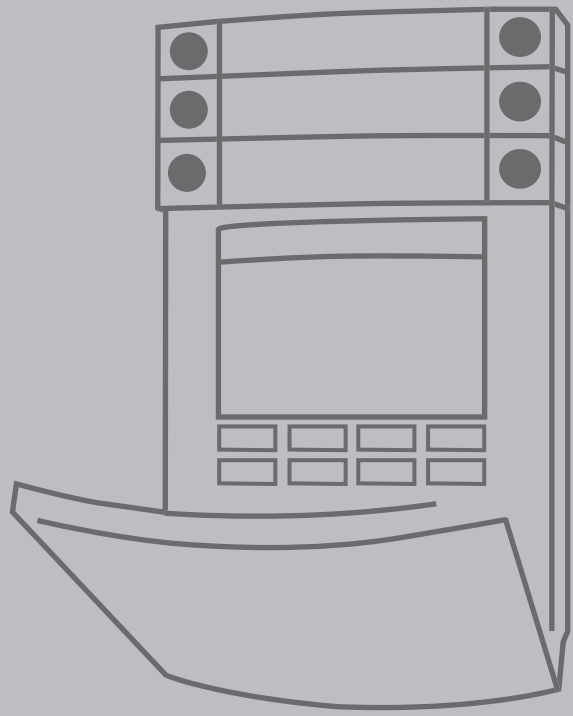


ekirja Használati Utasítás Gebruikershandleiding Bruke
de Utilizador Užívateľský návod Användarmanual Man
ti Utasítás Gebruikershandleiding Brukermanual Instru
vateľský návod Manuál Användarmanual Brugermanua
uikershandleiding Brukermanual Instrukcja użytkownik
vändarmanual Manuál Brugermanual Käyttöohjekirja
rukermanual Instrukcja użytkownika Manual de Utiliza
Brugermanual Käyttöohjekirja Használati Utasítás Ge
użytkownika Manual de Utilizador Užívateľský návod /
oohjekirja Használati Utasítás Gebruikershandleiding l
de Utilizador Užívateľský návod Manuál Användarman



ES

JABLOTRON 100+

TABLA DE CONTENIDOS

1. INTRODUCCIÓN	68	2.2.6.5. APP PARA SMARTPHONE MyJABLOTRON	84
2. MANEJO DEL SISTEMA JABLOTRON 100+	68	2.2.6.6. INTERFAZ WEB MyJABLOTRON	84
2.1. CONTROL EN LOCAL	71	2.2.6.7. LLAMADA PERDIDA	84
2.1.1. UTILIZANDO EL TECLADO DEL SISTEMA	71	2.2.6.8. MENSAJE SMS	84
2.1.2. CÓDIGO DE AUTORIZACIÓN	73	3. BLOQUEANDO/DESHABILITANDO EL SISTEMA	85
2.1.2.1. ARMAR LA ALARMA	75	3.1. BLOQUEO DE USUARIOS	85
2.1.2.2. DESARMAR LA ALARMA	75	3.2. BLOQUEO DE DETECTORES	85
2.1.2.3. ACCESO CON CÓDIGO DE COACCIÓN	76	3.3. DESHABILITAR CALENDARIO	85
2.1.2.4. ARMADO PARCIAL DE LA ALARMA	76	4. PERSONALIZANDO EL SISTEMA	85
2.1.2.5. FINALIZAR UN SALTO DE ALARMA	76	4.1. CAMBIAR CÓDIGO DE ACCESO DE USUARIO	85
2.1.2.6. CONTROL DE UNA PARTIÇÃO DESDE EL MENÚ DEL TECLADO CON PANTALLA LCD	77	4.2. CAMBIAR, ELIMINAR O AÑADIR TARJETA/TAG RFID	86
2.1.3. UTILIZANDO LOS TECLADOS DEL SISTEMA JA-110E Y JA-150E	77	4.3. CAMBIAR NOMBRE DE USUARIO O NÚMERO DE TELÉFONO	86
2.1.3.1. ARMAR LA ALARMA	79	4.4. AÑADIR/ELIMINAR UN USUARIO	86
2.1.3.2. DESARMAR LA ALARMA	80	4.5. AJUSTES DE EVENTOS POR CALENDARIO	86
2.1.3.3. ARMADO PARCIAL DE LA ALARMA	80	5. HISTORIAL DE EVENTOS	86
2.1.3.4. CONTROL DE ACCESO POR COACCIÓN	81	5.1. UTILIZANDO EL TECLADO LCD	87
2.1.3.5. FINALIZAR UN SALTO DE ALARMA	81	5.2. UTILIZANDO EL SOFTWARE JA-100-LINK Y UN ORDENADOR	87
2.1.4. MANEJANDO EL SISTEMA CON UN MANDO A DISTANCIA	82	5.3. INICIANDO SESIÓN EN MyJABLOTRON (WEB/SMARTPHONE)	87
2.2. CONTROL EN REMOTO	82	6. ESPECIFICACIONES TÉCNICAS	87
2.2.1. MANEJANDO EL SISTEMA USANDO LA APP PARA SMARTPHONE MyJABLOTRON	83		
2.2.2. MANEJANDO EL SISTEMA A TRAVÉS DEL INTERFAZ WEB MyJABLOTRON	83		
2.2.3. MANEJANDO EL SISTEMA USANDO EL MENÚ DE VOZ	83		
2.2.4. MANEJANDO EL SISTEMA A TRAVÉS DE COMANDOS SMS	83		
2.2.5. MANEJO DEL SISTEMA REMOTAMENTE USANDO UN ORDENADOR (JA-100-LINK)	83		
2.2.6. CONTROL DE SALIDAS PROGRAMABLES (PG)	84		
2.2.6.1. SEGMENTO DEL TECLADO	84		
2.2.6.2. AUTORIZACIÓN DE UN USUARIO EN EL TECLADO	84		
2.2.6.3. DESDE EL MENÚ DEL TECLADO CON PANTALLA LCD	84		
2.2.6.4. MANDO	84		



MANTENIMIENTO PERIÓDICO

- :: Es necesario realizar controles de mantenimiento periódicos y oportunos para asegurar un funcionamiento fiable del sistema. La mayor parte del mantenimiento es llevado a cabo por una empresa instaladora al menos una vez al año durante las inspecciones periódicas de mantenimiento.
- :: El mantenimiento del usuario consiste principalmente en mantener los dispositivos limpios. El ADMINISTRADOR del sistema puede cambiar el sistema a un modo MANTENIMIENTO para poder abrir los detectores (cambiar baterías) o eliminarlos de la instalación. Consulte la solicitud para configurar en modo MANTENIMIENTO con la empresa instaladora. Si el sistema se configura con el perfil del sistema "EN 50131-1, grade 2", el modo MANTENIMIENTO no está disponible.
- :: El sistema se puede cambiar a modo mantenimiento a través del software JA-100-Link o desde el menú del teclado con pantalla LCD. Después de la autorización se puede seleccionar el "Modo mantenimiento" con la selección de las particiones donde el mantenimiento es necesario. En el modo mantenimiento no generará alarmas en las particiones seleccionadas, incluyendo la apertura o eliminación de los detectores de la instalación.
- :: El modo mantenimiento se indica mediante el parpadeo verde del botón de activación (2 parpadeos cada 2 segundos) y a través del apagado de los botones de segmento de la partición particular.
- :: Tenga cuidado al manipular los dispositivos y evite dañar el plástico y los mecanismos de los detectores. a Por lo general, la cubierta está asegurada con una pestaña que solo necesita empujarse ligeramente hacia dentro del cuerpo del detector con una pequeña herramienta (ej. un destornillador) y después se puede quitar la cubierta. En algunos casos, la pestaña está asegurada con un pequeño tornillo de bloqueo que debe desatornillar primero.
- :: Al realizar el cambio de baterías del detector, siempre cambie todas las baterías del detector en particular al mismo tiempo (use baterías del mismo tipo y del mismo fabricante).
- :: Algunos dispositivos pueden requerir ser probados (detectores de fuego, por ejemplo). Para más información, por favor contacte con su técnico de servicio.

1. INTRODUCCIÓN

El sistema JABLOTRON 100* esta diseñado para un máximo de 600 usuarios y puede dividirse en 15 particiones independientes. Se pueden conectar hasta 230 dispositivos y el sistema ofrece hasta 128 salidas programables multipropósito (ej. domotica).

