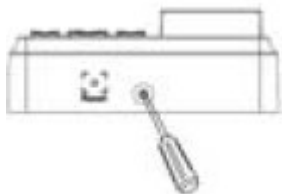


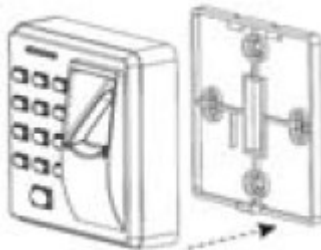
# Manual de usuario F010G

## 1 Instalación del Equipo

### Instalación en Pared



Quite el tornillo de la parte inferior



Quite la cobertura trasera



Fije la cobertura a la pared



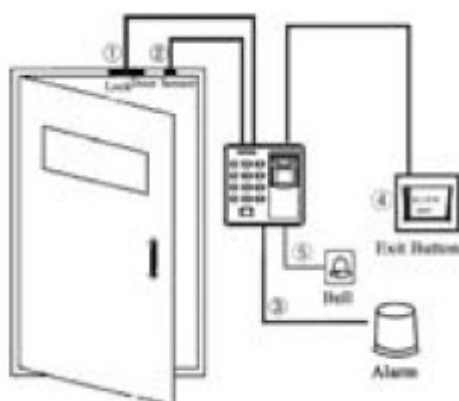
Fije el dispositivo a la cobertura Vuelva a colocar el tornillo en la trasera



parte inferior

## 2 Estructura y Funciones

### Funciones del sistema de control de acceso



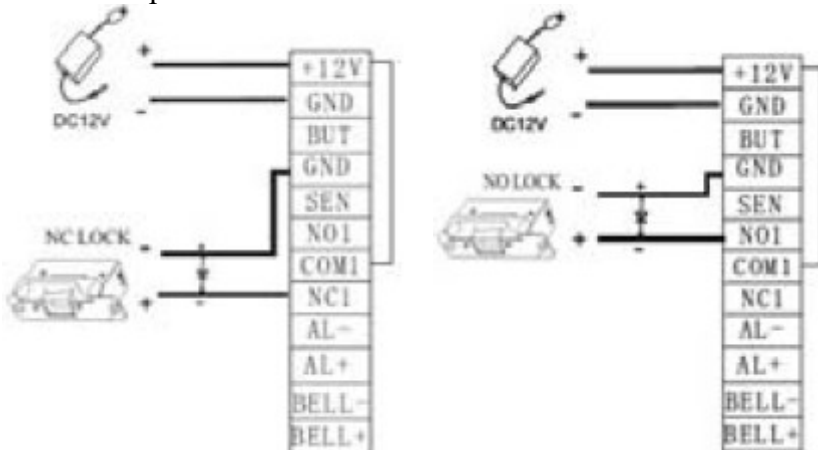
1. Si se verifica un usuario registrado, el dispositivo exportará la señal para desbloquear la puerta.
2. El sensor de puerta detecta el estado on-off. Si la puerta está abierta o no está cerrada correctamente se activará una alarma (valor digital).
3. Si el dispositivo se mueve de su localización emitirá una alarma.
4. Se recomienda el uso de botón de salida para abrir la puerta desde dentro.
5. Soporta timbre externo.

### 3 Conexión de Cerradero

El sistema soporta Bloqueo NA – NC. Por ejemplo NA (normalmente abierto cuando hay corriente) se conecta con el terminal “NO” y el NC se conecta con el terminal “NC”.

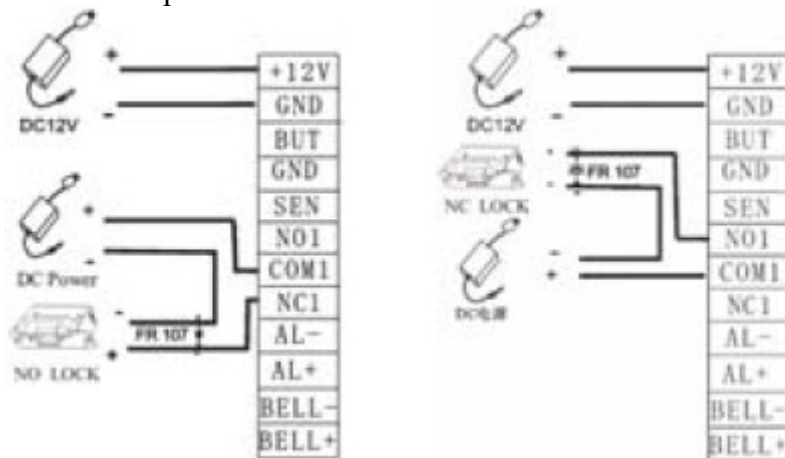
Cuando conecte un cerradero eléctrico al sistema de control de acceso necesitará paralelar un diodo FR107 (adjunto en el paquete) para prevenir que la auto-inductancia EMF afecte al sistema, no invierta las polaridades.

- Comparte la alimentación con el cerradero:



El dispositivo comparte alimentación con la cerradura:  
 ULOCK = 12 V  
 I-ILOCK > 1 A ①  
 Y el dispositivo está cerca del dispositivo.

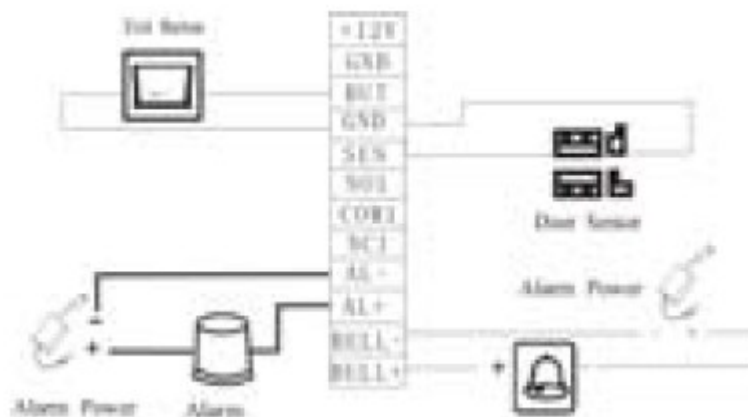
- No comparte la alimentación con el cerradero:



El dispositivo no comparte alimentación con el cerradero:  
 A. ULOCK = 12V I-ILOCK ≤ 1A;  
 B. ULOCK ≠ 12V;  
 C. El cerradero está lejos del dispositivo.

