



SPCK 420/421

Teclado LCD

Manual del usuario

3.6

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: 01.10.2015

Documento ID: A6V10217651

Contenido

1	Seguridad	5
1.1	Grupo objetivo	5
1.2	Instrucciones generales de seguridad	5
1.2.1	Información general	5
1.2.2	Funcionamiento	5
1.2.3	Servicio técnico y mantenimiento	5
1.3	Significado de los avisos escritos	6
1.4	Significado de los símbolos de peligro	6
2	Directivas y normas	7
2.1	Directivas de la UE	7
2.1.1	Normas de seguridad.....	7
3	Introducción	8
4	Información general de tipos de teclados	10
5	Uso de la interfaz del teclado LCD	11
6	Programación de usuario a través del teclado	14
6.1	Armado y desarmado del sistema.....	14
6.1.1	Desarmado comun.....	14
6.1.2	A.TOTAL	15
6.1.3	ARMADO PARCIAL.....	15
6.1.4	Armado forzado	16
6.1.5	VER y BORRAR ALERTAS	16
6.1.6	Restauración coded	18
6.2	Menús de usuario	18
6.2.1	ESTADO DE SISTEMA	19
6.2.2	AISLAR	20
6.2.3	ANULAR.....	20
6.2.4	FECHA/HORA	21
6.2.5	TEST	22
6.2.5.1	Test sirena	22
6.2.5.2	TEST INTRUSIÓN	22
6.2.5.3	Test PAT	22
6.2.5.4	Opciones audibles	23
6.2.5.5	Test sísmico.....	23
6.2.5.6	Indic. visuales	23
6.2.6	REG. INCIDENC.....	23
6.2.7	REGISTRO DE CONTROL DE ACCESOS.....	24
6.2.8	CHIME.....	24
6.2.9	USUARIOS	24
6.2.9.1	AÑADIR.....	24
6.2.9.2	Editar.....	25
6.2.9.3	CONTROL DE ACCESOS.....	25

6.2.9.4	Borrar	27
6.2.10	PERFILES USUARIO	28
6.2.10.1	AÑADIR.....	28
6.2.10.2	EDITAR	28
6.2.10.3	BORRAR.....	28
6.2.11	SMS	29
6.2.11.1	AÑADIR.....	29
6.2.11.2	EDITAR	30
6.2.11.3	BORRAR.....	30
6.2.11.4	Comandos de SMS.....	31
6.2.12	Cambio nombre.....	33
6.2.13	CONTROL PUERTA.....	33
6.2.14	Permiso acceso.....	34
6.2.15	TX a ENG.....	34
6.2.16	REGISTRO ALARMAS	34
7	Apéndice	35
7.1	Atributos de usuario.....	35
7.2	Códigos de usuario.....	37
7.3	Gráfico de zona	38

1 Seguridad

1.1 Grupo objetivo

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

A quién va destinado este documento	Formación	Actividad	Condición del producto
Usuario final	Requiere formación por parte de especialistas técnicos.	Realiza únicamente los procedimientos para el buen funcionamiento del producto.	El producto se instala y configura.

1.2 Instrucciones generales de seguridad

1.2.1 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 realice cambios ni modificaciones en el dispositivo a no ser que se mencionen expresamente en este manual y hayan sido aprobados por el fabricante.

1.2.2 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.

1.2.3 Servicio técnico y mantenimiento

Peligro de descarga eléctrica durante el mantenimiento

- El trabajo de mantenimiento debe ser realizado únicamente por personal especializado.



Peligro de descarga eléctrica al limpiar el dispositivo



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

1.3 Significado de los avisos escritos

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

1.4 Significado de los símbolos de peligro

	 ADVERTENCIA
	Advertencia de área de peligro

	 ADVERTENCIA
	Advertencia de voltaje eléctrico peligroso

2 Directivas y normas

2.1 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
-----------	------------

2.1.1 Normas de seguridad

El SPCK420.100 y el SPCK421.100 han sido aprobados conforme a las siguientes normas:

Producto	Estándar
SPCK420.100	EN 50131-3:2009 grado 3, clase II, tipo B
SPCK421.100	

