Manual de Usuario
MA300-BT

Anotaciones

Este documento contiene consejos, avisos importantes y precauciones . Las notas contenidas en este manual contienen:

- Información importante , incluidas todas las precuaciones, que deben ser leidas cuidadosamente para obtener el óptimo rendiemiento del equipo.

- Indicaciones de voz que el equipo genera. En caso de discrepancia entre las indicaciones de voz en este documento y las generadas por los productos reales, prevalecerá esta última.

CONTENIDO

1. Instrucciones 1
1.1 Posición del dedo 1
1.2 Instrucciones para pasar la tarjeta 2
1.3 Precauciones 2

2. Introducción del equipo 2
2.1 Vista de funciones del equipo 2
2.2 Apariencia del equipo 3
2.3 Uso del teclado externo 4
2.4 Estado de verificación 5
2.5 Tarjeta administradora (M-card) 5
2.6 Password del sistema 6
2.7 Tiempo expirado de operación 6

3. Operaciones del Equipo 6
3.1 Gestión de Tarjetas 6
3.1.1 Registrar tarjeta administradora 6
3.1.2 Registrar un usuario 8
3.1.3 Registrar tarjeta y huella (añadir usuario) 10
3.1.4 Borrar usuario 11
3.1.5 Cambio de la función RS485 13
3.2 Operación del teclado USB 14
3.2.1 Crear contraseña con teclado 16
3.2.2 Registrar usuarios usando el teclado 17
3.2.3 Borrar un usuario especifico 18
3.2.4 Borrar todos los usuarios 18
3.2.5 Resetear valores de fábrica 18
3.3 Funciones de control de acceso 20
3.3.1 Funciones de Control de Acceso 23
3.4 Verificación de usuario 24
3.5 USB 25
3.6 Botón de sabotaje 25

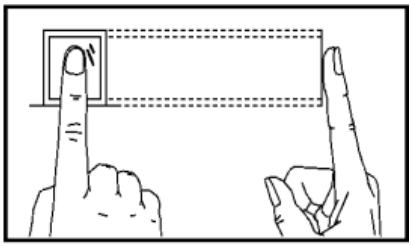
4. Apéndice 26
4.1 Lista de parámetros 26
4.2 Diagrama de cableado: power & comms 27
4.3 Diagrama de cableado: Normalmente Abierto y Normalmente Cerrado 28
4.4 Descripción del uso inocuo para el medio ambiente 30

1. Instrucciones

1.1 Posición del dedo

Se recomienda utilizar el dedo índice, dedo medio o dedo anular; evitar el uso del pulgar o dedo meñique.

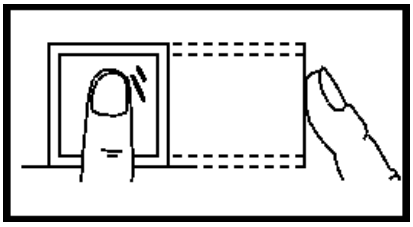
1. Forma correcta de colocar:



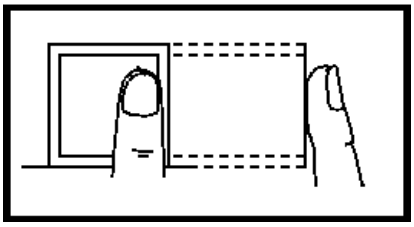
El dedo debe colocarse en una forma totalmente plana y centrado en el sensor.

1. Forma incorrecta de colocar:

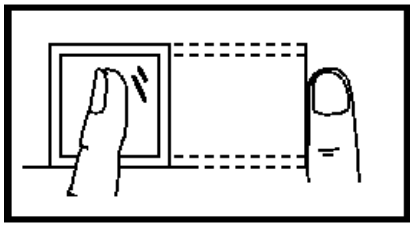
No plano



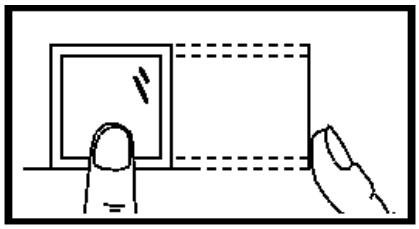
Fuera del centro



De lado



Fuera del centro



Nota: Utilice el método correcto de presionar para el registro y verificación de huellas digitales. Nuestra empresa no asume la responsabilidad por el rendimiento de la verificación baja causada por un funcionamiento incorrecto del usuario. Los derechos a la interpretación definitiva y enmienda son reservados

1.2 Instrucciones para pasar la tarjeta

Este producto se suministra con un RFID sin contacto integrado (125 MHz), lector de tarjetas de módulo. Al ofrecer múltiples modos de verificación tales como huella digital, tarjeta de RF y de huella digital más tarjeta de verificación de RF, este dispositivo puede satisfacer las necesidades de usuarios diversos.
Deslice su tarjeta a través de la zona del sensor después escuchara la voz una vez que el sistema la ha detectado
Para el área de tarjeta, consulte 2.2 Aspecto del producto.

1.3 Precauciones

Protege el dispositivo de la luz solar directa o luz fuerte, esto afecta en gran medida la recogida de huellas dactilares y conduce a un error de comprobación de huellas dactilares.
Se recomienda utilizar el dispositivo bajo una temperatura de 0-50 ° C a fin de lograr el rendimiento óptimo. En el caso de la exposición del dispositivo a la intemperie durante largos periodos de tiempo, se recomienda la adopción de sombrilla y disipación de calor instalaciones ya excesivamente alta o baja temperatura puede ralentizar el funcionamiento del dispositivo y provocar alta tasa de falso rechazo (FRR).

Cuando instale el dispositivo conecte el cable de alimentación después de conectar el resto de cables. Si el dispositivo no funciona correctamente, asegúrese de apagar la fuente de alimentación antes de realizar las inspecciones necesarias. Tenga en cuenta que cualquier trabajo en tensión puede provocar daños en el dispositivo lo cual no será cubierto por la garantía del equipo.

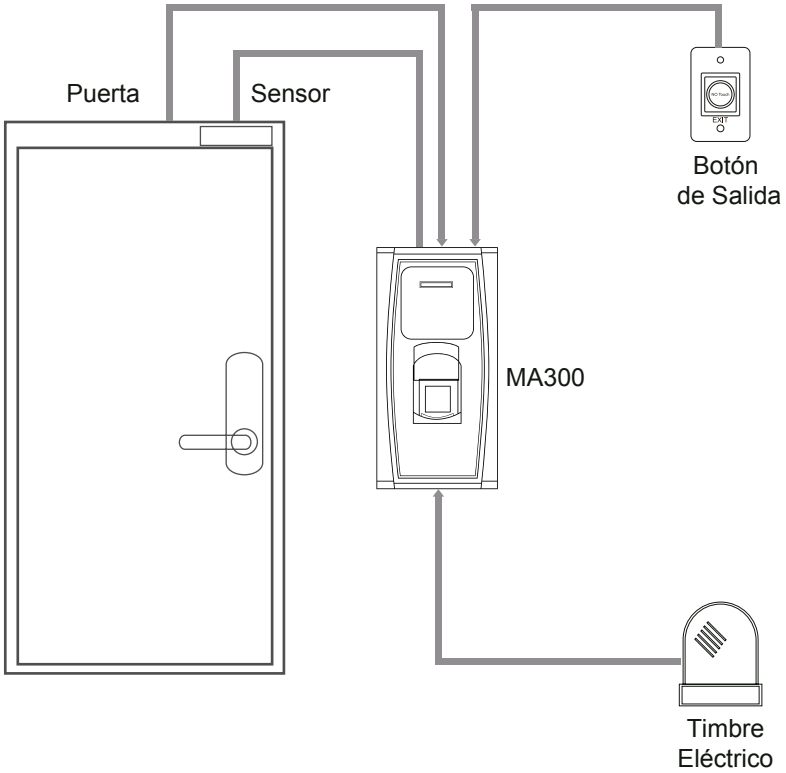
Para las cuestiones que no se tratan en este documento, por favor consulte los materiales relacionados, incluyendo la guía de instalación, manual de usuario del software de control de acceso.

2. Introducción del Equipo

2.1 Vista de las funciones del Equipo

Como una huella digital integrado y dispositivo de control de acceso, nuestro producto se puede conectar, ya sea con una cerradura electrónica o un controlador de acceso. Este dispositivo cuenta con operaciones simples y flexible y admite el uso de tarjetas de gestión. Con una tarjeta de gestión, puede realizar funciones tales como la inscripción sin conexión, eliminación y U-disco de gestión. La voz le guiará a través de todas las operaciones sin la pantalla display. Este dispositivo le permite conectar un teclado externo y ofrece múltiples modos de operación. Es compatible con la función de control de acceso para una gestión de la seguridad. Es compatible con múltiples modos de comunicación. El U-disco cuenta con operaciones sencillas y convenientes.

Con un diseño compacto y simple, este dispositivo permite a los usuarios conectar varios dispositivos a través de un PC y realizar la supervisión en tiempo real.

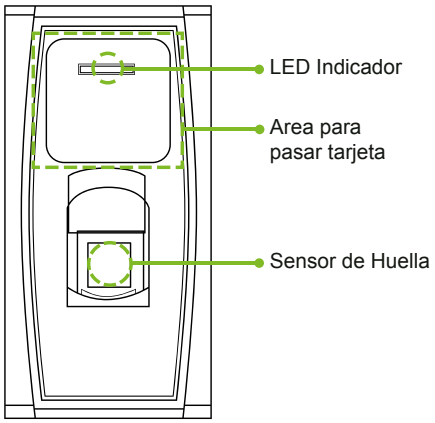


2.2 Apariencia del equipo

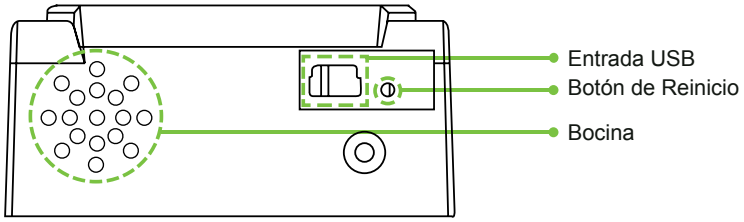
LEDs indicadores: Los LEDs indicadores se utilizan para mostrar los resultados de operación de dispositivos y los estados a excepción que se definen de la siguiente manera:

- **Comunicación:** si una operación es completada el indicador verde se iluminará por un segundo si no se iluminara el rojo por un segundo.
- **Estado de Registro:** El LED verde parpadea tres veces cada tres segundos.
- **Borrar un solo usuario:** El LED rojo parpadea tres veces cada segundo
- **Estado de verificación:** El LED verde parpadea una vez cada dos segundos.
- **Área para pasar la tarjeta:** Se refiere a la zona en el cuadro de línea roja se muestra en la figura

Vista frontal:

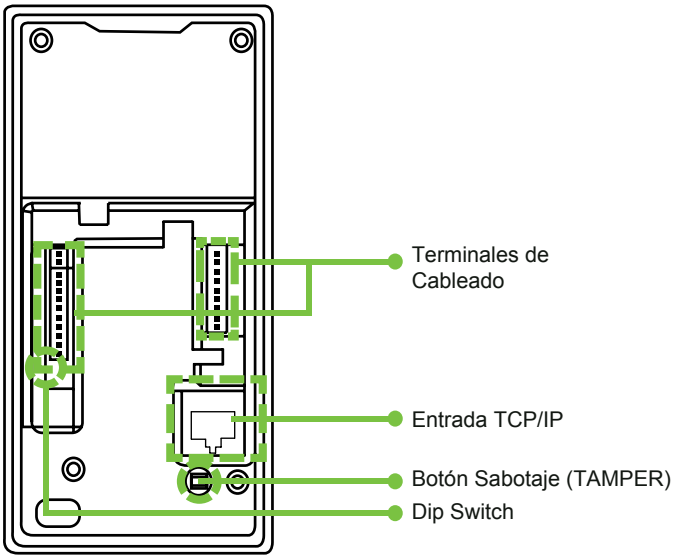


Vista desde abajo



- **Entrada USB:** Se usa para conectar una USB o un teclado exterior.
- **Botón de Reinicio:** Para reiniciar el equipo.
- **Bocina:** Esta será usada para corroborar las acciones del equipo como acceso correcto o negado

