



IXON
DIGITAL

MANUAL DE USUARIO TECLADO RFID AUTÓNOMO



REF.: TK2 (93001)

¿Quieres descargar el Manual?

Captúralo con tu móvil



Contenido

INFORMACIÓN DE SEGURIDAD	3
GARANTÍA	3
INTRODUCCIÓN	4
INSTALACIÓN.....	5
Diagrama de conexiones.....	5
Indicadores leds y sonidos.....	5
CONFIGURACIÓN RÁPIDA.....	6
Conexión con un alimentador de corriente continua:	6
Programación rápida habitual:	6
CONFIGURACIÓN BÁSICA:	7
Asignación de un código MASTER o de programación.....	7
Ajuste del modo de funcionamiento.....	7
MODO STANDALONE	8
CONEXIÓN BASICA CON FUENTE DE CONTINUA (12..28V DC).....	8
CONEXIÓN AVANZADA CON FUENTE DE CONTINUA (12..28V DC).....	8
CONEXIÓN BASICA CON TRANSFORMADOR DE ALTERNA (12..28V AC)	9
CONEXIÓN AVANZADA CON TRANSFORMADOR DE ALTERNA (12..28V AC).....	9
Altas/Bajas de usuarios:.....	10
Configuración del tiempo del relé:	12
Configuración de acceso combinado:.....	12
Alarma y bloqueo del dispositivo:	12
Detección de puerta abierta:.....	13
Alarma por sabotaje:	13
Configuración de las señales luminosas y audibles:.....	13
Utilización de la TARJETA MASTER para añadir y borrar usuarios	14
RESET (defecto de fábrica).....	14
MODO CONTROLLER	15
Programación	15
MODO WIEGAND.....	16
FUNCIONES AVANZADAS	17
Transferencia de información de los usuarios (clonación):.....	17
Función Interlock:	18

INFORMACIÓN DE SEGURIDAD

Le agradecemos la compra de este equipo. Le sugerimos encarecidamente que lea el manual de Instrucciones que se encuentra en la web y preste atención a esta información antes de manejar la unidad.

AVISO: Por favor, tenga en cuenta las siguientes precauciones de seguridad antes de utilizarlo.

Para reducir el riesgo de fuego o choque eléctrico, no exponga este equipo a la humedad.

Para reducir el riesgo de fuego, choque eléctrico no abra la cubierta cuando se encuentre en funcionamiento.

SOBRECARGA: No sobrecargue el enchufe, el cable de alimentación o el adaptador, ya que podría ocasionar fuego o descarga eléctrica.

LIMPIEZA: Desconecte el equipo de la alimentación antes de limpiarlo. No use disolventes.

VENTILACIÓN: Las ranuras del equipo han de estar siempre descubiertas para su ventilación.

CONEXIÓN: Desenchufe el cable de alimentación antes de conectar o desconectar el equipo.

EMPLAZAMIENTO: Evite que la unidad se encuentre expuesta a:

- El calor directo del sol, estufas y calefactores, hornos, etc.
- Alta temperatura (sobre los 35°C) o humedad superior al 90%.
- Excesivo polvo.
- Fuerte magnetismo o efecto electro estático.
- Vibración, impacto o cualquier superficie inclinada.



Esta marca indica que el equipo no debe ser retirado en el cubo de basura doméstico. Para evitar cualquier accidente en la recogida de basuras domésticas, elimine el producto a través del reciclaje de equipos electrónicos de su localidad.



Este producto ha sido fabricado acorde a la regulación del mercado de La Union Europea.

GARANTÍA

SATELITE ROVER S.A. ofrece garantía de tres años desde la fecha de compra y según los términos de la regulación de garantías de la UE. En el caso de países que no son miembros de la UE, se aplica la garantía legal que está en vigor en el momento de la venta. Se debe conservar la factura de compra para determinar la fecha en caso de reclamación.

Durante el periodo de garantía, la empresa SATELITE ROVER S.A. se encargará de los fallos producidos por defecto del material o defectos en fabricación, reparando el producto o sustituyéndolo.

No están incluidos en la garantía el uso inadecuado del producto, manipulación por terceros u otros accidentes que sean ajenos a SATELITE ROVER S.A.

INTRODUCCIÓN

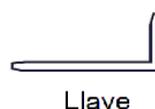
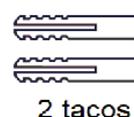
Sistema de control de accesos compacto que integra teclado y lector RFID EM125KHz. Puede ser utilizado en multitud de situaciones tanto como lector RFID o teclado formando parte de un sistema de control de accesos en red o como controlador que gestiona a otros lectores compatibles con Wiegand.

Fácil de instalar, montaje en superficie, carcasa metálica plateado, antivandálico IK07, estanco IP66, alimentación AC o DC (9..28V), salida con relé de hasta 2A libre de tensión, antitamper, alarma de puerta abierta.

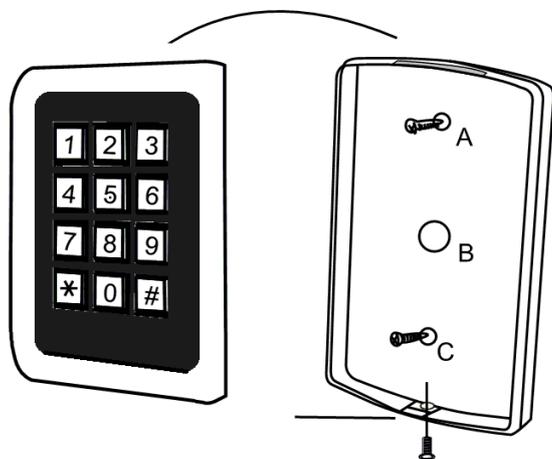
Características y especificaciones:

- Compatible con tarjetas RFID EM125KHz
- Uso en exteriores (estanco, antivandálico)
- Alimentación 12~24V (AC o DC)
- Un relé programable NO/COM/NC:
 - modo pulso 1-99 segundos
 - conmutador ON/OFF
- Modos de acceso combinados:
 - clave (4 a 6 dígitos) o RFID
 - clave (4 a 6 dígitos) + RFID
 - solo RFID (tarjetas, llaveros, etc.)
- 1000 usuarios
- Permite bajas sin disponer de la tarjeta.
- Entrada para contacto magnético de puerta.
- Entrada para pulsador de salida
- Sensor para detección de sabotaje.
- Salida de alarma
- 3 Leds de estado (rojo, amarillo, verde)