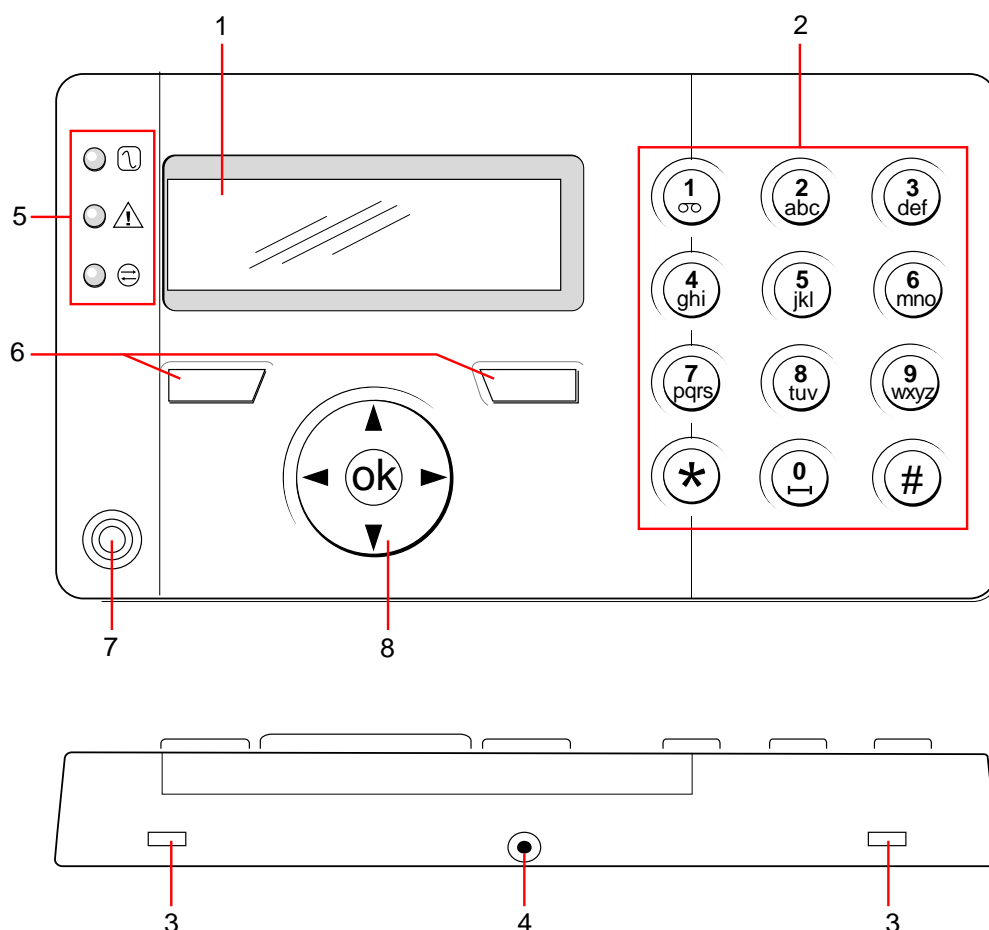
3 Introducción

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 [→ 10]).



Teclado LCD

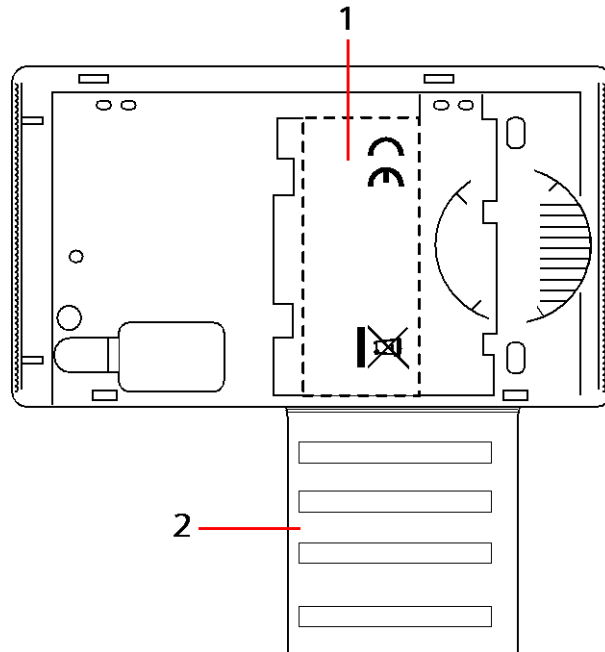
1	Pantalla LCD	La pantalla del teclado (2 líneas de 16 caracteres) muestra todos los mensajes de incidencias y de advertencia, además de proporcionar una interfaz visual para la programación del sistema (sólo programación de técnico). De la pantalla se puede ajustar el contraste y las condiciones en las que se produce la retroiluminación.
2	Teclas	El teclado alfanumérico permite la entrada tanto de datos numéricos como

	alfanuméricas	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 [→ 10]), los usuarios deberán colocar el mando Portable ACE dentro de un área de 1 cm para ARMAR/DESARMAR el sistema.
8	Tecla multifunción de navegación	La tecla multifunción de navegación, en combinación con la pantalla del teclado, proporciona una interfaz para programar el sistema.

LED		Estado
Toma de CA general (Verde)		Indica la existencia de tensión de red o de un fallo en la red. PARPADEANDO: fallo detectado en la 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.

4 Información general de tipos de teclados

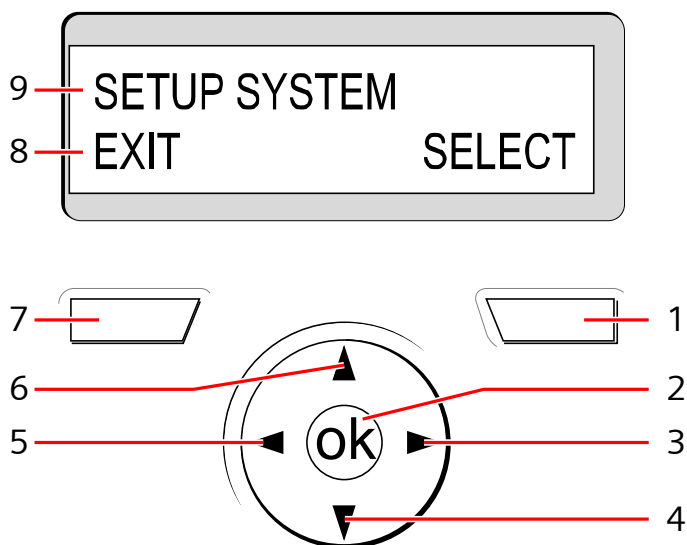
Tipo de teclado	Nº de modelo	Funcionalidad básica	Detección de proximidad	Audio
Teclado estándar	SPCK420	✓	-	-
Teclado con tarjeta	SPCK421	✓	✓	-
Teclado Confort	SPCK620	✓		-
Teclado confort con Audio/CR	SPCK623	✓	✓	✓



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.

