WCONTROL

MANUAL
DE INSTALACIÓN

IM_ESP_REV0126_WCONTROL

1.ÍNDICE

2.INTRODUCCIÓN

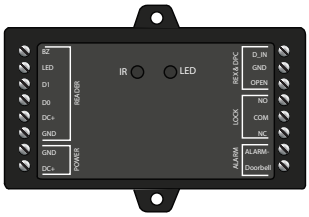
Manual de instalación para el dispositivo WControl. Este puede actuar como relé inteligente y permitir la activación del contacto de relé mediante la APP TUYA, así como actuar también como controladora ya que de conectar un lector Wiegand permitirá controlar identificaciones de proximidad y teclado.

Golmar garantiza un funcionamiento adecuado al conectar un lector, siempre y cuando se utilicen los siguientes modelos: CODEPROX-N, KEYBUS SE, KEYDUPROX, DUPROX y BLE-S.

3.ESPECIFICACIONES

Material	Plástico ABS color negro
Tensión de entrada	12Vcc
Corriente	Reposo: ≤ 100mA / Activo: ≤ 150mA
Capacidad	Uso de hardware: 1000 usuarios / Uso vía APP Tuya: 500 usuarios
Relé	NO, NC, común (2A máx.)
Identificaciones soportadas	Tarjeta, PIN, y APP TUYA
Formatos Wiegand soportados	Wiegand 26-44, 56 y 58 bits
Formatos de bits de salida de teclado soportados	4 bits o 8bits (ASCII)
Dimensión (Alto x Ancho x Profundidad):	91(An) x 48(Al) x 20(P)mm
Rango de humedad de trabajo:	0-90% (sin condensación)

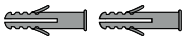
4.CONTENIDO



Controladora WControl

Diodo.

Varistores.

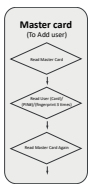


Tacos de fijación.

Tornillos.

Destornillador

Mando programación.

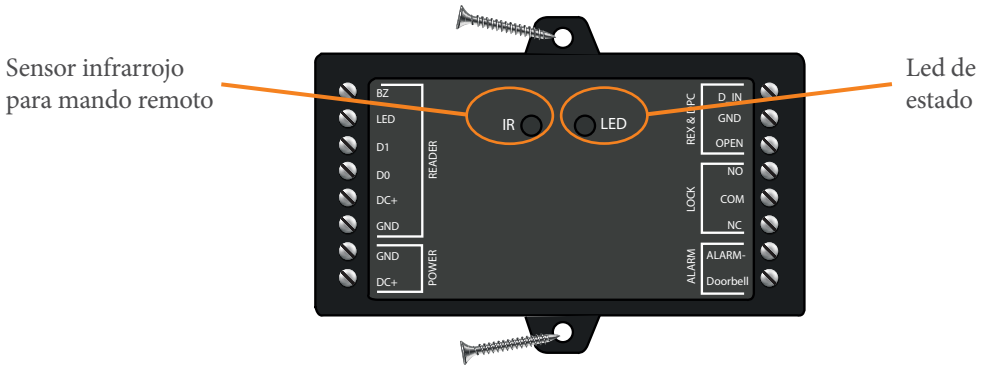


Tarjeta MASTER de programación.

IMPORTANTE:
Una vez programada la controladora tenga la tarjeta master y el mando de control remoto a buen recaudo para futuras programaciones.

5.INSTALACIÓN

Coloque la controladora en una caja de registro o habitáculo protegido y fíjela con los tornillos suministrados. Tenga presente antes de su colocación que en caso de hacer uso de la APP Tuya la controladora deberá de recibir cobertura WiFi del router de la instalación.



6.CONEXIÓN

BORNES IZQUIERDA	DESCRIPCIÓN	BORNES DERECHA	DESCRIPCIÓN
BZ	Control de buzzer	D_IN	Detección del estado de la puerta
LED	Control luces led	GND	Negativo contacto de puerta y salida
D1	Entrada Wiegand Data 0	OPEN	Conexión botón de salida
D0	Entrada Wiegand Data 1	NO	Salida de relé normalmente abierta
DC+	Salida positiva de alimentación	COM	Contacto común para salida de relé
GND	Salida negativa de alimentación	NC	Salida de relé normalmente cerrada
GND	Entrada negativa de alimentación	ALARM-	Negativo alarma
DC+	Entrada positiva de alimentación	DOOR BELL	Timbre externo

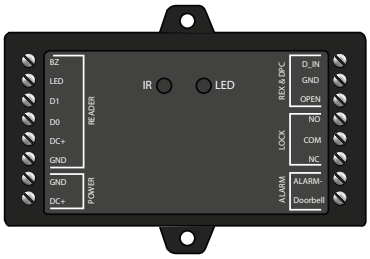
7.INDICADORES DE ESTADO

ESTADO OPERACIÓN	COLOR LED	TIMBRE
Reposo	Rojo	-
Entrada modo de programación	Parpadeo rojo	Pitido corto
En modo programación	Naranja	Pitido corto
Error de operación	-	3 pitidos
Salida modo programación	Rojo	Pitido corto
Puerta abierta	Verde	Pitido corto
Alarma	Parpadeo rojo rápido	Pitidos

GESTIÓN DE USUARIOS

8.GESTIÓN DE USUARIOS

La gestión de usuarios se puede realizar mediante la controladora o en el teléfono móvil a través de la APP Tuya:



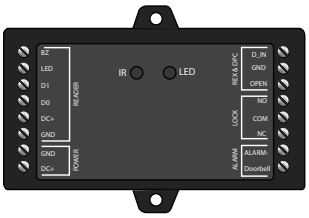
Mediante controladora

Mediante teléfono móvil a través de la APP Tuya

IMPORTANTE: antes de proseguir tenga presente que estas no se pueden trasladar de la controladora a la APP Tuya o viceversa.

8.1. GESTIÓN DE USUARIOS VÍA CONTROLADORA

La gestión de usuarios en la controladora como puede ver en los siguientes apartados es posible realizarla de varias maneras: básica (**8.1.1.Programación básica de usuarios**), recogida (**8.1.2.Programación mediante recogida de tarjetas**) o avanzada (**8.1.3.Programación avanzada**).



Gestión de usuarios en controladora

En caso de optar por la gestión de usuarios via APP prosiga el manual por el apartado "**9.2. Gestión de usuarios vía APP**".

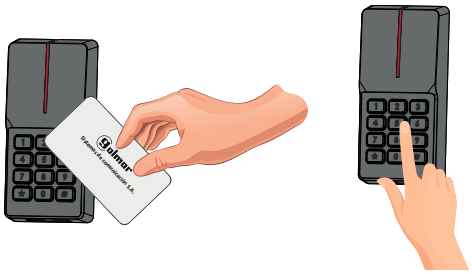
8.1.1.PROGRAMACIÓN BÁSICA DE USUARIOS

Programación básica (alta/borrado de usuarios) mediante la tarjeta "Master Card" suministrada con el producto.

ALTA DE USUARIO

1) Aproxime la tarjeta "Master Card" al lector.

2) Aproxime la tarjeta o introduzca PIN a dar de alta.
*Para PIN introduzca PIN de 4 a 6 digitos más #.

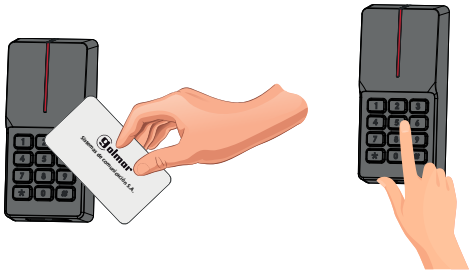


3) Aproxime la tarjeta "Master Card" al lector.

BORRAR USUARIO

1) Aproxime la tarjeta "Master Card" al lector 2 veces en un intervalo inferior a 5 segundos.

2) Aproxime la tarjeta o introduzca PIN a dar de baja.
*Para PIN introduzca PIN de 4 a 6 digitos más #.



3) Aproxime la tarjeta "Master Card" al lector.

NOTA: En caso de perdida de la TARJETA MASTER puede crear una realizando el proceso descrito en el apartado "10.4.Reset a valores de fábrica".

8.1.2.PROGRAMACIÓN MEDIANTE RECOGIDA DE TARJETAS

La controladora admite la programación de tarjetas en modo recogida. Lo que significa que una vez activado cualquier tarjeta que se aproxime al lector abrirá la puerta y quedará programada, una vez desactivado el modo recogida, la programación quedará completada (nuevas tarjetas no abrirán la puerta ni serán codificadas).

MODO RECOGIDA ON

* (CÓD.MAESTRO) # 93

PUERTA ES DESBLOQUEADA

USUARIO ES REGISTRADO

MODO RECOGIDA OFF

* (CÓD.MAESTRO) # 92

MODO RECOGIDA DE TARJETAS DESACTIVADO (valor de fábrica)

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	92	#

Ejemplo: * 987654 # 92 #

MODO RECOGIDA DE TARJETAS ACTIVADO

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	93	#

Ejemplo: * 987654 # 93 #

Este modo está orientado a instaladores ya que simplifica el trabajo, pudiendo estos entregar las credenciales al administrador de la instalación y desactivar el modo recogida transcurridos unos días (una vez todas las credenciales entregadas hayan sido utilizadas).