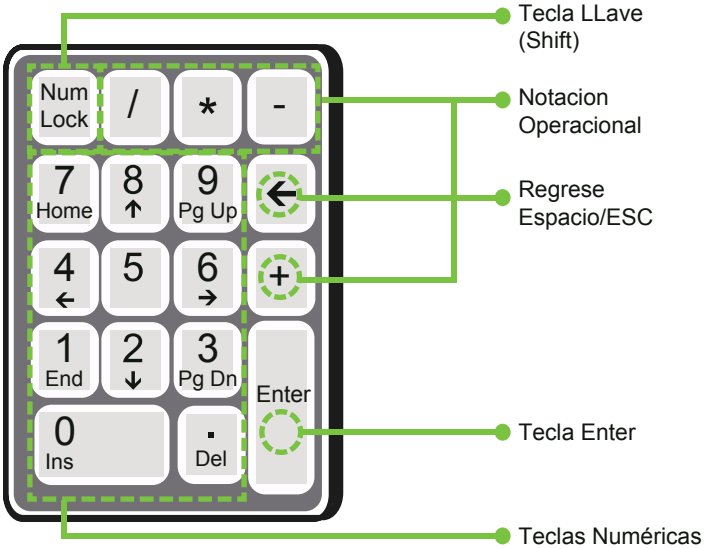
Vista trasera



- **Cableado de equipo:** Se muestra como conectar con el botón o
- **TCP/IP:** La interfaz de TCP / IP se conecta a un PC a través de un cable de red (para la conexión en cola por favor consulte la guía de instalación.
- **Tamper Switch:** Se utiliza para generar una alarma de sabotaje. Para obtener más información, consulte 3.6 alarma de sabotaje
- **DIP Switch:** El interruptor DIP tiene cuatro pines numerados 1, 2, 3 y 4. En la comunicación RS485 de utilizan 1, 2 a 3 ª para establecer el número de dispositivo y el cuarto pin se utiliza para seleccionar el estado de la resistencia terminal.

2.3 Usando un teclado USB externo

Para facilitar las operaciones del dispositivo, puede conectar el dispositivo con un teclado USB (comprado por los usuarios) y llevar a cabo operaciones tales como la incorporación de usuarios, eliminación y restauración de valores de fábrica, sobre todo cuando se especifica la ID de usuario durante la inscripción del usuario y eliminación.



Un teclado USB externo se muestra arriba (consulte al producto real):

NumLock es una tecla de modo del teclado numérico. Se activa de forma predeterminada. Si está activado, el indicador LED está encendido. Cuando el dispositivo está conectado a un teclado externo, sólo puede utilizar las teclas numéricas, la tecla "Retroceso" y la tecla "Enter" en el estado activado Bloq Núm.

2.4 Estado de verificación

Estado de verificación: Cuando el dispositivo está encendido, entrará en el estado de verificación si una tarjeta de gestión se ha inscrito antes o vuelve de otros estados.

En el estado de verificación todos los usuarios están autorizados para verificar su identidad y desbloquear la puerta (el administrador que lleva una tarjeta de gestión sólo puede abrir la puerta mediante el uso de su huella digital (s) previamente inscrita), el administrador puede realizar operaciones como usuario inscripción / eliminación, gestión del USB y el funcionamiento del teclado.

2.5 Gestionando la tarjeta (M-card)

Los usuarios de dispositivos se clasifican en administradores y usuarios comunes.

Administradores: Se permite un administrador para realizar todas las operaciones, incluido el usuario la matrícula (supresión de todos los demás usuarios, excepto a sí mismo / a sí misma) y gestión de USB. Los privilegios de los administradores de dispositivos se implementan a través de las tarjetas de gestión.

Usuarios Comunes: Los usuarios normales sólo pueden verificar su identidad y abrir la puerta.
Una tarjeta de gestión es una tarjeta especial asignada a un administrador. Cada equipo debe tener al menos una tarjeta de gestión de matrícula. Si no hay ninguna tarjeta de gestión inscrita no se puede realizar ninguna operación y el sistema generará un mensaje de voz ": Por favor, registrar la tarjeta de gestión". Puede aplicar diferentes funciones al deslizar una tarjeta de gestión de tiempos diferentes en una fila:

- Al pasar la tarjeta de gestión una vez se puede entrar en el estado de matricular un solo usuario.
- Al pasar la tarjeta de gestión de cinco veces seguidas, puede entrar en el estado eliminación de usuarios.
- USB conectada: Al pasar la tarjeta de gestión de una vez, se puede entrar en el estado de gestión de USB.
- Un Teclado externo está conectado: Al pasar la tarjeta de gestión de una vez, puede activar el teclado externo.

Pases de tarjetas consecutivos: Golpes consecutivos significa que el intervalo entre dos golpes consecutivos a menos de 5 segundos.

Las tarjetas de administración se pueden eliminar a través de "Clear All" función del teclado o a través de software antes de ser eliminados como tarjetas de identificación común. Para obtener más detalles, consulte el manual de usuario del software de control de acceso.

La FP de administrador (el que posee tarjeta de administración) puede ser inscrito a través de software o inscripción teclado.

Un equipo sin tarjeta de administrador: Si tiene la contraseña de teclado, puede activar el teclado externo y matricularse

Nota: Los usuarios que llevan tarjetas de administración sólo pueden verificar su identidad y desbloquear el uso de sus huellas digitales previamente inscritos.

2.6 Password del sistema

La clave del sistema es una contraseña que se utiliza para mejorar la seguridad de los datos del dispositivo en TCP/ IP O COMUNICACIONES RS485.

Nota: El pasword puede ser modificado o borrado desde el software de control de acceso.

2.7 Tiempo de operación expirado

Tiene 30 segundos antes de que la operación concluya, La voz le avisará cada 10 segundos 3 veces si no hay ninguna operación apropiada. Después de estos 30 segundos el sistema regresará al modo de verificación con el mensaje de "Tiempo expirado". El sistema vuelve al estado de verificación.

Nota: Usted podrá configurar este tiempo desde el software "control de acceso".

3. Operación del equipo

3.1 Tarjeta administradora

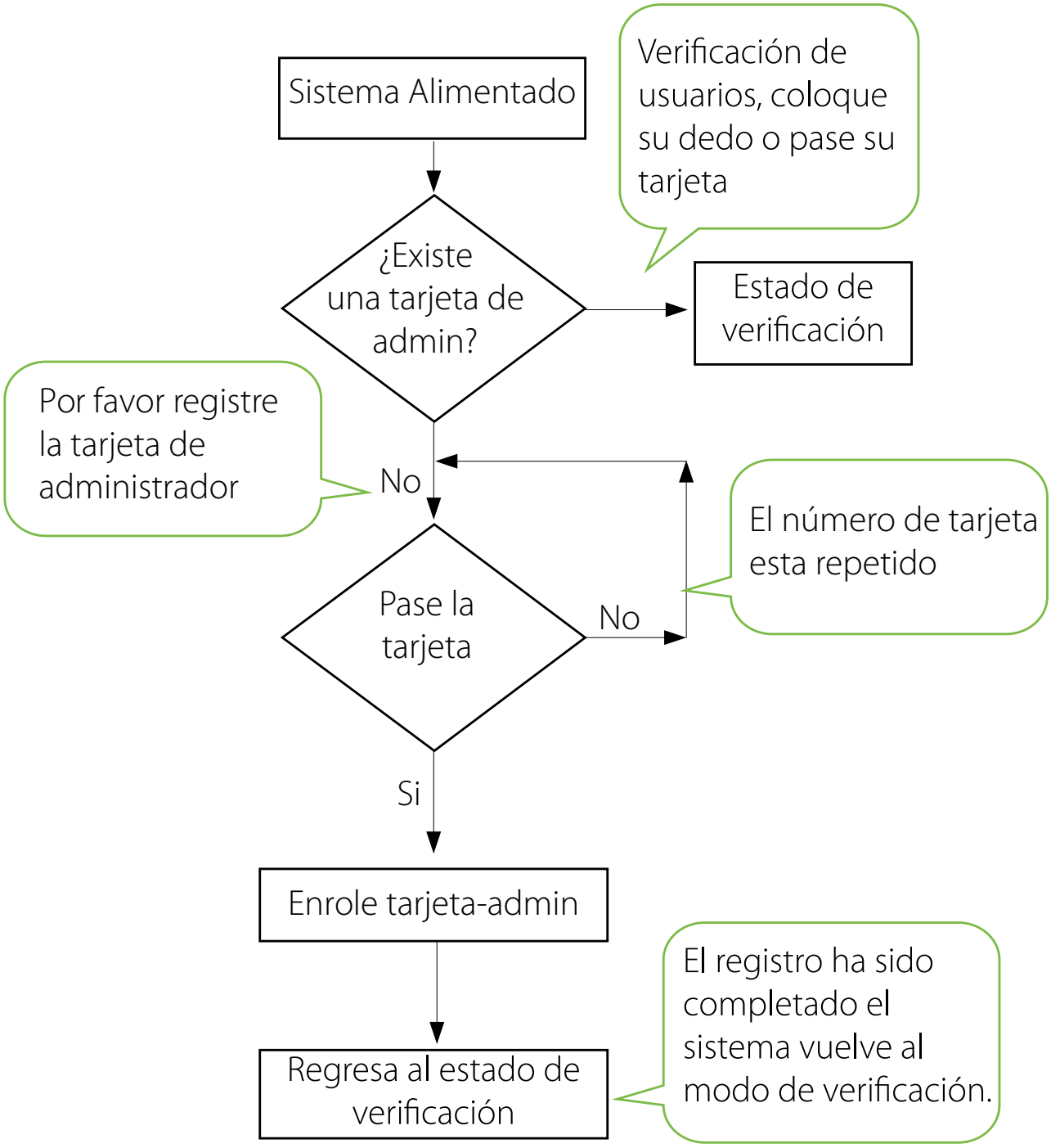
3.1.1. Registre una Huella

Para registrar una tarjeta de gestión, por favor haga lo siguiente:

1. El dispositivo se detecta automáticamente si existe una tarjeta de gestión.
2. Después de que el equipo diga la voz "por favor registre la tarjeta de administrador", puede pasar la tarjeta por el área indicada para registro.
3. Si esto falla el sistema dirá el siguiente comando "El número de tarjeta esta repetido" y regresa al paso 3; agregar tarjeta de administrador, el sistema generara el comando" La verificación ha sido completada el sistema vuelve al modo de verificación".

Nota: El sistema vuelve al modo de verificación si en cualquier operación no recibe respuesta después de 30 segundos, solo lo hará si presenta la tarjeta de administrador después de reiniciar el equipo.

Tabla de como enrolar una tarjeta de administrador:



3.1.2 Agregue un usuario ordinario

- Enrolar tarjeta ID

El modo para que ingrese el estado de inscripción usando la tarjeta de administración se conoce como el modo de inscripción de la tarjeta de administración. En este modo, sólo puede inscribir un usuario. Cuando se registra un nuevo usuario, el sistema asigna automáticamente un ID de inactividad mínimo al usuario. Además, también puede utilizar el modo de inscripción de teclado externo (para obtener más detalles, consulte 3.2.2 Registrar un usuario a través de un teclado) para implementar la inscripción del usuario con ID.