Capacidad	1000 tarjetas/PIN
Voltaje de operación	9-28V (AC o DC)
Corriente en reposo	50 mA
Corriente máxima	80 mA
Conexiones	Alimentación dual AC/DC Relé (NO, COM, NC) Entrada para botón EXIT Salida de Alarma Entrada contacto puerta Wiegand IN/OUT
Teclado	12 teclas: 0-9, #, *
Pin	4 a 6 dígitos
Lector de Proximidad	EM 125 KHz
Rango	2-6 cm
Relé	NO, COM, NC
Max. amperaje	2 A
Tiempo ajustable	0-99 segundos
Interface Wiegand	In/Out (26-44 bits)
Pin output Wiegand	4 , 8 bits, 10 digits virtual
Temperatura operación	-40°C ... 60°C
Humedad de operación	0%RH ... 98%RH
Acabado	Aleación de zinc
Dimensiones	112x71x21 mm. (LxAxP)
Peso	450g



INSTALACIÓN



- Desmonte la cubierta trasera
- Haga 2 agujeros (A, C) en la pared para los tacos y otro (B) para pasar el cable
- Pase el cable por el agujero de la pared y fije la cubierta sobre la pared con los 2 tornillos.
- Cierre el lector sobre su cubierta mediante el tornillo situado en el lado inferior.

Diagrama de conexiones

COLOR		FUNCION	DESCRIPCIÓN
FUNCIONES BÁSICAS			
Rojo		AC/DC	Alimentación 12-24V (AC/DC)
Negro		AC/DC	Alimentación 12-24 V (AC/DC)
Azul/Negro		NO	Salida relé (normalmente abierto)
Blanco/Negro		COM	Salida relé (común)
Verde/Negro		NC	Salida relé (normalmente cerrado)
Amarillo		OPEN	Entrada para pulsador SALIR (unir a GND)
BUS WIEGAND. Funciones de LECTOR ó CONTROLADOR			
Verde		Data 0	Salida Wiegand Data 0
Blanco		Data 1	Salida Wiegand Data 1
FUNCIONES AVANZADAS			
Gris		Alarm Output	Contacto negativo para alarma
Marrón		Contact Input	Entrada contacto puerta (normalmente cerrado)
Gris/Negro		GND	Masa para contacto puerta

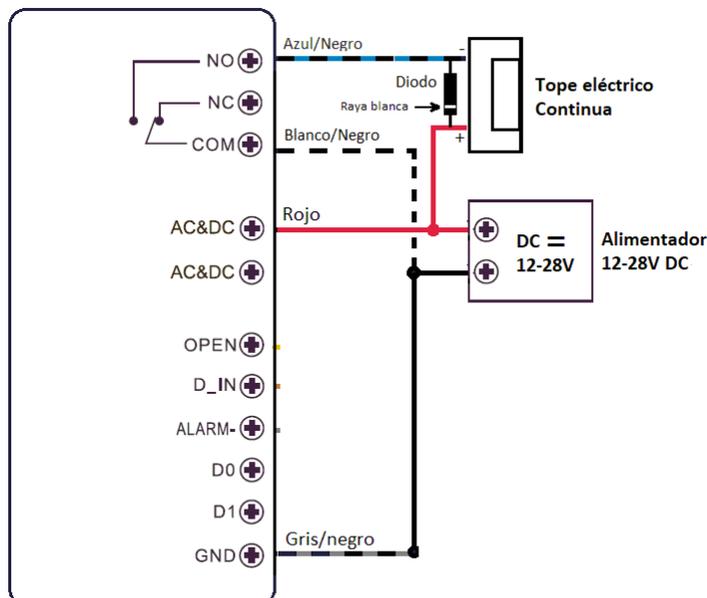
Indicadores leds y sonidos

ESTADO	LED		SONIDO
Reposo		Continuo	
Modo programación		Continuo	Un beep
Error de programación		-	Tres beeps
Puerta Abierta		COM	Un beep
Alarma		Intermitente	Beeps seguidos

CONFIGURACIÓN RÁPIDA

Conexión con un alimentador de corriente continua:

Para conectar con un transformador de alterna consulte los apartados posteriores.



Programación rápida habitual:

Los siguientes pasos asignarán una contraseña de acceso a su dispositivo. Para programaciones más avanzadas consulte los apartados posteriores de este manual.

ALTA DE CONTRASEÑA

1. Entrar en modo programación	* (CODIGO MAESTRO) # (123456 es el CÓDIGO MAESTRO de fábrica)
2. Añadir contraseñas	1 900 # (PIN) # PIN de 4 a 6 dígitos, excepto el 8888. Nota: ID asignado: 900
3. Salir modo programación	*

Ejemplo: Realice estas pulsaciones para asignar la contraseña: 5555
*123456 # 1 900 # 5555 *

APERTURA DE LA PUERTA

ABRIR PUERTA	(PIN) #
--------------	----------------

CAMBIO DE CONTRASEÑA DE USUARIO

Con esta función el usuario puede modificar su contraseña sin acceder al MODO PROGRAMACION

CAMBIAR CONTRASEÑA	* 900 # (pin antiguo) # (nuevo pin) # (nuevo pin) # ID es 990-999; PIN de 4 a 6 dígitos, excepto el 8888.
--------------------	---

Ejemplo: Realice estas pulsaciones para cambiar la contraseña a 6666
*900 # 5555 # 6666 # 6666 #

CONFIGURACIÓN BÁSICA:

Asignación de un código MASTER o de programación

Cualquier ajuste comienza por acceder al lector en modo programación con un código maestro. El código maestro de fábrica es 123456. Recomendamos que se modifique para evitar manipulaciones indebidas en el dispositivo

ENTRAR Y SALIR DEL MODO PROGRAMACIÓN

Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
Salir modo programación	*

MODIFICAR CÓDIGO MAESTRO

1. Entrar en modo programación	* (CODIGO MAESTRO) #
2. Cambiar el CÓDIGO MAESTRO	0 (Nuevo código) # (Repetir Nuevo código) # <i>El código es de 6 dígitos (000000 a 999999)</i>
3. Salir modo programación	*

Ajuste del modo de funcionamiento

El dispositivo tiene 3 modos de funcionamiento: Standalone. Controller y Wiegand Reader.