8.1.3.PROGRAMACIÓN AVANZADA

Para la programación avanzada será necesario el uso del mando de control remoto:

-Retire el plástico protector de la pila antes de empezar a utilizar el mando.
-Utilice el mando en una posición cercana a la controladora y apuntando al led "IR".

Realice la siguiente secuencia para entrar en programación:

Entrar en modo administrador		
*	CÓDIGO MAESTRO (Por defecto: 123456)	#

IMPORTANTE

La controladora indicará el acceso a programación con el encendido del led "verde" y a continuación el led parpadera en "rojo" . Al iniciar secuencia de programación (función a programar) el led se mostrará en "naranja".
Para salir de programación pulse "*" la controladora pasará a estar en reposo, led de estado "rojo fijo". En caso de no realizar ninguna pulsación, transcurridos 30 segundos la controladora también sale automáticamente de programación.

Una vez en programación, realizar la secuencia de programación deseada. A continuación, se detallan las diferentes programaciones del sistema.

8.1.3.1.CAMBIO DE CÓDIGO MAESTRO

Es recomendable modificar el código maestro para ello:

Entrar en modo administrador							
*	CÓDIGO MAESTRO	#	0	NUEVO CÓDIGO MAESTRO (6 DIGITOS)	#	NUEVO CÓDIGO MAESTRO (6 DIGITOS)	#

Ejemplo: * 123456 # 0 987654 # 987654 #

8.1.3.2.ALTA DE TARJETAS (AUTO ID)

Alta de tarjetas con registro automático.

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	1	APROXIMAR TARJETA

Ejemplo: * 987654 # 1 APROXIMAR TARJETA

8.1.3.3.ALTA DE TARJETAS (ID ESPECIFICO)

El número de registros máximo es de 990. IDs de usuario del 0 al 989.

Entrar en modo administrador						
*	CÓDIGO MAESTRO	#	1	ID DE USUARIO (0-989)	#	APROXIMAR TARJETA

Ejemplo: * 987654 # 1 1 # APROXIMAR TARJETA

IMPORTANTE: no introducir IDs de usuario con ceros previos al valor ID.

8.1.3.4.ALTA DE PIN (AUTO ID)

Alta de PINs con registro automático.

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	1	PIN	#

Ejemplo: * 987654 # 1 4543 #

8.1.3.5.ALTA DE PIN (ID ESPECIFICO)

El número de registros máximo es de 990. IDs de usuario del 0 al 989.

Entrar en modo administrador							
*	CÓDIGO MAESTRO	#	1	ID DE USUARIO (0-989)	#	PIN	#

Ejemplo: * 987654 # 1 1 # 4543 #

IMPORTANTE: no introducir IDs de usuario con ceros previos al valor ID.

8.1.3.6.BORRADO DE PIN

Borrado de PINs introduciendo PIN a borrar.

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	2	INTRODUCIR PIN	#

Ejemplo: * 987654 # 2 4543 #

8.1.3.7.BORRADO DE TARJETAS

Borrado de tarjetas aproximando tarjeta a borrar.

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	2	APROXIMAR TARJETA

Ejemplo: * 987654 # 2 APROXIMAR TARJETA

8.1.3.8.BORRADO DE TARJETA O PIN (ID ESPECIFICO)

Introducir el ID correspondiente al usuario a borrar.

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	2	ID DE USUARIO (0-989)	#

Ejemplo: * 987654 # 2 1 #

8.2. GESTIÓN DE USUARIOS VÍA APP

Este equipo cuenta con comunicación WiFi lo cual permite el uso de la APP Tuya.

NOTA: a continuación, se muestra información con todo detalle para la configuración de la APP TUYA. Puede consultar esta información de manera más simplificada en la guía rápida "QGI_ESP_REV0125_APP-TUYA-WCONTROL".

8.2.1.INSTALACIÓN APP TUYA

Instale la aplicación "TUYA" en su smartphone.
La puede descargar desde Google Play o Apple Store en función del sistema operativo de su smartphone.

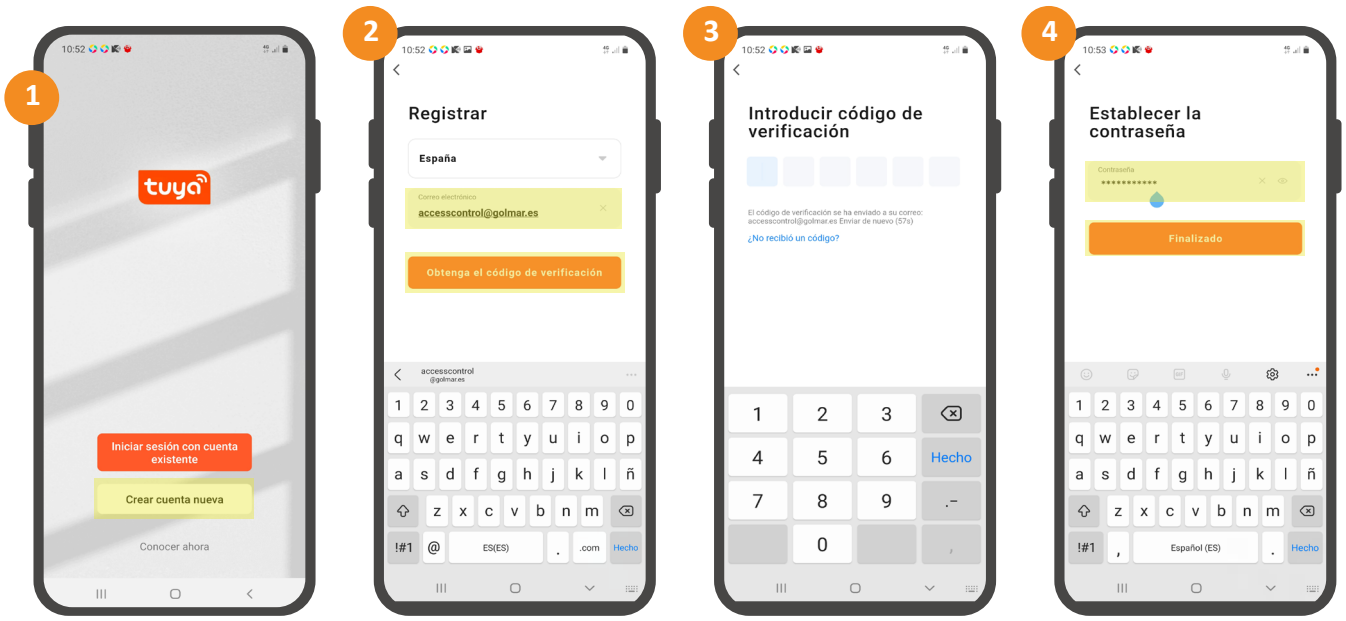
QR Play Store (Android)

QR Apple Store (IOS)

IMPORTANTE:
- Golmar no es desarrollador de la APP Tuya, Tuya es una plataforma en nube que permite la gestión de dispositivos IoT, Golmar ofrece la posibilidad de hacer uso de la controladora con la tecnología Tuya.
- La APP es compatible con smartphones con versión iOS (7.0 o superior) o Android (4.3 o superior).

8.2.2.REGISTRO Y LOGIN

1 - Pulse la opción "Crear cuenta nueva" en la pantalla inicial.
2 - Indique el correo electrónico del "super administrador" de la instalación. Tras esto pulse "Obtenga el código de verificación".
3 - Introduzca el código de verificación que habrá recibido al correo electrónico indicado.
4 – Establezca una contraseña.



NOTA: tras estos pasos probablemente le aparezca ventana en la que le indique "Necesitamos los siguientes permisos para ofrecerle mejores servicios", estos permisos no son necesarios para hacer uso de la aplicación, es a su elección declinarlos o aceptarlos.

8.2.3.AÑADIR CONTROLADORA

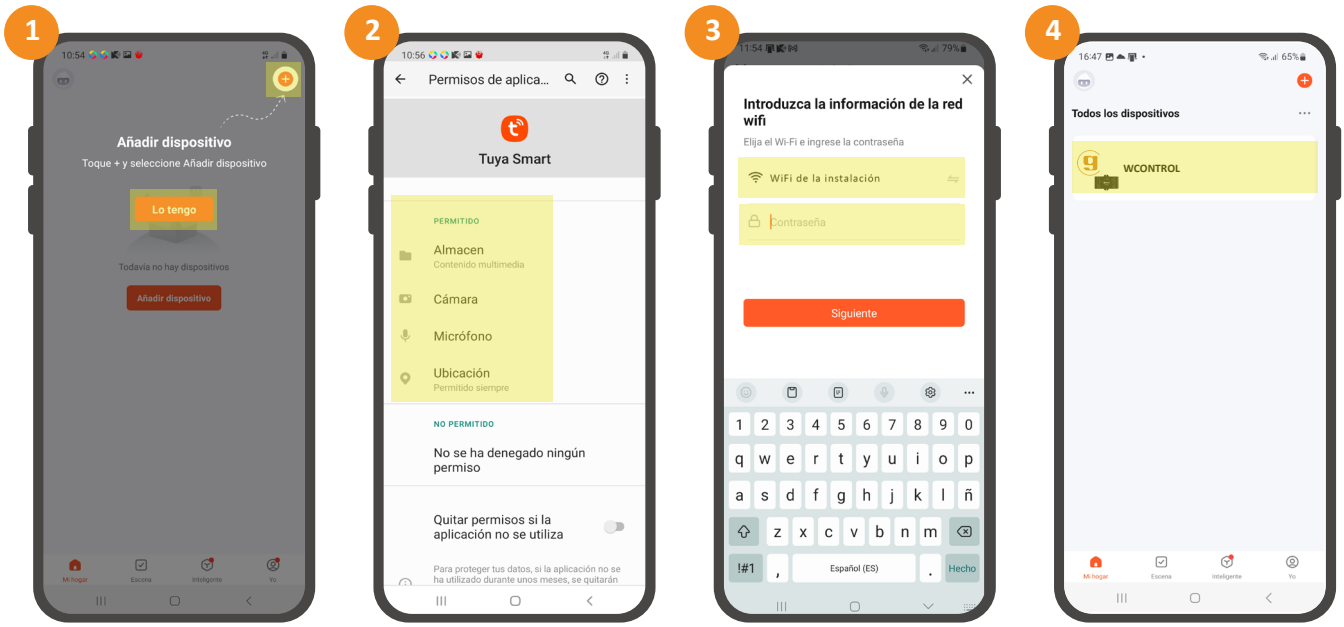
Una vez concluidos los pasos anteriores, la cuenta estará creada y con la sesión iniciada, el asistente de la APP le sugerirá añadir dispositivo. Prosiga de la siguiente manera:

1 - Pulse la opción "Lo tengo" y a continuación el simbolo "+" o "añadir dispositivo".