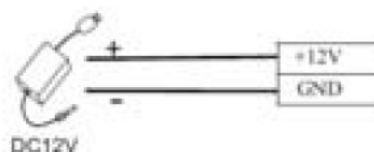
①: “I”: Dispositivo de salida de alimentación, “ULOCK”: Voltaje de cerradero, “ILOCK”: consumo de cerradero.

## 4 Conexión con otras partes



Salida de voltaje  $\leq$  DC 12V para alarma

## 5 Conexión con alimentación



Entrada DC 12V, 500mA (50mA Standby) Positivo está conectado con '+12V', negativo está conectado con "GND" (no invierta la polaridad).

## 6 Instrucciones

Procedimiento recomendado:

Paso 1: Instale el dispositivo y enciéndalo

Paso 2: Después de autenticar la contraseña de Administrador y cambiarla, registre las huellas de usuario, tarjetas o contraseñas.

Paso 3: Configure los parámetros de control de acceso, incluyendo la modificación de contraseñas de ocho dígitos para la apertura de puerta y la configuración de la duración de desbloqueo, modo de autenticación, modo sigilo, modo de sensor de estado de puerta y alarma.

Funciones del dispositivo

### 1. Gestión de Usuario

#### 1. Administrador de Operaciones

1. Autenticador de contraseña de administrador
2. Cambiar contraseña de administrador
3. Abrir puerta a través de contraseña de administrador
4. Contraseña de administrador olvidada

2. Añadir usuarios
  1. Añadir usuario
  2. Registrar tarjetas en lotes
3. Autenticación de usuarios
4. Eliminar usuarios
  1. Eliminar usuario
  2. Eliminar todos los usuarios
2. Gestión de control de acceso
  1. Cambiar la contraseña de ocho dígitos para abrir la puerta
  2. Configurar la duración de desbloqueo
  3. Configurar el modo de autenticación
  4. Configurar el modo oculto
  5. Configurar el modo sensor de puerta
  6. Configurar alarma
    1. Configurar ajustes de alarma
      1. Configurar error de operación – activación de alarma
      2. Configurar alarma tamper
      3. Configurar demora de alarma para el sensor de estado de puerta

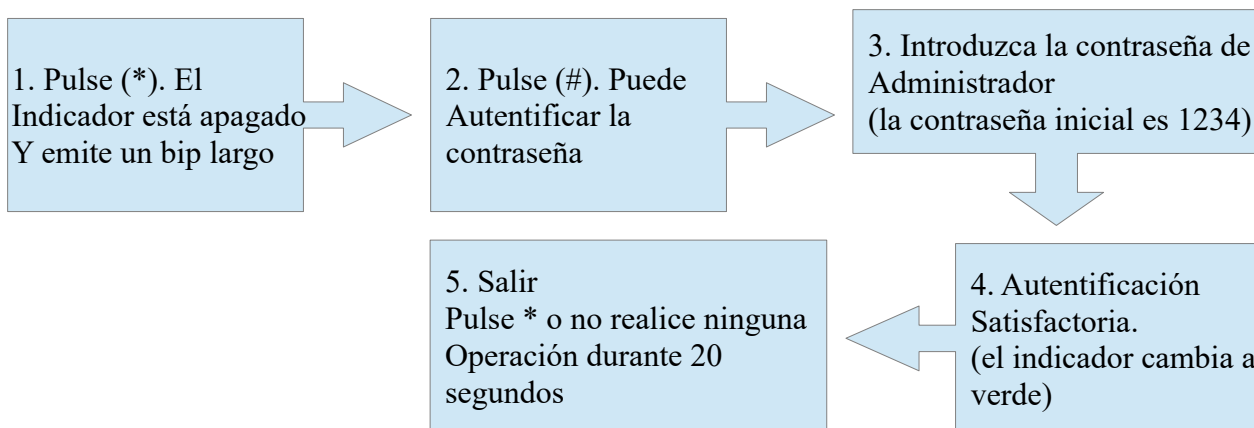
## 7 Instrucciones de Funcionamiento

### 7.1 Gestión de Usuarios

#### 7.1.1 Administrador de Operaciones

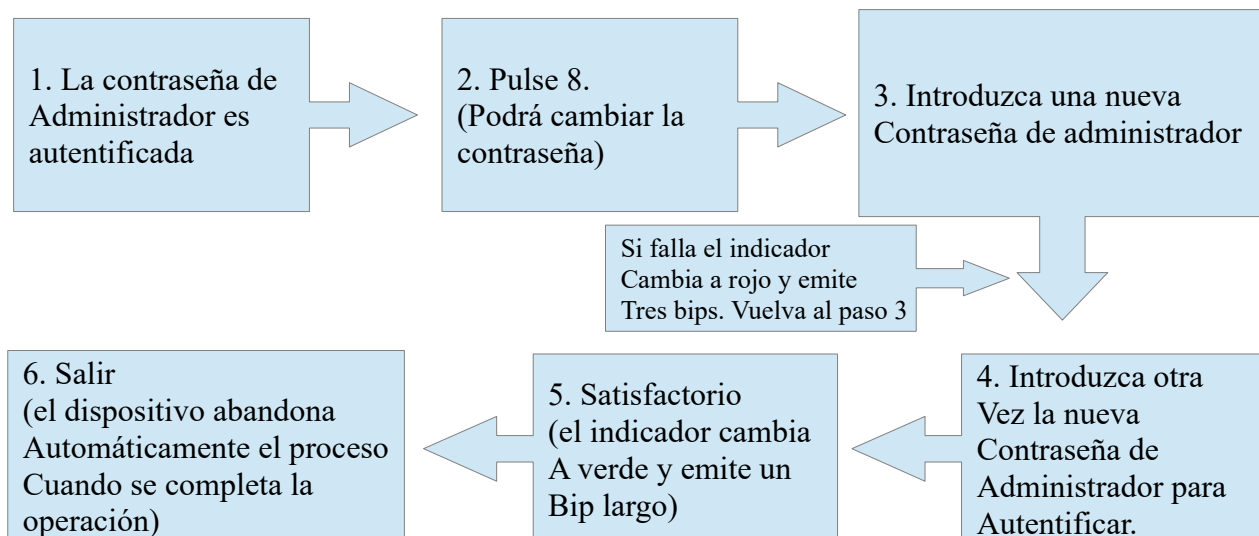
Para asegurar la autenticidad de los datos sólo podrá operar con el dispositivo después de haber autenticado la contraseña de administrador.