- **Standalone** (Modo por Defecto): Utiliza el lector RFID incorporado, el controlador para 1000 usuarios y el rele de activación de las puertas. Es el modo habitual en instalaciones pequeñas
- **Controller**: En este modo el dispositivo se conecta a otros lectores (teclados, RFID, biométricos, etc.) por medio del bus de comunicación (wiegand). Los llaveros RFID pueden pasarse por el lector externo y por el controlador.
- **Wiegand**: El dispositivo se usa en un entorno de red. En este modo el dispositivo actúa de lector RFID transfiriendo el identificador de la tarjeta RFID a través del bus Wiegand. El relé no se activa. El cable amarillo y marrón se utilizan para el control del LED y del BUZZER a través de la controladora del entorno de red. Véase esquema de conexiones en la página 13.

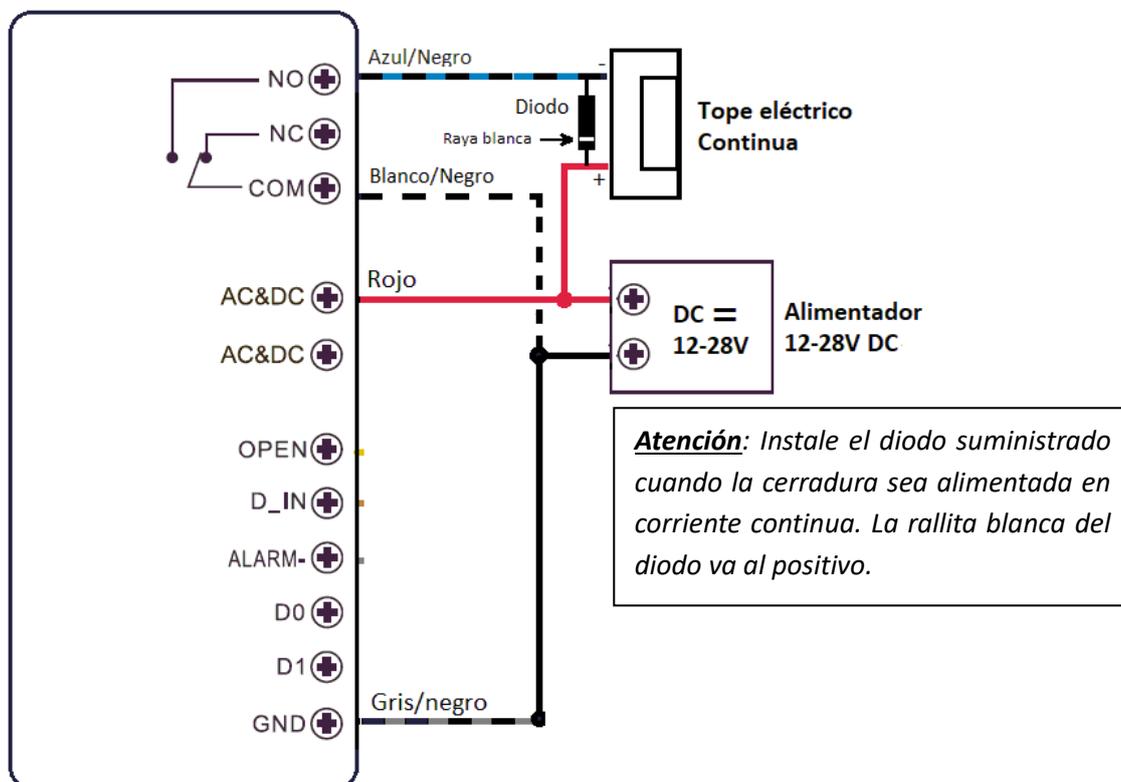
AJUSTE DEL MODO DE FUNCIONAMIENTO

1. Entrar en modo programación	* (CODIGO MAESTRO) #
2. Modo Standalone/Controller	7 7 # <i>Modo por defecto</i>
2. Lector Wiegand	7 8 #
3. Salir modo programación	*

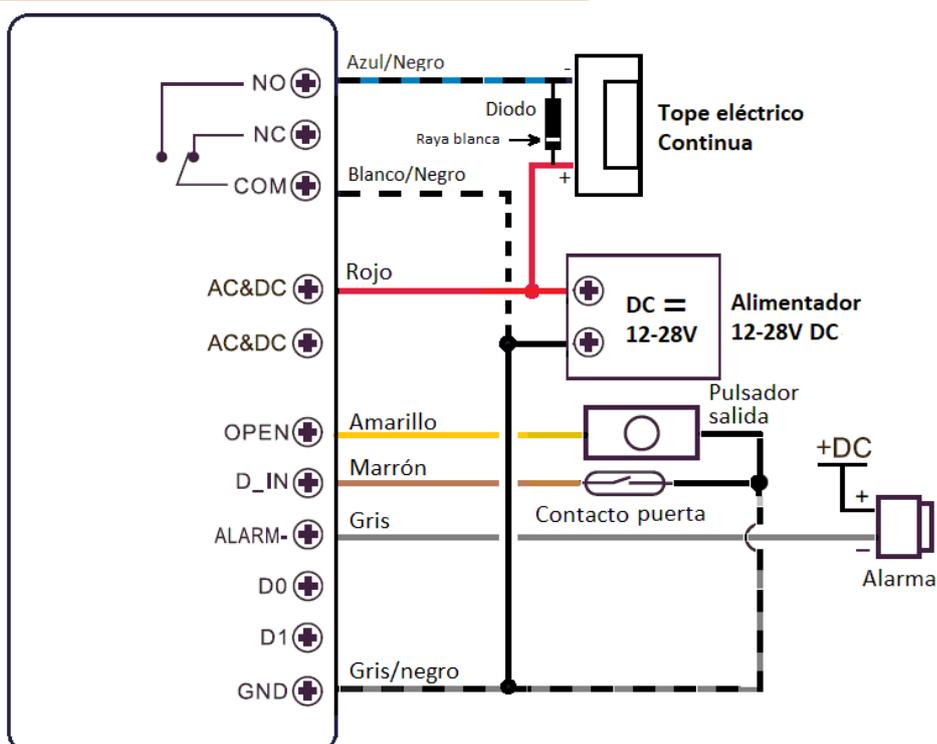
MODO STANDALONE

Standalone (7 7 #): Es el modo común de trabajo. Se usa para el control de una puerta.