2. MANEJO DEL SISTEMA JABLOTRON 100+

El sistema de seguridad se puede controlar de diferentes formas. Para desarmar la alarma, necesita siempre una autorización en forma de identificación de usuario. El sistema reconoce la identidad de los usuarios y les permite manejar aquellas partes del sistema que les han sido asignadas para controlar. Puede elegir diferentes tipos de armado con o sin autorización. Cuando se utiliza el tipo de autorización Estandar, no tiene que autorizarse ya que es posible armar el sistema solamente presionando el boton de segmento derecho del teclado. El nombre de usuario, la fecha y la hora se registran y guardan en la memoria del sistema cada vez que se accede al mismo. Esta informacion esta disponible indefinidamente. Cualquier usuario puede cancelar la alarma (la sirena deja de sonar) solo con una autorización en cualquier parte del sistema (dependiendo de sus derechos de acceso). Sin embargo, no puede desarmar el sistema automaticamente (a menos que el perfil del sistema se cambie).

Nota: Dependiendo de la configuración de la instalación y ajustes del sistema, algunas opciones descritas a continuación podrían no estar disponibles. Consulte la configuración de la instalación con su técnico de servicio.

Usuarios y permisos de acceso

CÓDIGO DE AUTORIZACIÓN	DESCRIPCIÓN
Código CRA	<p>Este código tiene el nivel más alto de autorización para configurar el comportamiento del sistema y permite exclusivamente realizar un desbloqueo del sistema tras un salto de alarma. Puede entrar en modo Servicio, acceder a todas pestañas con opciones que incluyen la comunicación con CRA, la cual se puede denegar el acceso al técnico de Servicio (código Servicio). Mientras el parámetro "Administrador restringe derechos Servicio/CRA" está desmarcado, el código CRA puede controlar todas las particiones y salidas PG utilizadas por el sistema. Este código permite añadir más Administradores y otros usuarios con un nivel más bajo de autorización y asignarles códigos, tags RFID y tarjetas. También tiene permiso para borrar la memoria de alarmas y alarmas de sabotaje.</p> <p>El número de códigos CRA está limitado solo por la restante capacidad del panel de control y no hay un código configurado por defecto.</p>
Código de Servicio (Servicio)	<p>Este código puede entrar en modo Servicio y configurar el comportamiento del sistema. Tiene acceso a todas las pestañas con opciones, incluyendo comunicación CRA a menos que el acceso esté limitado al técnico CRA. Mientras el parámetro "Administrador restringe derechos Servicio/CRA" está desmarcado, el código de Servicio puede controlar todas las particiones y salidas PG utilizadas en el sistema. Puede crear un usuario con permiso CRA, otros técnicos de Servicio, Administradores y otros usuarios con menor nivel de autorización y asignarles códigos de acceso, tags RFID y tarjetas. También tiene permiso para eliminar una memoria de alarma y sabotaje. El número de códigos de Servicio está limitado por la restante capacidad del panel de control.</p> <p>Por defecto, el código es el 1010. El usuario Servicio siempre está en la posición 0 y no puede ser eliminado.</p>
Código Administrador (Principal)	<p>Este código tiene siempre acceso total a todas las particiones y está autorizado para controlar todas las salidas PG. El Administrador puede crear otro Administrador y otros usuarios con menor nivel de autorización y asignarles acceso a particiones y salidas PG, códigos de acceso, tags RFID y tarjetas. Tiene permiso para borrar memoria de alarmas. Sólo puede haber un código de Administrador principal, el cual no puede ser borrado. Cuando "Administrador restringe derechos Servicio/CRA" está habilitado, el código de administrador debe autorizarse para confirmar el acceso de la CRA y técnicos de Servicio.</p> <p>Por defecto, el código es el 1234. El usuario Administrador siempre está en la posición 1 y no puede ser eliminado.</p>
Código Administrador (Otro)	<p>Este código tiene acceso a las particiones seleccionadas por el Administrador principal, en las cuales el otro Administrador puede añadir nuevos usuarios con el mismo o menor nivel de autorización para controlar particiones y salidas PG, asignarles códigos de acceso, tags RFID y tarjetas. Tiene permiso para borrar memoria de alarmas en las particiones asignadas. Cuando "Administrador restringe derechos Servicio/CRA" está habilitado, el código de administrador debe autorizarse para confirmar el acceso de la CRA y técnicos de Servicio.</p> <p>El número de códigos de Administrador (otro) está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>

CÓDIGO DE AUTORIZACIÓN	DESCRIPCIÓN
Código Usuario	<p>Este código tiene acceso a particiones y salidas PG asignadas por un Administrador. Los usuarios pueden añadir/borrar sus tags RFID y tarjetas de acceso, y cambiar sus números de teléfono. Los usuarios pueden cambiar sus propios códigos siempre que el sistema utilice Códigos con prefijo. Tienen permiso para borrar memoria de alarmas en las particiones asignadas. Usuarios específicos podrán tener el acceso a las particiones limitado por horario.</p> <p>El número de códigos de Usuario está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>
Código Armar	<p>Este código permite solamente armar una partición seleccionada y controlar salidas PG (ON/OFF) que requieran autorización. Los usuarios con este nivel de autorización no pueden cambiar sus propios códigos ni borrar memoria de alarmas.</p> <p>El número de códigos Armar está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>
Código Solo PG	<p>Permite al usuario controlar salidas programables solamente con autorización. Esto se aplica tanto al encendido como al apagado. Los usuarios con este nivel de autorización no pueden cambiar sus propios códigos ni borrar memoria de alarmas.</p> <p>El número de códigos Sólo PG está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>
Código Pánico	<p>Este código está permitido solamente para activar una alarma de Pánico. Un usuario con este código no puede cambiar su propio código ni borrar memoria de alarmas.</p> <p>El número de códigos Pánico está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>
Código Vigilancia	<p>Este es un código para la central receptora. Este nivel de autorización permite armar el sistema entero. Sin embargo, el código de vigilancia solo puede desarmar el sistema durante una alarma o después de una alarma mientras siga activa la memoria de alarmas. Un usuario con este código no puede cambiar su propio código ni borrar memoria de alarmas.</p> <p>El número de códigos de Vigilancia está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>
Código de Desbloqueo	<p>Este código está diseñado para desbloquear el sistema tras un Bloqueo del sistema por una alarma. Un usuario con este código no puede cambiar su propio código ni borrar memoria de alarmas.</p> <p>El número de códigos de desbloqueo está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.</p>

La seguridad de los códigos de acceso, dispositivos RFID sin contacto y mandos a distancia:

Un panel de control permite asignar a cada usuario un código de 4, 6 u 8 dígitos y hasta dos tags RFID para autorizarse en el sistema. Se requiere autorización de usuario durante cada manipulación vía teclado, menú de voz, ordenador, aplicaciones web o móviles. La longitud del código afecta al número de posibles combinaciones y por tanto a la seguridad del código.

El número de combinaciones de códigos depende de la configuración:

Parámetros del panel de control	4 DÍGITOS	6 DÍGITOS	8 DÍGITOS
“Código con prefijo” habilitado	$= 10^4 = (10.000)$	$= 10^6 = (1.000.000)$	$= 10^8 = (100.000.000)$
“Código con prefijo” y “Código de coacción” ambos deshabilitados	$= 10^4 - (1)$ (Número de usuarios - 1)	$= 10^6 - (1)$ (Número de usuarios - 1)	$= 10^8 - (1)$ (Número de usuarios - 1)

Parámetros del panel de control	4 DÍGITOS	6 DÍGITOS	8 DÍGITOS
“Código con prefijo” deshabilitado; “Código de coacción” habilitado	$\leq 10^4 - ((\text{Número de usuarios} - 1) * 3)$	$\leq 10^6 - ((\text{Número de usuarios} - 1) * 3)$	$\leq 10^8 - ((\text{Número de usuarios} - 1) * 3)$
Usando sólo una tarjeta RFID con un rango de 14 caracteres (6 constantes + 8 variables)	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$
“Código con prefijo” y “Confirmación de tarjeta con un código” ambos habilitados	$= (10^8 * 10^4) = 10^{12} = (1.000.000.000.000)$	$= (10^8 * 10^6) = 10^{14} = (100.000.000.000.000)$	$= (10^8 * 10^8) = 10^{16} = 1.000.000.000.000.000$
“Código con prefijo” deshabilitado; “Confirmación de tarjeta con un código” habilitado	$= 10^8 * (10^4 - (\text{Número de usuarios} - 1))$	$= 10^8 * (10^6 - (\text{Número de usuarios} - 1))$	$= 10^8 * (10^8 - (\text{Número de usuarios} - 1))$

Formas de mejorar la protección contra la adivinación de un código válido:

- :: Utilizando un código con más dígitos (códigos con 6 u 8 dígitos),
- :: Tipos más avanzados de autorización (como “Confirmación de tarjeta con un código” o “Doble autorización”).