En estos dos modos de inscripción, puede inscribir a nuevos usuarios. Cada usuario puede inscribir 10 huellas dactilares y una tarjeta de identificación.

Para enrolar un usuario, proceda de la siguiente manera:

1. En el estado de verificación, el sistema pasa al estado de inscripción de usuario normal después de pasar una tarjeta de administración una vez (En el estado de inscripción, pasar una tarjeta de administración una vez le devolverá al estado de verificación).

2. Después de que el sistema genere el mensaje de voz: " Regístrar usuarios. Por favor, presione el dedo o pase su tarjeta", puede iniciar la inscripción del usuario.Hay dos casos siguientes:

(1) Deslizar tarjeta ID

a. Cuando pase su nueva tarjeta de identificación y logre enrolar a un usuario, el dispositivo generará un mensaje de voz: Número de usuario **. (** se refiere al ID asignado automáticamente al usuario por el sistema, lo mismo debajo) y puede continuar con el paso b, si el enrolamiento del usuario falla, el sistema genera el mensaje de voz: El número de tarjeta se repite " Y regresa al estado de inscripción, esperando que presione su dedo o pase su tarjeta.

b. Después de que el dispositivo genere el prompt de voz : "Registrar". Presione el dedo ", el sistema ingresa al estado de inscripción de huellas dactilares especificado. Presione el mismo dedo sobre el sensor tres veces siguiendo las indicaciones de voz.

c. Si el enrolamiento de huellas digitales tiene éxito, el sistema genera el mensaje de voz: "El registro se ha realizado correctamente. Pulse el dedo "e ingrese directamente al siguiente estado de inscripción de huellas, si la inscripción de huellas digitales falla, el sistema genera el mensaje de voz: "Presione nuevamente el dedo "y repita el paso b.

d. El sistema regresa automáticamente al estado de verificación cuando se inscriben tanto los 10 dedos como la tarjeta de identificación, la tarjeta de administración se pasa una vez o la operación se agota.

1. Primero presione los dedos

a. Presione el mismo dedo sobre el sensor tres veces siguiendo las indicaciones de voz adoptando la colocación apropiada de la huella digital. Si el enrolamiento de huellas digitales tiene éxito, el sistema genera el número de usuario de voz **. El registro es exitoso y puede continuar con el paso b; Si la inscripción de huellas dactilares falla, el sistema genera el mensaje de voz " (: Presiona de nuevo el dedo" y vuelve al estado de inscripción, esperando que presiones el dedo o deslices tu tarjeta.

b. Después de generar el mensaje de voz " Registrar. Por favor, presione su dedo o deslice su tarjeta", el sistema ingresa el estado de inscripción de información de usuario especificado, esperando que pase su nueva tarjeta de identificación o presione su dedo.

c. Si el ID de la tarjeta de identificación tiene éxito, el sistema genera el mensaje de voz "*": El registro se ha realizado correctamente. Por favor presione con el dedo "e ingresa directamente al estado de inscripción de huellas digitales, si pulsa un dedo que no está registrado antes y logra la inscripción de este dedo, el sistema genera el mensaje de voz:" * ":

El registro es exitoso. Después de inscribir 10 huellas dactilares, el sistema generará el mensaje de voz " (: Pase su tarjeta" para enrolar su tarjeta de identificación si su tarjeta de identificación No está enrolada.

d. El sistema regresa automáticamente al estado de verificación cuando se inscriben tanto los 10 dedos como la tarjeta de identificación, la tarjeta de administración se pasa una vez o la operación se agota.

3. Si ya está asignado con un ID, hay dos casos siguientes para que pueda registrar sus huellas dactilares o tarjeta:

(1) Enrole huellas dactilares cuando ya haya registrado la tarjeta

a. Después de deslizar la tarjeta registrada, el sistema generará el mensaje de voz Número de usuario **. Registro. Presione el dedo "(** se refiere a la ID asignada a usted, lo mismo a continuación) e ingrese el estado de enrolamiento de huellas digitales. Las huellas dactilares registradas sobrescribirán todas las huellas digitales anteriores.

b. Presione el mismo dedo sobre el sensor tres veces siguiendo las indicaciones de voz adoptando la colocación apropiada de la huella digital. Si la inscripción de huellas digitales tiene éxito, el sistema genera el número de usuario de voz **. El registro es exitoso "y se prepara para la inscripción de la siguiente huella digital.

c. El sistema regresa automáticamente al estado de verificación cuando se inscriben tanto los 10 dedos como la tarjeta de identificación, la tarjeta de administración se pasa una vez o la operación se agota.

1. Las huellas dactilares inscritas en este paso sobrescribirán todas las huellas digitales previamente registradas.

(2) Enrole tarjetas cuando ya hayas registrado huellas

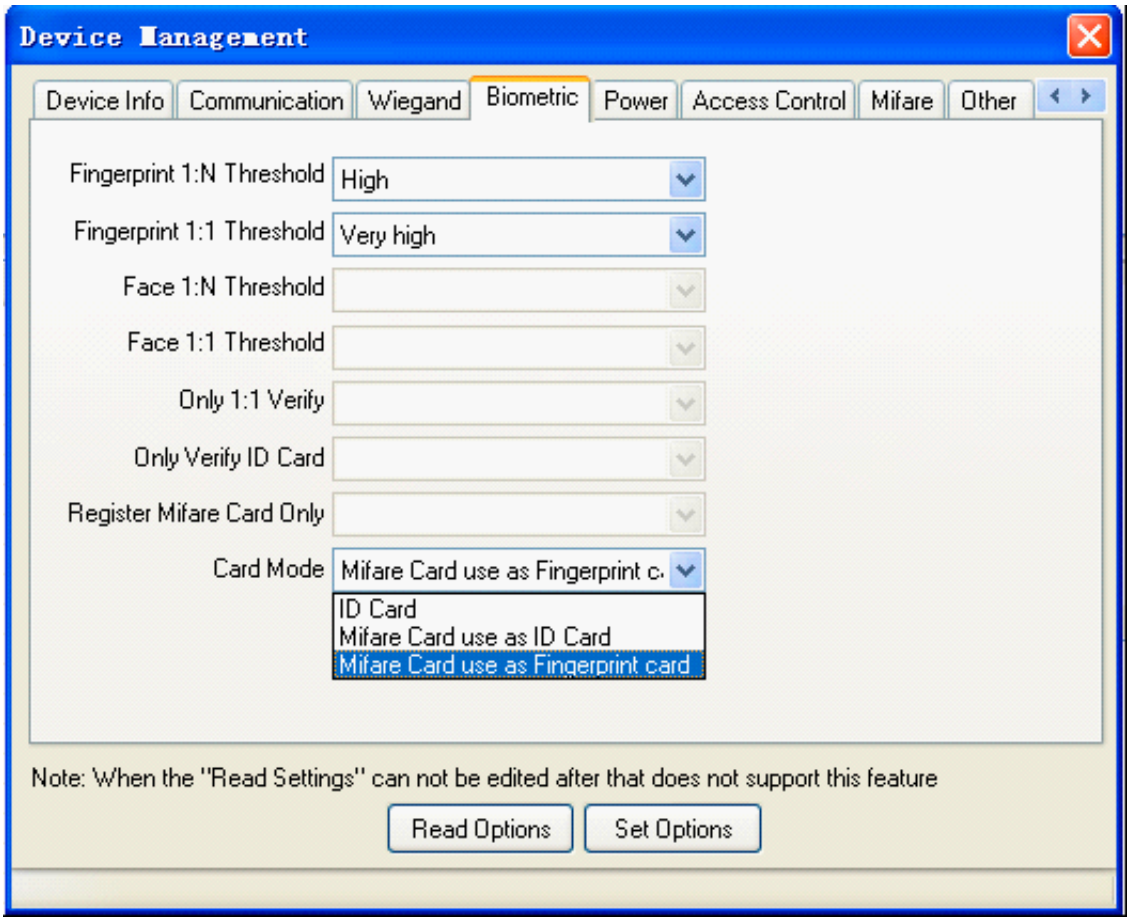
a. Pulse el dedo con la huella digital ya inscrita tres veces siguiendo las indicaciones de voz. Si se identifica como la misma persona en cada intento de verificación, el sistema ingresa al estado de inscripción de la huella digital.

b. Si la matrícula de la tarjeta de identificación tiene éxito, el sistema genera el mensaje de voz "*": El registro se ha realizado correctamente. Registro. Por favor presione con el dedo "e ingresa directamente al estado de inscripción de huellas dactilares, si pulsa un dedo que no está inscrito y tiene éxito en la inscripción de este dedo, el sistema genera el mensaje de voz:" * ": El registro se ha completado. O pase su tarjeta "y puede continuar inscribiendo nuevas huellas dactilares y tarjeta. Después de inscribir 10 huellas dactilares, el sistema generará el mensaje de voz "*": Pase su tarjeta "para inscribir su tarjeta de identificación si su tarjeta de identificación no está registrada.

- Enroll Mifare Card

1. Utilice para la tarjeta de la identificación, refiera por favor a las configuraciones antedichas de la tarjeta de la identificación del registro.:
En el estado de verificación, deslice la tarjeta de administración por una vez para entrar en el estado de inscripción de usuario normal (en el estado de inscripción, pasar una tarjeta de administración una vez volverá al estado de verificación). Después de que el sistema genere el mensaje de voz ": Registrar usuarios. Por favor presione su dedo o pase su tarjeta", puede iniciar la inscripción del usuario. Cuando pase una nueva tarjeta de identificación en el área de la tarjeta, inicie la tarjeta de huellas dactilares de registro, ahora el mensaje de voz ": Por favor, pulse el dedo durante tres veces consecutivas y tener éxito en la inscripción de un usuario, el dispositivo generará un mensaje de voz" Tarjeta de huellas dactilares, por favor espere más tarde, por favor, vuelva a golpear la tarjeta de nuevo ", tener éxito en la inscripción de un usuario después de tarjeta de golpe, el mensaje de voz" * ": Número de usuario **. (** se refiere al ID asignado automáticamente al usuario por el sistema).

Tip: Si la tarjeta de Mifare considera que la tarjeta de identificación o tarjeta de huellas digitales para el uso de cambio, debe obtener a través de "software de control de acceso" de operación, los detalles de las siguientes configuraciones: [Gestión de dispositivos] (seleccione el nombre del dispositivo) - [Biométrico] - [Modo tarjeta], puede seleccionar lo que desea:



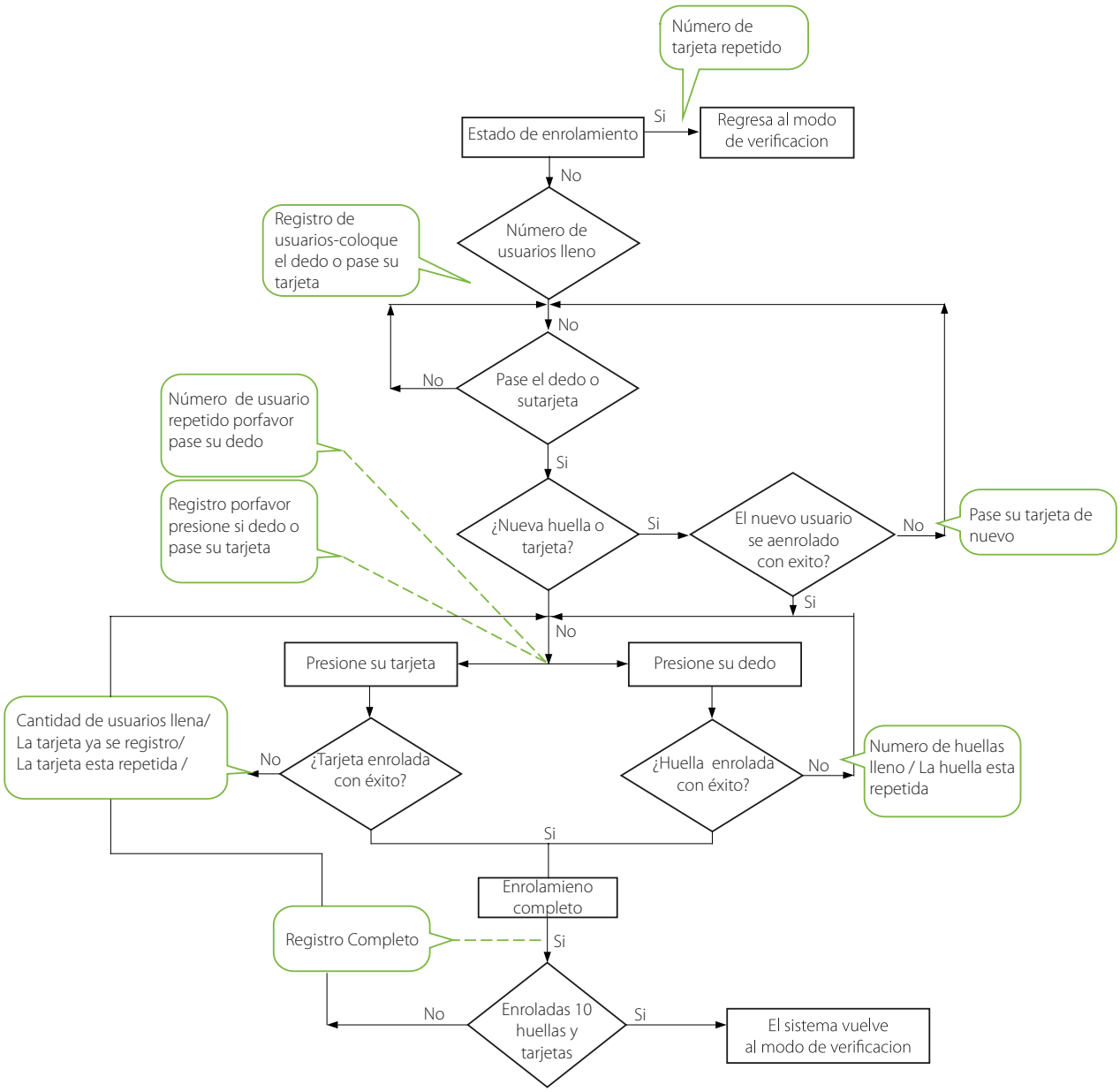
3.1.3 Enrolar tarjeta y huella (s) cuando ya este enrolada una huella (s)

- Presione el dedo con la huella digital que ya inscribieron tres veces siguiendo las indicaciones de voz, que usted este identificado como la misma persona en cada uno de los intentos de verificación.

- Después de generar el mensaje de voz "número de usuario *. Registrarse Por favor, pulse el dedo.

- Si la inscripción de la tarjeta de identificación tiene éxito, el sistema genera el comando "Registro completado por favor presione el dedo." Y entrará en el estado de gestión de huellas dactilares si presiona un dedo que no se enrolo antes y logra el registro de este dedo, el sistema generara el comando": Registro completo. Por favor, pulse el dedo o pase la tarjeta "y usted puede seguir registrando nuevas huellas digitales o tarjetas. Después de que se hayan grabado 10 huellas el sistema pedirá volver a enrolar una tarjeta de administrador.

- El sistema volverá al modo de verificación una vez que 10 huellas y una tarjeta de administrador sean grabadas.

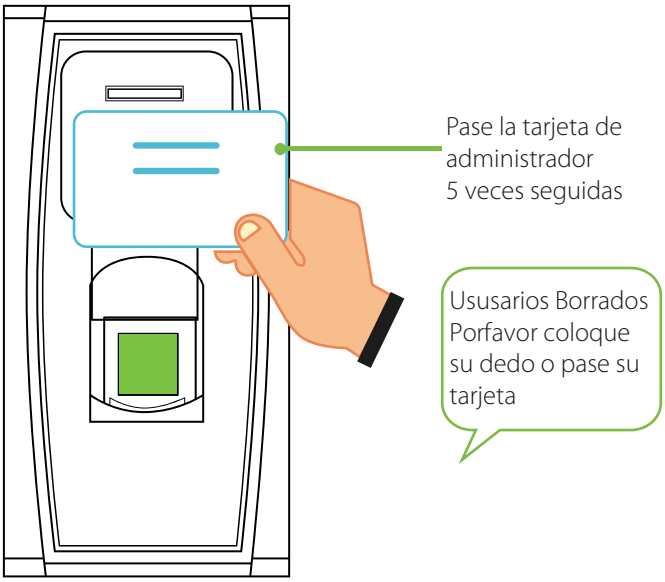


3.1.4 Borrar a un usuario

Borrar un usuario usuando la tarjeta de administrador Modo de borrado de un usuario simple y borrando un usuario con el teclado exterior es Modo de borrado de un usuario especifico . (Ver 3.2.3 borre un usuario especificado).

Pasos para borrar un usuario simple:

- En estado de verificacion, pase su tarjeta de administrador por 5 veces consecutivas para entrar al modo de borrado de usuario (pase su tarjeta una vez mas y volevera al modo de verificacion).

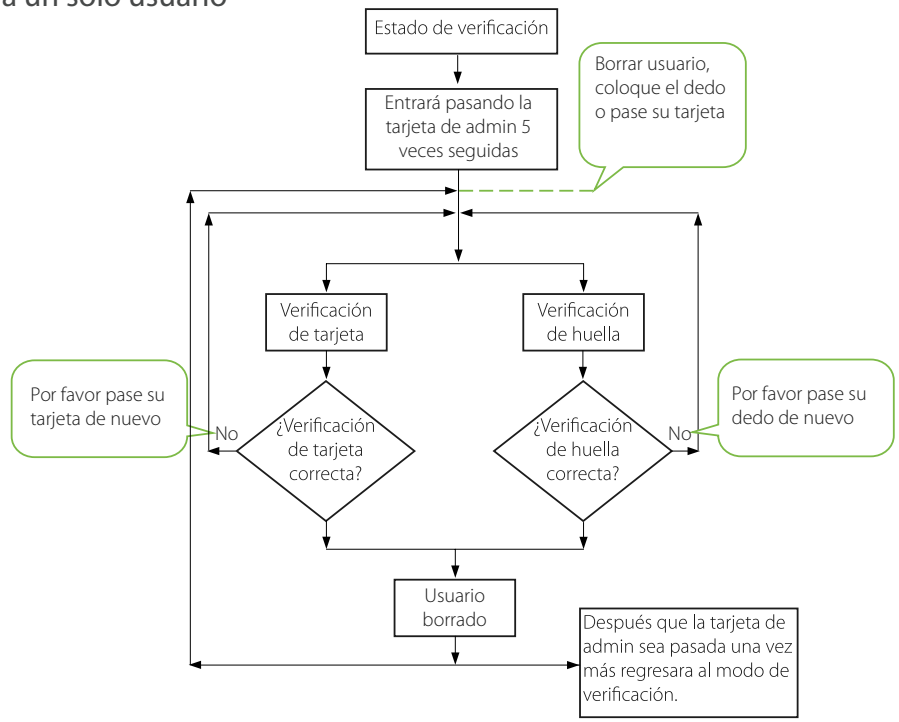


Pulse uno de sus dedos registrados correctamente en el sensor. Si la verificación tiene éxito, el sistema generará el indicador de voz ": Número del usuario. ** Borrado con éxito. Eliminar usuarios. Por favor, pulse el dedo o pase su tarjeta. "(** Indica el número de identificación del usuario) y volverá automáticamente al estado de borrado. Si la verificación falla, el sistema generará el indicador de voz ": Por favor, pase de nuevo.

- Pase su tarjeta sobre el lector para borrar un usuario.
- Pase una tarjeta registrada sobre el lector si la verificación se completa el sistema dará el comando de voz ": número de usuario**. borrado con éxito. Borrado de usuarios. presione su dedo o pase su tarjeta." y automáticamente regresara al modo de borrado. si la verificación falla, el sistema generara el comando de voz ": por favor pase su tarjeta de nuevo."
- Si pasa su tarjeta una vez mas o se tarda en el tiempo de operación, el sistema volverá al modo de verificación.

Nota: En el modo de borrado de un solo usuario simple las tarjetas de administración no se pueden eliminar porque al pasar la tarjeta de administración se regresara al sistema o modo de verificación.

Tabla para borrar a un solo usuario



3.1.5 Cambio de la función RS485

El MA300-BT admite la función de lector RS485 y se puede conectar al lector FR1200 a través del RS485. La función del lector RS485 se puede conmutar girando la tarjeta de gestión siete veces

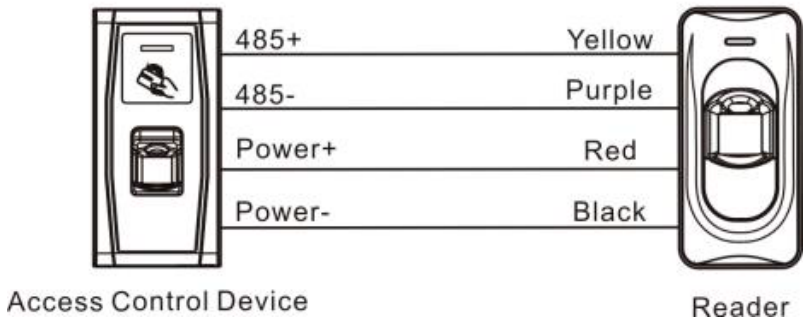
1) Después de que un usuario pase la tarjeta de administración siete veces, si la última vez que MA300-BT emite un pitido una vez, significa que la función de lector RS485 ha sido desactivada. El MA300-BT se comunica con el ordenador en modo RS485.

2) Después de que un usuario pase la tarjeta de gestión siete veces, si la última vez

El MA300 se conecta por RS485.

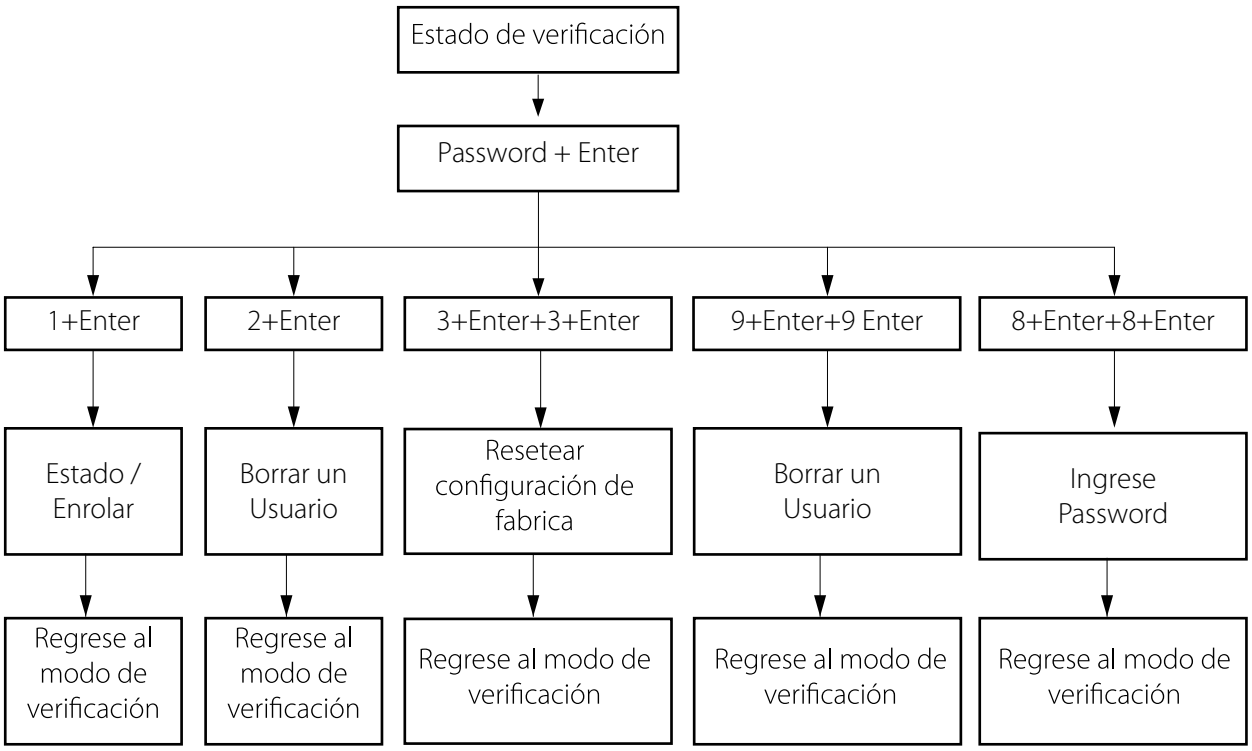
Nota: Para la función de comunicación del RS485, necesitas reiniciar el dispositivo.
Al mimso tiempo, puede ser conectado en con un lector RS485 maestro/esclavo Modo.Es decir, el MA300-BT sirve como el maestro y el RS485 El lector sirve como el esclavo. Además, la función RS485 anti-pasback es compatible. Si la función de lector RS485 está activada, el MA300-BT

Comunicarse con el ordenador en modo RS485.