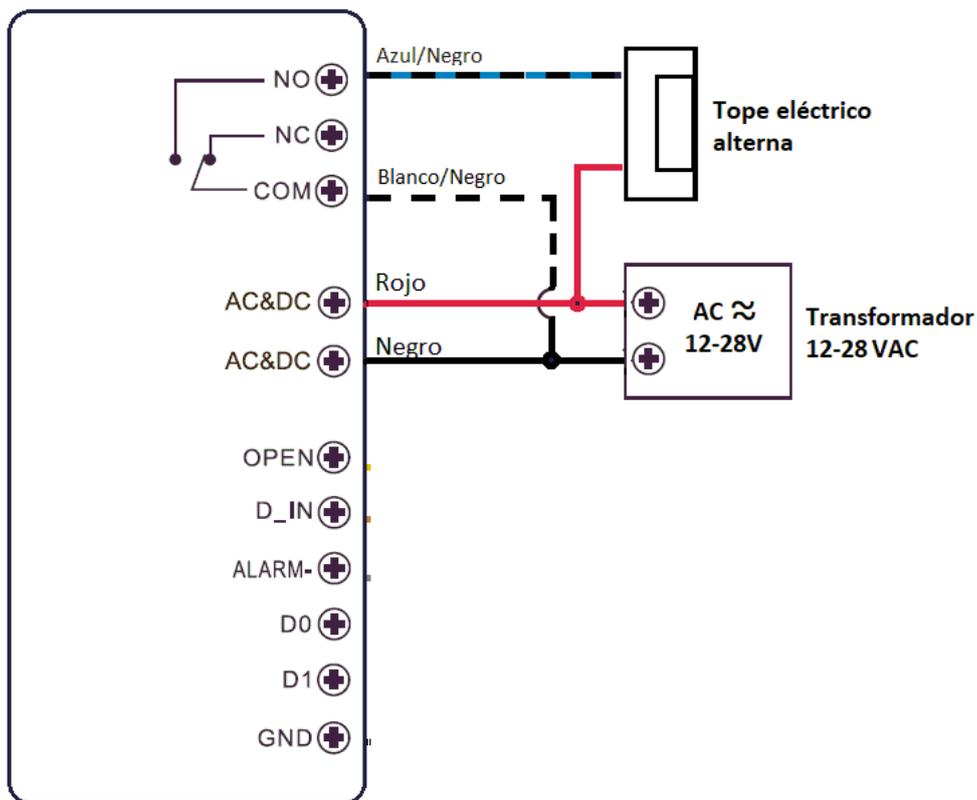
CONEXIÓN BÁSICA CON FUENTE DE CONTINUA (12..28V DC)



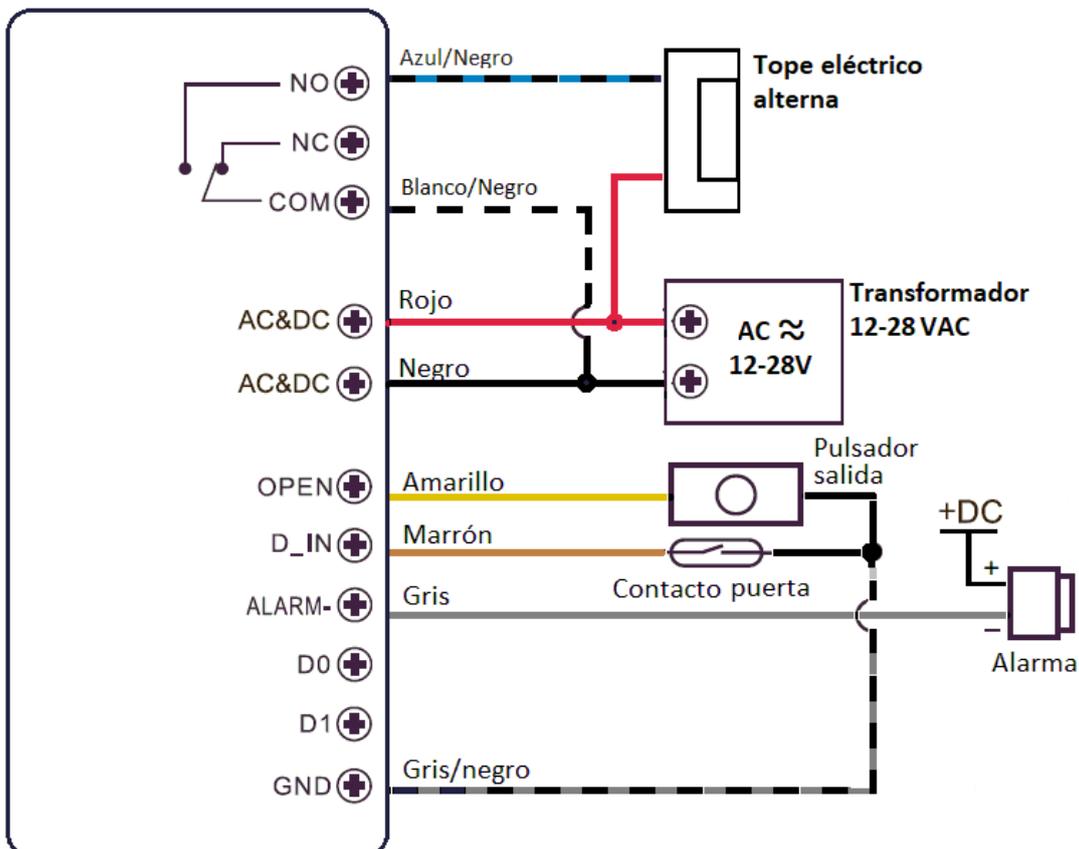
CONEXIÓN AVANZADA CON FUENTE DE CONTINUA (12..28V DC)



CONEXIÓN BÁSICA CON TRANSFORMADOR DE ALTERNA (12..28V AC)



CONEXIÓN AVANZADA CON TRANSFORMADOR DE ALTERNA (12..28V AC)



Altas/Bajas de usuarios:

La programación varía dependiendo del identificador de usuario que se asigne de la siguiente manera:

- Usuarios normales: → ID: 0-987
- Usuario Pánico: → ID 988-989
- Visitantes: → ID: 990-999

ATENCIÓN: Los ID no tienen que ir precedidos de ceros.