Formas de controlar el JABLOTRON 100+

En local:

- :: Teclado del sistema
- :: Mando del sistema
- :: Ordenador a través de conexión por cable USB y software JA-100-Link

De forma remota:

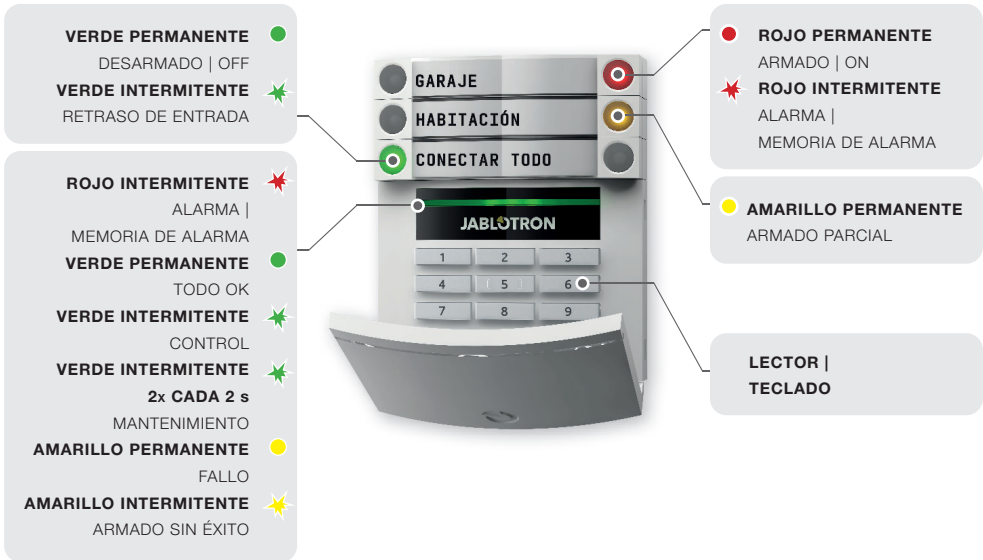
- :: Aplicación smartphone MyJABLOTRON
- :: Ordenador a través del interfaz web MyJABLOTRON
- :: Menú de voz usando el teléfono
- :: SMS a través del teléfono
- :: Ordenador a través de internet con el software JA-100-Link
- :: Llamada perdida desde un número de teléfono autorizado (sólo para controlar salidas programables)



2.1. CONTROL EN LOCAL

2.1.1. UTILIZANDO EL TECLADO DEL SISTEMA

El sistema JABLOTRON 100+ puede ser controlado a través de diversos módulos de acceso, los cuales le permiten, no solo controlar, sino también visualizar el estado de cada segmento individual. El sistema se puede controlar directamente (armar o desarmar el sistema y funciones de automatización) usando los segmentos de dos botones del teclado. Los botones de segmento están claramente identificados y coloreados (usando la lógica del semáforo) de manera que el estado de cada segmento está indicado claramente. Un segmento también puede utilizarse para indicar un estado (ej. puerta del garaje abierta) o para controlar diferentes dispositivos automatizados (por ejemplo, la calefacción o las persianas). El número máximo de segmentos que se pueden añadir a un módulo de acceso es de 20. También se puede configurar un segmento para llamar solicitando ayuda en caso de emergencia (alarma médica o de pánico).



Los diferentes tipos de módulos de acceso y sus combinaciones

Lector de tarjetas RFID

Permite controlar el sistema a través de los segmentos y autorización por métodos sin contacto (tarjeta / tag RFID).



Teclado con lector de tarjetas

el usuario puede controlar el sistema a través de los segmentos y autorización, tanto introduciendo un código o el método sin contacto (tarjeta / tag RFID), o una combinación de ambas para mayor seguridad.



Teclado con pantalla LCD y lector de tarjetas

el usuario puede controlar el sistema a través de los segmentos y autorización, tanto introduciendo un código, método sin contacto (tarjeta / tag RFID), ambos código y tarjeta / tag para mayor seguridad, o autorizando y utilizando las opciones disponibles en la pantalla LCD del teclado.



Cuando desarmamos la alarma utilizando los botones del segmento siempre se requiere de una autorización de usuario.

Para armar la alarma y controlar procesos automatizados a través de los botones del segmento, la autorización de usuario es opcional

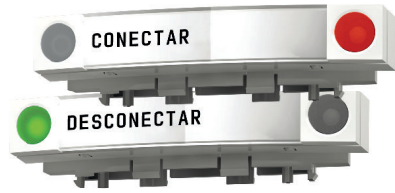
para cada segmento.



dos chips RFID

Los usuarios pueden autorizarse introduciendo su código asignado o a través de su tarjeta / tag RFID.

Cada usuario puede disponer de un código y hasta (tarjetas o tags).



Tags recomendados: JABLOTRON 100+, Oasis u otros de terceros compatibles con 125 kHz EM. Si se requiere una mayor seguridad, el sistema de alarma puede ser armado por un usuario con autorización configurada utilizando tags RFID y códigos (opcional).

Si el usuario quiere controlar múltiples segmentos simultáneamente, debe autorizarse y después presionar los segmentos de las particiones particulares. De esta forma los usuarios pueden, por ejemplo, armar la casa y desarmar el garaje con una sola autorización.

Si el parámetro "Código con prefijo" está habilitado, la autorización por código en el teclado puede consistir en hasta 11 dígitos: un prefijo (de uno a tres dígitos), un asterisco * (que separa el prefijo y el código principal), y un código de 4,6 u 8 dígitos en función de la configuración (por ejemplo: 123*12345678, o 1*12345678). Todos los usuarios pueden cambiar sus propios códigos, que siguen el prefijo. El código puede ser cambiado desde la pantalla LCD del teclado, desde el software JA-100-Link o la app MyJABLOTRON.

Si el parámetro "Código con prefijo" está habilitado, los usuarios pueden estar habilitados para cambiar sus códigos. Si el parámetro "Código con prefijo" está deshabilitado, los códigos solamente pueden ser cambiados por el Administrador.

2.1.2. CÓDIGO DE AUTORIZACIÓN

La autorización de un usuario con código se realiza tecleando un código válido en el teclado o con un tag RFID.

Es posible usa códigos de **4, 6 u 8 dígitos** en el sistema.

El sistema puede ser configurado para ser utilizado con códigos con o sin prefijo (ajuste por defecto). Para sistemas de alarma con un mayor número de usuarios se pueden habilitar los prefijos. Para cambiar esta opción, por favor contacte con el técnico de servicio de su sistema de alarma.

Código sin prefijo: CCCC

cccc es un código de 4, 6 u 8 dígitos, códigos permitidos desde 0000 a 99999999

Código de panel de control por defecto Administrador: **1234; 123456; 12345678;**

Código con prefijo: nnn*cccc

- nnn** es el prefijo, que se corresponde con el número de posición del usuario (posición 0 a 600)
- *** es un separador (tecla *)
- cccc** es un código de 4, 6 u 8 dígitos, códigos permitidos desde 0000 a 99999999

Código de panel de control por defecto Administrador: **1*1234; 1*123456; 1*12345678;**

ADVERTENCIA: El código de Administrador principal empieza con el prefijo **1**

El código de Servicio principal empieza con el prefijo **0**

Para cambiar el código, por favor contacte con el técnico de servicio de su sistema de alarma.

Estructura y descripción del menú interno del teclado LCD:

Autorización
de Administrador
o Usuario
a través de
código o tarjeta
/ tag RFID

CANCELAR INDICACIÓN DE MEMORIA DE ALARMA

Permite cancelar una indicación de alarma / armado sin éxito en todas las particiones a las que el usuario tiene derecho de acceso.

CONTROL DE PARTICIONES

Permite controlar las particiones del sistema a las que el usuario tiene derecho de acceso y están habilitadas en los ajustes internos.

CONTROL DE PGS

Permite controlar las salidas programables PG a las que el usuario tiene permiso y de acuerdo con los ajustes internos.

MEMORIA DE EVENTOS

Muestra una lista detallada de eventos en memoria.

SE EVITÓ LA CONEXIÓN

Muestra una lista de todos los detectores que evitan el armado del sistema, siempre que esta opción esté activada en la configuración del panel de control.

AVERÍAS DEL SISTEMA

Muestra una lista de todos los detectores que indican fallos en el sistema desde las particiones a las que el usuario tiene derechos.

DETECTORES APAGADOS

Muestra una lista de todos los detectores bloqueados en las particiones a las que el usuario tiene derecho de acceso.

ESTADO DEL SISTEMA

Muestra el estado del sistema (lista de detectores activos, contactos de sabotaje activos, bajas baterías, autobypasses, etc.).

CONFIGURACIÓN

Permite editar usuarios y dispositivos (sólo cuando el USB está desconectado).

AJUSTES DE PANTALLA

Permite ajustar el brillo de la iluminación y el contraste de la pantalla.

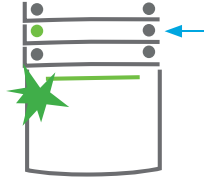
MODO MANTENIMIENTO

Permite al Administrador particiones asignadas al modo Mantenimiento.