5 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	Esta tecla se utiliza para seleccionar la opción que se muestra en el lado

	PROGRAMABLE IZQUIERDA	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

6 Programación de usuario a través del teclado

Las opciones de programación del usuario están disponibles mediante los teclados LCD y confort. Los menús y las opciones disponibles en el panel de control de intrusión son programados por el técnico instalador. Si los usuarios no pueden ver una opción descrita en este manual, no dispondrán de los atributos necesarios para acceder a esa función.

Para acceder a la programación de usuario:

1. Introduzca un código de usuario válido.
 2. Con las flechas arriba/abajo, desplácese hasta la opción de programación deseada.
 3. Dentro de una opción de menú, pulse # para seleccionar o habilitar/deshabilitar un parámetro (por ejemplo, un derecho de usuario). El parámetro seleccionado aparece con un * (por ejemplo, *Inhibición).
- ⇒ El teclado muestra ACTUALIZADO momentáneamente para indicar un cambio de parámetro.

6.1 Armado y desarmado del sistema

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

1. Introduzca un código de usuario válido.
2. Para seleccionar una opción de programación, utilice las flechas arriba/abajo o introduzca el dígito que aparece listado en la tabla que figura a continuación.

1	Desarmado comun	Realiza un desarmado en el sistema. Si se definen varias particiones, cada una de ellas se presentará en un submenú. En un sistema de una sola partición, esta opción aparece únicamente cuando el sistema está armado.
2	A.TOTAL	Realiza un armado total en el sistema. Si se definen varias particiones, cada una de ellas se presentará en un submenú. En un sistema de una sola partición, esta opción aparece únicamente cuando el sistema está desarmado.
3	ARMADO PARCIAL A	Realiza un Armado parcial A en el sistema. Si se definen varias particiones, cada una de ellas se presentará en un submenú.
4	ARMADO PARCIAL B	Realiza un Armado parcial B en el sistema. Si se definen varias particiones, cada una de ellas se presentará en un submenú.

6.1.1 Desarmado comun

Para desarmar el sistema:

1. Especifique un código de usuario válido.
 - ⇒ El teclado muestra un mensaje para confirmar el desarmado del sistema.
2. Pulse SELECC.
 - ⇒ La pantalla del teclado indica, en la línea inferior de la misma y durante aproximadamente cinco segundos, que el sistema está desarmado. Una vez transcurrido este tiempo, la línea inferior se muestra en blanco.
3. Si se ha activado la alarma, introduzca el código de usuario.
 - ⇒ Al hacerlo se silenciarán todas las sirenas y flashes.
 - ⇒ En el teclado aparecerá el mensaje PANEL DESARMADO durante aproximadamente 5 segundos.
 - ⇒ El origen de la condición de alarma se muestra en el teclado y el LED de alerta parpadea.

⇒ El teclado sigue mostrando la alerta hasta que se restaura dicha alerta.

6.1.2 A.TOTAL

La opción A.TOTAL proporciona la siguiente función:

- Protección completa de un edificio (la apertura de zonas de alarma activa la alarma)
- La apertura de zonas de entrada/salida inicia el contador del tiempo de entrada.

Si la alarma no se ha desarmado antes de que termine el tiempo de entrada, la alarma se activa.

Para seleccionar la opción A.TOTAL:

1. Desplácese a A.TOTAL.
2. Pulse SELECC.
 - ⇒ La segunda línea muestra el tiempo de salida y suena el zumbador para indicar que el usuario debería salir del edificio.
 - ⇒ Una vez armado el sistema por completo, la pantalla LCD muestra A.TOTAL en la línea inferior durante aproximadamente 10 segundos.



El sistema falla en el armado si se detecta una condición abierta o con fallos en una zona de alarma cuando la opción A.TOTAL o A.PARC.A/B están seleccionadas. El teclado muestra el número de la zona y la descripción.

Para armar el sistema, busque la zona y cierre o solucione el fallo. Repita la operación A.TOTAL o A.PARC.A/B.



Las zonas que están aisladas o en pruebas se muestran cuando se arma el sistema. Seleccione la opción Aislada o En pruebas y utilice las teclas de flecha hacia arriba y hacia abajo para desplazarse por la lista de zonas.

!	<p>AVISO</p> <p>El sistema no se puede ARMAR cuando hay un tamper activo.</p> <p>Los siguientes fallos también impiden el armado del sistema:</p> <ul style="list-style-type: none"> - Fusible sirena exterior - Fusible sirena interior - Tamper de sirena <p>En un sistema de grado 3, se necesita un código de técnico para anular la prevención de armado.</p> <p>Si se ha impedido el armado al final del período de salida ampliada, se indicará mediante una alerta acústica en el teclado. También se mostrará un mensaje en el teclado.</p>
----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6.1.3 ARMADO PARCIAL

La opción A.PARC. proporciona la siguiente función:

- Protección del perímetro de un edificio, al mismo tiempo que permite el movimiento libre por la salida y las particiones de acceso.
- Exclusión de las zonas Excl.A.Parc.A/B de la protección.
- Activación instantánea de la alarma en la selección del modo; por defecto, no existen tiempos de salida asociadas con A.parc.A/B.

Para seleccionar A.parc.A/B:

1. Desplácese a A.parc.A o a A.parc.B.
 2. Pulse SELECC.
- ⇒ La pantalla LCD muestra A.parc.A/B. ARMADO en la línea inferior durante aproximadamente 10 segundos.



El sistema falla en el armado si se detecta una condición abierta o con fallos en una zona de alarma cuando la opción A.TOTAL o A.PARC.A/B están seleccionadas. El teclado muestra el número de la zona y la descripción.

