Manual de Usuario

BIOPROX 700-BT

Version: 1.0

Abril 2018

Anotaciones

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

• Información importante, incluidas todas las precauciones, que deben ser leídas cuidadosamente para
obtener el óptimo rendimiento 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.

Introducción

BIOPROX 700-BT es un terminal autónomo biometrico para instalación en exterior, que permite la gestión de control de acceso a través de verificación por huella y/o tarjeta de proximidad. Incorpora un sistema guiado por voz para facilitar las operaciones y además permite la apertura de accesos a través de un smartphone (APP) vía Bluetooth 4.0

Para el uso y gestión de la APP consultar el manual de usuario de BIOBT.

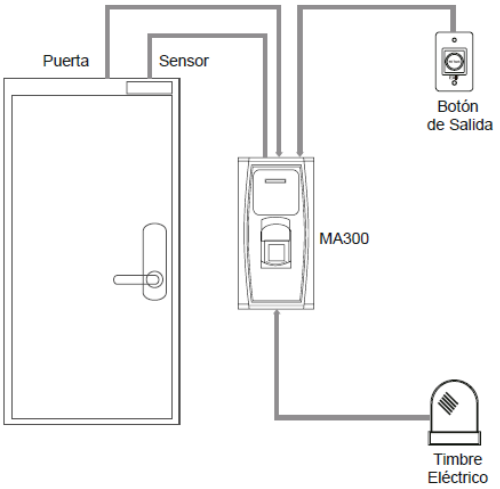
Desde GOLMAR, Le agradecemos que haya escogido y confiado en nuestro producto.

ÍNDICE

1. ESTRUCTURA Y FUNCIONES

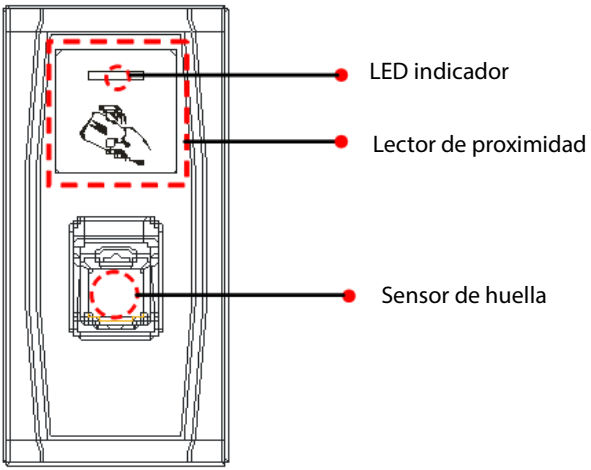
1.1 Funciones del sistema de control de acceso:

1. Cuando se verifica un usuario registrado, el terminal enviará una señal para realizar la apertura de puerta.
2. El sensor de puerta detectará el estado de la cerradura, si esta fuera forzada o quedase mal cerrada, se generaría una señal de alarma**(opcional)**
3. Soporta un pulsador interno de salida para la apertura de puerta.
4. Puede añadirse un dispositivo externo que se activa a través de una segunda salida de relé.