##### 7.1.1.1 Autenticador de Contraseña de Administrador



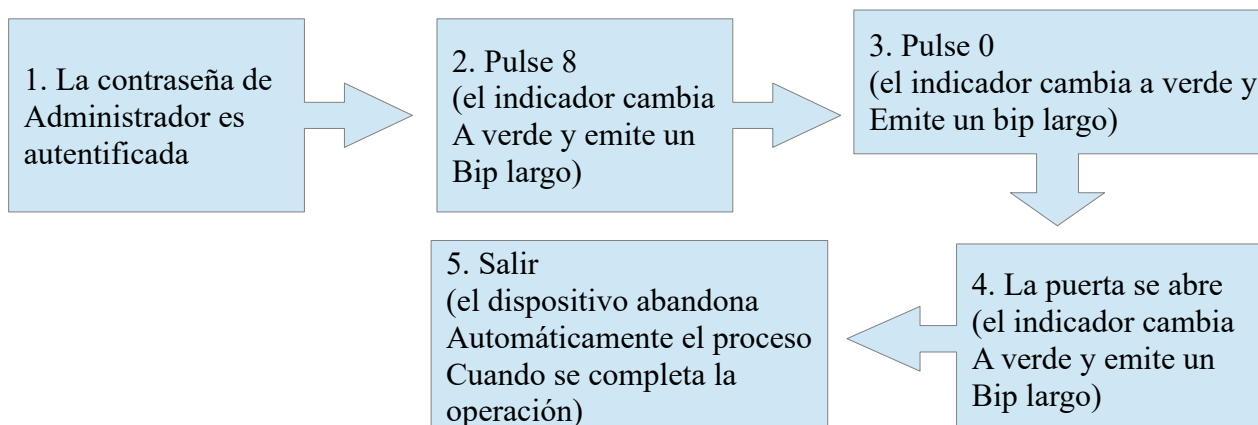
Nota: La contraseña de administrador por defecto es 1234, se le solicitará el cambio de la misma la iniciar el sistema

### 7.1.1.2 Cambiar contraseña de Administrador



Nota: Las contraseñas de 4 dígitos son verificadas automáticamente, para contraseñas con menos dígitos, pulse # para entrar en el proceso de verificación.

### 7.1.1.3 Abrir la Puerta mediante la Contraseña de Administrador



Nota: Esta función puede usarse para abrir la puerta.

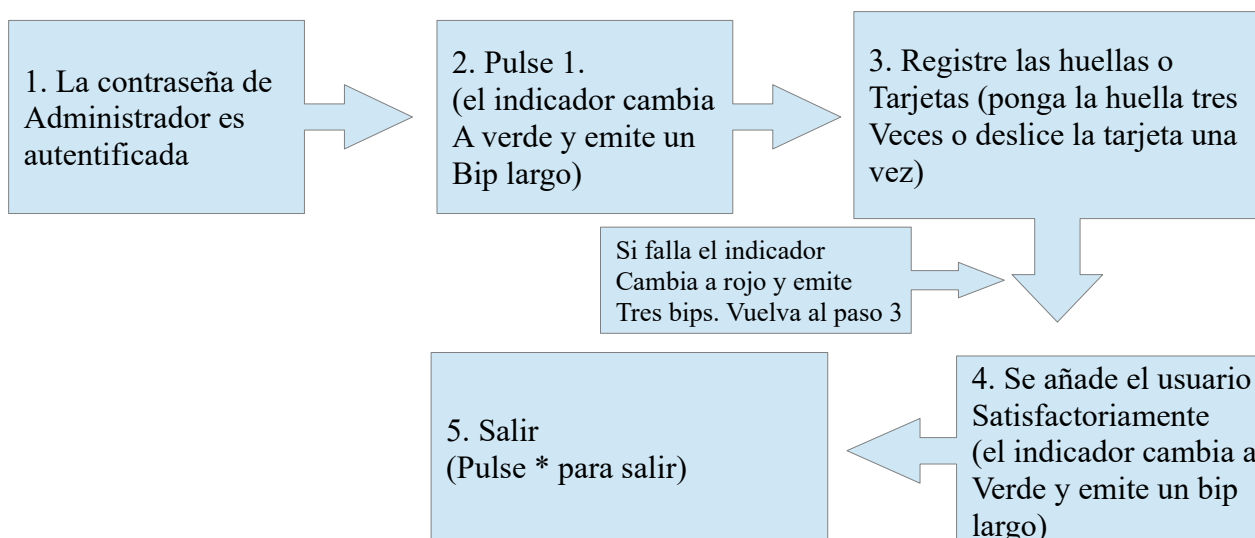
### 7.1.1.4 Olvidó la Contraseña de Administrador

Si olvidó la contraseña de administrador puede pulsar la tecla de desmontaje tres veces para resetear la contraseña y volver a la contraseña inicial de fábrica de 30 a 60 segundos después de haber desmontado el equipo de la pared (emitirá un bip largo 30 segundos después de haber desmontado el equipo de la pared)