NOTAS:

- Llaveros de proximidad: 125 KHz EM
- PIN: de 4 a 6 dígitos, excepto el 8888 que es reservado.

ALTAS DE CONTRASEÑAS DE ACCESO

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Añadir contraseñas ó 2. Añadir Llaveros RFID con ID	1 (PIN) # <i>PIN de 4 a 6 dígitos, excepto el 8888.</i> <i>Puede añadir más contraseñas continuamente. No pueden repetirse</i> 1 (ID) # (PIN) # <i>ID es cualquier número de 0-987</i>
3. Salir modo programación	*

ALTAS DE LLAVEROS

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Añadir Llaveros RFID usando el ID automático ó 2. Añadir Llaveros RFID con ID Manual ó 2. Añadir Llaveros por su numeración. ó 2. Añadir muchos llaveros con ID consecutivo.	1 (acercar llavero) # <i>Puede añadir llaveros continuamente</i> 1 (ID) # (acercar llavero) # <i>ID es cualquier número de 0-986</i> 1 (8/10 dígitos del llavero RFID) # <i>ID es cualquier número de 0-986</i> 1 (ID) # cantidad # (8/10 dígitos del primer llavero) # <i>ID es cualquier número de 0-986</i>
3. Salir modo programación	*

NOTA ADICIONAL DE SEGURIDAD:

Hay un modo de ocultar la contraseña pulsando 10 dígitos de la siguiente manera.

Ejemplo: PIN: 123434

Puede usar: ** 123434 ** ó **1234

("*" puede ser cualquier número del 0-9)

ALTA DE USUARIO DE PÁNICO.

El usuario de pánico abrirá la puerta como cualquier otro usuario y activará la salida de alarma.

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Añadir llavero de pánico ó 2. Añadir contraseña de pánico	1 (ID) # (acercar tarjeta o introduzca 8/10 dígitos del llavero) # <i>ID es 988-989</i> 1 (ID) # (PIN) # <i>ID es 988-989. PIN de 4 a 6 dígitos, excepto el 8888.</i>
3. Salir modo programación	*

ALTAS DE USUARIO VISITANTES

El usuario de VISITANTE abrirá la puerta un número de veces determinado hasta un máximo de 10.

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Añadir Llavero RFID de visitante ó 2. Añadir contraseña de visitante	1 (ID) # (Usos) # (acercar tarjeta o introduzca los 8/10 dígitos) # <i>ID es 990-999; Usos: 0-9 es el número de veces que la tarjeta se puede usar.</i> 1 (ID) # (Usos) # (PIN) # <i>ID es 990-999; Usos: 0-9 es el número de veces que la tarjeta se puede usar. PIN de 4 a 6 dígitos, excepto el 8888.</i>
3. Salir modo programación	*

CAMBIO DE CONTRASEÑA DE USUARIO

Con esta función el usuario puede modificar su contraseña sin acceder al MODO PROGRAMACION

CAMBIAR CONTRASEÑA	* (ID) # (pin antiguo) # (nuevo pin) # (nuevo pin) # <i>ID es 990-999; PIN de 4 a 6 dígitos, excepto el 8888.</i>
EN MODO COMBINADO PIN+RFID	* (acercar llavero) (pin antiguo) # (nuevo pin) # (nuevo pin) # <i>PIN de 4 a 6 dígitos</i> <i>El modo combinado configura el pin 8888 al añadir el llavero RFID..</i>

BORRADO DE USUARIOS

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Borrar contraseña 2. Borrar Llavero 2. Borrar usuario con ID 2. Borrar Llavero por su numeración --- ó --- 2. Borrar TODOS los Llaveros	2 (PIN) # ; Puede borrar contraseñas continuamente 2 (acercar llavero) # ; Puede borrar contraseñas continuamente 2 (ID) # 2 (8/10 dígitos del llavero RFID) # 2 (CODIGO MAESTRO) #
3. Salir modo programación	*

Configuración del tiempo del relé:

El relé puede activarse hasta 99 segundos o programarse en modo NO TEMPORIZADO. El modo NO TEMPORIZADO requiere barrer el llavero una vez para activar el relé y otra vez para desactivarlo. Por ejemplo para un motor-bomba de agua

TIEMPO DEL RELÉ	
1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Modo pulso --- ó ---	3 (1-99) # <i>Por defecto es 5 segundos.</i>
2. Modo NO TEMPORIZADO	3 0 # <i>Modo NO TEMPORIZADO: Pase una vez para abrir y otra vez para cerrar</i>
3. Salir modo programación	*

Configuración de acceso combinado:

Hay 4 modos de acceso:

- **Tarjeta o PIN** (Modo por Defecto): El usuario acerca una tarjeta validada o introduce el PIN con el mando remoto seguido de # para acceder.
- **Solo tarjeta:** El usuario acerca una tarjeta validada para acceder.
- **Tarjeta + PIN:** El usuario debe primero acercar la tarjeta valida y seguidamente su PIN seguido de # para acceder.
- **Multi tarjeta:** Es requerido de 2 hasta 9 tarjetas/pines para autorizar el acceso. El intervalo de tiempo entre una y otra tarjeta no puede exceder de 5 segundos.

ACCESO COMBINADO	
1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Acceso con llaveros/tarjetas --- ó ---	4 0 #
2. Acceso con PIN --- ó ---	4 1 #
2. Acceso con llaveros + PIN --- ó ---	4 2 #
2. Acceso con llaveros ó PIN --- ó ---	4 3 # <i>Modo por defecto de fábrica</i>
2. Acceso MULTI-USUARIO	4 3 (2-9) # <i>Solo después de (2-9) usuarios validados, la puerta se abre.</i>
3. Salir modo programación	*

Alarma y bloqueo del dispositivo:

El dispositivo puede programarse para que frente al barrido repetido de 10 tarjetas/llaveros no autorizados se bloquee durante 10 minutos o se dispare la alarma (buzzer) durante un tiempo determinado.