Para armar el sistema, busque la zona y cierre o solucione el fallo. Repita la operación A.TOTAL o A.PARC.A/B.



Las zonas que están aisladas o en pruebas se muestran cuando se arma el sistema. Seleccione la opción Aislada o En pruebas y utilice las teclas de flecha hacia arriba y hacia abajo para desplazarse por la lista de zonas.



AVISO

El sistema no se puede ARMAR cuando hay un tamper activo.

Los siguientes fallos también impiden el armado del sistema:

- Fusible sirena exterior
- Fusible sirena interior
- Tamper de sirena

En un sistema de grado 3, se necesita un código de técnico para anular la prevención de armado.

Si se ha impedido el armado al final del período de salida ampliada, se indicará mediante una alerta acústica en el teclado. También se mostrará un mensaje en el teclado.

6.1.4 Armado forzado

Es posible forzar el armado del sistema a la vez que se encuentra abierta una zona de alarma.

Una operación de "Armado forzado" anula estas zonas y arma el sistema normalmente.

Para forzar el armado del sistema:

1. Desplácese a A.TOTAL o A.parc.A/B.
2. Pulse SELECC.
 - ⇒ La primera línea de la pantalla indica las zonas que están abiertas.
3. Seleccione FORZAR con la tecla de función derecha.
4. Seleccione ARMADO FORZADO.
 - ⇒ El sistema se arma.

6.1.5 VER y BORRAR ALERTAS

Las condiciones de alerta en el sistema SPC se indican en el teclado con un LED amarillo de alerta que parpadea y con la activación de un zumbador.

La opción VER ALERTA en el teclado indica la ubicación y la causa de la condición de alerta.

La posibilidad de que un usuario borre las alertas depende de la configuración del grado de seguridad del sistema (según las normas). Una condición de alerta sólo se puede borrar una vez que el fallo o la zona que provocaron la alerta hayan sido restablecidos físicamente a su estado de funcionamiento normal; p. ej. una zona abierta se ha cerrado de nuevo o una conexión de X-BUS se ha restablecido. El sistema SPC NO ofrece la opción de BORRAR ALERTA sin la detección del fallo restaurado.

Puede que el uso de la función BORRAR ALERTA esté restringido para los usuarios si un técnico ha elegido no seleccionar **Restaurar** dentro del menú Derechos de usuario para usuarios seleccionados. Los usuarios que no puedan borrar una alerta reciben mensajes de error en el teclado hasta que la condición de zona o fallo se anula o se inhibe.



Una condición de alerta sólo se muestra en el teclado cuando el sistema está DESARMADO. Si se produce una condición de alerta cuando el sistema está ARMADO, el teclado no ofrecerá ninguna indicación de la condición de alerta hasta el momento en que el sistema esté DESARMADO.

Para VER una condición de alerta activada por la apertura de una zona:

1. Introduzca un código de usuario válido en el teclado.
2. Seleccione la opción VER ALERTAS.
3. Desplácese por las alertas.
4. Pulse (*) para ver la condición de alarma para cada partición.
 - ⇒ El teclado muestra la zona y el tipo de alerta con el formato "Zone 1 <XX>", definiendo XX el tipo de alerta como se indica a continuación:
A - Alarma
T - Tamper
TR - Problema
M - Enmascarado
PA - Post-alarma
5. Salga del sistema.

Para BORRAR una condición de alerta activada por la apertura de una zona:

1. Restaure el detector de alarma a su estado normal cerrando la puerta o la ventana, o bien
2. especifique un código de usuario válido y seleccione la opción BORRAR ALERTAS.
3. Pulse la tecla de menú derecha para BORRAR la alerta.
 - ⇒ Se muestra el mensaje TODAS LAS ALERTAS BORRADAS.
 - ⇒ El LED intermitente de alerta se apaga.

Para condiciones de alerta de tipo de sistema o comunicaciones (fallo de corriente o desconexión del X-BUS):

1. Localice el origen de la condición de alerta.
2. Compruebe que todos los cables estén correctamente conectados.

Para una alerta de tamper:

1. Asegúrese de que las tapas de todas las cajas y dispositivos estén correctamente cerradas.



Si no es posible restaurar el fallo físico a su estado de funcionamiento normal, póngase en contacto con el técnico instalador.

2. El sistema de alarmas continúa funcionando si se anula o inhibe la condición del fallo.

!	AVISO
	No se mostrará el mensaje de "Borrar alertas" si se introduce un código de coacción en teclado. Solo se mostrará tras borrarse la coacción.

6.1.6 Restauración coded

Esta función ofrece al usuario la posibilidad de restaurar condiciones de alerta que normalmente sólo estarían disponibles para el técnico instalador. Para ofrecer al usuario esta posibilidad, es necesario proteger esta función con un código.

Para realizar una reposición de código en el sistema:

- ▷ El grado de seguridad del sistema debe estar configurado en Grado 3 o Modo libre.
 - ▷ Asegúrese de que la zona o fallo que causó la condición de alerta haya sido restaurado físicamente a su estado de funcionamiento normal.
 - ▷ Póngase en contacto con el instalador antes de entrar en la programación de usuario y seleccionar la función Reposición código. Los datos de contacto del instalador deberían estar disponibles en la etiqueta desplegable debajo del teclado.
1. Pulse SELECC. en la opción **Reposición código**.
 - ⇒ Se muestra un código de restablecimiento de 6 dígitos en la línea superior.
 2. Indique al instalador el código de 6 dígitos.
 3. Reciba del instalador el nuevo código que él ha generado.
 4. Introduzca el código nuevo en la ventana CÓDIGO AUT.
 5. Pulse SELECC.
 - ⇒ Aparecerá el mensaje SISTEMA RESTAURADO en la línea superior de la pantalla.