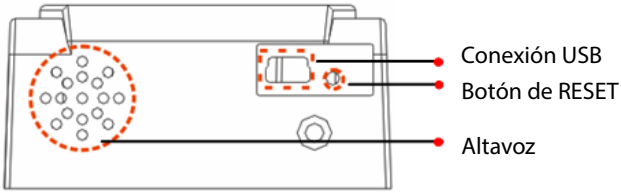


1.2 Apariencia del equipo

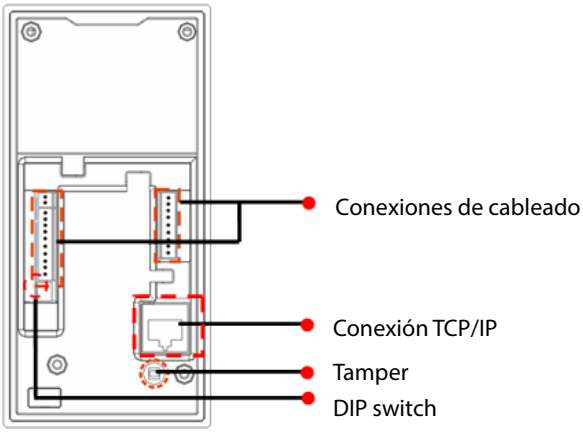
1. Vista frontal



2. Vista inferior:

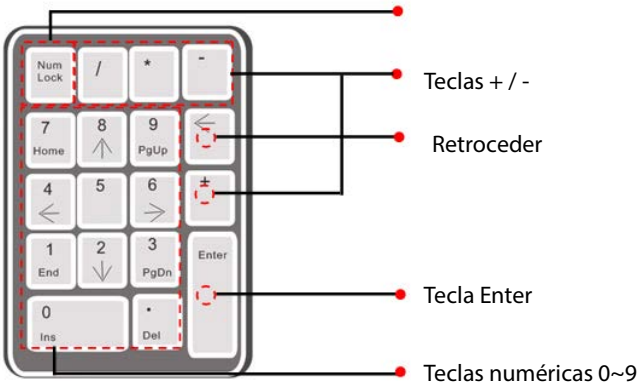


3. Vista trasera:



1.3 Uso de un teclado externo USB

Para facilitar las operaciones de usuario es posible usar un teclado USB externo al terminal. Para activarlo será necesario pulsar la Tecla **Num Lock** una vez lo hayamos conectado.



2 INSTRUCCIONES DE PUESTA EN MARCHA

1. Conectar el equipo a la corriente eléctrica una vez montado y con todas las conexiones realizadas. Tras 20-30 segundos, el terminal emite un beep corto y el led de estado parpadea en verde y se genera la locución **"por favor,registre la tarjeta de administrador"**
2. Registrar el administrador del terminal **(Ver Gestión del administrador)**
3. Añadir usuarios al terminal **(Ver añadir/editar usuarios)**
4. Configurar el resto de parámetros del terminal según se precise.

3. GESTION DEL ADMINISTRADOR

Para poder gestionar los parámetros de control de accesos, así como añadir usuarios y poder vincular smartphones al terminal, es necesario crear un administrador.

3.1 Como crear un administrador

1. Una vez conectado el terminal esperar 30 segundos
2. El terminal emite un beep corto y el led de estado parpadea en verde y se genera la locución **"Por favor,registre la tarjeta de administrador"**
3. Pasar la tarjeta o llavero negro (incluido)
4. El terminal genera una locución **"Proceso de registro correcto,el terminal vuelve a modo de verificación"**

Nota: La tarjeta o llavero de adminitrador puede ser una tarjeta de tipo ID que trabaje con frecuencia de 125Khz (Prokey-Tagkey).

3.2 Como cambiar o borrar el administrador

Si se tuviera que cambiar o borrar el administrador del terminal, hemos de hacerlo a través del teclado USB.

Tambien es posible usar el terminal a través de teclado USB (en caso de perder la tarjeta de administrador) para ello,se ha de haber registrado primero el mismo a través de la tarjeta de administrador.

El teclado puede protegerse con una contraseña para reforzar la seguridad.

3.3 Password del sistema

Esta contraseña se utiliza para proteger al dispositivo, en el caso de estar conectado en una red ya sea por TCP/IP o RS485.

Dicha contraseña se establece a través del software ZKACCESS 3.5

3.4 Tiempo de operación

El tiempo de operación es de 30 segundos.Si no se realiza ninguna acción, el sistema regresa a modo de verificación (reposo) Cuando el tiempo transcurre se genera la locución **“Excedido el tiempo para esta operación, el sistema vuelve a modo de verificación”**

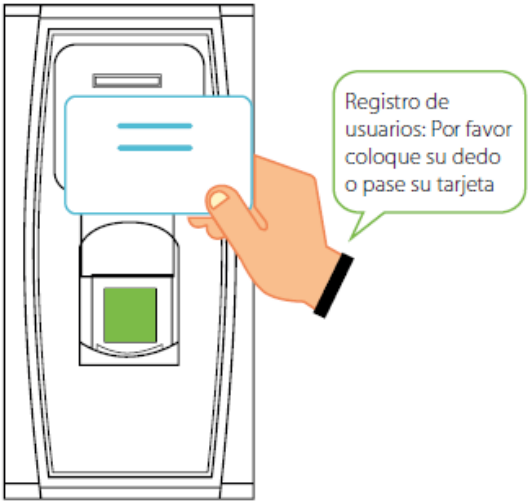
Este tiempo se puede modificar a través del software ZKACCESS 3.5