ALARMA Y BLOQUEO DEL DISPOSITIVO	
1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>

2. Alarma y bloqueo desactivado --- ó ---	6 0 # <i>Modo por defecto de fábrica</i>
2. Bloqueo activado --- ó ---	6 1 #
2. Alarma activado	6 2 # 5 (0-3) # <i>(0-3) Tiempo de la alarma, por defecto es 1 minuto</i> <i>Para silenciar la alarma pase cualquier llavero activado</i>
3. Salir modo programación	*

Detección de puerta abierta:

Si utiliza un contacto magnético en la puerta conectado al dispositivo y la puerta permanece abierta más de 1 minuto sonará el buzzer para recordar que la puerta debe cerrarse. La alarma sonará durante el tiempo establecido o puede desconectarse cerrando la puerta o barriendo un llavero validado.

Alarma por sabotaje:

Si utiliza un contacto magnético en la puerta conectado al dispositivo y la puerta se abre por medios ajenos al controlador (Ejemplo: patada en la puerta), sonará el buzzer y se activará la salida de alarma para avisar del sabotaje. La alarma se desactivará una vez transcurrido el tiempo programado o al barrer una tarjeta autorizada.

La alarma también se dispara si el dispositivo es manipulado indebidamente una vez esté conectado. El dispositivo incorpora una fotocélula en su interior de forma que detecta la manipulación.

ALARMA SABOTAJE

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Desactiva detección puerta abierta --- ó ---	6 3 # <i>Modo por defecto de fábrica</i>
2. Activa detección puerta abierta	6 4 # 5 (0-3) # <i>(0-3) Tiempo de la alarma, por defecto es 1 minuto</i> <i>Para silenciar la alarma pase cualquier llavero activado</i>
3. Salir modo programación	*

Configuración de las señales luminosas y audibles:

Puede conectar o desconectar los leds y señales audibles cada vez que se produzca un acceso autorizado.

CONFIGURACION LEDS Y SEÑALES AUDIBLES

1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO MAESTRO de fábrica)</i>
2. Señales audibles (pitidos) --- ó ---	7 0 # <i>Apagar los pitidos</i> 7 1 # <i>Encender los pitidos (Defecto de fábrica)</i>
2. LEDs --- ó ---	7 2 # <i>Apagar los LEDs</i> 7 3 # <i>Encender los LEDs (Defecto de fábrica)</i>
2. Iluminación TECLADO	7 4 # <i>El teclado siempre apagado</i> 7 5 # <i>El teclado siempre encendido</i> 7 6 # <i>Defecto de fábrica. El teclado se enciende al pulsar cualquier tecla y</i>

	<i>al cabo de 20 segundos se apaga.</i>
3. Salir modo programación	*

Utilización de la TARJETA MASTER para añadir y borrar usuarios

TARJETA MASTER	
Añadir llaveros o contraseñas con tarjeta MASTER	<ol style="list-style-type: none"> 1. Pase la tarjeta MASTER 2. Pase los llaveros o introduzca una contraseña. Repita el paso 2 para añadir continuamente. 3. Pase la tarjeta MASTER de nuevo.
Borrar llaveros o contraseñas con tarjeta MASTER	<ol style="list-style-type: none"> 1. Pase la tarjeta MASTER 2 veces 2. Pase los llaveros o introduzca una contraseña. Repita el paso 2 para añadir continuamente. 3. Pase la tarjeta MASTER de nuevo.

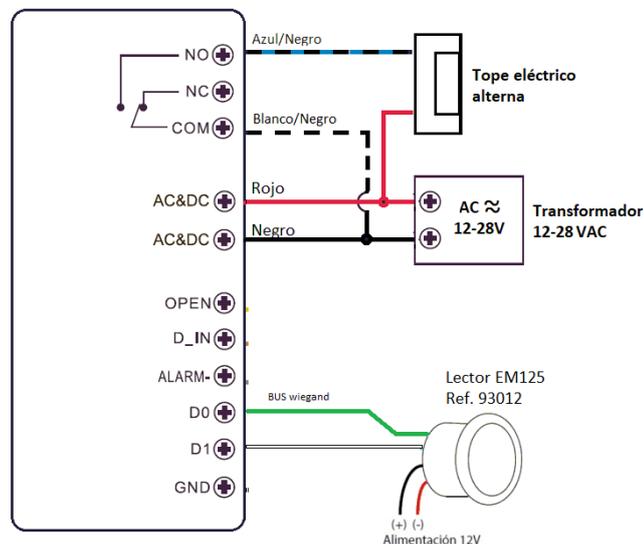
RESET (defecto de fábrica)

El reset vuelve los ajustes al estado de fábrica **sin perder los datos de los usuarios**. En caso de que haya extraviado la tarjeta MASTER puede generar una nueva haciendo un RESET.

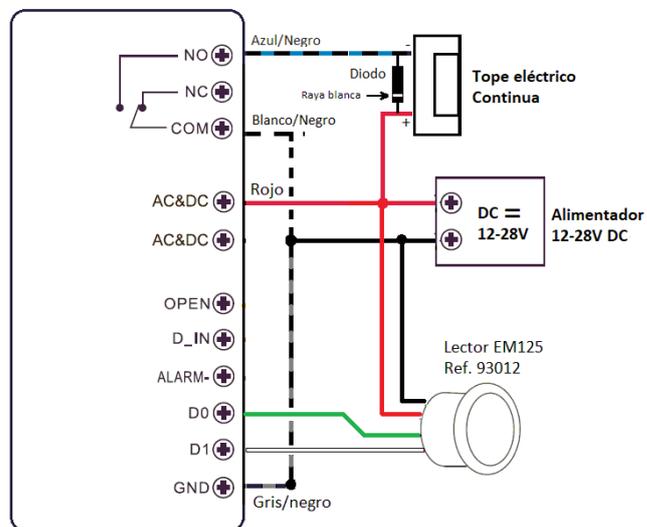
- Desconecte la alimentación del controlador
- Mantenga unido el cable amarillo con el gris-negro (masa) y conecte la alimentación
- Oirá dos “beep” y el LED se iluminará en naranja. Inmediatamente desconecte el cable amarillo.
¡Ojo! Si se ha retrasado 5 segundos oírás un pitido largo y la tarjeta master no quedará configurada.
- Seguidamente acerque una tarjeta EM125KHz para validarla como MASTER y el LED volverá a rojo.