6.2 Menús de usuario

1. Introduzca un código de usuario válido.
2. Desplácese hasta MENÚS y pulse SELECC.
3. Para seleccionar una opción de programación, utilice las flechas arriba/abajo o introduzca el dígito que aparece listado en la tabla que figura a continuación.

ESTADO DE SISTEMA	Permite al usuario ver el estado de lo siguiente:
-------------------	---------------------------------------------------

	<ul style="list-style-type: none"> ● ZONAS ABIERTAS ● INCIDENCIAS ● PRUEBAS ● ELEMENT.AISLADOS ● BATERÍA ● AUX
ANULAR	Permite a los usuarios anular una zona.
AISLAR	Permite a los usuarios aislar una zona.
FECHA/HORA	Permite a los usuarios establecer la hora y la fecha.
TEST	Permite a los usuarios realizar un TEST SIRENA, TEST DE INTRUSIÓN (ANDANDO), TEST PAT o cambiar las OPCIONES AUDIBLES.
REG. INCIDENC.	Permite a los usuarios ver un registro de las incidencias más recientes del sistema.
REGISTRO ACCESO	Permite a los usuarios ver un registro de los accesos más recientes al sistema.
REGISTRO ALARMAS	Permite a los usuarios ver un registro de las alertas más recientes generadas por particiones configuradas en el sistema.
CHIME	Permite al usuario habilitar o deshabilitar la función de Chime en todas las zonas para las que se haya programado el Chime como una función de alerta acústica.
USUARIOS	Permite al usuario añadir, editar y borrar usuarios si está autorizado con el perfil de usuario correspondiente.
PERFILES USUARIO	Permite al usuario añadir, editar y borrar perfiles de usuario si está autorizado con el perfil de usuario correspondiente.
SMS	Permite a los usuarios añadir, editar o borrar servicios de SMS para enviar mensajes de texto cortos a teléfonos móviles a través de la línea RTB. Los ID de SMS se configuran con un número de teléfono móvil, un código PIN y una selección de operaciones de control por SMS que se pueden realizar remotamente, y una selección de incidencias SMS que pueden recibir. Un ID de SMS está asignado a un usuario.
Cambio PIN	Permite a los usuarios cambiar su código de usuario.
CONTROL PUERTA	Permite al usuario controlar puertas. El usuario puede bloquear/desbloquear y restaurar la puerta a su funcionamiento normal.
ACCESO PERMITIDO	*Permite a los usuarios conceder acceso de técnico o fabricante al sistema.
TX a ENG	Permite al usuario solicitar que se envíen al técnico, por SMS, las 10 últimas incidencias en el registro. Estas 10 incidencias pueden requerir más de un SMS, dependiendo del tamaño de sus cadenas de caracteres.



Si el grado de seguridad del sistema está ajustado en "Modo libre", puede que en el menú de usuario no aparezcan las opciones de ANULACIÓN, INHIBICIÓN y PERMISO ACCESO. Solo algunos tipos de perfil de usuario específicos habilitan el acceso a los menús de programación de usuario.

6.2.1 ESTADO DE 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.

Opción de menú	Descripción
ZONAS ABIERTAS	Muestra todas las zonas abiertas.
INCIDENCIAS	Se muestran las alarmas actuales en el sistema
PRUEBAS	Se muestran todas las zonas en pruebas
ELEMENT.AISLADOS	Se muestran las zonas que están aisladas.
FALLO AL ARMAR	Se muestran todas las particiones que han fallado al armar. Seleccione cada partición para ver detalles de por qué no se ha conseguido armar la partición.
BATERÍA	Se muestra el voltaje y la corriente de la batería.
AUX	Se muestra el voltaje y la corriente de la alimentación auxiliar.

6.2.2 AISLAR

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

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

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

ZONA	Seleccione la zona correspondiente y cambie la configuración de NO INHIBIDA a INHIBIDA.
Sistema	Inhiba la alerta del sistema deseada.
XBUS	Inhiba la alerta que desee desde MÓDULOS DE EXPANSIÓN o TECLADOS: <ul style="list-style-type: none"> ● Perdida comunic. ● FALLO FUSIBLE XBUS (sólo módulos de expansión) ● Tamper X-Bus
Ver aislam.	Para ver una lista de las zonas, alertas del sistema y alertas de dispositivos X-BUS que se hayan inhibido.

6.2.3 ANULAR

Las zonas y alertas de dispositivos X-BUS se pueden anular manualmente desde el teclado. Al anularse una zona, ésta se elimina del sistema únicamente para el período configurado de una alarma.