2 - Conceda permiso a la APP para que esta haga uso de diferentes prestaciones del smartphone (cámara, micrófono, ubicación, …).

3 - A continuación, acerque el smartphone a la controladora (el Bluetooth deberá estar activado ya que es requerido durante el emparejamiento). Seguidamente seleccione y establezca la contraseña de la conexión WiFi a la que se conectará la controladora para disponer de internet.

4 - Controladora añadida.



IMPORTANTE

- La red WiFi a la que conectar la controladora deberá ser frecuencia 2.4GHz.
- En caso de que la controladora no sea detectada de forma automática, realice la siguiente secuencia mediante el mando emisor:

* código maestro # 9 código maestro #

La conectividad será reseteada, realice esta secuencia únicamente en caso de que el dispositivo no sea detectado.

8.2.4.COMPARTIR DISPOSITIVO

El usuario que añade inicialmente la controladora es por defecto "administrador", este podrá gestionar lo siguiente:

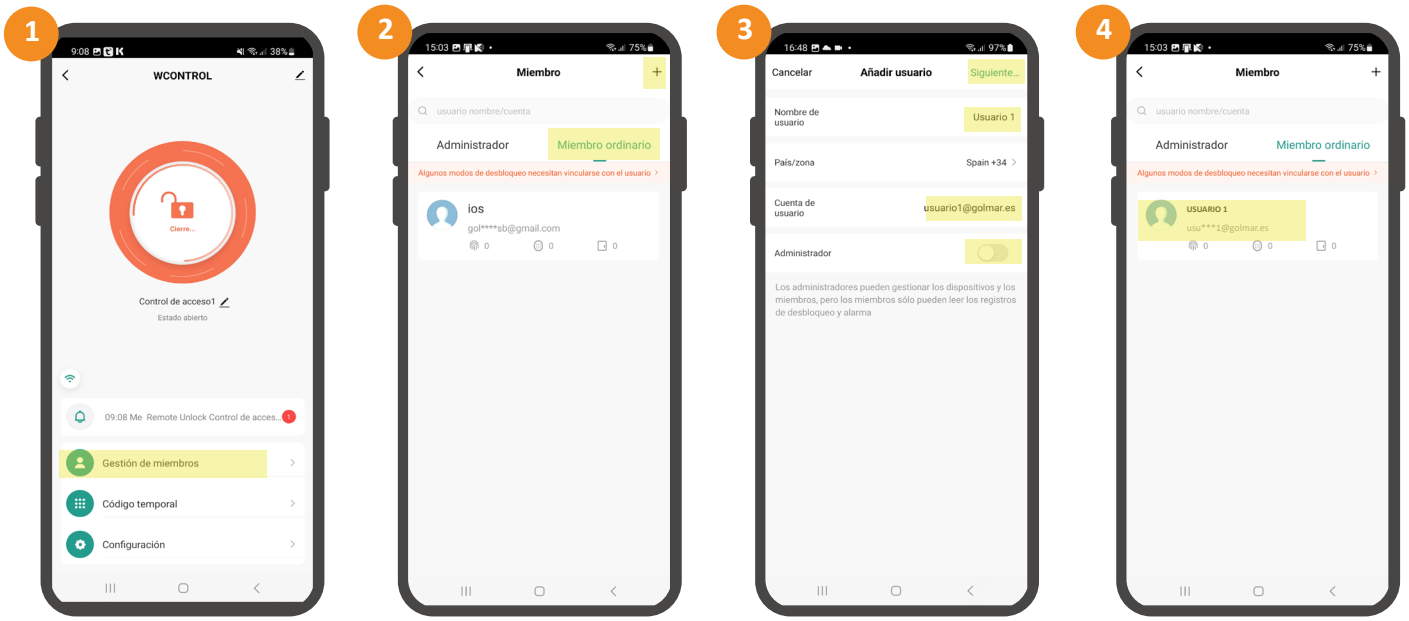
FUNCIÓN	ADMINISTRADOR
APERTURA DE PUERTA	SI
GESTIÓN DE ADMINISTRADORES Y USUARIOS	SI
GESTIÓN DE USUARIOS	SI
DEFINIR USUARIOS COMO ADMIN	SI
VER TODOS LOS REGISTROS	SI
AJUSTAR TIEMPOS DE RELÉ	SI

Este podrá compartir la instalación a otros usuarios los cuales pueden ser "administradores" o "usuarios" (miembro ordinario). Estos podrán gestionar lo siguiente:

FUNCIÓN	ADMINISTRADOR	USUARIO (miembro ordinario)
APERTURA DE PUERTA	SI	SI
GESTIÓN DE ADMINISTRADORES Y USUARIOS	SI	NO
GESTIÓN DE USUARIOS	SI	NO
DEFINIR USUARIOS COMO ADMIN	NO	NO
VER TODOS LOS REGISTROS	SI	NO
AJUSTAR TIEMPOS DE RELÉ	SI	NO

1 - Pulse sobre la opción “Gestión de miembros” ubicada en la parte inferior de la pantalla principal de la controladora.
2 - A continuación, pulse la pestaña “miembro ordinario” y seguidamente “+”.
3 - Registre un nombre identificativo en el campo“nombre de usuario” e indique la dirección de correo electrónico del usuario TUYA en “cuenta de usuario”, desmarque la casilla “administrador”, finalmente pulse “siguiente”.
4 - El dispositivo ha sido compartido. En el momento que el usuario acepte la invitación podrá comenzar a hacer uso del dispositivo.

IMPORTANTE
El usuario al que se le comparta la instalación tendrá que disponer de cuenta (haberse registrado en la APP, apartado “9.2.2. Registro y login”).

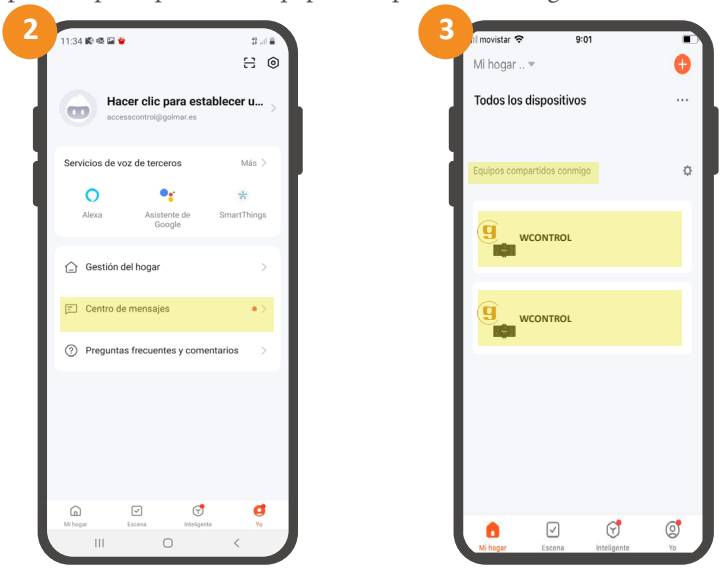


NOTAS
1 - El usuario en este momento podrá realizar la apertura con el smartphone, para otorgarle otros métodos de acceso vea el punto nº6.
2 - Si desea añadir más usuarios, repita el proceso.
3 - Si se desea borrar un usuario acceda al listado (pantalla paso 2), seleccione el usuario y luego pulse la opción “eliminar miembro”.
4 - De desear añadir el usuario con derechos de “administrador”, no desmarque la casilla “administrador” en el paso 3.