## 7.1.2 Añadir Usuarios

Registrar huellas o tarjetas de un usuario o registrar tarjetas en lotes

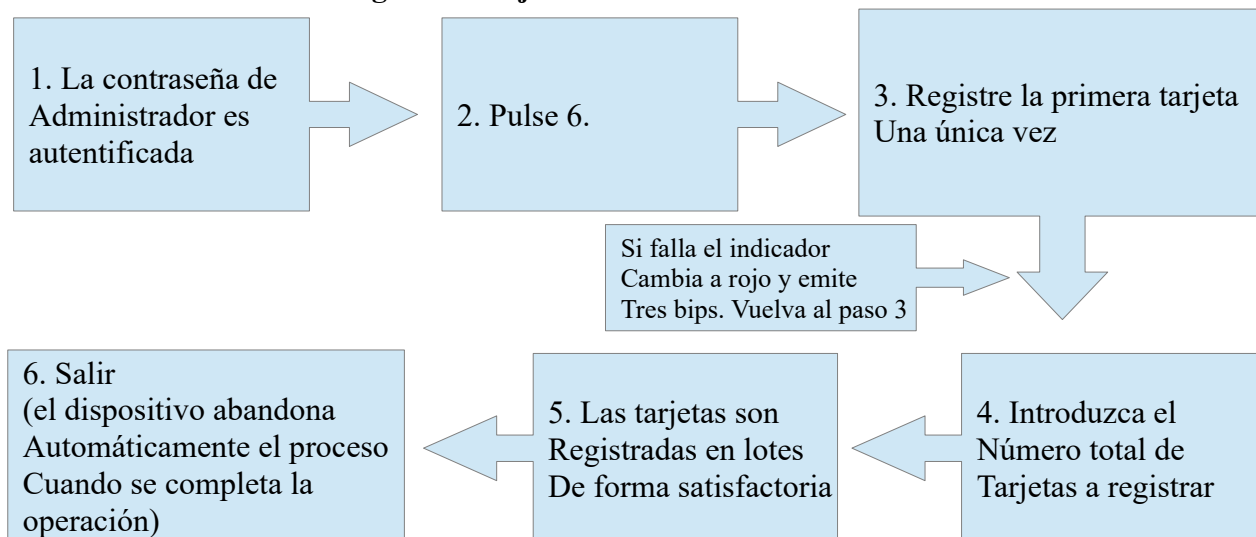
### 7.1.2.1 Añadir Usuario



Nota 1: En el proceso de registro, la ID de usuario se incrementa automáticamente. El dispositivo entra en el proceso de registro del siguiente usuario cuando un usuario ha sido registrado satisfactoriamente.

Nota 2: El proceso de registro falla si la huella es de mala calidad o si la huella o la tarjeta ya están previamente registradas. Después de que el indicador cambie a verde podrá registrar el siguiente usuario. No debe intentar registrar usuarios previamente registrados.

### 7.1.2.2 Registrar Tarjetas en lotes

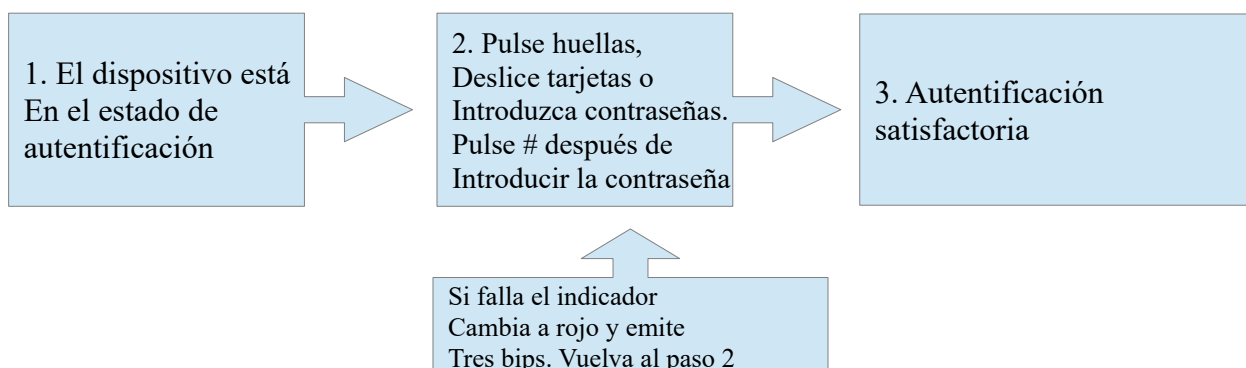


Nota 1: En el proceso de introducir el número total de tarjetas a registrar, se verifican automáticamente números de tres cifras. Para números con menos dígitos pulse # para entrar en el modo verificación. Pulse \* para reintroducir el número total de tarjetas.

Nota 2: Debe eliminar todos los usuarios registrados antes de registrar las tarjetas en lotes. Los números de ID de las tarjetas deben ser consecutivos.

### 7.1.3 Autenticación de Usuarios

Después de que el dispositivo se ha encendido, entra en el estado de autenticación de usuarios para desbloquear la puerta

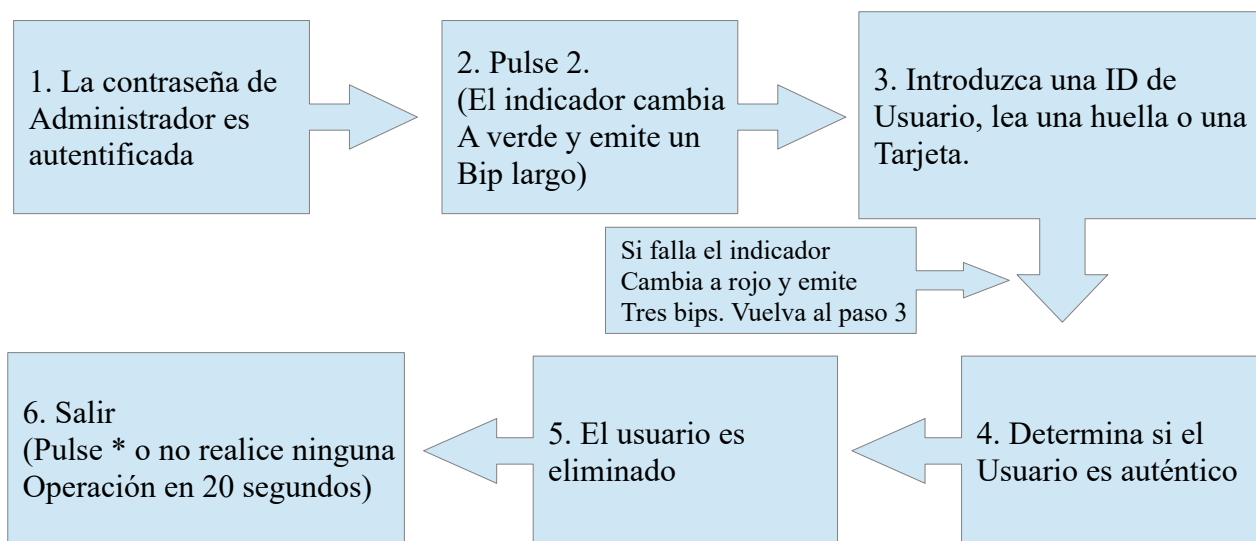


Nota: Pulse # después de introducir una contraseña para autenticarla. La puerta se abre si la contraseña introducida corresponde con la contraseña de apertura por defecto, que es 8888. Compruebe cómo cambiar la contraseña de apertura en el apartado 7.2.1.