Para inhibir zonas o alertas desde dispositivos X-BUS:

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

ZONAS	Seleccione la zona correspondiente y cambie la configuración de NO ANULADA a ANULADA.
-------	---------------------------------------------------------------------------------------

Sistema	<p>Seleccione la alerta del sistema requerida y cambie la configuración de DESHABILITADA a HABILITADA para inhibirla.</p> <ul style="list-style-type: none"> ● FALLO RED C. A. ● FALLO BATERÍA ● FALLO FUSIB.AUX. ● FALLO FUSIB.EXT.FALLO FUSIB.INT. ● Tamper sirena ● TAMPER AUX 1 ● TAMPER AUX 2 ● TAMPER ANTENA ● FALLO LINEA TX 1 ● FALLO LINEA TX 2 ● FALLO CABLEAD. ● FALLO TX ● FALLO FUENTE ALIMENTACIÓN
XBUS	<p>Inhiba la alerta que desee desde MÓDULOS DE EXPANSIÓN o TECLADOS:</p> <ul style="list-style-type: none"> ● PERDIDA COM. XBUS ● FALLO FUSIBLE XBUS (sólo módulos de expansión) ● TAMPER DE X-BUS
VER INHIBIC.	<p>Para ver una lista de las zonas, alertas del sistema y alertas de dispositivos X-BUS que se hayan anulado.</p>



Solo es posible anular en el sistema SPC los tipos de zona de ALARMA, E/S, SALIDA DE INCENDIOS y LÍNEA. El resto de tipos de zona no se muestran en los menús de anulación.

6.2.4 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.

6.2.5 TEST

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

6.2.5.1 Test sirena

Para realizar un test de sirena:

- Desplácese a TEST > TEST SIRENA y 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.

6.2.5.2 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 descende 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
	Solo ALARMA, E/S y SALIDA INCENDIO son tipos de zona válidos incluidos en un test de intrusión de usuario

6.2.5.3 Test PAT

Para realizar un test PAT, el instalador debe haber dado de alta el PAT.

1. Desplácese a TEST > TEST PAT.
2. Pulse SELECC.
 - ⇒ La pantalla del teclado mostrará Activar PAT.
3. Pulse y mantenga pulsados los tres botones del PAT.
 - ⇒ El LED del PAT se enciende.

⇒ En el teclado se muestra el ID, el estado y la intensidad de la señal del transmisor PAT.

6.2.5.4 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.

6.2.5.5 Test sísmico

Para realizar un test sísmico:

1. Desplácese a TEST > TEST SÍSMICO.
2. Pulse SELECC.
3. Seleccione TEST TODAS PART., o seleccione una partición concreta para comprobar.
4. Si selecciona una partición individual para comprobar, puede seleccionar TEST TODAS ZONAS o bien una zona sísmica específica para comprobar.
 - ⇒ Mientras se está realizando el test, en el teclado se muestra el mensaje "TEST SÍSMICO".
 - ⇒ Si el test falla, se muestra el mensaje "FALLO SÍSMICO". Si se pulsa la tecla "I" o "VER", se muestra una lista de las zonas con fallo por la que es posible desplazarse.
 - ⇒ Si el test es satisfactorio, se muestra "SÍSMICO OK".

Véase también Comprobación de detectores sísmicos.

6.2.5.6 Indic. visuales

Esta opción comprueba los LED y todos los píxeles en la pantalla del teclado.

Para comprobar los LED y las pantallas:

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

Se activan todos los LED, y se comprueban todos los píxeles de la pantalla durante 12 segundos. La prueba se puede cancelar pulsando el botón Atrás.

6.2.6 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.

6.2.7 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.

6.2.8 CHIME

La función de Chime se puede habilitar o deshabilitar en todas las zonas para las que se haya programado el Chime como una función de alerta acústica.

Para habilitar o deshabilitar la función de Chime:

1. Desplácese hasta CHIME y pulse SELECC.
2. Alterne entre HABILITADO y DESHABILITADO para el Chime.

6.2.9 USUARIOS

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

6.2.9.1 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.

6.2.9.2 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: <ul style="list-style-type: none"> ● AÑADIR TARJETA ● ALTA TARJETA Si el usuario tiene una tarjeta asignada: <ul style="list-style-type: none"> ● EDITAR TARJETA <ul style="list-style-type: none"> - 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.

6.2.9.3 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.


6.2.9.3.1 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.

6.2.9.3.2 ALTA TARJETA

	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.

	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.

6.2.9.3.3 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.

Atributo	Descripción
Prioridad	<p>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.</p> <p>El número máximo de usuarios prioritarios es:</p> <ul style="list-style-type: none"> ● SPC4xxx – todos los usuarios ● SPC5xxx – 512 ● SPC6xxx - 512
Visita	<p>La función de Visita obliga a los titulares de tarjetas con este privilegio a acompañar a otros titulares de tarjetas por puertas específicas. Si esta función está habilitada en una puerta, se debe presentar primero una tarjeta con la atribución de Visita para permitir abrir la puerta a otros titulares de tarjeta sin 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.</p>
Custodia	<p>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.</p> <p>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.</p> <p>Identifica al titular de esta tarjeta como responsable. El usuario con atributo de responsable debe ser el primero en entrar en un grupo de puertas que requiera un titular de tarjeta de responsable, y debe ser el último en abandonar dicho grupo de puertas.</p>

6.2.9.3.4 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.

6.2.9.3.5 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.

6.2.9.4 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.

6.2.10 PERFILES USUARIO

6.2.10.1 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 personalizado y pulse INTRO.
⇒ El teclado confirma que se ha creado el nuevo perfil de usuario.

6.2.10.2 EDITAR

Para editar perfiles de usuario en el sistema:

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

CAMBIAR NOMBRE	Edite el nombre del perfil si es necesario.
CAMBIAR PARTICIONES	Seleccione las particiones relevantes para este perfil.
CALENDARIO	Seleccione un calendario configurado o NINGUNO.
DERECHO	Habilita o deshabilita características del sistema para este perfil. Véase Derechos de usuario.
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.

6.2.10.3 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.

6.2.11 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.

Si alguna de las funciones descritas en este manual no aparece en los menús del teclado del usuario, éste no tiene permiso para utilizar dicha funcionalidad. Consulte con un técnico instalador autorizado sobre los atributos y ajustes apropiados.