4. AÑADIR /EDITAR USUARIOS

4.1 Registrar un usuario

1. Con el terminal en modo de verificación (Reposo) pasar la tarjeta de administrador.
2. Se genera la locución **“Registro de usuarios, por favor, coloque su dedo o acerque su tarjeta”**
3. En el caso de querer introducir una huella, poner el dedo en el sensor. El terminal emite 1 beep y se genera la locución **“por favor, coloque su dedo de nuevo”**
4. Volver a poner el dedo en el sensor por segunda vez, el terminal emite 1 beep y se genera la locución **“por favor, coloque su dedo por última vez”**
5. Volver a poner el dedo en el sensor por tercera vez, el terminal emite 1 beep y se genera la locución **“Número de usuario (2),proceso de registro correcto” Registrar, por favor, coloque su dedo o acerque su tarjeta”**
6. Si se desea grabar otra huella, volver a repetir los pasos **de 3 a 5.** Cuando se registre una segunda huella, el terminal emite la locución **“Proceso de registro correcto” por favor coloque su dedo o acerque su tarjeta.**
7. En caso de querer registrar una tarjeta,cuando el terminal emita la locución **“Registro de usuarios,por favor, coloque su dedo o acerque su tarjeta”**
   pasar la tarjeta una sola vez por el lector, el terminal emite un beep y se genera la locución **“Número de usuario (X),proceso de registro correcto” Registrar, por favor, coloque su dedo”**

8. Si se desea cambiar de usuario para registrar,pasar la tarjeta de administrador.**El terminal emite la locución "El sistema vuelve a modo de verificación". A continuación volver a pasar la tarjeta de administrador y el terminal emitirá la locución: "Registro de usuarios, por favor, coloque su dedo o acerque su tarjeta".En ese momento, se puede pasar la huella o tarjeta del nuevo usuario.**
9. Para salir del menú y volver al modo de verificación (reposo) pasar la tarjeta de administrador, el terminal emite un beep y se genera la locución **"El sistema vuelve a modo de verificación"**



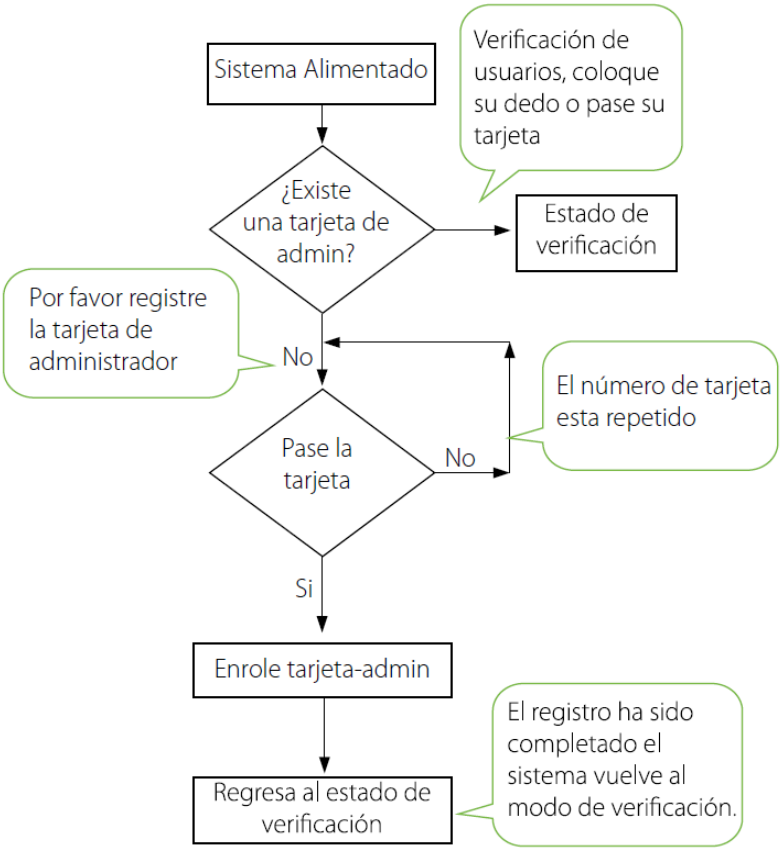
Notas:

1.Cada usuario puede grabar hasta 10 huellas distintas y 1 tarjeta. Si la huella a grabar o tarjeta ya existiera, el terminal genera la locución ”Huella duplicada” en caso de la tarjeta “la tarjeta ha sido registrada”

2.El sistema volverá al modo de verificación si el usuario registra 10 huellas y 1 tarjeta.

3.El usuario 1 por defecto, es el administrador, al tener la tarjeta del mismo ya registrada, solo tendremos la opción de añadir huellas para este.Esta operación solo se puede hacer a través de teclado USB.

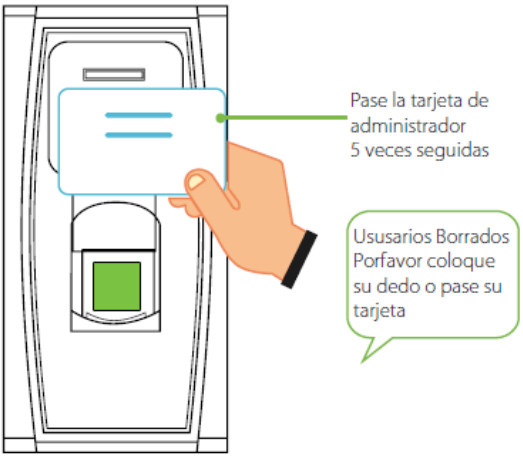
Tabla de como enrolar una tarjeta de administrador:



5. BORRAR USUARIO

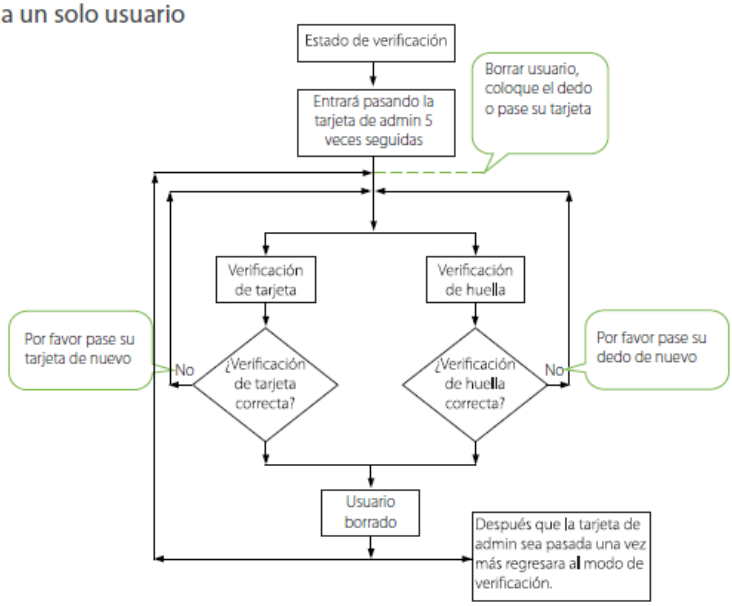
5.1.Borrar usuario

1. Pasar la tarjeta de administrador 5 veces seguidas.
2. El terminal emite un beep largo y genera la locución **“Borrado de usuarios, por favor coloque su dedo o acerque su tarjeta.**
3. Pasar la tarjeta, o huella por el lector correspondiente.
4. El terminal emite un beep largo y genera la locución **“Borrado de usuario,correcto”**
5. En caso de error, el terminal genera la locución **“Por favor, intente de nuevo o pase de nuevo la tarjeta”**
6. Para borrar otro usuario, pasar la tarjeta de administrador, el terminal emite la locución,**“Borrado de usuarios, por favor coloque su dedo o acerque su tarjeta.**
7. Repetir el paso 3.