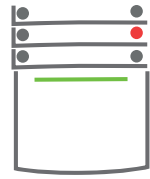
2.1.2.1. ARMAR LA ALARMA



1. Autorizarse usando el teclado. Las particiones que pueden ser controladas se iluminan y el botón indicador retroiluminado empezará a parpadear en verde.



2. Presione el botón derecho (uno que no este iluminado) para armar una partición en particular. Es posible armar mas particiones de forma consecutiva. El retraso entre la selección de particiones no debe sobrepasar los 2 segundos.



3. El comando es ejecutado y el teclado indica acusticamente el retaso de salida. La particion se arma ahora y solo los detectores con reaccion "Zona retrasada" proporcionan el tiempo para dejar el area vigilada durante el retraso de salida. El boton del segmento de la particion armada se enciende en rojo.

Durante el armado de la alarma, si hay algún detector activo (ej. una ventana abierta) el sistema reaccionará de una de las siguientes formas (en base a la configuración del sistema):

:: Los detectores vigilarán automáticamente después de que vuelven a su estado normal (ajuste por defecto).

:: El sistema indicará ópticamente los detectores activos con un parpadeo rojo del segmento durante 8 segundos, tras los cuales el sistema se armará automáticamente.

:: El armado de la partición con detectores activos también es posible simplemente pulsando de nuevo el botón de la derecha del segmento. De esta forma el usuario confirma su intención de armar la partición con un detector activo (ej. una ventana abierta). De otro modo, la partición no se armará con un detector activo.

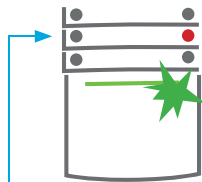
:: Un detector active evitará el armado de la partición. Este estado se indica ópticamente por un parpadeo del botón rojo del segmento. El detector que evita el armado se mostrará en el menú de la pantalla del teclado LCD.

Un armado sin éxito se indica a través del parpadeo amarillo del botón indicador (el parámetro "Armado sin éxito" debe estar habilitado). [Consulte con su técnico de servicio a fin de programar el comportamiento deseado del sistema.](#)

2.1.2.2. DESARMAR LA ALARMA

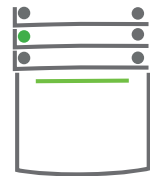


1. Cuando entra en un edificio (activando un detector con reaccion "Zona retrasada"), el sistema empieza a indicar el retraso de entrada con un tono continuo y parpadeo del boton verde del segmento que tiene esa particion asociada, en la



que se ha generado el retraso de entrada.

Autorizese utilizando el teclado – la luz de indicacion verde del panel de autorizacion empieza a parpadear.



2. Presionar el botón izquierdo del segmento de las particiones que quiere desarmar.

3. El comando se ejecuta y los segmentos se volveran verdes indicando que las particiones estan desarmadas.

Nota: Si el parámetro "Desarmar partición con autorización solo durante el retraso de entrada" está habilitado, entonces la mera autorización desarmará la partición donde se haya generado el retraso de entrada. [Consulte con su técnico de servicio a fin de programar el comportamiento deseado del sistema.](#)

2.1.2.3. ACCESO CON CÓDIGO DE COACCIÓN

Esta función permite desarmar el sistema de un modo especial. El sistema aparentemente se desarma, sin embargo, también genera una alarma de pánico silencioso, que es reportada a los usuarios seleccionados (incluyendo CRA). El desarmado bajo coacción se lleva a cabo sumando 1 al último número de un código válido.

Ejemplo para un código con prefijo:

Código válido: 2*9999

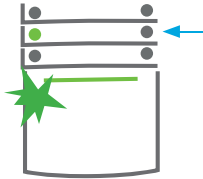
Código para desarmar bajo coacción: 2*9990

Ejemplo para un código sin prefijo:

Código válido: 9999

Código para desarmar bajo coacción: 9990

2.1.2.4. ARMADO PARCIAL DE LA ALARMA



1. Autorícese utilizando el teclado (introduzca un código o pase una tarjeta o tag por el lector). El botón indicador retroiluminado verde empezará a parpadear.

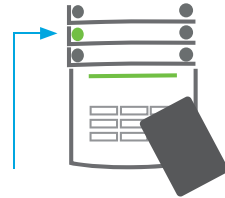
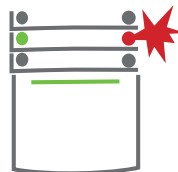
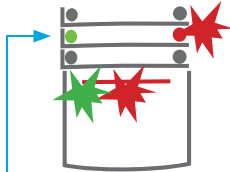
2. Presione el botón derecho del segmento de la partición seleccionada.

3. El comando se ejecuta y el segmento se volverá amarillo indicando que la partición está armada parcialmente.

El sistema también puede configurarse para ser armado de forma parcial, lo que permite la vigilancia solo de ciertos detectores en una partición. **Ejemplo:** por la noche, es posible armar solamente los detectores de puertas y ventanas, dejando los detectores de movimiento interiores sin ninguna reacción.

Para armar totalmente la partición que tiene el armado parcial habilitado, se tendrá que hacer una doble pulsación en el botón de armar. Tras la primera pulsación del botón parpadeará en amarillo y tras la segunda pulsación parpadeará en rojo. Si el sistema está armado en parcial – indicado por una iluminación continua en amarillo – el sistema se puede armar totalmente a través de una autorización y pulsación del botón amarillo. Una vez que el botón es presionado, el sistema se armará totalmente y el botón se vuelve rojo.

2.1.2.5. FINALIZAR UN SALTO DE ALARMA



1. Autorícese utilizando el teclado (introduzca un código o pase una tarjeta o tag por el lector).

2. Presione el botón izquierdo del segmento de la partición donde se ha generado una alarma.

3. Se desarma el sistema y las sirenas se silencian. El parpadeo del botón verde indica el desarmado de la partición indicada. El parpadeo rojo indica una memoria de alarma.

4. Autorícese y presione el botón verde de nuevo para cancelar la indicación de memoria de alarma.

5. El segmento indica el desarmado de la partición con la iluminación permanente del botón verde.

Un salto de alarma en curso se indica con un parpadeo rápido del botón rojo del segmento e indicación del botón retroiluminado del teclado. Es necesario autorizarse utilizando el teclado para terminar la alarma. La partición continúa armada, y un parpadeo rápido del botón rojo del segmento indica la memoria de alarma. La indicación se mantendrá activada incluso después de que el sistema haya sido desarmado.

Si la indicación de la memoria de alarma fue activada durante su ausencia, busque la causa de la alarma en el historial de eventos y extreme las precauciones al acceder e inspeccione la instalación o espere a que llegue el guardia de seguridad (en caso de que su sistema esté conectado a una Central Receptora de Alarmas).

La indicación de memoria de alarma permanece en el segmento hasta que el sistema se arma de nuevo. También puede ser cancelada desarmando el sistema una vez más. Además, la indicación de memoria de alarma se puede cancelar desde el Menú principal de un teclado con pantalla LCD – Cancelar memoria de alarma.

La indicación de la activación de una alarma de sabotaje solo puede finalizarse a través del técnico de Servicio o Administrador.

Nota: Cuando se utiliza el perfil del sistema “EN 50131-1, grade 2”, siempre es necesario autorizarse primero y después realizar la acción deseada.

Terminar una alarma utilizando un mando a distancia también desarmará la partición correspondiente.

2.1.2.6. CONTROL DE UNA PARTICIÓN DESDE EL MENÚ DEL TECLADO CON PANTALLA LCD

Los estados de las particiones se muestran en la parte superior izquierda de la pantalla. Un armado total de una partición se muestra a través de un número en un rectángulo con el fondo color negro **2**; un armado parcial se representa a través de un número enmarcado **4**.

Control desde el menú del teclado:

:: Autorícese a través de un código válido o un chip RFID.

:: Acceda al menú pulsando ENTER.

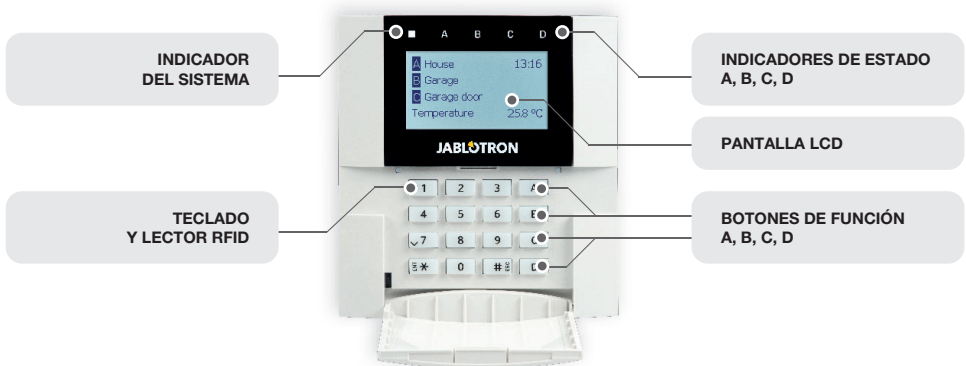
:: Control de particiones → ENTER.