Dependiendo del modo de AUTENTIFICACIÓN SMS seleccionado por el técnico instalador, la autenticación del usuario por SMS puede variar utilizando 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

6.2.11.1 AÑADIR

- ▷ Hay un módem instalado e identificado por el sistema.

- ▷ La función **Autenticación SMS** está activada en OPCIONES.
- 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.

6.2.11.2 EDITAR

- ▷ Hay un módem instalado e identificado por el sistema.
- ▷ La función **Autenticación SMS** está activada en OPCIONES.
- 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 [→ 31]

!	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.

6.2.11.3 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.

6.2.11.4 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 PIN o el ID de quien llama. El tipo de código PIN depende de lo establecido en cuanto a la autenticación de SMS.

La tabla siguiente muestra todos los comandos de SMS disponibles. La acción y la respuesta posteriores también se indican.

Los comandos de SMS se envían en forma de texto al número de teléfono de la tarjeta SIM del controlador.

Para los comandos que usan un código PIN, el formato del texto es:

****.comando o **** comando,

siendo **** el código PIN y "comando" el comando, es decir, el código PIN seguido de un espacio o un punto. Por ejemplo, el comando "ATOT" se introduce como:

**** ATOT o ****.ATOT. También se puede utilizar la versión completa del comando, si aparece en la lista. Por ejemplo, ****.Armado total.

Si el usuario no dispone de derechos suficientes para ejecutar un comando, en el sistema se indica Acceso denegado.

Si está habilitado el ID de quien llama, y está configurado el número de SMS de la persona que envía el mensaje, no es necesario el prefijo del código.

COMANDOS (**** = código)			
Utilización del código	Identificación número teléfono llamada entrante	Acción	Respuesta
**** AYUD ****.AYUD	AYUD	Se muestran todos los comandos disponibles	Todos los comandos disponibles
**** ATOT ****.ATOT ****. A.TOTAL	ATOT A.TOTAL	Se arman todas las particiones a las que tiene acceso el usuario.	Hora/fecha de armado del sistema. Si fuera aplicable, responde con zonas abiertas o de armado forzado
**** DESM ****.DESM ****. DESARMADO	DESM DESARMAD O	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 <ul style="list-style-type: none"> ● 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	Habilitar acceso de técnico	Acceso a técnico

****.ATEC.ON			
**** ATEC.OFF ****.ATEC.OFF	ATEC.OFF	Deshabilita el acceso del técnico	Acceso retirado a técnico
**** AFAB.ON ****.AFAB.ON		Habilita el acceso de fabricante	Estado de fabricante
**** AFAB.OFF ****.AFAB.OFF		Deshabilita el acceso de fabricante	Estado de fabricante
**** 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. Consulte Opciones	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. Consulte Opciones 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)


6.2.12 Cambio nombre

Para cambiar un código:

1. Desplácese hasta CAMBIO CÓDIGO y pulse SELECC.
⇒ Aparecerá un código generado de forma aleatoria.
2. Seleccione este código nuevo o sobrescríballo introduciendo un nuevo código y pulsando INTRO.

	AVISO
	El número de dígitos del código PIN varía en función de la configuración de seguridad del sistema. El sistema no aceptará un código con un número menor de dígitos que el configurado. Consulte a su técnico instalador.

3. Confirme el código nuevo y pulse SALVAR.
4. Pulse ATRÁS para volver a la pantalla anterior y corregir el código.
⇒ Si se agota el tiempo de la pantalla durante el proceso, el código antiguo seguirá siendo válido.

	AVISO
	Si la función CÓDIGO 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 de usuario.

6.2.13 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.

6.2.14 Permiso acceso

!	AVISO
	Estas opciones de menú no están disponibles si las opciones ACCESO TÉCNICO o ACCESO A FABRICANTE están deshabilitadas en el menú OPCIONES. Estas opciones solo se pueden habilitar o deshabilitar cuando el sistema está en "Modo libre".

Cuando se concede acceso al técnico o al fabricante, el teclado muestra el texto Habilit.técnico o Habilit.fabric. Una vez concedido el acceso, el usuario no puede acceder al sistema hasta que el técnico haya cerrado su sesión.

Para permitir acceso técnico:

1. Desplácese hasta ACCESO PERMITIDO y pulse SELECC.
2. Seleccione Acceso técnico y, a continuación, seleccione HABILITADO.
3. Seleccione Acceso fabric. y, a continuación, seleccione HABILITADO.
4. Haga clic en el botón Actualiz. ID de Registro para mostrar el ID de Registro en la tabla ATS.
5. Para deshabilitar el acceso de técnico/fabricante, siga el mismo proceso, cambie a DESHABILITADO y pulse SELECC.



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.

6.2.15 TX a ENG

El usuario puede solicitar que se envíen al técnico, por SMS, las últimas 10 incidencias en el registro.

1. Desplácese a TX a ENG y pulse SELECC.
2. Habilite o deshabilite esta opción según sea necesario.

Nota: Estas 10 incidencias pueden requerir más de un SMS, dependiendo del tamaño de sus cadenas de caracteres.

6.2.16 REGISTRO ALARMAS

El registro de alarmas muestra una lista de las incidencias de alarma. En este registro se muestran los siguientes tipos:

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

7 Apéndice

7.1 Atributos de usuario

Según las funciones operativas del sistema SPC que se describen más abajo, los usuarios tienen atribuciones asignadas a los perfiles de usuario. El técnico de instalación informará a los usuarios sobre las atribuciones asignadas a cada perfil de usuario. En función de cómo se haya programado el sistema, los usuarios pueden disponer de atribuciones para todas las características, o para algunas de éstas.