Nota: Si el usuario dispone de mas de una huella, al borrar una de ellas, las demás tambien se borran de forma automática,así como las tarjetas.

Tabla para borrar a un solo usuario

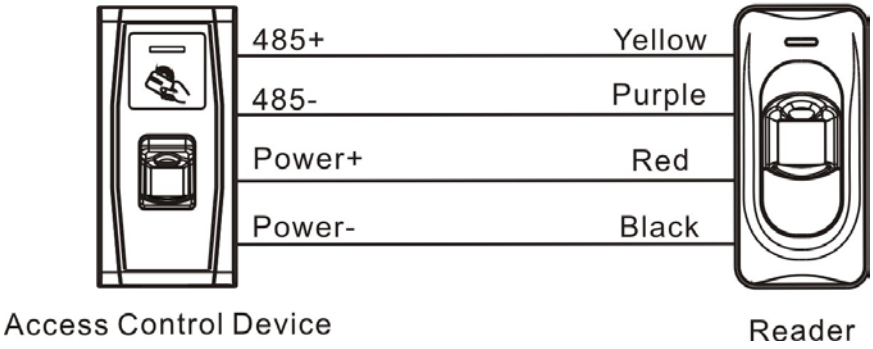


6.FUNCION RS485 PARA AÑADIR LECTOR BIOMETRICO ESCLAVO

Es posible añadir un lector biometrico modelo (FR1200) como lector esclavo del BIOPROX 700BT a través de comunicación por RS485.

1. En estado de verificación, pasar la tarjeta de administrador 7 veces.
2. Si el terminal emite un beep,la comunicación por RS485 con lector esclavo se deshabilita.
3. Si el terminal emite 2 beeps, la comunicación por RS485 con lector esclavo se habilita.

4. Para intercambiar el proceso de activar / desactivar la comunicación pasar la tarjeta de administrador 7 veces.
5. Una vez habilitada la comunicación, reiniciar el dispositivo.
6. Realizar las conexiones según esquema. **(Los GND deben unificarse para asegurar la correcta comunicación)**



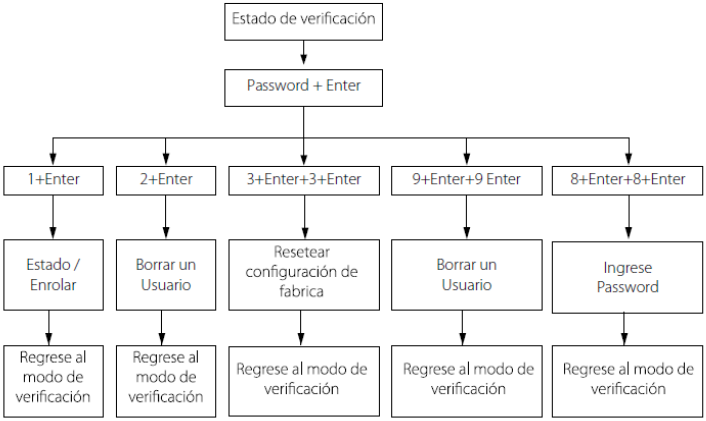
7. OPERACIONES CON EL TECLADO USB

El terminal BIOPROX 700BT puede gestionarse con un teclado USB externo **(No incluido)** Para conectar el teclado al terminal, usar el cable **USB TipoA-Hembra/Mini- USB** de color gris incluido con el mismo.

El interfaz de conexión para el cable está en la parte inferior derecha del terminal protegido por una tapa de goma.

A continuación se muestra una tabla con las operaciones que se pueden efectuar con el teclado.