:: Seleccione la partición deseada utilizando las flechas.

:: Pulsando ENTER repetidamente cambiará los estados de la partición (armado parcial / armado / desarmado).

:: Pulse ESC para salir al menú.

2.1.3. UTILIZANDO LOS TECLADOS DEL SISTEMA JA-110E Y JA-150E



Los estados de cada partición individual son indicados por los indicadores de estado A, B, C, D sobre el display LCD y los botones de función. El panel de control se puede manejar directamente (armar o desarmar la alarma y otras funciones de automatización) utilizando los botones de función del teclado. Los botones de función y los indicadores de estado A, B, C, D están retroiluminados para indicar claramente el estado de la partición.

:: VERDE – Desarmado :: AMARILLO – Armado parcial :: ROJO – Armado

La autorización se puede señalar introduciendo un código de acceso en el teclado o utilizando una tarjeta/tag RFID asignada al usuario en particular. Cada usuario puede tener un código y un chip RFID (tarjeta o tag). Si el usuario quiere controlar múltiples particiones simultáneamente, debe autorizarse y después presionar los botones de función de las particiones particulares consecutivamente. De esta forma el usuario puede desarmar todas las particiones (por ejemplo, la casa y el garaje) con una simple autorización.

Estructura y descripción del menú interno del teclado LCD:

Autorización
de Administrador
o Usuario
a través de
código o tarjeta
/ tag RFID

CANCELAR INDICACIÓN DE MEMORIA DE ALARMA

Permite cancelar una indicación de alarma / armado sin éxito en todas las particiones a las que el usuario tiene derecho de acceso.

CONTROL DE PARTICIONES

Permite controlar las particiones del sistema a las que el usuario tiene derecho de acceso y están habilitadas en los ajustes internos.

CONTROL DE PGS

Permite controlar las salidas programables PG a las que el usuario tiene permiso y de acuerdo con los ajustes internos.

MEMORIA DE EVENTOS

Muestra una lista detallada de eventos en memoria.

SE EVITÓ LA CONEXIÓN

Muestra una lista de todos los detectores que evitan el armado del sistema, siempre que esta opción esté activada en la configuración del panel de control.

AVERÍAS DEL SISTEMA

Muestra una lista de todos los detectores que indican fallos en el sistema desde las particiones a las que el usuario tiene derechos.

DETECTORES APAGADOS

Muestra una lista de todos los detectores bloqueados en las particiones a las que el usuario tiene derecho de acceso.

ESTADO DEL SISTEMA

Muestra el estado del sistema (lista de detectores activos, contactos de sabotaje activos, bajas baterías, autobypasses, etc.).

CONFIGURACIÓN

Permite editar usuarios y dispositivos (sólo cuando el USB está desconectado).

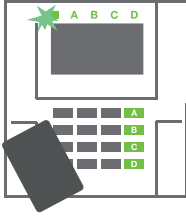
AJUSTES DE PANTALLA

Permite ajustar el brillo de la iluminación y el contraste de la pantalla.

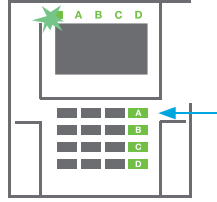
MODO MANTENIMIENTO

Permite al Administrador particiones asignadas al modo Mantenimiento.

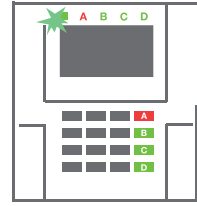
2.1.3.1. ARMAR LA ALARMA



1. Autorícese utilizando el teclado. Los botones de función A, B, C, D de particiones que tiene permittidos controlar se encenderán y el indicador del sistema empezará a parpadear en verde.



2. Presione el botón de función para armar la partición particular. Es posible armar más particiones consecutivamente. El retraso entre la selección de las particiones no debe ser mayor a 2 segundos.



3. El comando se ejecuta y el teclado indica acústicamente el retraso de salida. La partición está ahora armada, solo los detectores con reacción "Zona retrasada" proporcionan tiempo para dejar el área vigilada durante el retraso de salida. El indicador de estado y el botón de función de armado de la partición se encenderán en rojo.

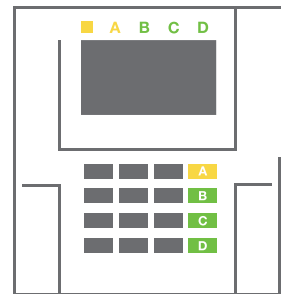
Durante el armado de la alarma, si hay algún detector activo (ej. una ventana abierta) el sistema reaccionará de una de las siguientes formas (en base a la configuración del sistema):

- :: El panel de control se armará. Los detectores activos serán bloqueados automáticamente. *)
- :: El sistema indicará ópticamente los detectores activos con un parpadeo rojo del botón de función durante 8 segundos, tras los cuales el panel de control se armará automáticamente (los detectores activos serán bloqueados). *)
- :: Armar la partición con detectores activos también es posible simplemente presionando el botón de función de nuevo. El usuario debe confirmar la intención de armar la partición con un detector activo (ej. una ventana abierta). De otro modo el sistema no se armará.
- :: Un detector active evitará el armado. Este estado se indica ópticamente por un parpadeo rojo del botón de función. El detector que evita el armado se mostrará en el menú de la pantalla del teclado LCD.

*) **ADVERTENCIA:** Las opciones a) y b) no son compatibles con EN 50131, grade. 2 (perfil de sistema del panel de control)

Si un detector con la reacción "Alarma de zona instantánea" se activa durante un retraso de salida o si un detector con reacción "Alarma de zona retrasada" permanece activo una vez finalizado el retraso de salida, el panel de control se desarmará de nuevo. Se indicará un armado sin éxito a través del indicador del sistema parpadeando en amarillo, se reportará a la CRA y se indicará a través de la sirena externa (aplica para seguridad Grado 2).

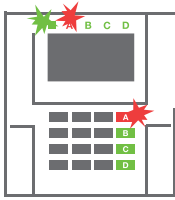
Si el panel de control está configurado para armar sin autorización, entonces no es necesario autorizarse. Todo lo que tiene que hacer es presionar el botón de función de la partición particular. Es posible configurar el panel de control para armar simplemente a través de autorización.



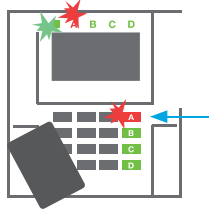
ADVERTENCIA: Armar automáticamente sin autorización disminuye el frado máximo de seguridad a Grado 1. Considere todos los posibles riesgos al utilizar esta función.

Consulte la instalación con un consultor de proyecto o un técnico de servicio para programar el comportamiento deseado del sistema de alarma.

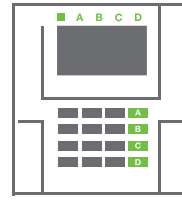
2.1.3.2. DESARMAR LA ALARMA



1. Cuando entre en el inmueble (activando un detector con reacción "Zona retrasada"), el sistema empieza a indicar el retraso de entrada con un tono continuo, el indicador de sistema y un botón de función, ambos parpadeando en rojo, de la partición en que se ha generado el retraso de entrada.



2. Autorícese utilizando el teclado – el indicador de sistema empezará a parpadear en verde.



3. El Presione los botones de función de las particiones que quiere desarmar.

4. Comando es ejecutado. Los botones de función y el indicador de sistema se vuelven verdes indicando las particiones desarmadas.

Nota: Si el parámetro "Desarmar partición a través de autorización solo durante el retraso de entrada" está habilitado, entonces la mera autorización desarmará la partición donde se haya generado el retraso de entrada. Esta opción se debe utilizar con precaución cuando se utilizan múltiples particiones.

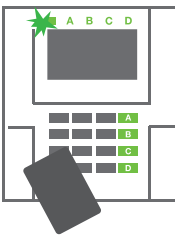
Consulte la instalación con un técnico de servicio para programar el comportamiento deseado del sistema de alarma.

2.1.3.3. ARMADO PARCIAL DE LA ALARMA

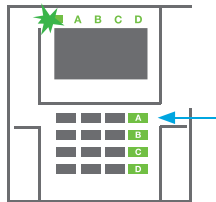
ADVERTENCIA: Esta es una función adicional del sistema de alarma.

El sistema también puede ser configurado para ser armado parcialmente, lo que permite que solo ciertos detectores vigilen en una partición.