8.2.5. USUARIOS

1 - El usuario recibirá una notificación push indicándole que le han compartido un nuevo dispositivo:

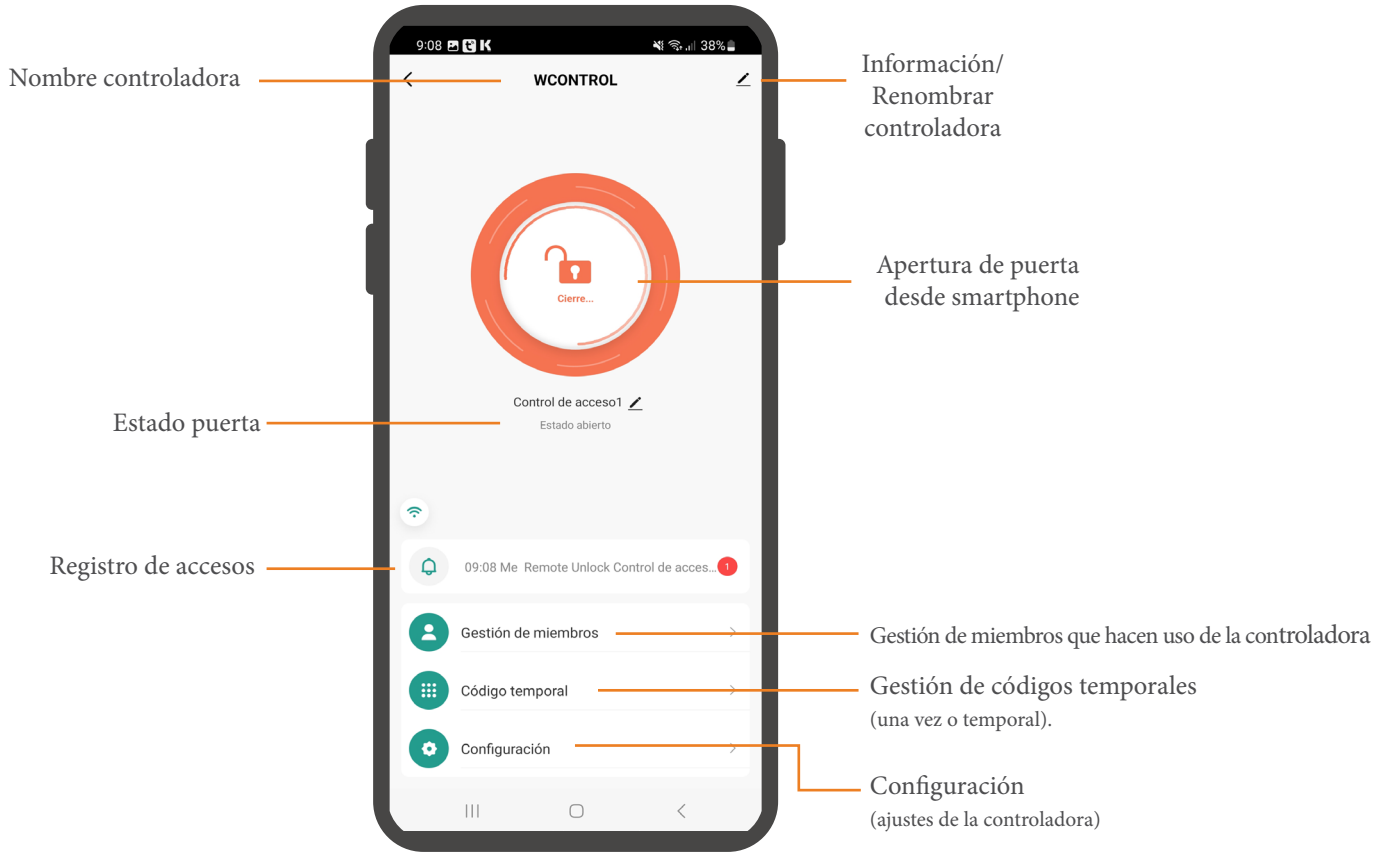
2 - Esta puede ser comprobada desde el “centro de mensajes” (pestaña “yo” de la pantalla principal).
3 - El dispositivo aparecerá en la pantalla principal como “equipos compartidos conmigo”.



NOTA: las notificaciones push pueden variar en función del sistema operativo del smartphone.

8.2.6.PANTALLA PRINCIPAL DE LA CONTROLADORA

A continuación, se describe la pantalla principal de la controladora:



NOTA: los miembros ordinarios (usuarios) no tendrán posibilidad de hacer uso de las funciones "Gestión de miembros", "Código temporal" y "configuración".

8.2.7.CREDENCIALES DE ACCESO

Antes de proceder con las credenciales de acceso tenga presente que el usuario que realice esta gestión deberá ser "administrador".

8.2.8.ALTA DE CREDENCIALES DE ACCESO

1 - En la pantalla principal de la controladora pulse "Gestión de miembros".

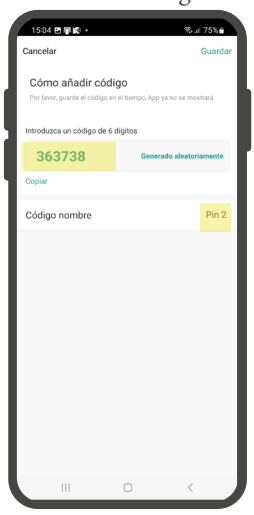
2 - Seleccione usuario al que dar de alta credencial.

3 - Pulse "Añadir" en el tipo de identificación a registrar (código o tarjeta).

A continuación, se describe como es el proceso de alta en los diferentes tipos de identificación:

8.2.9.ALTA DE CÓDIGO PIN

Establezca un PIN de 6 dígitos y un nombre con el que identificar el PIN registrado, para finalizar pulse “guardar”.

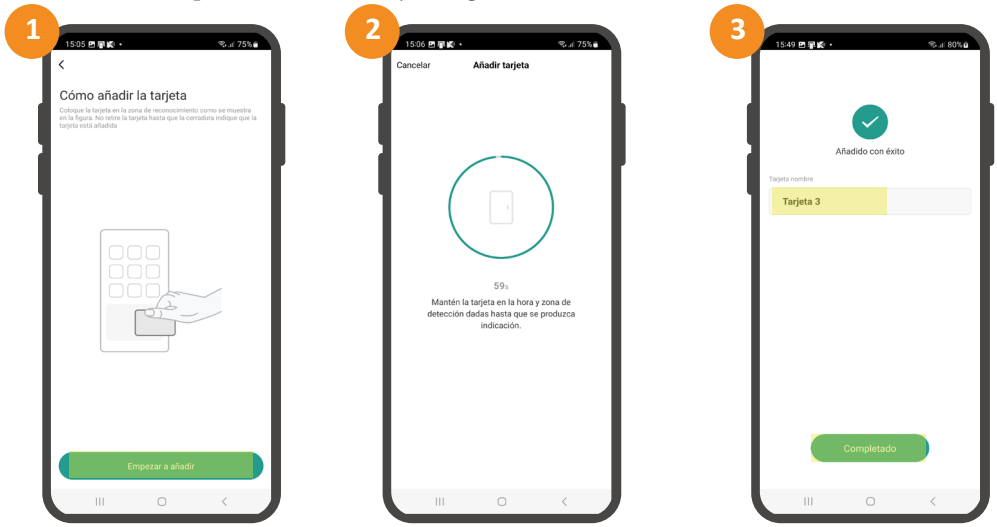


8.2.10.ALTA DE TARJETA

1 - Pulse sobre la opción “Empezar a añadir”.

2 - Aproxime la tarjeta a registrar sobre el lector que se haya conectado a la controladora.

3 - Introduzca un nombre con el que identificar la tarjeta registrada.

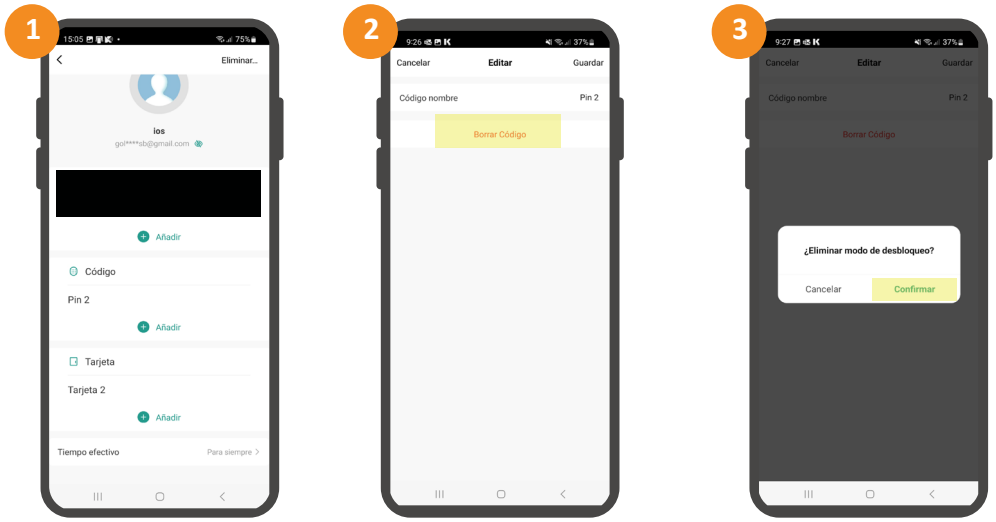


8.2.11.BORRADO DE CREDENCIAL

1 - Seleccione la credencial de acceso del usuario que se desee borrar.

2 - Pulse la opción “borrar” resaltada en rojo.

3 - Pulse “confirmar” para completar el proceso de borrado.