3.2 Operación del Teclado USB

Tabla de operaciones con teclado



3.2.1 Configurar Password para Teclado

Si el usuario necesita un teclado externo puede conectarlo directamente al aparato y solo pasar la tarjeta de administrador.
El sistema permite asignar un password al teclado.

Pasos de Operación:

- En el estado de verificación conecte el teclado con el dispositivo a través de USB.
- Pase su tarjeta de admin para activarlo y se generara un comando que dirá: "por favor presione el teclado".
- Escriba de "8" y pulse "Enter" A continuación, escriba "8" y pulse "Enter" de nuevo. El sistema genera el mensaje de voz ": Por favor, establecer una contraseña." Escriba su contra-seña deseada y pulse la tecla "Enter". El sistema genera el mensaje de voz ": La operación se completó. "Si no hay pulsaciones de tecla en 30 segundos, el sistema generará el indicador de voz": Tiempo de la operación terminado. El sistema de volverá al modo de verificación. (la contraseña deberá ser de entre 4 y 6 dígitos).
- E l usuario podrá usar el teclado para la gestión de usuarios únicamente ingresando el password antes de usarlo si este no detecta movimiento automáticamente se bloqueará.

Nota:

1. Si se equivoca de pasword en seis ocasiones, El teclado se bloqueará y solo podrá ingresar de nuevo quitando la alimentación.

2. Si no hay actividad del teclado en 30 segundos este de desactivará automáticamente.

3. El teclado deberá ser conectado después de 15 segundos de otra manera el sistema no podrá identificar su estado.

3.2.2 Enrolar usuario mediante el teclado

Enrolar un usuario mediante el teclado externo es llamado Modo de Enrolamiento base. En este modo usted puede registrar un usuario con un numero especifico de ID.

Pasos de Operación:

- Como se muestra 3.2 Tabla de Operaciones de teclado USB, escriba "1" y presione "Enter" para entrar al estado de enrolamiento.

- Cuando el sistema genera el comando: Registro de usuarios por favor ingrese el número de usuario. o ingrese el ID de usuario.

- El sistema generara el comando numero**. Registro de usuarios por favor coloque el dedo o pase su tarjeta. (** indica el número de identificación del usuario El sistema entra en el estado específico de inscripción ID.

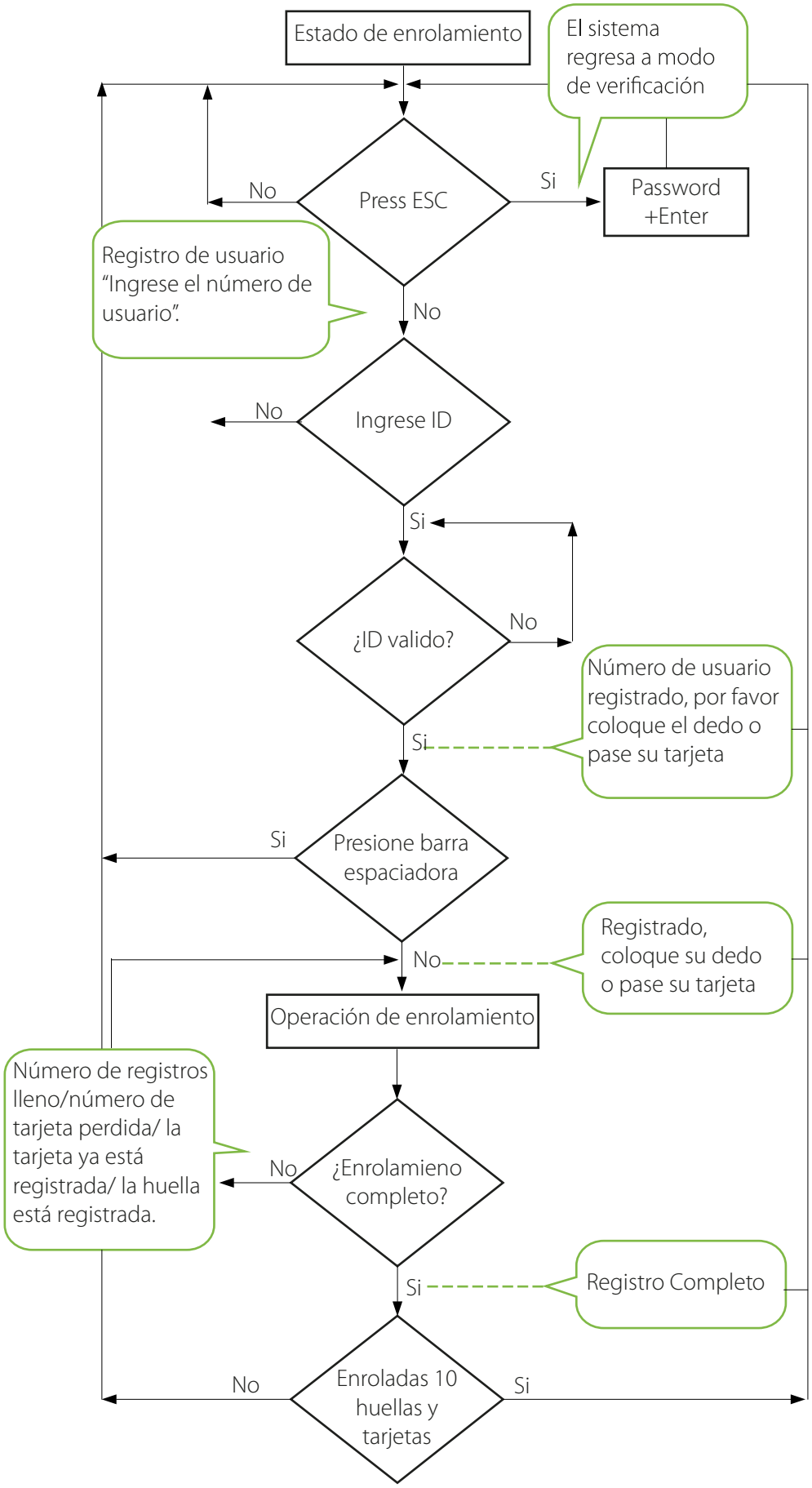
Nota: Si el usuario ya está registrado con tarjeta se escuchará un comando que dirá "por favor coloque su dedo".

- Si el usuario está registrado en el sistema como un usuario ID con 10 huellas se generará el comando: número de usuario **.por favor pase su tarjeta."

- En el estado de espera del ID de usuario registrado presione ESC para regresar al modo de verificaciones si esto no responde presione ESC 2 veces para regresar al estado o modo de verificación.

Nota: En el modo de enrolamiento con el teclado externo puede realizar los registros consecutivamente y el teclado regresara por sí mismo el estado de modo de verificación por sí mismo.

Tabla de enrolamiento base con teclado:



Información adicional:

1. En el modo basado en teclado si los tiempos de efectuar cualquier operación sobrepasan el tiempo el sistema automáticamente le solicita esta operación una vez cada otra 10 segunda y vuelve al estado de verificación después le pide tres veces.
2. Las huellas recién agregadas se sobrepondrán a las originales basado en inscripción cualquier huella sobrescrita remplazara a la antigua.
3. Un usuario solo puede inscribirse con una sola tarjeta. Cuando el usuario se inscribe en una tarjeta del sistema genera el mensaje de voz:" Por favor, pulse el dedo". Cuando el usuario para la tarjeta, el sistema genera el mensaje de voz:" La tarjeta ha sido registrada."
4. No se puede registrar una tarjeta dos veces, de lo contrario el sistema generará el comando: "Tarjeta repetida". Al pasar la tarjeta diferentes usuarios no pueden inscribir la misma huella en ella de lo contrario el sistema generará el indicador de voz: "La huella digital esta repetida". Durante el registro de huellas dactilares, las nuevas huellas de un usuario siempre se sobreponen a las existentes.

La diferencia entre estos dos modos de inscripción de usuarios es cómo se vuelve al modo verificación:

1. Con la tarjeta de administrador con un ID de usuario específico, el sistema de vuelve al estado verificación después de que pase la tarjeta una vez.
2. Con el teclado solo será necesario el presionar en dos ocasiones la tecla ESC para que el sistema vuelva al modo de verificación, el mismo dirá el comando el sistema se encuentra en modo de verificación.

3.2.3 Borrar un usuario especificado

Borrando un usuario especificado con el teclado se llama Borrado de usuario especifico.

Pasos de Operación:

- Conecte su teclado y pase la tarjeta de administración e ingrese el password si se cuenta con uno