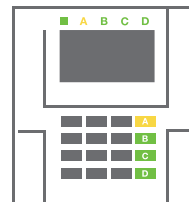
Ejemplo: Por la noche, es posible armar solamente los detectores de puerta y ventanas, mientras los detectores de movimiento seleccionados no generarán una alarma cuando alguien se mueva dentro de la partición.



1. Autorícese utilizando el teclado (introduzca un código o pase una tarjeta o tag por el lector). El botón indicador de sistema empezará a parpadear en verde.



2. Presione el botón de función de la partición seleccionada.



3. El comando es ejecutado y el botón de función se vuelve permanentemente amarillo para indicar el armado parcial de la partición.

Para armar totalmente la instalación en la cual está habilitado el armado parcial, mantenga presionado el botón para armar el panel de control durante 2 segundos o presiónelo dos veces. Después de presionar una vez el botón este se muestra continuamente iluminado en amarillo, tras la segunda pulsación se muestra iluminado continuamente en rojo.

Si el sistema ya está armado en parcial – el botón de función se muestra continuamente iluminado en amarillo – el sistema se puede armar totalmente a través de una autorización y presionando el botón amarillo durante un tiempo más largo. Una vez soltado el botón, el sistema estará totalmente armado y el botón se vuelve rojo.

El armado parcial puede ser configurado de tal manera que no se requiera autorización.

Para desarmar el panel de control cuando está parcialmente armado, presione el botón amarillo. El panel de control se desarmará y el botón se vuelve verde.

2.1.3.4. CONTROL DE ACCESO POR COACCIÓN

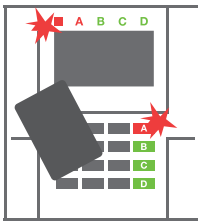
Le permite desarmar el panel de control de un modo especial. El sistema aparentemente se desarma, sin embargo, genera una alarma de pánico silencioso que es reportada a los usuarios seleccionados (incluyendo CRA).

El desarmado bajo coacción se lleva a cabo sumando 1 al último número de un código válido. Contacte con su técnico de servicio si quiere utilizar esta funcionalidad.

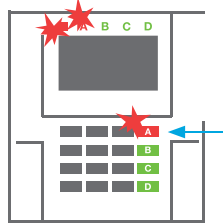
Ejemplo: Código válido: 9999

Código para desarmar bajo coacción: 9990

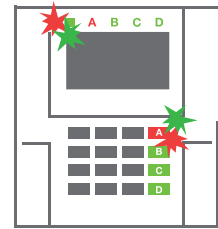
2.1.3.5. FINALIZAR UN SALTO DE ALARMA



1. Autorícese utilizando el teclado (introduzca un código o pase una tarjeta o tag por el lector).



2. Presione el botón de función de la partición en la cual se ha generado la alarma.



3. Se desarma el sistema y las sirenas se silencian. Los botones de función parpadean alternativamente (verde/rojo) y los indicadores de estado indican la memoria de alarma.

Un salto de alarma en curso se indica por el parpadeo rojo del indicador estado y el botón de función. Es necesario autorizarse utilizando el teclado para terminar la alarma. La partición continúa armada, y un parpadeo rápido rojo del botón de función indica la memoria de alarma. La indicación se mantendrá activa incluso después de que el sistema haya sido desarmado.

ADVERTENCIA: Si la indicación de la memoria de alarma fue activada durante su ausencia, extreme siempre las precauciones al acceder, busque la causa de la alarma en el historial de eventos y tenga mucho cuidado al inspeccionar la instalación o espere a que llegue el guardia de seguridad (en caso de que su sistema esté conectado a una Central Receptora de Alarmas).

La indicación de memoria de alarma permanece en el sistema hasta que el sistema se arma de nuevo. Alternativamente, puede ser cancelada desde el menú del teclado. Menú principal – Cancelar memoria de alarma. La indicación de una alarma de sabotaje solo puede finalizarse a través de un técnico de Servicio o un Administrador.

Nota: Cuando se utiliza el perfil del sistema "Por defecto", es posible seleccionar una acción en particular y presionar un botón de función primero y después confirmarla a través de autorización utilizando el teclado.

Terminar una alarma utilizando un mando a distancia también desarmará la partición correspondiente.

2.1.4. MANEJANDO EL SISTEMA CON UN MANDO A DISTANCIA

El mando debe estar asignado al sistema por su instalador. Puede estar asociado a usuarios específicos lo que evitará notificaciones por SMS al usuario que está interactuando con el sistema (si los parámetros de notificaciones están configurados de esa manera). Los mandos controlan e indican el estado de su batería y están equipados con un indicador óptico y acústico.

MANDOS BIDIRECCIONALES

Las funciones del botón se diferencian por los iconos del candado. El candado cerrado arma las particiones programadas; el icono con el candado abierto las desarma. La ejecución correcta de un comando se confirma a través del LED; desarmado – verde, armado – rojo. Un fallo de comunicación (fuera de rango del panel de control) se indica a través de un parpadeo amarillo del LED. Los botones con símbolos de círculo y circunferencia pueden controlar otra partición. Los botones del mando también pueden configurarse para controlar salidas PG de diferentes modos: el primer botón activa/ el Segundo desactiva, cada botón puede tener una función individual cuando se utilicen las funciones impulso o cambio. Para más funciones, es posible presionar los dos botones al mismo tiempo. De esta forma, el mando de 4 botones puede tener hasta 6 funciones individuales o estados de salidas PG (ej. encender y apagar luces), alternativamente dos salidas PG (ej. una puerta de garaje y cerradura eléctrica).

Si el sistema está configurado para Armar después de confirmación (capítulo 2.1.1) el detector indicará el armado sin éxito con el encendido del LED verde si el dispositivo está activado. Es necesario confirmar el armado presionando el botón del candado cerrado de nuevo. El armado de la partición será confirmado a través del LED rojo.

Los botones del mando se pueden bloquear para evitar pulsaciones accidentales. El comando será enviado entonces cuando se presione el botón repetidamente. La indicación de batería baja se indica acústicamente (con 3 tonos) y ópticamente con un parpadeo amarillo del LED después de la presionar un botón.

Para más información consulte la configuración del mando con su técnico de servicio.

MANDOS UNIDIRECCIONALES

Los mandos unidireccionales envían una señal cada vez que se pulsa un botón sin recibir confirmación por parte del panel de control. El envío de la señal se confirma solamente por un parpadeo corto rojo del LED y con un tono.

2.2. CONTROL EN REMOTO

El servicio MyJABLOTRON proporciona la mayor comodidad para controlar y administrar el sistema de forma remota. El interfaz web MyJABLOTRON es el único servicio que permite el acceso on-line a los dispositivos JABLOTRON. Esto permite al usuario final monitorizar y controlar el sistema. Está disponible tanto en forma de app para smartphone como en aplicación web. El servicio MyJABLOTRON permite a los usuarios:

- :: Ver el estado actual del sistema,
- :: Armar / desarmar el sistema al complete o parte de él,
- :: Control de salidas programables,
- :: Ver el historial de eventos,
- :: Envío de reportes a usuarios seleccionados vía SMS, e-mail o notificaciones PUSH,
- :: Captura de imágenes desde dispositivos de foto-verificación y navegar a través de la pestaña Galería de fotos o directamente en los Eventos recientes,
- :: Monitorizar temperatura actual o consumo de energía, incluyendo una historia de registros o gráficos,
- :: Y otras características útiles.

Dependiendo de su país o región, un socio JABLOTRON autorizado puede crearle una cuenta web para MyJABLOTRON. El login es la dirección email del usuario. La contraseña para el primer inicio de sesión se enviará a ese email. Esta contraseña puede cambiarse en los ajustes del usuario en cualquier momento.

2.2.1. MANEJANDO EL SISTEMA USANDO LA APP PARA SMARTPHONE MyJABLOTRON

Una vez que se ha creado la cuenta de usuario, el usuario puede monitorizar y controlar el sistema a través de la app MyJABLOTRON para Smartphones Android e iOS.

2.2.2. MANEJANDO EL SISTEMA A TRAVÉS DEL INTERFAZ WEB MyJABLOTRON

El sistema JABLOTRON puede manejarse fácil y convenientemente utilizando su ordenador a través de internet y el interfaz web MyJABLOTRON, que está accesible desde www.myjablotron.com.

2.2.3. MANEJANDO EL SISTEMA USANDO EL MENÚ DE VOZ

El sistema puede controlarse desde un teléfono mediante un simple menú de voz, el cual guía al usuario a través de una serie de opciones en el lenguaje configurado previamente. Para acceder al menú de voz solamente tiene que llamar al número de teléfono de su sistema de alarma.