9.FUNCIONES ADICIONALES APP TUYA

9.1. CÓDIGO TEMPORAL POR PERIODO DE TIEMPO

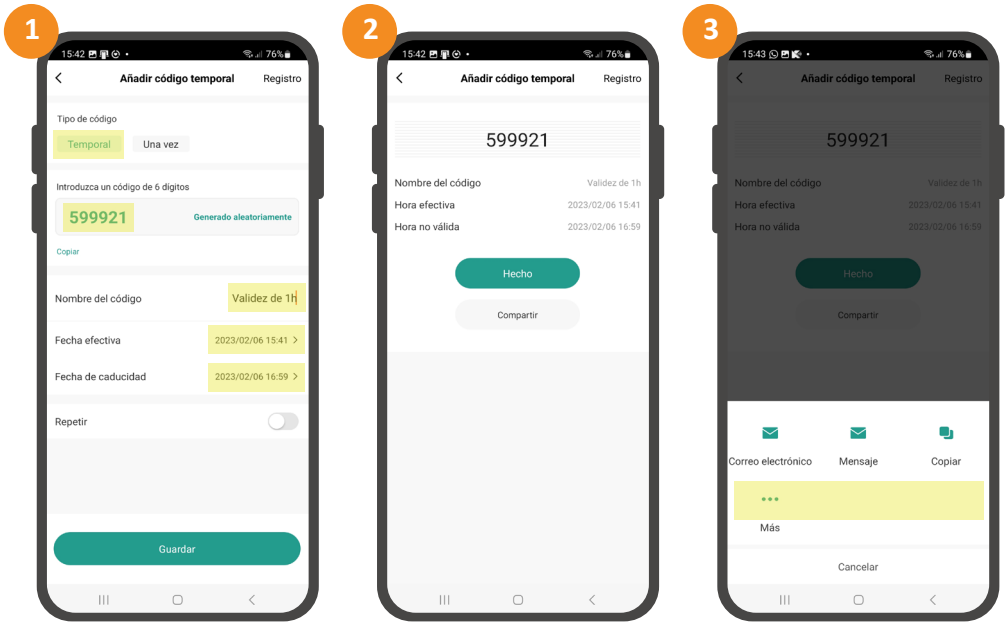
Pulse sobre la opción "código temporal" situado en la parte inferior de la pantalla de gestión del dispositivo.

1 - Rellene los campos de generación de código temporal:

- Seleccione tipo de código "Temporal".
- Introduzca código de 6 dígitos que permitirá la apertura o pulse sobre la opción "Generado aleatoriamente".
- Nombre el acceso temporal que esta apunto de generar.
- Determine el periodo de validez del acceso.

2 - Se mostrará confirmación del acceso temporal generado.

3 - Pulse compartir y seleccione el método con el que enviar el código de activación. Si este no aparece en las opciones visibles, pulse sobre la opción "más".



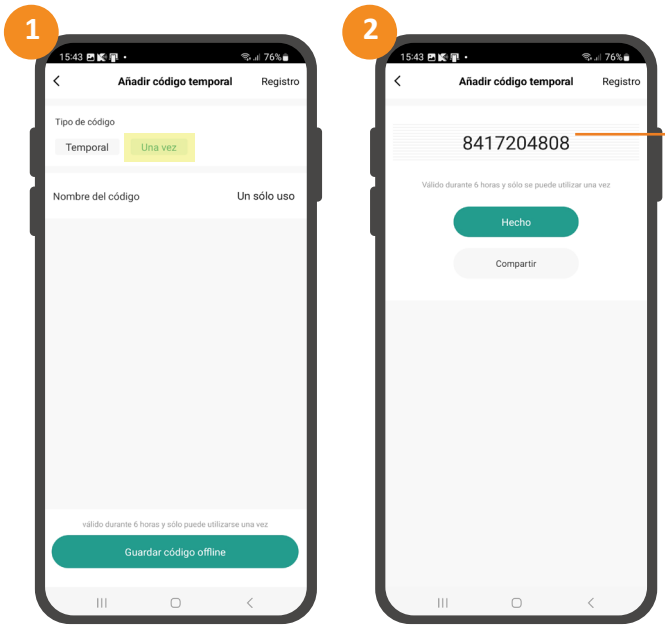
9.2. CÓDIGO TEMPORAL DE UN SOLO USO

Pulse sobre la opción "código temporal" situado en la parte inferior de la pantalla de gestión del dispositivo.

1 - Seleccione tipo de código "Una vez".

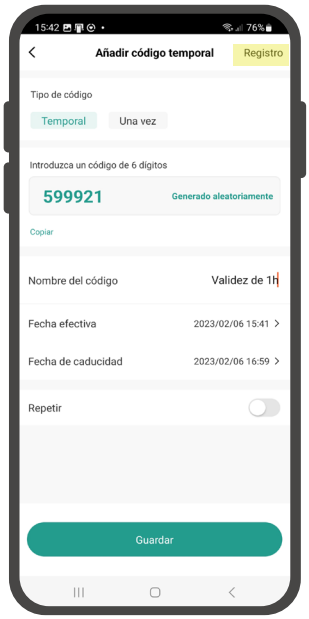
- Nombre el acceso temporal que esta apunto de generar.

2 - Se mostrará confirmación del acceso temporal generado. Si desea compartir el código siga el paso 3 descrito en el punto anterior.



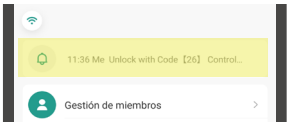
El código será válido durante 6h desde su generación.

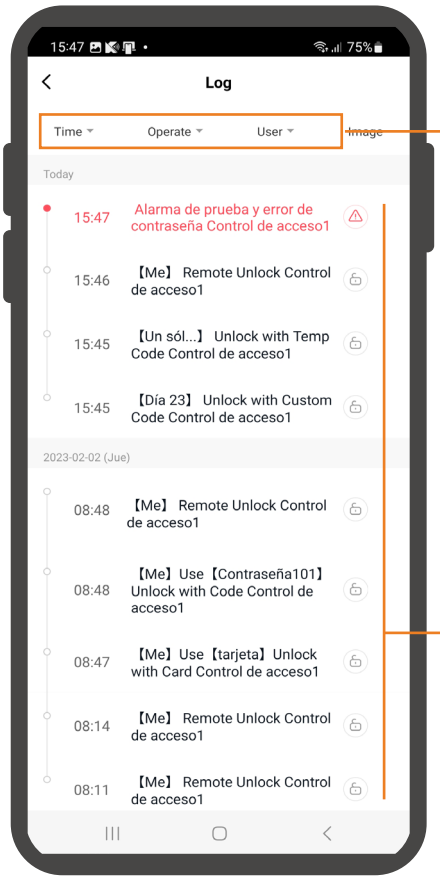
NOTA: es posible comprobar los códigos temporales generados desde la opción “Registro” del menú “código temporal”:



9.3. LOGS (REGISTRO DE EVENTOS)

Pulse sobre la opción “registro de accesos” de la pantalla principal de la controladora para supervisar los accesos:





Filtros:

TIME: muestra todos los eventos “All tiem”, los de los últimos 3 días “Nearly three days”, últimos 7 días “Nearly seven days”, último mes “Nearly a month” o definir el rango de tiempo deseado “Custom”.

OPERATE: muestra todos los accesos “All records”, únicamente los autorizados “Door opening record” o únicamente los denegados “Alarm record”.

USER: muestra todos los usuarios “All user” o bien es posible seleccionar usuario/s a mostrar.

Registros:

Registros de accesos autorizados.

Registros de accesos no autorizados.

Las líneas de registro incluyen fecha y hora del registro, así como datos identificativos del evento registrado: usuario, tipo de identificación y nombre de la credencial.

9.4.VALIDEZ DE LAS CREDENCIALES DE USUARIO

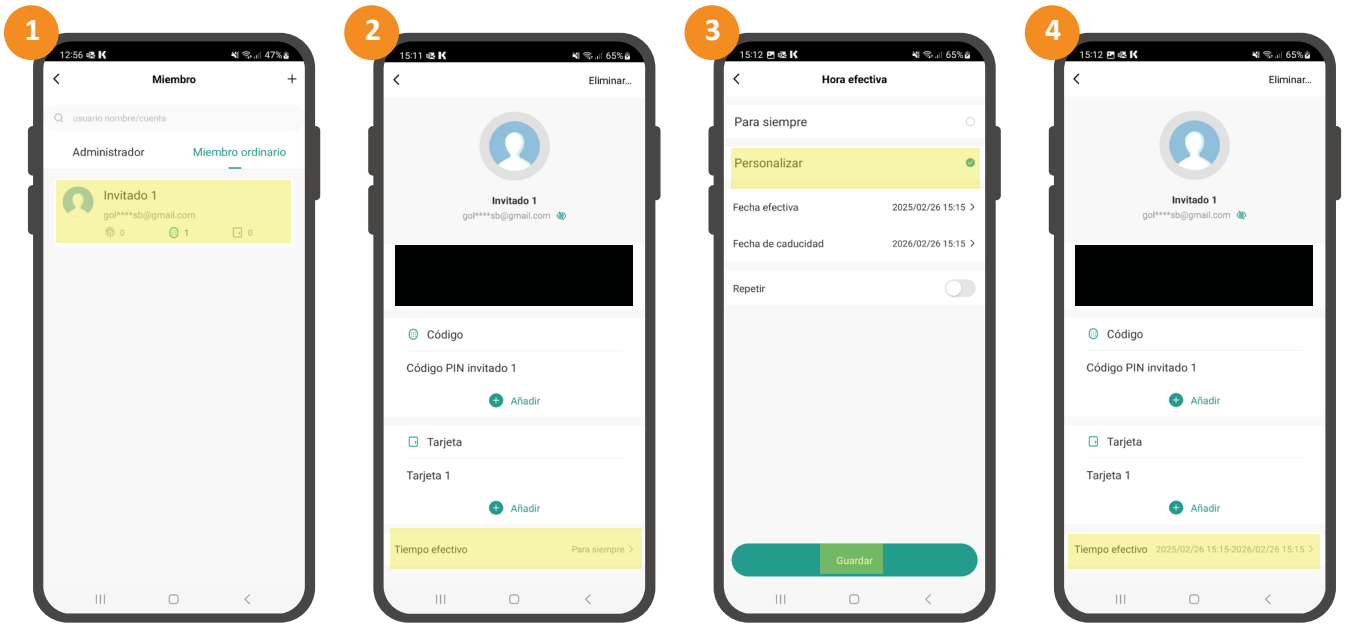
Para gestiones temporales de acceso, se recomienda hacer uso de la opción "código temporal por periodo de tiempo" explicada en los apartados "10.1" de este manual, no obstante, la aplicación permite establecer la validez de las credenciales del usuario de la siguiente manera:

1 - Desde "Gestión de miembros" seleccione el usuario sobre el cual desea limitar el periodo de tiempo de uso.