### 7.1.4 Eliminar Usuarios

Eliminar un usuario de huella o tarjeta registrado o eliminar todos los usuarios

#### 7.1.4.1 Eliminar Usuario

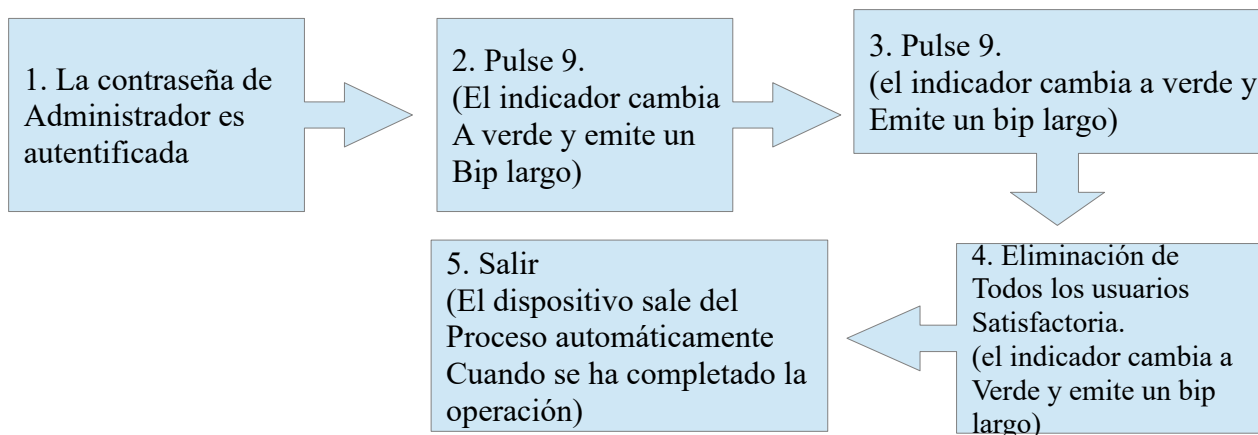


Nota 1: Durante el proceso de introducción de ID los números de 5 dígitos son verificados automáticamente. Para ID con menos dígitos pulse # para entrar en el proceso de verificación.

Nota 2: El dispositivo entra automáticamente en el proceso de eliminación del siguiente usuario cuando elimina un usuario.



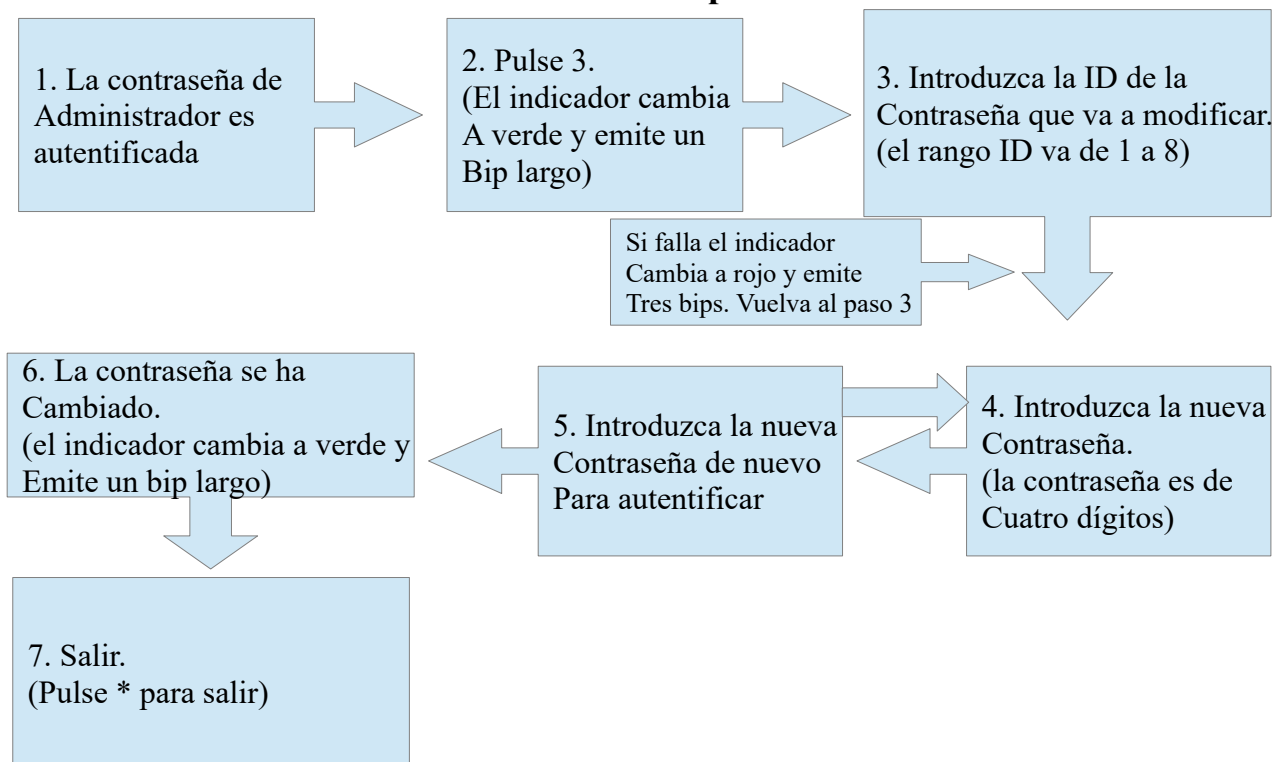
### 7.1.4.2 Eliminar todos los Usuarios



Nota: Pulse 9 para confirmación automática. Otros valores son considerados no válidos. Si se introduce un valor no válido, el indicador del dispositivo cambia a rojo y el dispositivo emite un bip largo y sale del proceso.