El acceso al menú de voz se puede habilitar para todos los números sin restricciones o solamente para números de teléfono autorizados y guardados en el panel de control. Dependiendo de la configuración, se requerirá autorizarse introduciendo un código válido a través del teclado del teléfono. Cuando el usuario entra en el menú, el sistema le dará información actualizada del estado actual de todas las particiones asignadas al usuario. El remitente de la llamada puede controlar esas particiones, tanto individual como colectivamente, utilizando el teclado del teléfono y las opciones del menú disponibles.

Por defecto, el sistema está configurado para responder las llamadas entrantes después de tres tonos (aproximadamente 15 segundos).

2.2.4. MANEJANDO EL SISTEMA A TRAVÉS DE COMANDOS SMS

Los comandos SMS pueden controlar particiones individuales y salidas programables igual que los botones de un segmento del teclado. La forma del mensaje de texto para manejar el sistema es: CODIGO_COMANDO. Los comandos actuales están predefinidos (ARMAR/DESARMAR) con un parámetro numérico adicional que identifica una partición específica. Un SMS puede controlar múltiples particiones al mismo tiempo. En ese caso, añada los números de las particiones en el comando.

Ejemplo de un comando SMS para armar las particiones 2 y 4:

CODIGO_CONECTAR_2_4

Los comandos para manejar salidas programables pueden ser programados por el instalador del sistema. Por ejemplo, podría elegir CERRAR PERSIANAS como su comando para cerrar las persianas de sus ventanas. También es posible configurar el sistema para que no se requiera un código antes de un comando. En este caso el comando es simplemente identificado automáticamente una vez que el sistema reconoce el número de teléfono del usuario desde el que fue enviado el SMS. Esta configuración es realizada por un técnico de servicio.

2.2.5. MANEJO DEL SISTEMA REMOTAMENTE USANDO UN ORDENADOR (JA-100-LINK)

El sistema JABLOTRON 100+ puede ser controlado remotamente utilizando un ordenador con el software JA-100-Link. Se puede descargar desde la sección "Descargas" de la página www.myjablotron.com.

2.2.6. CONTROL DE SALIDAS PROGRAMABLES (PG)

2.2.6.1. SEGMENTO DEL TECLADO

Una salida PG se puede activar pulsando el botón derecho de un segmento y desactivarla pulsando el botón izquierdo. Si la salida está configurada como impulso, se desactivará una vez pase el tiempo preconfigurado. El control de la PG puede ser guardado, o no, en la memoria de eventos del panel de control. Esta configuración la realiza el técnico de servicio.

Puede requerir autorización, o no, en base a la configuración del sistema.

2.2.6.2. AUTORIZACIÓN DE UN USUARIO EN EL TECLADO

Es posible activar una salida PG solamente con la autorización de un usuario (introduciendo un código o utilizando tag RFID). La salida PG debe ser configurada para activarse desde un teclado asignado.

2.2.6.3. DESDE EL MENÚ DEL TECLADO CON PANTALLA LCD

Después de la autorización del usuario se pueden controlar las salidas programables desde el menú del teclado con pantalla LCD. El usuario tendrá acceso a las salidas programables dependiendo de sus permisos.

Control desde el menú del teclado:

::Autorícese con un código válido o un chip RFID.

::Acceda al menú pulsando ENTER.

::Control PG → ENTER.

::Seleccione el grupo de PGs deseado utilizando las flechas (1–32), (33–64), (65–96), (97–128) → ENTER.

::Seleccione la PG deseada utilizando las flechas → ENTER.

::Presionando ENTER repetidamente cambiará el estado de la PG (el estado activo de la PG se muestra con el número de la PG un rectángulo con el fondo color negro).

::Presionar ESC para salir al menú.

2.2.6.4. MANDO

A través de la pulsación de un botón asignado en el mando. El mando bidireccional confirma la activación de una salida PG con el indicador LED.

2.2.6.5. APP PARA SMARTPHONE MyJABLOTRON

Pulsando ON/OFF en la pestaña Automatización (PG).

2.2.6.6. INTERFAZ WEB MyJABLOTRON

Pulsando ON/OFF en la pestaña Automatización (PG).

2.2.6.7. LLAMADA PERDIDA

Cada número de teléfono almacenado en el sistema (un usuario puede tener un número de teléfono) puede controlar la PG a través de una llamada perdida (sin establecer la llamada). La llamada perdida consiste en llamar al número de la tarjeta SIM utilizada por el sistema de seguridad y colgar antes de que el sistema conteste la llamada. Por defecto, el sistema contestará la llamada después de tres tonos (aproximadamente 15 segundos).

2.2.6.8. MENSAJE SMS

Enviando un SMS puede activar/desactivar una PG en particular. Puede requerir autorización, o no, en base a la configuración del sistema.

Ejemplo: CODIGO_TEXTO CONFIGURADO

3. BLOQUEANDO/DESHABILITANDO EL SISTEMA

3.1. BLOQUEO DE USUARIOS

Cualquier usuario puede ser temporalmente bloqueado (ej. cuando un usuario pierde su tarjeta/tag o se revela su código). Cuando se bloquea un usuario, su código ID o tarjeta/tag no serán aceptados por el sistema. El usuario tampoco recibirá ninguna alerta por mensaje de texto ni informe de voz en su teléfono.

Solo el administrador del sistema o el técnico de servicio pueden bloquear un usuario. Un método para retirar permisos de acceso es a través del teclado LCD, seleccionando Configuración / de los usuarios / Usuario / Bypass y seleccionar "SI". Otra opción es bloquear un usuario, local o remotamente, utilizando el software JA-100-Link en Ajustes / Usuarios / Bloqueo de usuarios.

Un usuario bloqueado (deshabilitado) se marcará con un círculo rojo hasta que el bloqueo sea cancelado.

3.2. BLOQUEO DE DETECTORES

Un detector puede bloquearse temporalmente de un modo similar al de un usuario. Un detector se desactiva cuando no su activación no es deseada temporalmente (por ejemplo, un detector de movimiento en una habitación con una mascota o deshabilitar el sonido de una sirena). El sistema todavía supervisa el estado del contacto de sabotaje y envía eventos de servicio, pero la función de alarma está desactivada.

Sólo el administrador o el técnico de servicio pueden bloquear un detector. Se puede realizar a través del teclado LCD seleccionando Configuración / Dispositivos periféricos / bypass y seleccionar "SI". Otra opción es utilizar el software JA-100-Link, pulsando en Ajustes/ Diagnóstico / Deshabilitar en el detector individual. Un detector bloqueado se marcará con un círculo amarillo hasta que se cancele el bloqueo utilizando el mismo procedimiento. También se puede bloquear un detector a través de la app para smartphone MyJABLOTRON.

3.3. DESHABILITAR CALENDARIO

Para deshabilitar eventos programados automáticamente por el calendario del Sistema, se puede deshabilitar ese calendario. Deshabilitando un evento de calendario (ej. desarmar el sistema para vigilancia nocturna a una hora predeterminada) se detendrá la ejecución de ese evento (ej. durante las vacaciones).

El calendario se puede deshabilitar local o remotamente a través del software JA-100-Link seleccionando Ajustes / Calendarios / Bloqueado. Un calendario deshabilitado se marcará con un círculo rojo hasta que se vuelva a habilitar utilizando el mismo procedimiento.

4. PERSONALIZANDO EL SISTEMA

4.1. CAMBIAR CÓDIGO DE ACCESO DE USUARIO

Si el sistema está configurado con códigos sin prefijo, solamente el administrador y el técnico de servicio pueden cambiar los códigos de seguridad. El administrador del sistema puede realizar los cambios tanto desde el menú del teclado LCD como desde el software JA-100-Link y la app para smartphone MyJABLOTRON. El código puede cambiarse tras la autorización seleccionando Configuración / de los usuarios / Usuario / Código. Para introducir un nuevo código debe entrar en modo editar presionando Enter (el código empezará a parpadear), introducir el nuevo código y confirmarlo presionando Enter de nuevo. Una vez realizados los cambios, estos deben ser confirmados seleccionando Guardar cuando el sistema le indique "Guardar configuraciones?"

Si el sistema está configurado con códigos con prefijo, los usuarios individuales pueden ser habilitados para cambiar sus propios códigos desde el menú del teclado LCD.

4.2. CAMBIAR, ELIMINAR O AÑADIR TARJETA/TAG RFID

Si el sistema esta configurado con códigos sin prefijo, solamente el administrador y el técnico de servicio pueden cambiar los códigos de seguridad. El administrador del sistema puede realizar los cambios tanto desde el menu del teclado LCD como desde el software JA-100-Link y la app para smartphone MyJABLOTRON. El Código puede cambiarse tras la autorizacion seleccionando Configuración / de los usuarios / Usuario / Código. Para introducir un nuevo código debe entrar en modo editar presionando Enter (el código empezara a parpadear), introducir el nuevo código y confirmarlo presionando Enter de nuevo. Una vez realizados los cambios, estos deben ser confirmados seleccionando Guardar cuando el sistema le indique "¿Guardar configuraciones?".