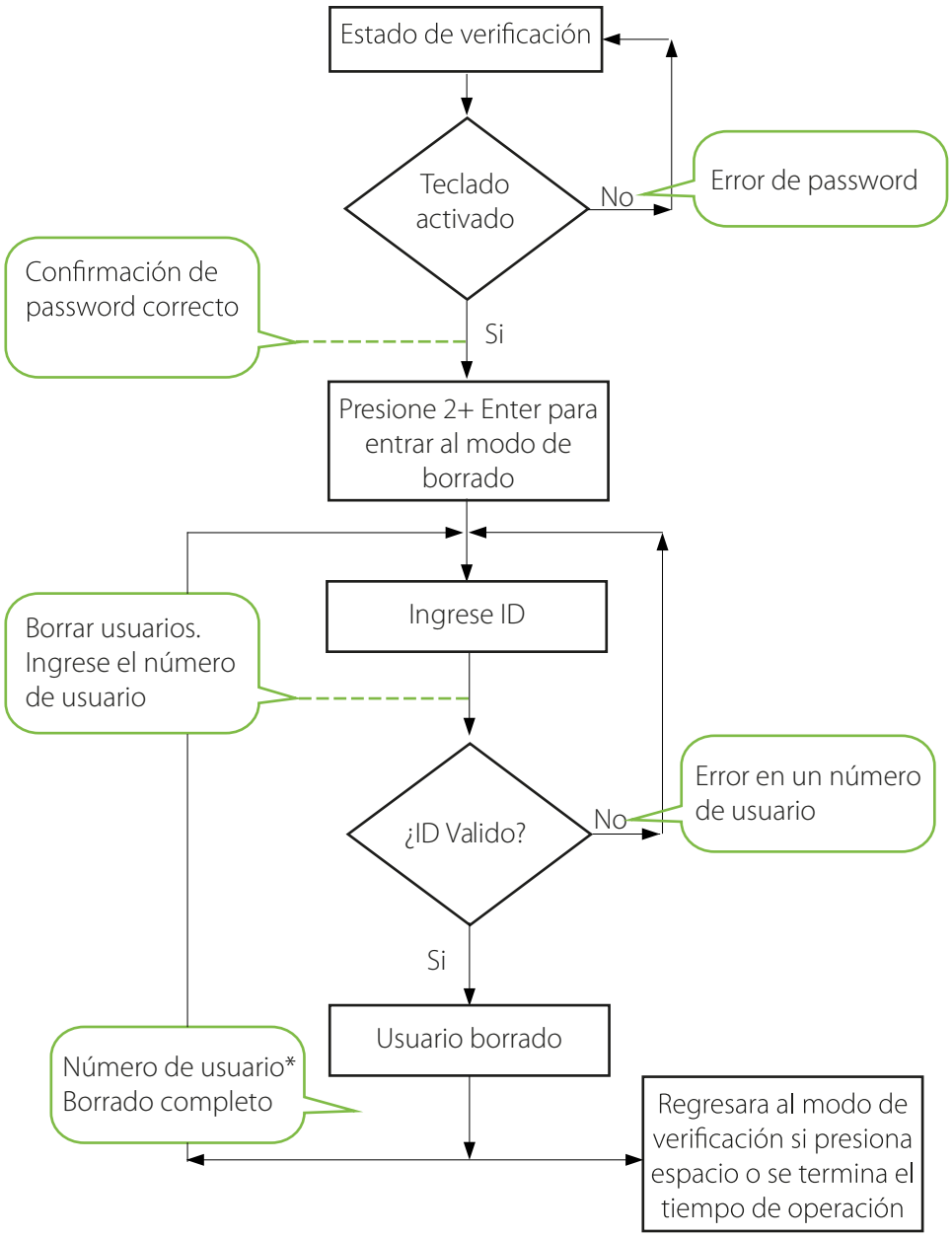
- Presione "2" y "Enter"; para entrar al modo de borrado de usuarios específicos el sistema generara el comando :" Borrado de usuarios por favor agregue el número de usuario." y después procederá al paso 3.

- Entre el numero ID del usuario y este se encargará de checar y confirmar el proceso

- Si el ID de usuario es válido, el sistema generará el indicador de voz ": Número del usuario. ** Borrado con éxito. borrado de usuarios. Por favor, introduzca el número de usuario. "Y automáticamente volverá al estado de borrado. Si el ID de usuario no es válido, el sistema generará el indicador de voz: "Error de número de usuario"

- Si presiona "ESC" o rebasa el tiempo de operación el sistema automáticamente volverá al modo de verificación.

Nota:
- En el modo de eliminación de un usuario específico el ID de usuario y ID de tarjeta de administración que están inscritos en el sistema se considerarán validos
- En el modo de borrado del teclado deshabilitara temporalmente la función del sensor de huellas o lector de tarjetas.



3.2.4 Borrando todos los usuarios

Pasos de Operación

- Conecte su teclado y pase su tarjeta de administrador para activarlo.
- Presione "9" + "Enter". después "9" + "Enter" de nuevo y se borraran los usuarios.
- Si se logra con éxito el sistema dirá el siguiente comando:" Borrado de usuarios la operación ha sido completada. El sistema vuelve al modo de verificación por favor registre la tarjeta de administrador.

Nota:

- Usted puede borrar un administrador usando la función de borrar todo
- Puede también usar esta función parar borrar transacciones, usuarios y passwords.
- Extrema precaución porque después de borrar toda esta información no habrá forma de recobrarla

3.2.5 Restablecer Valores de Fabrica

Pasos de Operación: Con teclado.

- Conecte un teclado y actívelo pasando su tarjeta ingrese el password si se cuenta con uno
- Presione "3" + "Enter". después presione "3" + "Enter" de nuevo y el sistema restablecerá los valores de fábrica.
- Después de la operación completada el sistema generara el comando: "restablecer valores de fábrica completado. El sistema regresa al modo de verificación" usted también puede restablecer los valores de fábrica usando el tamper botón vea en 3.6 Botón Tamper. después de que se han restablecido los valores toda la información será reiniciada de fábrica, incluyendo número, password, dirección IP, Dirección RS485 y password de teclado.

Pasos de Operación: Sin el Teclado.

- Desconecte la alimentación, presione y mantenga el BOTON TAMPER . después que regrese la alimentación espere por el comando de voz después suelte el botón y espere 40 segundos, después presione el botón 3 veces TAMPER y el relay se activara 3 veces y solo lo suelta al final. repítalo si no funciona a la primera.

Nota: La información de los usuarios, así como ellos mismos no serán borrados

3.3 Funciones de Control de Acceso

3.3.1 Funciones de Control de Acceso

Configuración de Control de Acceso es para que usuarios abran puertas en zonas de tiempo y el equipo controle parámetros para la apertura de electroimanes.

Para abrir, el usuario debe cumplir con las siguientes condiciones:

- La hora actual debe coincidir al acceso de la zona horaria del usuario o el huso horario de acceso al grupo que él / ella pertenece
- El grupo en el que el usuario es debe estar será una de las combinaciones de desbloqueo. El primer grupo es el grupo por defecto para todos los nuevos usuarios. El grupo en el que el usuario debe ser es el control de acceso / grupo de combinación de desbloqueo (unlock) (el usuario puede modificar el ajuste correspondiente de control de acceso, a través del software de control de acceso).

Nota: La función de control de acceso del dispositivo será necesario establecerla y modificarla a través del software de control de acceso, para los detalles, por favor consulte el manual de usuario del software.

La configuración de Control de Acceso de usar para que el usuario habrá la puerta en una zona de tiempo especifica controlando los parámetros del electroimán.

Para abrir el usuario registrado debe cumplir con las siguientes condiciones:

- El tiempo de apertura ocurrente debe coincidir con la zona de tiempo editada y el grupo de acceso.

- El grupo donde el usuario este debe estar en el control de acceso (o del mismo control de acceso de un grupo para abrir la puerta juntos). El sistema por defecto albergará la zona de default del grupo usted puede agregar o modificar las zonas de tiempo para los grupos desde el software.

Nota: Las zonas de tiempo en el equipo deben ser creadas y modificadas desde el software y después transmitidas a este se recomienda crearlas primero antes de agregar usuarios.

1. Zonas de Tiempo de Control de Acceso:
   Las zonas de tiempo son las unidades mínimas para el acceso de un usuario están podrán ser creadas desde el software y agregadas a por usuarios, también puede agregarlas a los grupos y agregar un usuario a este grupo el sistema le brindara la zona de tiempo del grupo por default.

2. Configuración de Acceso días Festivos:
   Este tiempo de control de acceso especial tal vez sea necesario durante las vacaciones. Es difícil modificar el tiempo de control de acceso de cada persona. Así que se recomienda revisar directamente el manual del software para realizar esta función.

3. Acceso de Grupos con Zonas de Tiempo:
   Agrupando y gestionando grupos los empleados agregados en grupos usarán las zonas de tiempo de estos grupos por default de hecho a cada empleado de este grupo también se le puede configurar una zona, los grupos siempre mantendrán sus zonas la opción siempre existirá de agregar un nuevo usuario a diferentes grupos.

4. Configuración de Combinación de desbloqueo (UNLOCK):
   Para mejorar el nivel de seguridad puede utilizar esta función Para abrir la puerta, 5 personas diferentes de 5 grupos diferentes se necesitan, lo que significa que la puerta no se puede abrir a menos que todos los 5 de estas personas pasaron el proceso de verificación.

5. Parámetros de Control de Acceso:
   Retardo de Control de Bloqueo (lock control delay): Se aplica para determinar el tiempo de desbloqueo, la unidad de medida mínima es de 20 ms en las condiciones normales es 100-200ms.

Anti-Passback: Configurable a "Nada", "salir ", "entrar", "entrar/salir".

Estado de Registro del Maestro: Configurable a "nada", "salir", "entrar".

Modo del sensor: Este modo puede configurarse a "nada", "Normal abierto (NOpen)", "Normal Cerrado (NClose)" ese sería el estado de este.
Retardo del sensor (Sensor Delay):
Configura el retardo del sensor después que la puerta fue abierta si la puerta no está cerrada dentro del

tiempo de retardo del sensor se activa la alarma El rango de dispositivos de pantalla blanco y negro es 0-254 y dispositivo de pantalla a color es de 0-99.

Sensor de Alarma: Configure el tiempo de retardo de la alarme después de la activación de esta (externa)se disparará configurable a un rango de 0-999 segundos.

Tiempo de Errores de Alarma: Definir los tiempos de error máximo para activar la alarma. Cuando no se pasa la cautela de verificación y exceden los tiempos definidos, la señal de alarma se activará automáticamente.

6. **Configuración de Anti-Pass back:**
   Anti-Pass back función; por favor revise 4.2 Anti-Pass back.

7. **Deshabilitar Alarma:**
   (Tipo de alarma: alarma de puerta y alarma de tamper) cuando el dispositivo está en estado de alarma, la verificación del usuario puede desactivar la alarma y este volverá a su estado normal o de lo contrario se activará nuevamente

3.4 Verificación de usuarios

La verificación por default en el equipo es FP y RF puede modificar este modo de verificación desde el software como RF o FP al igual que RF+FP o solo uno de estos dos para mayor información visite el manual del software

Pasos de Operación:

- Cuando el equipo está en el modo de verificaciones sistema dirá el comando: "Verificación de usuarios por favor pase su dedo o coloque su tarjeta".

- Comenzará la verificación de usuarios el equipo soporta 4 modos diferentes de verificación usuarios: FP/RF, FP, RF y FP&RF.

Verificación de huella digital (FP).

Solo presione su dedo en forma planee en el sensor si la verificación es correcta el sistema pronunciara el comando "Numero de usuario**. Gracias." y después brindara el acceso si la verificación falla el sistema pronunciará el comando: "coloque su dedo otra vez."

Verificación con Tarjeta

Solo pase su tarjeta por el área recomendada si el acceso es correcto el sistema pronunciara el siguiente comando: "Numero de usuario **. gracias." y le brindara el acceso, pero si la verificación falla el sistema pronunciara el siguiente comando: "Por favor pase su tarjeta otra vez.".
Verificación con Huella digital + Tarjeta

Configure el modo primero a FP & RF desde el software la operación de la verificacion sera la siguiente:

Coloque el dedo primero:

Coloque el dedo en la posición apropiada y si la verificación fue correcta el sistema dirá el comando:" Número de usuario **, por favor pase su tarjeta." después será brindado el acceso si la verificación falla el sistema generar el comando: "Por favor pase su tarjeta de nuevo.

Pase la Tarjeta Primero:

Pase su tarjeta por el área recomendada si la verificación es correcta
el sistema generara el comando: " Numero de usuario **, por favor coloque su dedo."
si todo es correcto brindara el acceso si el modo de verificación falla el sistema generara el siguiente comando:
"Por favor coloque su dedo otra vez."