MODO CONTROLLER

El dispositivo puede operar como controlador conectado a otros lectores externos por el bus wiegand (modo 7 7 #). La conexión de ambos dispositivos se realiza de la siguiente forma:



Usando un transformador de alterna



Usando alimentación de corriente continua

¡Atención!

Si está usando una fuente de corriente continua es recomendable instalar el diodo que se suministra en la caja. Preste atención en la polaridad del diodo. El diodo tiene una raya que identifica el terminal que debe conectar al positivo de la cerradura

FORMATO WIEGAND

1. Entrar en modo programación	* (CODIGO MAESTRO) #
2. Formato Wiegand	8 (26-44) # Defecto de fábrica: 26 bits
3. Bit de paridad deshabilitado	8 0 # Para conectar lectores Wiegand con salida de 32, 40 bits, el bit de paridad debe estar deshabilitado
Bit de paridad habilitado	8 1 # Defecto de fábrica
4. Salir modo programación	*

Programación

La programación es la misma que en el MODO STANDALONE.

Únicamente hay las siguientes excepciones:

Para dispositivos conectados con lectores externos:

Lectores EM: Los llaveros pueden ser barridos en el lector externo o en el controlador

Lectores HID: Los llaveros deben ser barridos en el lector externo.

Lectores biométricos: Primero configure las huellas en el lector biométrico y a continuación opere el controlador como si fuera dar de alta un llavero RFID pero en vez de barrer el llavero ponga el dedo en el visor del lector biométrico el cual enviará un código virtual al controlador.

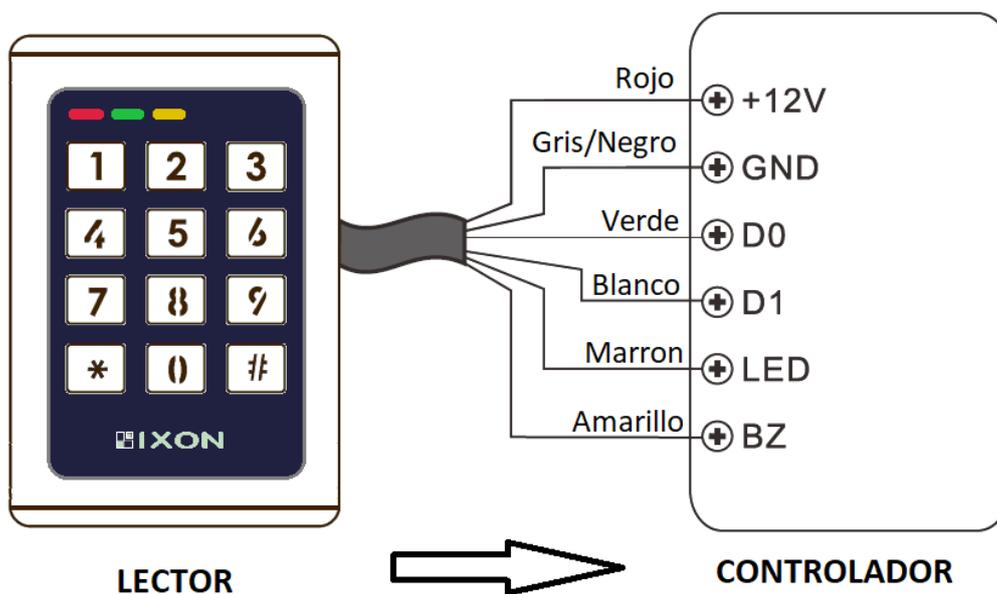
Lectores de teclado: El controlador puede ser configurado para 4 bits, 8 bits (ASCII) o 10 bits. El alta y borrado de los pines de usuario pueden realizarse sobre el teclado o con el mando remoto en el controlador. Configure el formato de bits de la siguiente manera para que se entienda con el lector.

1. Entrar en modo programación	* (CODIGO MAESTRO) #
--------------------------------	-----------------------------

2. Formato Wiegand	8 (4 /8 /10) # <i>Defecto de fábrica: 4 bits</i>
4. Salir modo programación	*

MODO WIEGAND

El dispositivo puede operar como lector Wiegand estándar. (modo 7 8 #). La conexión con la controladora se realiza de la siguiente forma:



Este modo utiliza el dispositivo como un lector Wiegand en un sistema en red de control de accesos. La unidad de relé queda desactivada. El cable marrón se utiliza para el control del LED verde (el LED se activa al poner el cable a masa) y el cable amarillo para el control del buzzer (el buzzer se activa al poner el cable a masa).

El dispositivo puede funcionar con formato 26 bits a 44 bits. Utilice el teclado para programarlo de la siguiente manera:

FORMATO SALIDA WIEGAND	
1. Entrar en modo programación	* (CODIGO MAESTRO) #
2. Longitud Bits Wiegand	8 (26-44) # <i>Defecto de fábrica: 26 bits</i>
Longitud Bits del PIN	8 (4, 8, 10) # <i>Defecto de fábrica: 4 bits</i>
3. Bit de paridad deshabilitado	8 0 # <i>Para conectar controladores Wiegand con salida de 32, 40 bits, el bit de paridad debe estar deshabilitado</i>
Bit de parida habilitado	8 1 # <i>Defecto de fábrica</i>
4. Salir modo programación	*