Si el sistema esta configurado con códigos con prefijo, los usuarios individuales pueden ser habilitados para cambiar sus propios códigos desde el menu del teclado LCD.

4.3. CAMBIAR NOMBRE DE USUARIO O NÚMERO DE TELÉFONO

Si el sistema esta configurado con códigos con prefijo, los usuarios pueden números, cambiar o borrar sus números de telefono o cambiar sus nombres a través del menu del teclado LCD. Esto se puede realizar tras autorizarse, seleccionando Configuración / de los usuarios / Usuario / tel. El usuario debe entrar en modo editar para hacer los cambios. Esto se hace pulsando Enter. Despues de hacer los cambios, deben confirmarse pulsando Enter de nuevo. Para borrar un numero de telefono introduzca "0" en el campo del numero de telefono. Una vez realizados los cambios, estos deben ser confirmados seleccionando Guardar cuando el sistema le indique "¿Guardar configuraciones?"

El administrador del sistema y el técnico de servicio pueden añadir, cambiar y eliminar números de teléfono o nombres de usuarios tanto desde el menú del teclado LCD como desde el software JA-100-Link.

4.4. AÑADIR/ELIMINAR UN USUARIO

Sólo el administrador del Sistema o el técnico de servicio pueden añadir nuevos usuarios al Sistema (o eliminarlos). Los nuevos usuarios pueden ser añadidos al sistema (o eliminados de él) solamente a través del software JA-100-Link, o el software F-Link en el caso del técnico.

Al crear un nuevo usuario, es necesario asignarle permisos de acceso (derechos), particiones que el usuario puede manejar, salidas programables que puede controlar y el tipo de autorización que será necesaria.

4.5. AJUSTES DE EVENTOS POR CALENDARIO

Es posible configurar eventos por calendario (desarmar/armar/ armar parcialmente, control o bloqueo de salidas PG). Los calendarios se pueden configurar a través del JA-100-Link en la pestaña Calendarios.

Para cada evento de calendario se puede activar, partición o salida PG y el tiempo del evento. El día se puede definir como un día de semana, mes o año. Para el día seleccionado puede configurar hasta 4 eventos para realizar una acción o armado de partición en intervalos regulares.

Por lo tanto, los eventos de calendario se pueden personalizar no solo para el control de particiones sino también para controlar varias tecnologías en el objeto utilizando salidas PG.

5. HISTORIAL DE EVENTOS

El sistema de seguridad almacena todas las acciones realizadas y eventos (armados, desarmados, alarmas, fallos, mensajes enviados a usuarios y CRAs) en la tarjeta micro SD del panel de control del sistema. Cada entrada incluye la fecha, hora (inicio y fin), y fuente (causa / origen) del evento.

Las diferentes vías de buscar a través del historial de eventos del sistema:

5.1. UTILIZANDO EL TECLADO LCD

El acceso al historial de eventos a través del teclado requiere la autorización del usuario. Una vez autorizado, se mostraran las opciones disponibles (en base a los permisos del usuario) y podrá encontrar Memorias de eventos. Los registros pueden verse utilizando las flechas.

5.2. UTILIZANDO EL SOFTWARE JA-100-LINK Y UN ORDENADOR

La memoria del sistema puede visualizarse utilizando el software JA-100-Link. Los eventos se pueden descargar del panel de control en grupos reducidos (sobre 1,200 eventos) o grandes (sobre 4,000 eventos). Pueden ser filtrados en detalle, marcados en colores para una identificación mas sencilla o guardados en un archivo de su ordenador.

5.3. INICIANDO SESIÓN EN MyJABLOTRON (WEB/SMARTPHONE)

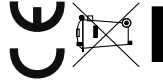
Todos los eventos del sistema pueden verse despues de iniciar sesion en el interfaz web/ Smartphone MyJABLOTRON. La cuenta muestra el historial en el rango que corresponde a los permisos de los usuarios.

6. ESPECIFICACIONES TÉCNICAS

PARÁMETRO	JA-103K	JA-103K-7 Ah	JA-107K
Alimentación del panel de control	~ 110-230 V/50-60 Hz, máx. 0.28 A con fusible F1.6 A/250 V Protección clase II	~ 110-230 V/50-60 Hz, máx. 0.28 A con fusible F1.6 A/250 V Protección clase II	~ 110-230 V/50-60 Hz, máx. 0.85 A con fusible F1.6 A/250 V Protección clase II
Batería de respaldo	12 V; 2,6 Ah (gel)	12 V; 7 Ah (gel)	12 V; 7 to 18 Ah (gel)
Tiempo de carga máximo para la batería	48 h	48 h	48 h
Voltaje en el BUS (rojo - negro)	12,0 a 13,8 V	12,0 a 13,8 V	12,0 a 13,8 V
Máximo consumo continuo de corriente tomado del panel de control	1000 mA	1000 mA	2000 mA permanente 3000 mA por 60 minutos (máx. 2000 mA para un BUS)
Máximo consumo continuo de corriente para 12 h de respaldo	JA-103K – 2.6 Ah Backup-Batterie Sin comunicador GSM LAN – OFF: 115 mA LAN – ON: 88 mA	JA-103K – 7 Ah Backup-Batterie Sin comunicador GSM LAN – OFF: 334 mA LAN – ON: 300 mA	JA-107K – 18 Ah Backup-Batterie Sin comunicador GSM LAN – OFF: 1135 mA LAN – ON: 1107 mA
Máximo consumo continuo de corriente para 24 h de respaldo	Con comunicador GSM LAN – OFF: 80 mA LAN – ON: 53 mA	Con comunicador GSM LAN – OFF: 302 mA LAN – ON: 270 mA	Con comunicador GSM LAN – OFF: 1100 mA LAN – ON: 1072 mA
Máximo consumo continuo de corriente para 24 h de respaldo	Sin comunicador GSM LAN – OFF: 21 mA	Sin comunicador GSM LAN – OFF: 160 mA LAN – ON: 125 mA	Sin comunicador GSM LAN – OFF: 535 mA LAN – ON: 499 mA
Número máx. de equipos	50	50	230
Comunicador LAN	Interfaz Ethernet, 10/100BASE 268 X 225 X 83 MM	Interfaz Ethernet, 10/100BASE 357 X 297 X 105 MM	Interfaz Ethernet, 10/100BASE 357 X 297 X 105 MM
Dimensiones			

PARAMETR	JA-103K	JA-103K-7 Ah	JA-107K
Peso con/sin AKU	1844 g/970 g	3755 g/1665 g	7027 g/1809 g
Reacción ante código de entrada inválido	Alarma tras 10 intentos erróneos		
Memoria de eventos	Aprox. últimos 7 millones de eventos, incluyendo fecha y hora		
Fuente de alimentación	Tipo A de acuerdo con EN 50131-6 T 031 nota: En caso de un fallo de la alimentación principal, se hace una copia de seguridad del sistema durante 24 horas y al mismo tiempo se envía un informe de fallo a la CRA.		
Clasificación	Seguridad grado 2 de acuerdo con EN 50131-1		
Ambiente operacional	Environmental class II (indoor general) according to EN 50131-1		
Rango de temperatura operacional	-10 °C a +40 °C		
Humedad operacional media	75 % RH, sin condensación		
Cumple con	EN 50131-1 ed. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1, EN 50131-6 ed. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN IEC 63000		
Frecuencia de radio (con módulo JA 11XR)	868,1 MHz		
Emissiones de radio	ETSI EN 300 220-1,-2 (module R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)		
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7		
Conformidad de seguridad	EN IEC 62368-1		
Identificación de llamadas (CLIP)	ETSI EN 300 089		
Condiciones de operación	ERC REC 70-03		
Organismo certificador	Trezor Test s.r.o. (no. 3025)		

Nota: Los parámetros pueden diferir si utiliza otro tipo de panel de control.



JABLOTRON a.s. declara mediante la presente que los paneles de control JA-103K, JA-103K-7Ah y JA-107K cumplen con la legislación relevante de la Unión Europea: Directivas No: 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU, cuando se utiliza como se indica.

La declaración original se puede encontrar en www.jablotron.com – sección Descargas.

Nota: La eliminación correcta de este producto ayudará a ahorrar recursos valiosos y evitar cualquier posible efecto negativo sobre la salud humana y el medioambiente, que de otro modo podría surgir de una manipulación inadecuada de los residuos. Por favor, devuelva el producto al distribuidor o póngase en contacto con su autoridad local para obtener más información sobre su punto de recogida designado más cercano.



www.jablotron.com

M-ESJA100+-USER