Verificación Finger print/Huella o Tarjeta

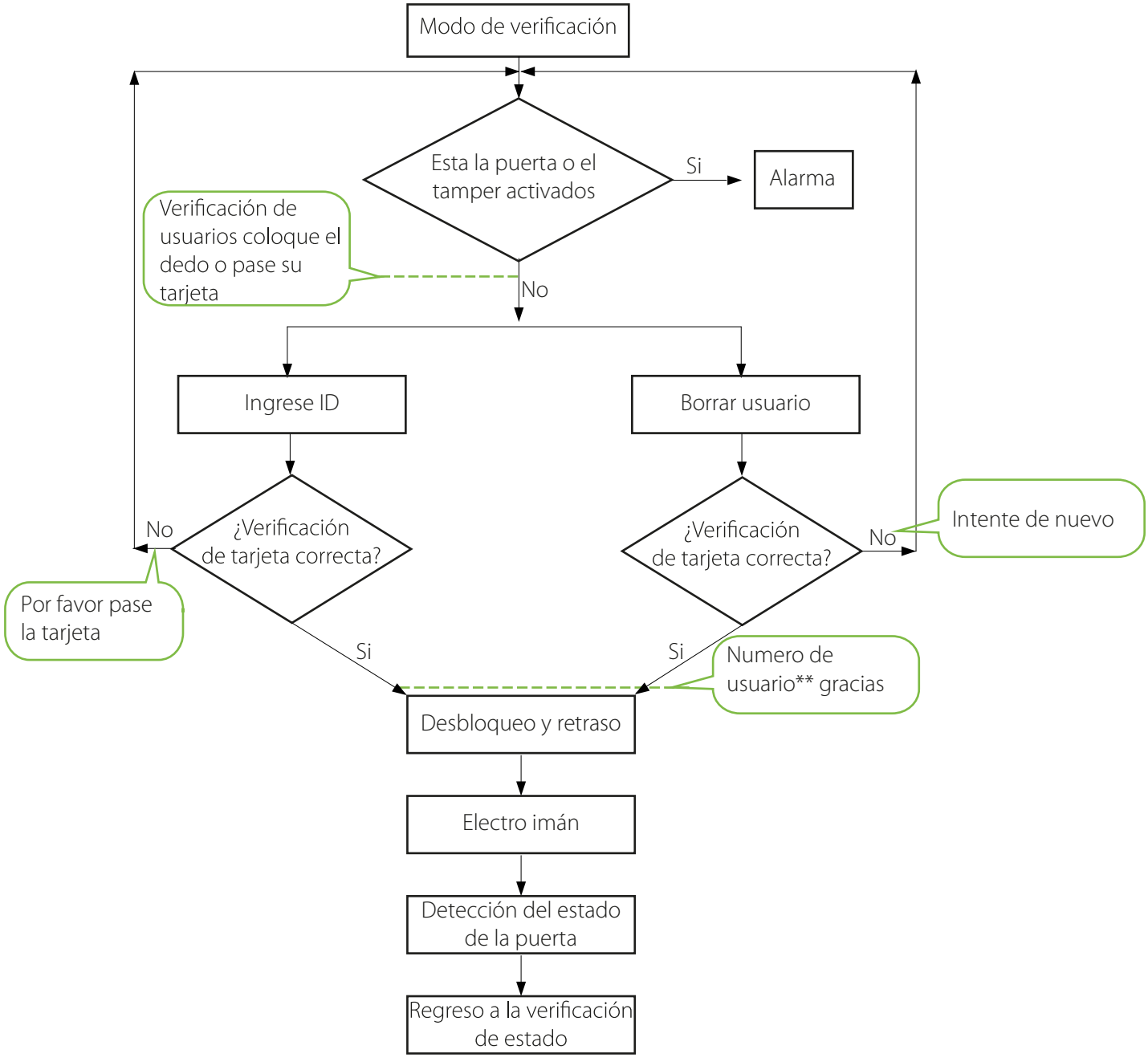
Ese es solo un modo de verificación (1) de (2) a escoger.

Nota:

- Si el usuario no cuenta con una zona de acceso valida el sistema generará el comando: "zona de acceso invalido".

- Si el usuario no usa el modo de verificación que se le ha otorgado no podrá acceder y el sistema generar el comando:" Modo de verificación invalido".

Tabla de Verificación de usuarios:


Modo de verificación
Esta la puerta o el tamper activados
Si
Alarma
Verificación de usuarios coloque el dedo o pase su tarjeta
No
Ingrese ID
Borrar usuario
¿Verificación de tarjeta correcta?
No
Por favor pase la tarjeta
Si
¿Verificación de tarjeta correcta?
No
Intente de nuevo
Si
Numero de usuario** gracias
Desbloqueo y retraso
Electro imán
Detección del estado de la puerta
Regreso a la verificación de estado

3.5 Memoria USB

El usuario puede descargar reportes, descargar usuarios, subir usuarios y actualizar el firmware del equipo mediante la memoria USB.

- **Descargar Reportes:** Descargue los reportes de asistencia de todos los usuarios con la memoria USB.
- **Descarga de Usuarios:** Descargue los usuarios con su información incluyendo los templetes de las huellas digitales de los mismos.
- **Subir Usuarios:** Suba información de usuarios con su memoria USB al equipo.
- **Actualice Firmware:** La actualización del firmware mediante la USB.

La creación y modificación de estos archivos puede ser realizada usando el software de control de acceso para referencia diríjase al manual del software.

Nota: Por favor no actualice los firmwares a discreción porque puede crear un daño irreversible a los equipos, recuerde que el firmware es creado para un equipo en específico y no puede ser instalado en otros dispositivos aun sean el mismo modelo.

La Operación de USB incluye cualquiera de los siguientes dos casos:

- Si conecta la memoria USB la configuración del equipo del sistema automáticamente le brindara los comandos de seguimiento para secuencias.
- Después de conectar la USB en el equipo pase su tarjeta para entrar al modo de gestión de memoria USB (U-DISK).
- El sistema generar el comando:"****. por favor pase su tarjeta de administrador para confirmar." (**** indica las cuatro posiciones de trabajo en la secuencia, lo mismo más adelante).
- Si quiere modificar la gestión de USB, confirme con su tarjeta. Si la operación se completa, el sistema generara el comando: "operación completada y podrá pasar al siguiente paso al finalizar con los cuatro pasos, el sistema generara el comando: "el sistema regresa al modo de verificación. si la operación falla, este generara el comando: "La operación fallo el sistema vuelve al modo de verificación".
- Si no pasa la tarjeta de administrador el sistema automáticamente saltara los pasos después de 5 segundos y lo enviara al siguiente paso. al termino de los cuatro pasos el sistema regresara al modo de verificación automáticamente.
- Si usted conecta una memoria USB que ya ha sido configurada en el equipo al conectarla este respetara las configuraciones ya estipuladas
- Después de conectar la memoria USB en el equipo solo es necesario para su tarjeta para entrar al modo de gestión de USB (U_DISK).

- El sistema obtiene los comandos de operación del USB leyendo un archivo en esta misma después generara el comando: "Releyendo configuración de memorias (U_DISK) pase su tarjeta para confirmar."
- Después de pasar su tarjeta y realizar las operaciones el sistema generara el comando:" ****. Operación completada. "así mismo al término de cada secuencia si alguna de estas fallas escuchara el comando:" ****. La operación ha fallado."

- Después de terminar con las operaciones el sistema generará el comando:" el sistema regresa al modo de verificación."

Nota: Por favor, espere 8 segundos después de insertar la USB en el dispositivo, de lo contrario, el sistema no puede detectarlo correctamente.

3.6 Botón de Sabotaje (tamper)

Se presiona el interruptor de sabotaje manteniéndolo así con la base trasera. Cuando se desmonta el dispositivo el interruptor de seguridad se levantará y luego se enviará una señal de alarma para activar una alarma externa.

Reconocer Alarma: El usuario puede desactivar la alarma de sabotaje abriendo la puerta con una verificación correcta de usuarios registrados.

Restablecer Valores de Fabrica: Los valores de fábrica pueden ser restablecidos con el mismo boto de sabotaje Cuando el sistema genere una alarma por 30–60 segundos el usuario puede presionar el botón tres veces (escuchara un beep) para restablecer los valores, incluyendo numero de equipo, password de sistema, dirección IP, dirección 485 y password de teclado externo.

Nota:
- Toda la información de usuarios NO será borrada después de restablecer los valores de fábrica.
- Los valores de fábrica pueden ser restablecidos incluso usando el teclado externo, vea 3.2.5 restablecer valores de fábrica.

4. Apéndice

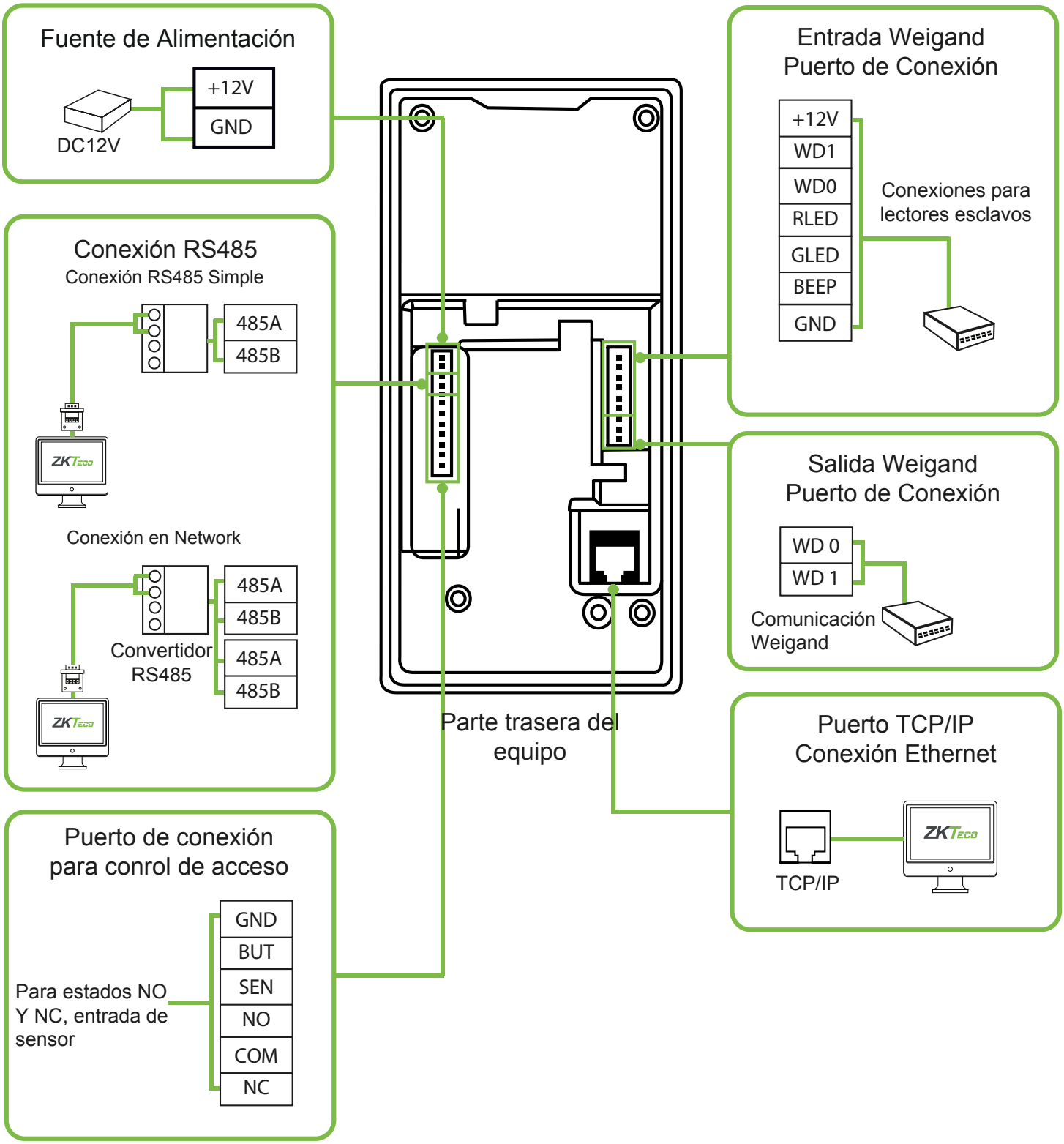
4.1 Lista de parámetros

En la tabla siguiente se enlistan los parámetros funcionales básicos del dispositivo:

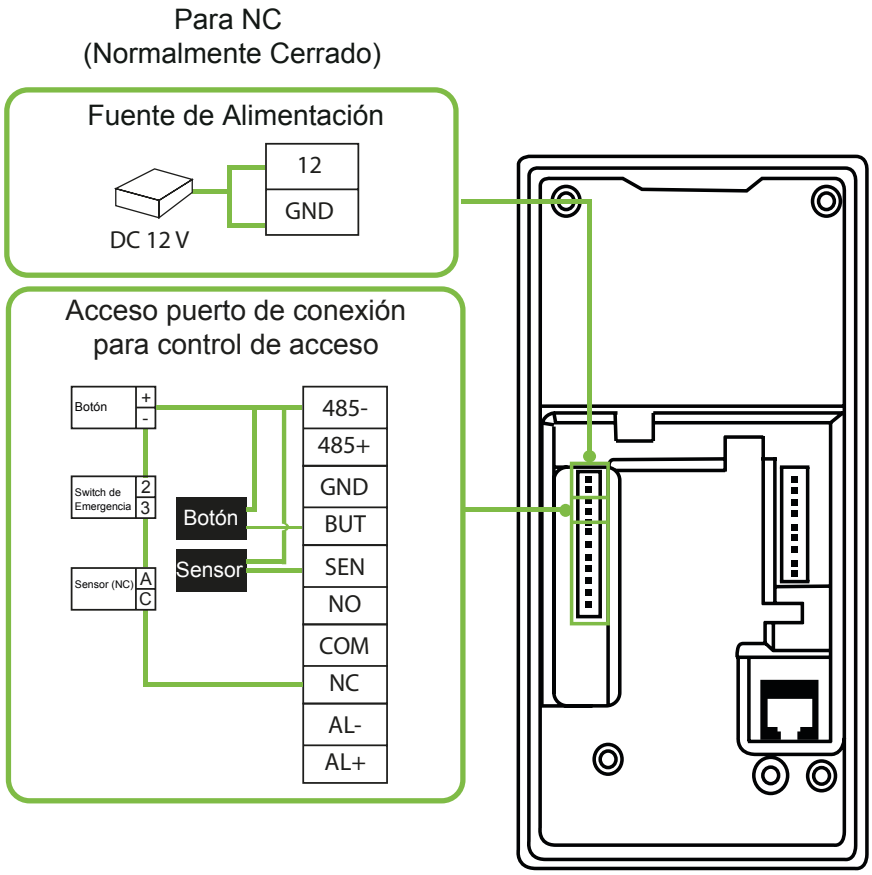
Artículo	Nota
Fuente de alimentación	12V 3A
Función	Dispositivo de control de acceso, estado de la puerta / alarma / bloqueo / interruptor de control de acceso
	Una entrada wiegand y una salida wiegand
Cantidad del usuario	10000 (Huella Digital y tarjeta ID)
Capacidad de registro	100000 Piezas de registros
Capacidad de matrícula (huella dactilar y tarjeta)	1500 huellas digitales / 10000 tarjetas
Modo de verificación	Tarjeta de identificación (Mifare), huella dactilar
Comunicaciones	TCP/IP, RS485, U-disk
Altavoz	Mensaje de voz
LED	Indicación bicolor (rojo/verde)
Teclado	Claves válidas:0-9, Enter Esc

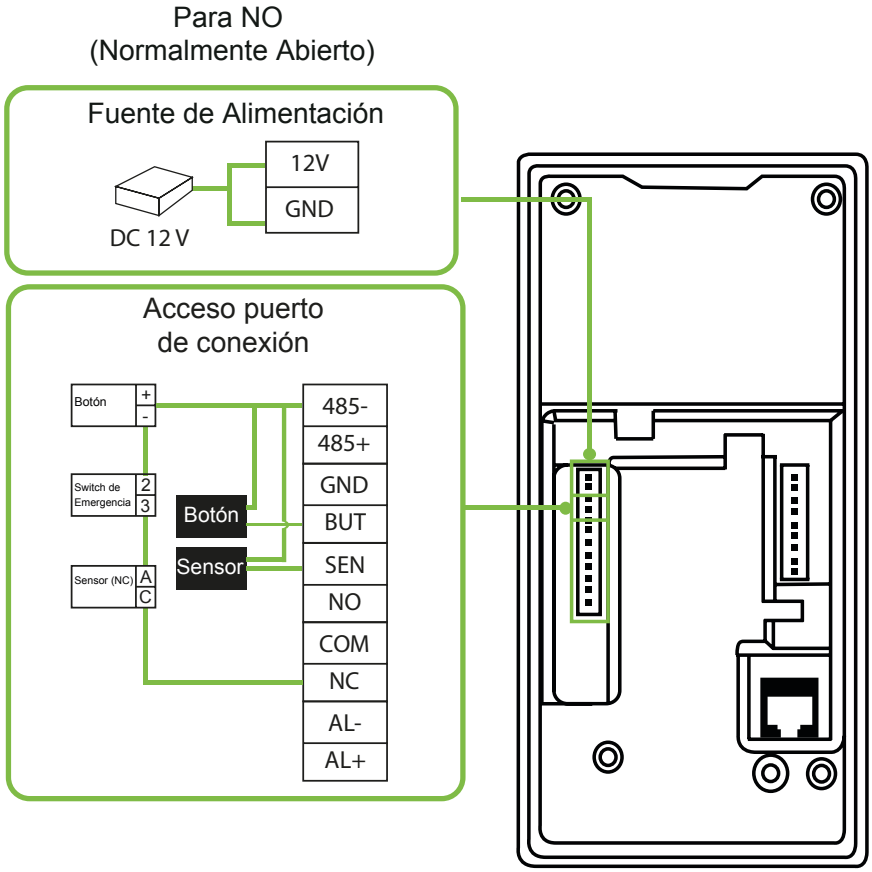
4.2 Diagrama de cableado: power & comms.

Diagrama de cableado para la conexión de puntos de alimentación y comunicación

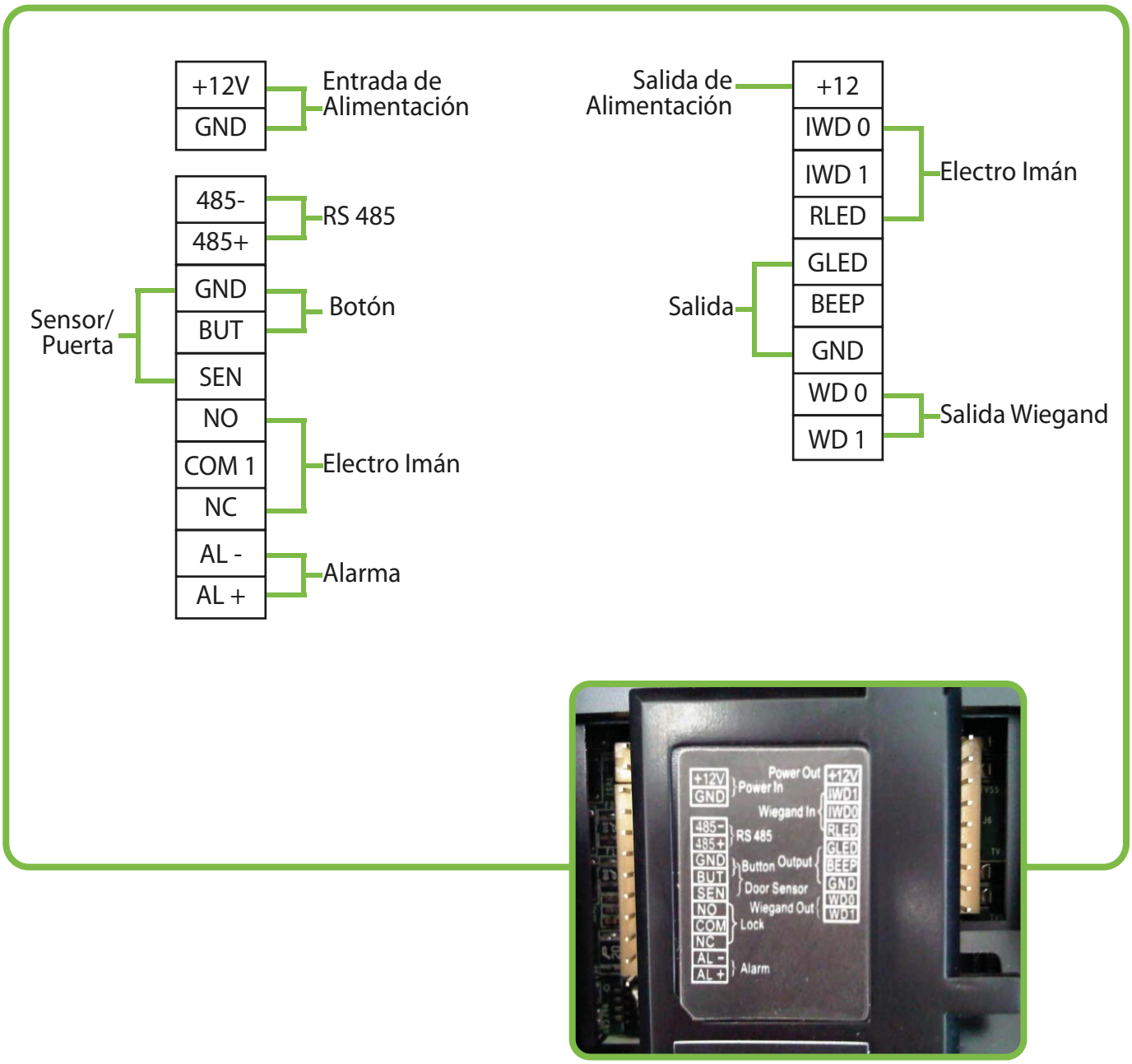


4.3 Diagrama de cableado: Normalmente Abierto y Normalmente Cerrado





Plugs de Salida del MA300



4.4 Descripción del uso inocuo para el medio ambiente

El período de uso inocuo para el medio ambiente (EFUP), marcado en este producto, se refiere al periodo seguro de tiempo, en el cual el producto es usado bajo las condiciones especificadas en las instrucciones, sin fugas de sustancias nocivas o peligrosas.
El EFUP de este producto no cubre a las partes consumibles que necesitan ser reemplazadas con regularidad como baterías y similares. El EFUP de las baterías es 5 años.

Nombres y concentración de sustancias y elementos tóxicos o peligrosos						
Nombre de la parte	Sustancias y elementos tóxicos o peligrosos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	x	o	o	o	o	o
Chip capacitor	x	o	o	o	o	o
Chip inductor	x	o	o	o	o	o
Chip diodo	x	o	o	o	o	o
ESD componentes	x	o	o	o	o	o
Sirena	x	o	o	o	o	o
Adaptador	x	o	o	o	o	o
Tornillos	o	o	o	x	o	o

o: Indica que esta sustancia peligrosa o tóxica, contenida en todos los materiales homogéneos para esta parte, está por debajo de los límites planteados en SJ/T11363-2006.

x: Indica que esta sustancia peligrosa o tóxica, contenida en al menos uno de los materiales homogéneos para esta parte, está por encima del límite requerido en SJ/T11363-2006.

Nota: 80% de las partes de este product o están fabricadas con materiales no peligrosos y amigables con el medio ambiente. Las sustancias o elementos peligrosos presentes no pueden ser reemplazadas, con materiales inocuos para el medio ambiente, en el presente y debido a limitaciones económicas o técnicas.

German Centre 3-2-02, Av. Santa Fe No. 170, Lomas de Santa Fe,
Delegación Alvaro Obregón, 01210 México D.F.
Tel: +52 (55) 52-92-84-18
www.zktecolatinoamerica.com
www.zkteco.com

Derechos de Autor © 2016, ZKTeco CO, LTD. Todos los derechos reservados.
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.
El logo ZKTeco y la marca son propiedad de ZKTeco Inc.