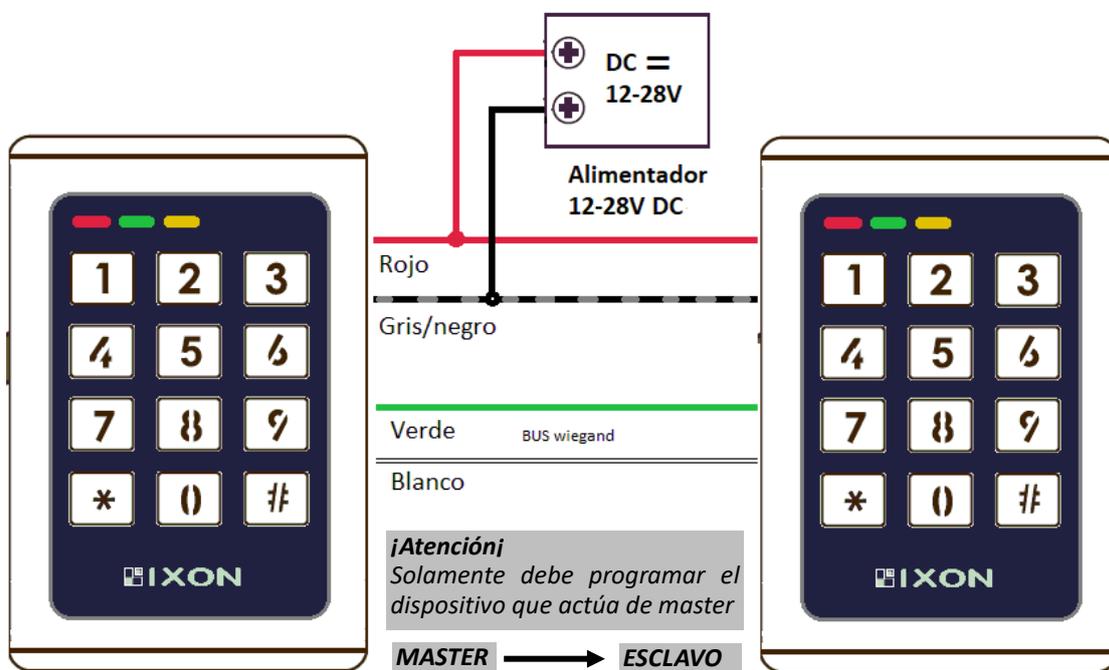
FUNCIONES AVANZADAS

Transferencia de información de los usuarios (clonación):

Este modo permite transferir toda información de los usuarios (ID y tarjetas) desde un dispositivo (llamado MASTER) a otro semejante (llamado ESCLAVO).

Atención:

- El dispositivo MASTER y el ESCLAVO deben ser del mismo modelo
- El código master de programación debe ser el mismo en los dos dispositivos.
- Solamente debe programar en el dispositivo MASTER
- Si el dispositivo ESCLAVO tiene llaveros programados estos serán reemplazados
- Para 1000 usuarios, la transferencia tarda sobre 30 segundos.



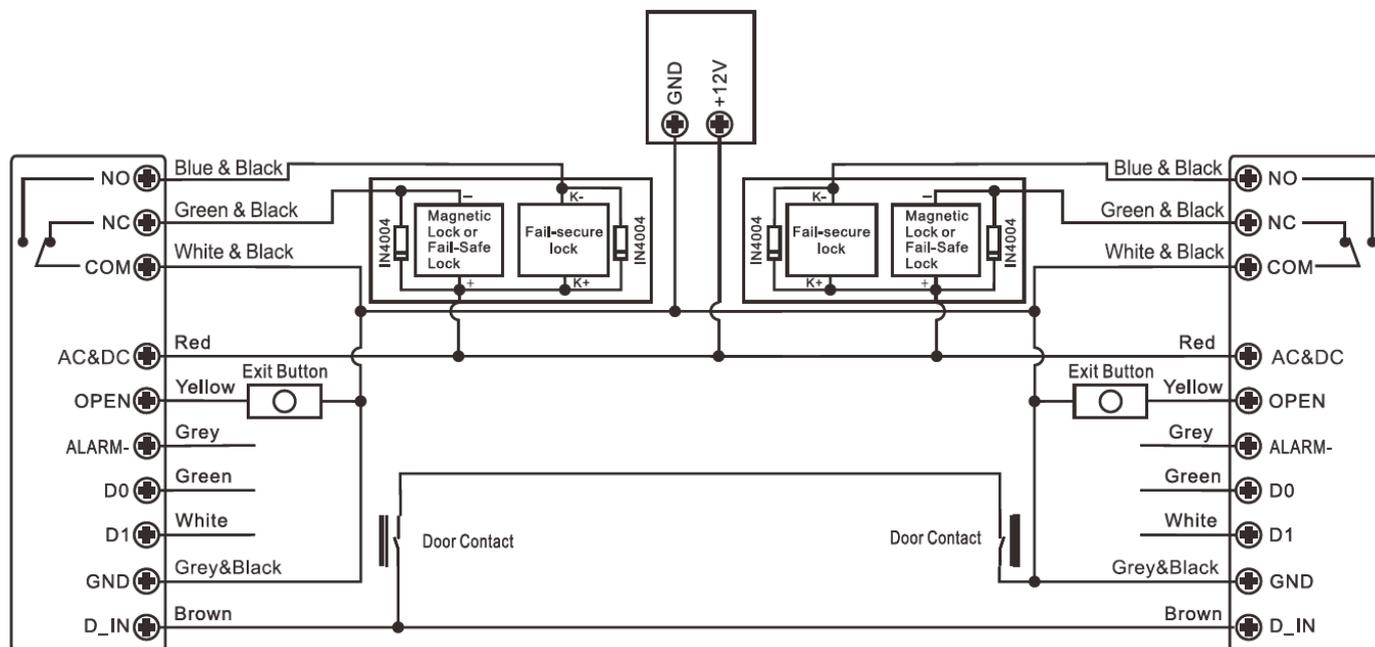
FUNCION TRASPASO DE USUARIOS

1. Entrar en modo programación	* (CODIGO MAESTRO) # (123456 es el CÓDIGO de fábrica)
2. Inicia TRASPASO	9 8 # LED parpadeara en verde en ambos dispositivos. Esperar 3 minutos hasta que el LED vuelva a rojo.
4. Salir modo programación	*

Función Interlock:

Este dispositivo soporta la función interlock para mantener una esclusa entre dos puertas. Esta función se utiliza habitualmente en bancos, prisiones y otras instalaciones que requieren un alto nivel de seguridad.

El esquema de conexiones corresponde al siguiente diagrama.

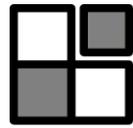


Configuración:

1. Configure las tarjetas/pines de los usuarios en el Lector A.
2. Transfiera la información de los usuarios al Lector B mediante la función clonación
3. Configure en ambos lectores la función Interlock (9 1 #)

FUNCION INTERLOCK	
1. Entrar en modo programación	* (CODIGO MAESTRO) # <i>(123456 es el CÓDIGO de fábrica)</i>
2. Activa la función Interlock	9 0 # Defecto de fábrica
2. Desactiva la función Interlock	9 1 #
3. Salir modo programación	*

Mientras la puerta 2 permanezca abierta el lector A no autorizará la entrada a la puerta 1



I X O N
D I G I T A L