2 - Pulse sobre la opción "Tiempo efectivo"

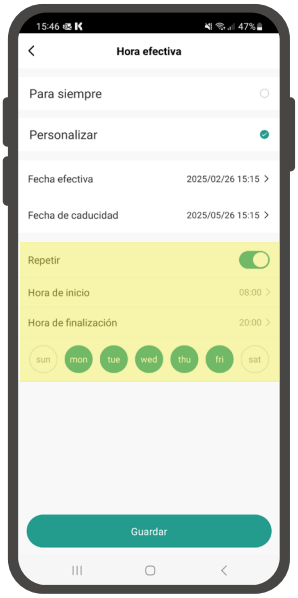
3 - Active la opción "Personalizar", a continuación, establezca fecha de inició y fin de la validez, complete la configuración pulsando en "Guardar".

4 - El ajuste estará completado y el usuario únicamente se podrá identificar de manera valida durante el periodo de tiempo establecido.

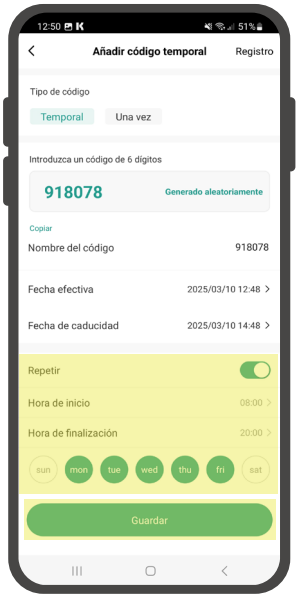


9.5.HORARIOS

A la "validez de las credenciales de usuarios" así como a "código temporal por periodo de tiempo" se le podrá establecer un horario de uso:



Configuración de horario en validez de credenciales de usuario

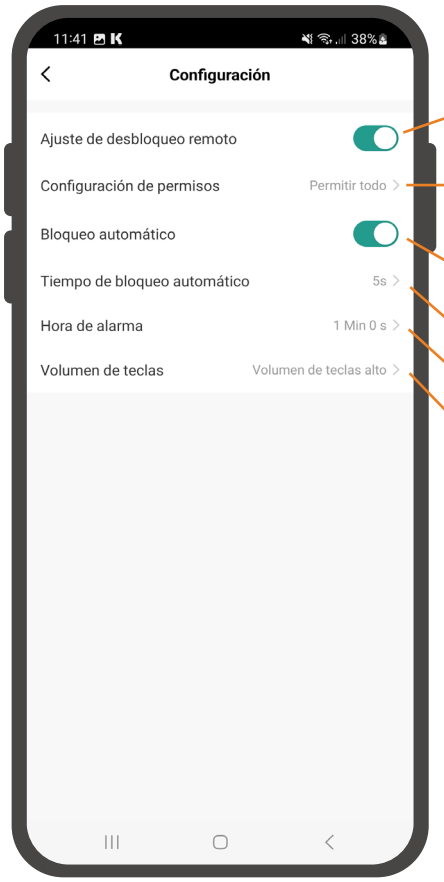


Configuración de horario en código temporal por periodo de tiempo

Como se puede observar el ajuste horario permite establecer que días y en que intervalo de tiempo será posible el acceso.

9.6. AJUSTES EN APP

De pulsar el menú "Configuración" de la página principal del dispositivo podrá realizar los siguientes ajustes:



Activado, permite activar el contacto de relé vía APP.

Permiso admin, los miembros ordinarios no pueden activar el contacto de relé vía APP.

Permiso todo, todos los usuarios pueden activar el contacto de relé vía APP.

* De requerir que ciertos usuarios no hagan uso de la APP, opte por no registrar el correo electrónico al añadirlos.

Bloqueo automático activado, modo pulso.

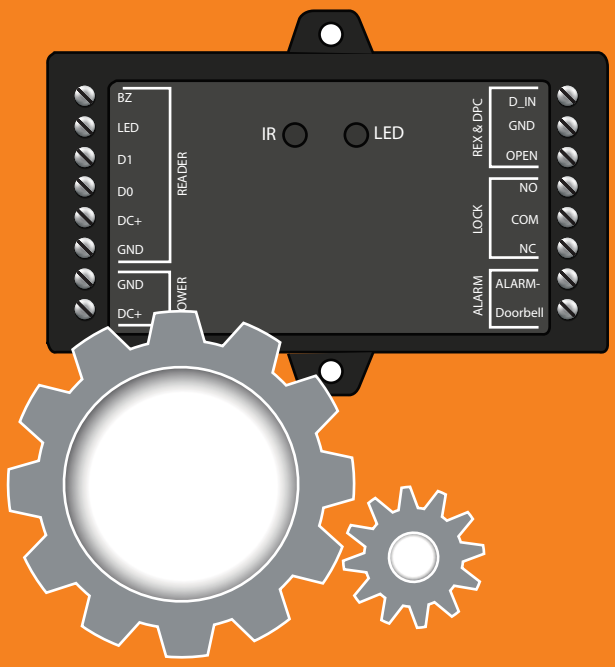
Bloqueo automático desactivado, modo enclavado.

Tiempo de apertura, ajustable en modo pulso (1-100 segundos).

Tiempo de alarma, , alarma por intentos fallidos, puerta abierta,... (1-180 segundos).

Volumen de teclas, volumen de pitido confirmación al pulsar teclas de mando remoto.

CONFIGURACIÓN CONTROLADORA



10.OTRAS PROGRAMACIONES

10.1. MODO DE IDENTIFICACIÓN

10.1.1.IDENTIFICACIÓN POR TARJETA O PIN

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	43 (valor de fábrica)	#

Ejemplo: * 987654 # 43 #

10.1.2.IDENTIFICACIÓN SOLO POR PIN

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	41	#

Ejemplo: * 987654 # 41 #

10.1.3.IDENTIFICACIÓN SOLO POR TARJETA

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	40	#

Ejemplo: * 987654 # 40 #

10.2. AJUSTES DE TIEMPO DE ALARMA (TAMPER)

10.2.1.ACTIVAR TAMPER

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	5(0-3)	#

Ejemplo: * 987654 # 52 #

El tiempo de activación de la alarma tamper es de 0 a 3 minutos. En el ejemplo se ha introducido el valor 52 por lo que estaría activa 2 minutos.
Valor de fábrica: 51 (1 minuto).

10.3. AJUSTES DE RELÉ

10.3.1.MODO PULSO

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	3	1-99	#

Ejemplo: * 987654 # 3 15 #

El pulso puede estar activo de 1 a 99 segundos. En el ejemplo se ha introducido el valor 15 por lo que estaría activo 15 segundos.
Valor de fábrica: 5 segundos.

10.3.2.MODO ENCLAVADO

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	3	0	#

Ejemplo: * 987654 # 3 0 #

El relé pasa a estar en modo ON/OFF.

10.4. ALARMA DE BLOQUEO (INTENTOS FALLIDOS)

La alarma de bloqueo se activará después de 10 intentos fallidos. El valor predeterminado de fábrica es OFF, pero se puede configurar para denegar el acceso durante 10 minutos o para activar la alarma después de dispararse.

10.4.1.BLOQUEO DESACTIVADO

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	60 (valor de fábrica)	#

Ejemplo: * 987654 # 60 #

10.4.2.BLOQUEO DE ACCESO DE 10 MINUTOS

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	61	#

Ejemplo: * 987654 # 61 #

El led comenzará a parpadear y el equipo quedará bloqueado durante 10minutos. Para volver al estado normal esperar 10minutos o reiniciar la controladora.

10.4.3.ALARMA

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	62	#

Ejemplo: * 987654 # 62 #

La alarma quedará activada, en caso de que se produzcan 10 intentos fallidos sonará el tiempo que se haya definido en el apartado "11.2. AJUSTE DE TIEMPO DE ALARMA (TAMPER)". En caso de aproximar tarjeta de usuario, introducir código PIN de usuario o aproximar tarjeta MASTER la alarma se detendrá.

10.5. DETECCIÓN DE PUERTA ABIERTA

Se sugiere conectar contacto de puerta en el dispositivo. De lo contrario, en la APP móvil el estado de la puerta se mostrará siempre en "ON". Conecte el contacto de puerta a los bornes "D_IN" y "GND".