## 7.2 Gestión de Control de Acceso

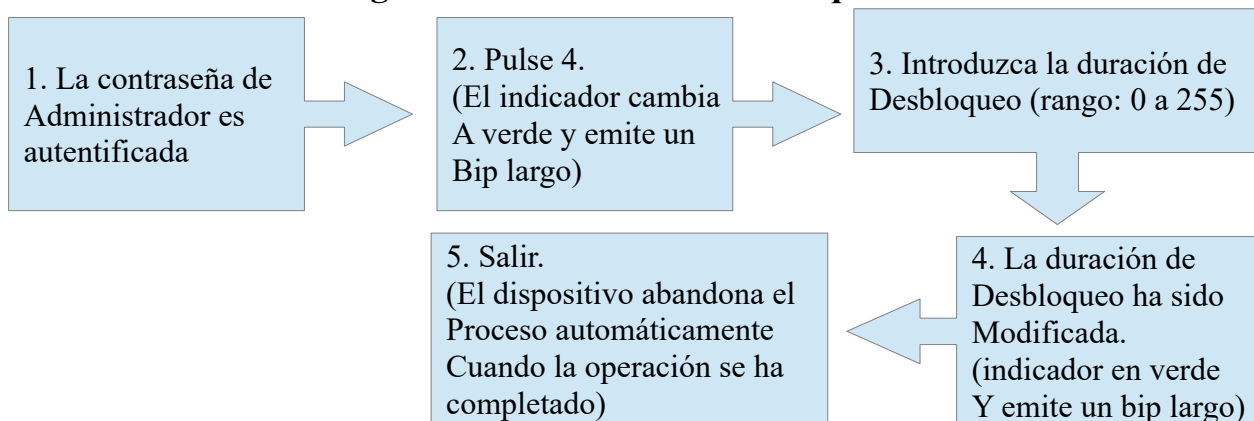
### 7.2.1 Cambiar Contraseña de Apertura



Nota 1: Si configura una contraseña de todo ceros después de introducir la ID, esta contraseña será bloqueada y no podrá usarla para abrir la puerta.

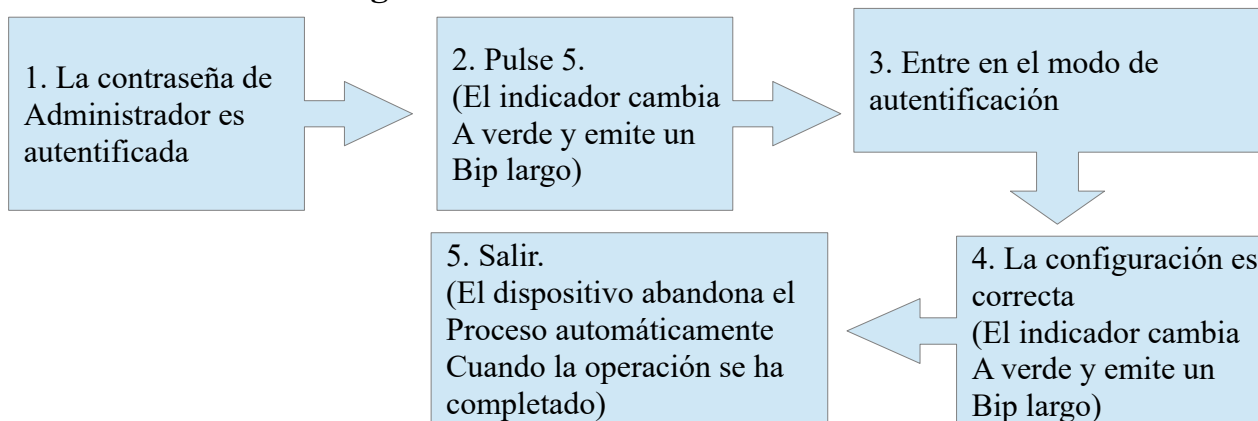
Nota 2: Si una contraseña se cambia satisfactoriamente, introduzca la ID de la contraseña a ser cambiada para cambiar la siguiente contraseña.

### 7.2.2 Configurar la Duración de Desbloqueo



Nota: Los dígitos de 3 dígitos se verifican automáticamente. Para valores con menos dígitos pulse # para entrar en el modo verificación. Los valores superiores a 254 no son válidos.

### 7.2.3 Configurar Modo de Autenticación

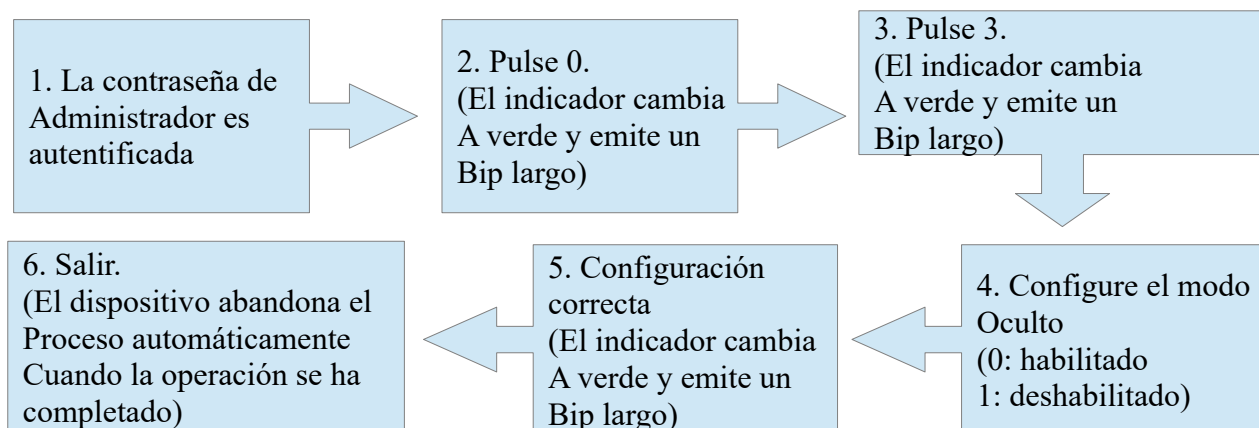


Nota: Los detalles sobre el modo de autenticación son los siguientes:

Modo de autenticación	Tipo	Descripción
Modo 1 (número 1)	PW	Sólo verificación de contraseña
Modo 2 (número 2)	RF	Sólo verificación de tarjetas RF
Modo 3 (número 3)	FP	Sólo verificación por huella
Modo 4 (número 4)	FP/PW/RF	Huella o Contraseña o Tarjeta
Modo 5 (número 5)	RF&PW	Tarjeta y Huella
Modo 6 (número 6)	FP&PW	Huella y Contraseña

### 7.2.4 Configurar Modo Oculto

Si el modo Oculto está habilitado, el indicador estará desconectado cuando se encuentre en modo descanso.

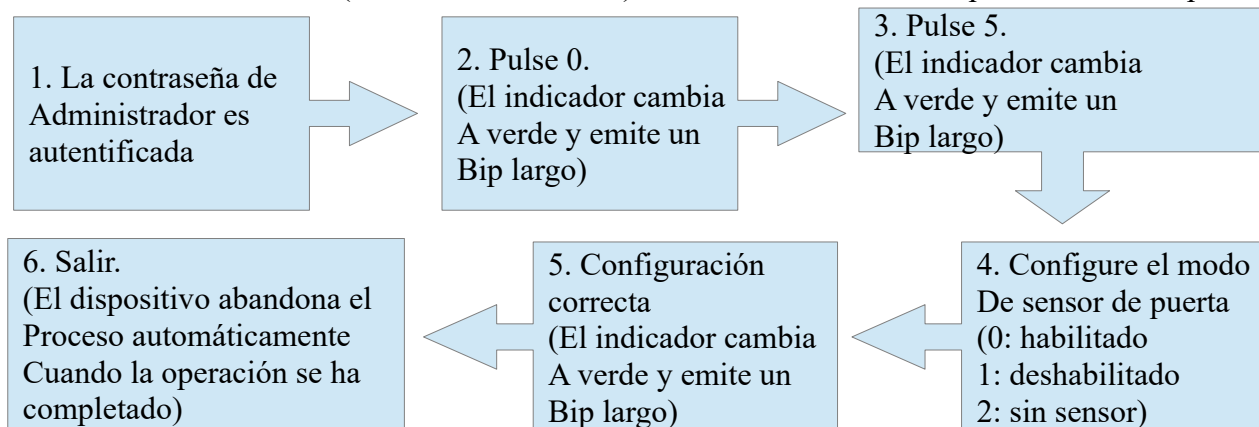


Nota: Un indicador parpadea para indicar el estado de esta función cuando los usuarios están autenticando sus tarjetas o huellas.

## 7.2.5 Configurar Modo Sensor de Puerta

El sensor de puerta incluye tres modos:

- NONE (ninguno): No se usa el sensor de puerta.
- NO (normalmente abierto): el cerradero está abierto mientras la puerta está abierta
- NC (normalmente cerrado): el cerradero se cierra después de cerrar la puerta.



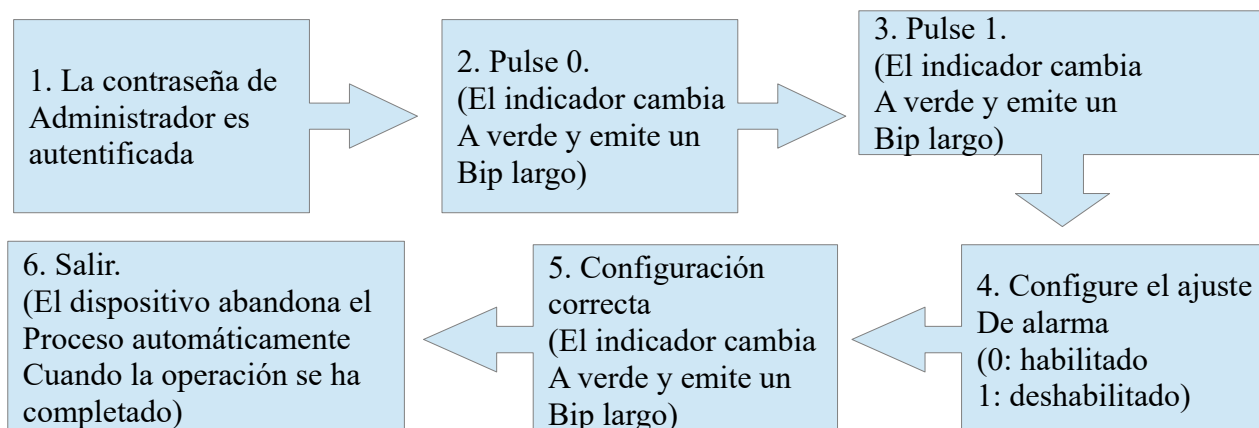
Nota: El modo de sensor de puerta configurado aquí se usa como base para el sensor de alarma de puerta.

## 7.2.6 Configurar Alarma

Nota: Si salta una alarma, el zumbador del dispositivo genera una alarma. 30 segundos después, la alarma se envía a modo de alerta. La alarma puede terminarse después de que el usuario se ha identificado.