Atributos de usuario

Perfil de usuario por defecto	Tipo de usuario	Descripción
Armado total	Maestro estándar limitado	<p>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).</p> <p>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.</p> <p>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.</p>
Armado parcial A	Maestro estándar	<p>La opción ARMADO PARCIAL A [→ 15] proporciona protección al perímetro de un edificio, a la vez que permite el movimiento libre por la salida y las particiones de acceso.</p> <p>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.</p>
Armado parcial B	Maestro estándar	<p>La opción ARMADO PARCIAL B proporciona protección a todas las zonas, con excepción de aquellas clasificadas como Excl.A.Parc.B.</p> <p>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.</p>
Armado forzado	Maestro estándar	<p>La opción ARMADO FORZADO [→ 16] 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).</p> <p>Al seleccionarse esta opción, se arma la alarma y se anula la zona para ese período establecido.</p>
Desarmado	Maestro estándar limitado	<p>La operación DESARMADO [→ 14] desarma la alarma. Esta opción de menú sólo aparece en el teclado tras activarse la alarma e introducirse un código de usuario válido.</p>
Restaurar	Maestro estándar	<p>Con la función RESTAURAR [→ 16] se restaura la condición de alerta en el sistema y se borra el mensaje</p>

Perfil de usuario por defecto	Tipo de usuario	Descripción
		de alerta asociado a dicha condición. Una condición de alerta se puede restaurar únicamente tras restaurar las zonas o fallos que hayan activado la alerta a su estado de funcionamiento normal y una vez seleccionada la opción RESTAURAR para esa zona en la programación del usuario.
Aislar	Maestro* estándar	Al aislar una zona se desactiva la misma hasta que transcurra el tiempo establecido para anular el aislamiento. Es posible inhibir todos los tipos de zona del SPC. 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.
Inhibir	Maestro estándar	Al anularse una zona [→ 20], dicha zona se desactiva para el período establecido de la alarma. Sólo es posible anular tipos de zona de alarma, entrada/salida, salida de incendios y línea. 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.
Cambio de código	Maestro estándar	Esta opción de menú permite a los usuarios cambiar sus códigos de usuario.
Técnico	Maestro	Esta opción permite a los usuarios conceder acceso a la programación del técnico o del fabricante.
Fecha/hora	Maestro estándar	Utilice esta opción de menú para programar la hora y la fecha en el sistema. 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.
Test	Maestro estándar	Esta opción de menú proporciona las siguientes funciones de test: 1. Test sirena(s): este test activa las sirenas exteriores, el flash, las sirenas interiores y el zumbador en turnos de cinco segundos para comprobar su correcto funcionamiento. 2. Test de intrusión: un test de intrusión permite comprobar el funcionamiento de todos los detectores de alarma de un sistema. Al seleccionarse esta opción, el teclado muestra el número de zonas que se van a probar en el sistema. Active todos los detectores de alarma (abriendo puertas o ventanas) y compruebe que suena un pitido perceptible en el teclado. Las zonas inhibidas o anuladas no se incluyen en el test de intrusión. 3. Opciones acústicas: esta opción permite a los usuarios seleccionar qué dispositivos se activarán durante el test de intrusión y cuáles permanecerán en silencio.
Ver registro	Maestro estándar	Esta opción de menú muestra la incidencia más reciente en la pantalla del teclado. El registro de incidencias informa sobre la hora y la fecha de cada incidencia registrada.

Perfil de usuario por defecto	Tipo de usuario	Descripción
Chime	Maestro estándar	Todas las zonas con el atributo CHIME [→ 24] 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.
SMS	Maestro* estándar	Esta característica permite a los usuarios configurar el servicio de mensajes SMS si se ha instalado un módem en el sistema.
Usuarios	Maestro	El usuario puede configurar otros usuarios en la central.
Retardo autoarmado	Maestro* estándar	El usuario puede retardar el autoarmado.
Ignorar retardo	Maestro estándar	El usuario puede anular automáticamente el Retardo desarmado. Sólo disponible para instalaciones Financieras. Consulte Armado/desarmado
Actualizar	Maestro	El usuario puede autorizar al fabricante el acceso a la central para actualizar el firmware.
X-10	Control de acceso Maestro estándar	Activación y desactivación de los dispositivos X-10 configurados.
Control de puertas	Control de acceso Maestro estándar*	El usuario puede bloquear/desbloquear puertas.
Acceso web	Maestro* estándar	El usuario puede acceder a la central a través del navegador web.
Salidas	Maestro estándar	El usuario puede activar o desactivar salidas (salidas de sistema). Consulte
Test PAT	Maestro estándar	El usuario puede comprobar un PAT.
* Estas funciones no están habilitadas por defecto para este usuario, pero se pueden seleccionar.		

7.2 Códigos de usuario

El sistema admite códigos PIN de 4, 5, 6, 7 u 8 dígitos para cada usuario. La conversión de las correspondientes cantidades de combinaciones/variaciones lógicas se especifica en la tabla que figura a continuación.

Número de dígitos	Número de variaciones
4	10.000
5	100.000
6	10.000.000
7	10.000.000
8	100.000.000

Editado por
Vanderbilt

Clonshaugh Business and Technology Park
Clonshaugh
Dublin
D17 KV84
www.service.vanderbiltindustries.com

© Vanderbilt, 2015
Reservadas las posibilidades de suministro y modificaciones técnicas.