10.5.1.DETECCIÓN PUERTA ABIERTA ACTIVADA

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	64	#

Ejemplo: * 987654 # 64 #

10.5.2.DETECCIÓN PUERTA ABIERTA DESACTIVADA

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	63 (valor de fábrica)	#

Ejemplo: * 987654 # 63 #

10.6. AJUSTES VISUALES Y SONOROS

10.6.1.BUZZER ACTIVADO

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	71 (valor de fábrica)	#

Ejemplo: * 987654 # 71 #

10.6.2.BUZZER DESACTIVADO

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	70	#

Ejemplo: * 987654 # 70 #

10.6.3.LED ACTIVADO

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	73 (valor de fábrica)	#

Ejemplo: * 987654 # 73 #

10.6.4.LED DESACTIVADO

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	72	#

Ejemplo: * 987654 # 72 #

10.7. RESET A VALORES DE FÁBRICA

El reset restablece la controladora a valores de fábrica, reseteando la configuración y el código maestro (la información correspondiente a los usuarios será conservada).

1. Retire la alimentación.
2. Mantenga presionado el botón de salida*.
3. Conecte la alimentación.
4. Cuando escuche 2 pitidos, deje de pulsar el botón de salida*.
5. El led se iluminará en amarillo.
6. Aproxime una tarjeta por el lector (el tipo de tarjeta deberá ser reconocible por el lector conectado).
7. La luz se iluminará en rojo y el equipo se habrá restablecido a valores de fábrica.

*Requiere tener conectado pulsador de salida, hilo amarillo (OPEN) y el hilo negro (GND).

NOTA

- Este proceso genera una tarjeta MASTER reemplazando la anterior.
- En caso de no desear reemplazar la tarjeta master actual, mantenga pulsado el botón de salida*, en lugar de realizar el paso 6 para finalizar el reset.

10.8. BORRADO DE TODOS LOS USUARIOS

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	2	CÓDIGO MAESTRO	#

Ejemplo: * 987654 # 2 987654 #

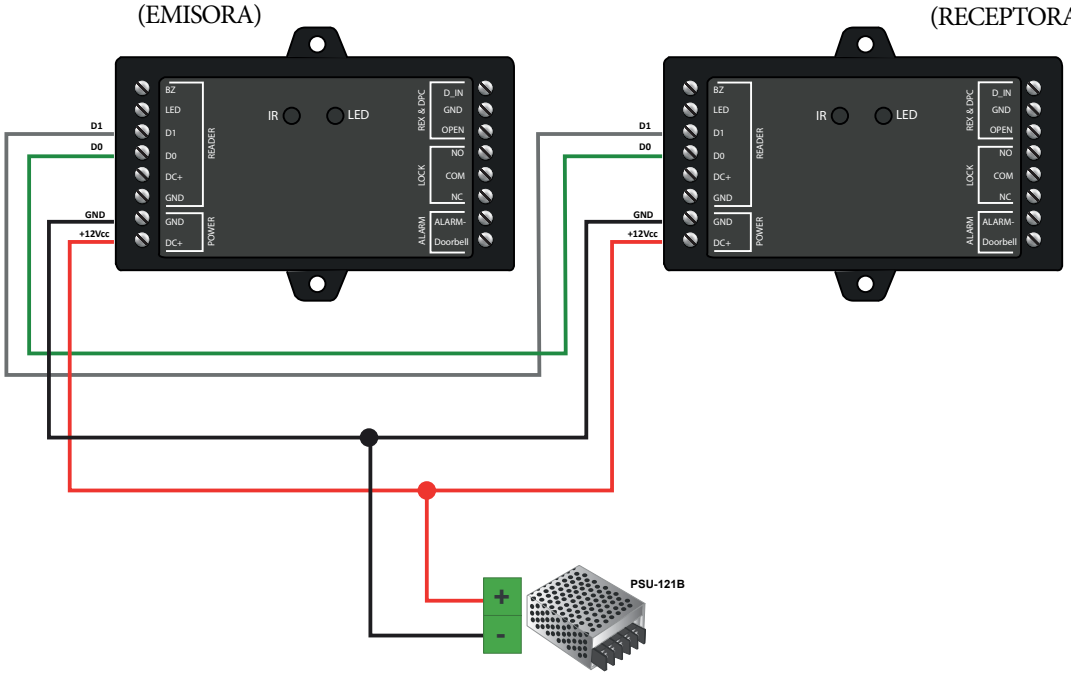
IMPORTANTE: Antes de avanzar con esta función asegúrese que no hay problema en ELIMINAR todos los usuarios registrados previamente.

11.TRANSFERIR INFORMACIÓN DE USUARIOS

Es posible volcar la información de usuarios registrados de una unidad a otra. Para ello realice la siguiente conexión entre controladoras:

CONTROLADRA CON USUARIOS (EMISORA)

CONTROLADORA SIN USUARIOS (RECEPTORA)



A continuación realizar la siguiente secuencia en la controladora que contiene los usuarios registrados (emisor):

Entrar en modo administrador				
*	CÓDIGO MAESTRO	#	98	#

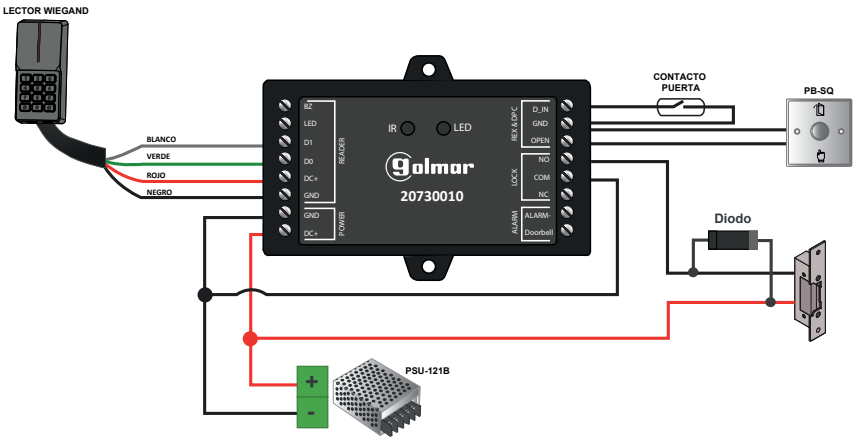
Ejemplo: * 987654 # 98 #

En un intervalo de 30 segundos, el led verde brilla, después de un pitido, el led se convertirá en rojo, lo que significa que la información del usuario se ha transferido con éxito. Una vez completada la transferencia pulse "*" o espere a que la controladora vuelva al estado de reposo.

IMPORTANTE: el código maestro establecido en la controladora emisora y en la controladora receptora deberá ser el mismo. De disponer la controladora receptora de usuarios registrados estos quedaran eliminados.