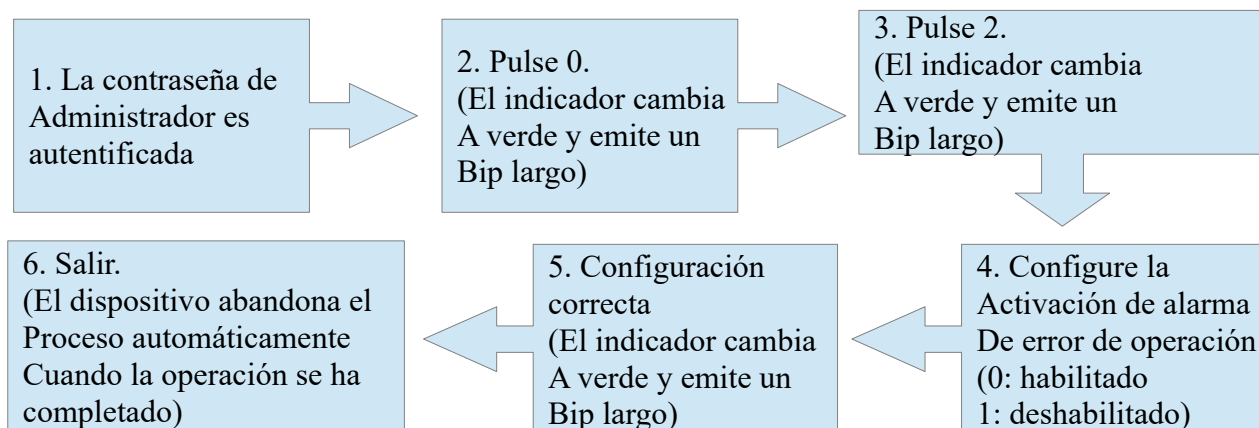
### 7.2.6.1 Ajustes de Alarma

Por defecto debe estar activado, cuando está configurado para estar cerrado, se activará una alarma de Error de Operación, Tamper, Demora de alarma cuando el estado de sensor de puerta esté deshabilitado.



#### 7.2.6.1.1 Error de Operación – Activación de Alarma

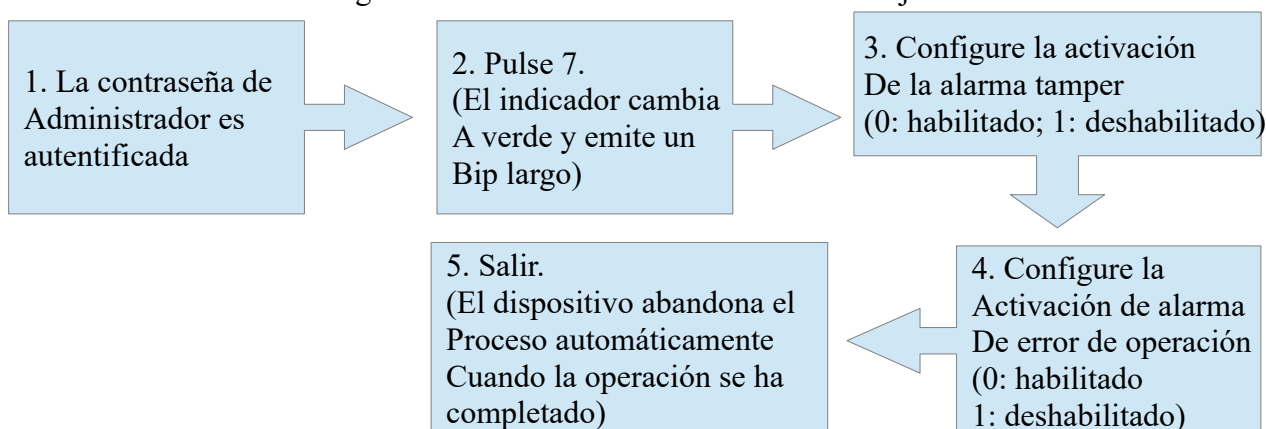
Si esta función está habilitada, las alarmas serán generadas si un usuario falla en el registro después de tres intentos. La autenticación de administrador no estará permitida durante los 20 segundos siguientes después de generarse la alarma.



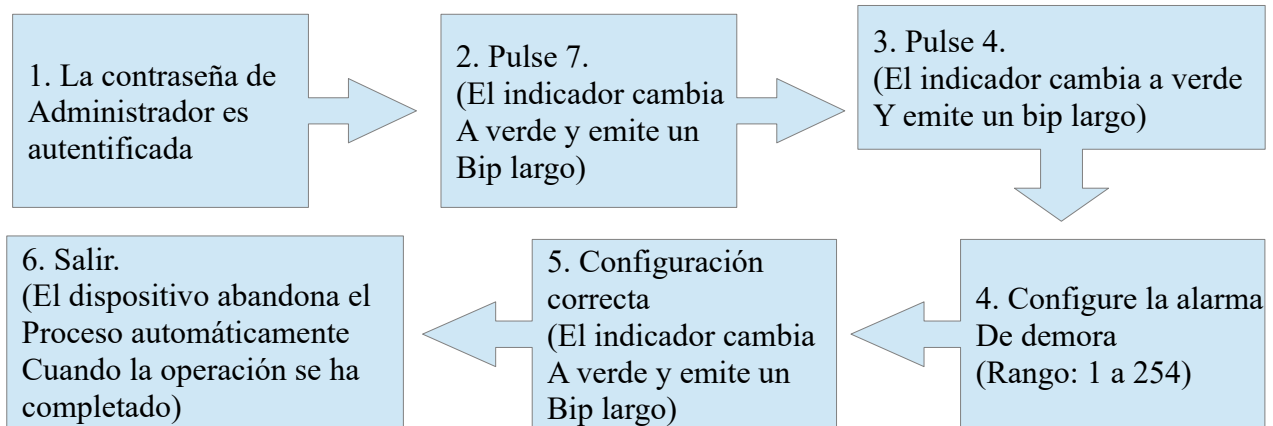
#### 7.2.6.1.2 Configurar Alarma Tamper

Si esta función está habilitada, las alarmas se generarán después de desmontar el equipo.

Configure cómo habilitar la alarma de desmontaje.



7.2.6.1.3 Configurar Demora de Alarma para El Sensor de Estado de Puerta  
Dsen. Delay (Demora de Sensor de Puerta): indica la demora en comprobar la puerta después de que la puerta se ha abierto. Si el estado del sensor de puerta es inconsistente con el estado normal configurado, se generará una alarma, y este periodo de tiempo es denominado como “demora de sensor de puerta”



Nota: Los valores de tres dígitos son verificados automáticamente. Para valores con menos dígitos, pulse # para entrar en el proceso de verificación. Los valores superiores a 254 son considerados no válidos.