V10276963
Edition 01.05.2016