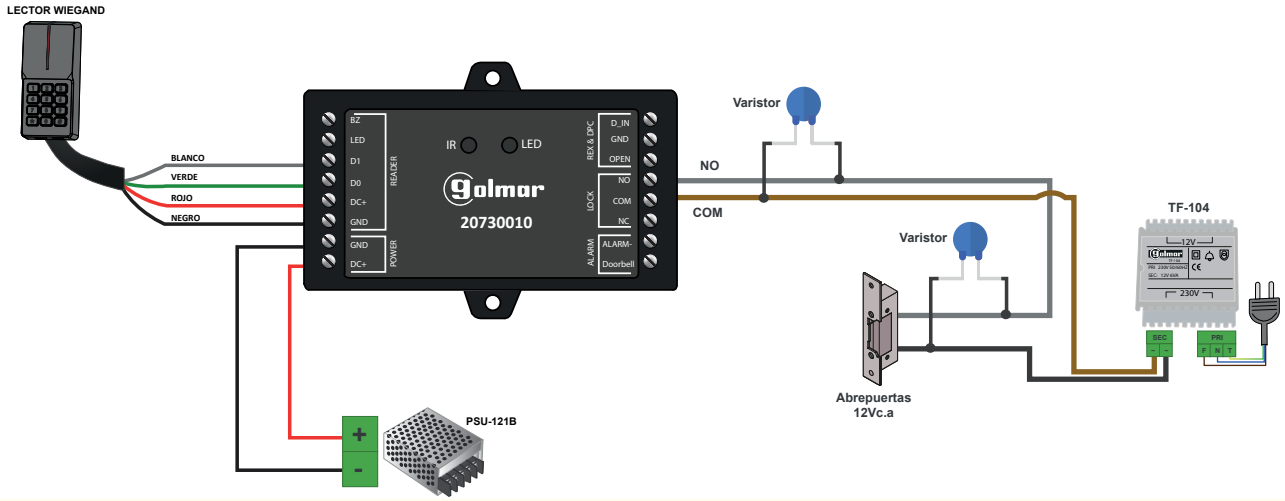
12.ESQUEMAS DE CONEXIÓN

12.1.ESQUEMA CON ABREPUERTAS CC



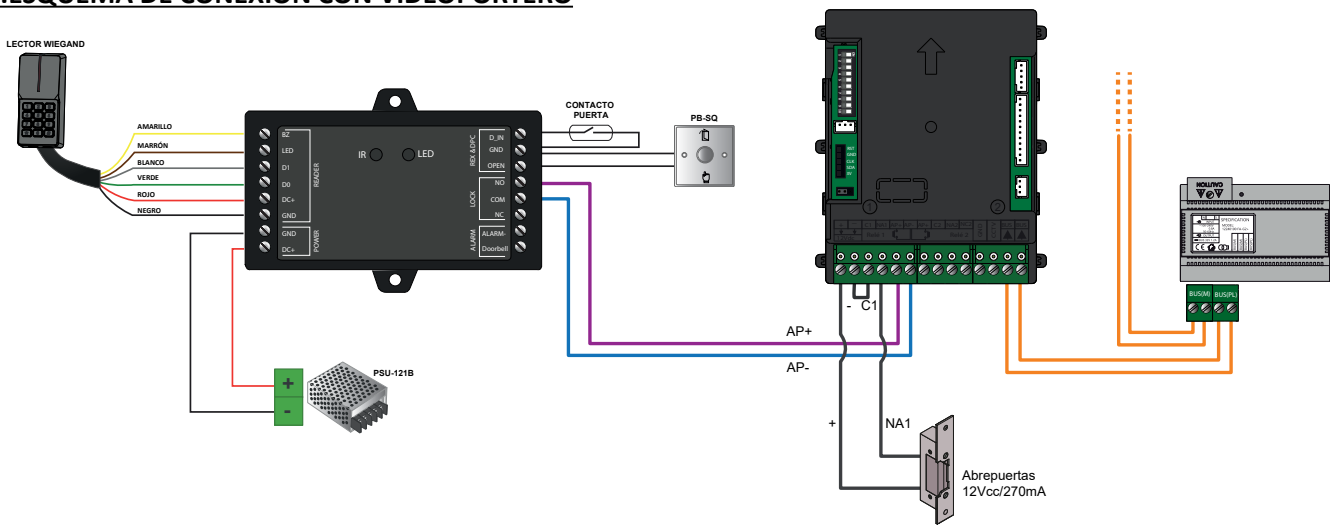
IMPORTANTE: No olvide conectar el diodo suministrado en paralelo al abrepuertas para proteger el equipo.

12.2.ESQUEMA CON ABREPUERTAS CA



IMPORTANTE: Golmar recomienda utilizar abrepuertas de corriente continua, ya que la conexión de un abrepuertas de corriente alterna puede generar picos de tensión elevados que dañen el dispositivo o provoquen un funcionamiento inadecuado. En caso de hacerlo, proteja el equipo colocando un varistor en la salida del contacto del relé y otro en paralelo al abrepuertas.

12.3.ESQUEMA DE CONEXIÓN CON VIDEOPORTERO



NOTA: El AP (apertura de puerta) del portero no activa el abrepuertas hasta que el pulso de la controladora ha finalizado. Para evitar demoras en la apertura, establezca el pulso mínimo de 1 segundo en la controladora:

Entrar en modo administrador					
*	CÓDIGO MAESTRO	#	3	1	#

13.ANEXO

13.1.DISPOSITIVO COMPARTIDO NO SE MUESTRA

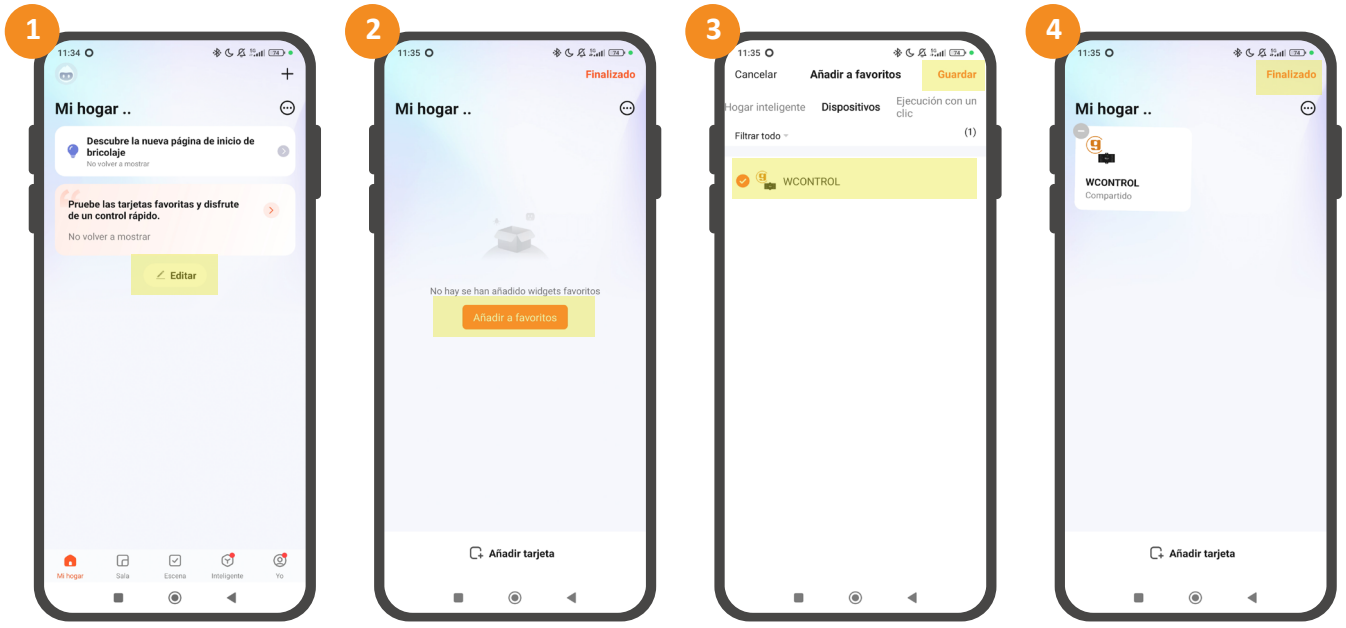
En algunos casos al compartir el administrador el dispositivo con otro usuario la aplicación podría no mostrar directamente el dispositivo en la pagina principal (home) del usuario invitado. De experimentar esa situación el invitado deberá proceder como se muestra a continuación:

1 - Pulse la opción “Editar” ubicada en la página “Mi hogar”.

2 - Pulse la opción “Añadir a favoritos” a continuación.

3 - Seleccione la controladora “WCONTROL” y seguidamente pulse en “Guardar”.

4 - Complete el proceso pulsando sobre la opción “Finalizado”.



13.2.CONECTIVIDAD CON LA CONTROLADORA

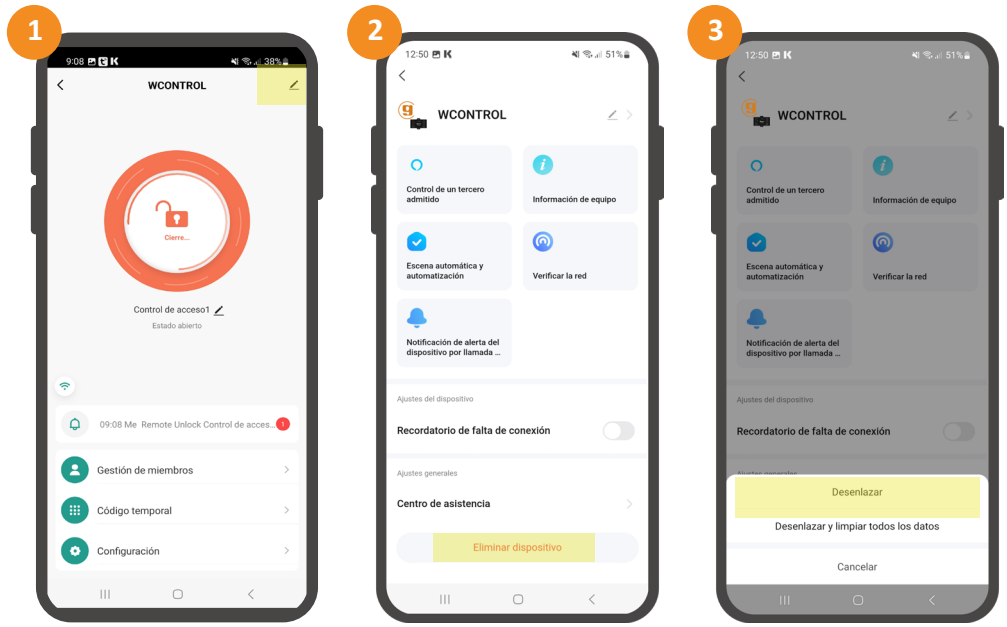
A continuación se indica como proceder en caso de experimentar diferentes casuísticas de conectividad:

1) Dificultades para vincular la controladora, pruebe a realizar la siguiente secuencia:

* código maestro # 9 código maestro #

Esta reiniciará la conectividad de la controladora. Recuerde que la red WiFi a la que conectar la controladora deberá ser frecuencia 2.4GHz.

2) Problemas del administrador para realizar la gestión en la APP, pulse en el icono del “lápiz” en la pantalla principal del dispositivo y a continuación sobre la opción “Desenlazar”.



Esto desvinculará al administrador del dispositivo (no elimina la información).

IMPORTANTE: De presionar sobre la opción “Desenlazar y limpiar todos los datos” la controladora se desvinculará y toda la información se perderá. Utilice esta otra opción únicamente de requerir dejar a cero todo lo realizado en la APP.

Sistemas de comunicación S.A.

C/ Silici 13. Poligon Industrial Famadas
08940 – Cornellà del llobregat – Spain
golmar@golmar.es
Telf: 93 480 06 96
www.golmar.es