Tabla de operaciones con teclado



7.1 Añadir/modificar contraseña de acceso al teclado

1. Conectar el teclado al terminal y pulsar la tecla **Num.lock para activar las teclas.**
2. Pasar la tarjeta del administrador. El terminal emite un beep y genera la locución **"Pulse el teclado,por favor"**
3. Ahora debemos fijar la contraseña de acceso para el teclado.
4. Pulsamos **8 + enter (2 veces)** el terminal genera la locución **"Por favor, establezca una clave de acceso"**
5. Marcamos la contraseña deseada **(entre 4 y 6 dígitos)** y pulsamos **Enter.**
6. El terminal emite la locución **"Operación correcta,el sistema vuelve a modo de verificación)**
7. Una vez establecida la clave,no es necesario usar la tarjeta de administración para acceder a la gestión del terminal. Con el teclado conectado, introducir la **clave + Enter** y se emite la locución: **Confirmación de clave de acceso correcta y ya podemos operar el terminal con el teclado.**

7.2 Añadir usuarios con el teclado

1. Introducir **contraseña + Enter**
2. El terminal emite la locución "**Confirmación de clave de acceso correcta"**
3. Pulsar **1+Enter**
4. El terminal emite la locución **"Registro de usuarios, por favor introduzca número de usuario"**
5. Introducir **número de usuario(1,2,3,4…) + Enter**
6. Se genera la locución **"Nº de usuario (x),registro de usuarios, por favor, coloque su dedo o acerque su tarjeta"**
7. **(El usuario 1 por defecto, es el administrador, al tener la tarjeta del mismo ya registrada, solo tendremos la opción de añadir huellas para este) Con lo que la locución del terminal será: "Nº de usuario (1),registro de usuarios, por favor, coloque su dedo"**
8. En el caso de querer introducir una huella, poner el dedo en el sensor. El terminal emite 1 beep y se genera la locución **"por favor, coloque su dedo de nuevo"**
9. Volver a poner el dedo en el sensor por segunda vez, el terminal emite 1 beep y se genera la locución **"por favor, coloque su dedo por última vez"**
10. Volver a poner el dedo en el sensor por tercera vez, el terminal emite 1 beep y se genera la locución **"Número de usuario (X),proceso de registro correcto" Registrar, por favor, coloque su dedo o acerque su tarjeta"**
11. Si se desea grabar otra huella, volver a repetir los pasos de 3 a 5. Cuando se registre una segunda huella, el terminal emite la locución **"Proceso de registro correcto" por favor coloque su dedo o acerque su tarjeta.**

12. En caso de querer registrar una tarjeta,cuando el terminal emita la locución **“Registro de usuarios,por favor, coloque su dedo o acerque su tarjeta”**
13. Pasar la tarjeta una sola vez por el lector, el terminal emite un beep y se genera la locución **“Número de usuario (X),proceso de registro correcto” Registrar, por favor, coloque su dedo”**
14. Si se desea cambiar de usuario para registrar,pulsar la tecla **Back Space/Esc (1 vez) El terminal emite la locución “Registro de usuarios, por favor introduzca número de usuario”**
15. Para salir del menú y volver al modo de verificación (reposo) pulsar **Back Space/Esc (2 veces)**

7.3.Borrar usuarios con el teclado

1. Introducir **contraseña + Enter**
2. El terminal emite la locución “**Confirmación de clave de acceso correcta”**
3. Pulsar **2+Enter**
4. El terminal emite la locución **“Borrado de usuarios, por favor introduzca número de usuario”**
5. Introducir **número de usuario(1,2,3,4…) + Enter**
6. Se genera la locución **“Nº de usuario (x),borrado correcto.**
7. Esta operación borra tanto las huellas como las tarjetas.
8. Para borrar otro usuario, pulsar **Back Space/Esc (1 vez),el terminal emite la locución“Borrado de usuarios, por favor introduzca número de usuario”**
9. Repetir el paso 5.

10. Para salir del menú y volver al modo de verificación (reposo) pulsar **Back Space/Esc (2 veces)**

7.4.Restablecer valores de fábrica

1. Introducir contraseña + Enter
2. El terminal emite la locución "**Confirmación de clave de acceso correcta"**
3. Pulsar 3+Enter **(2 veces)**
4. El terminal emite la locución **"Restaurar terminal con configuración por defecto,operación correcta, el sistema vuelve a modo de verificación.**
5. Los usuarios registrados no se borran en este proceso, ni tampoco la tarjeta de administrador. Si que se pierde la contraseña de acceso del teclado USB.

7.5 Borrado completo del terminal

1. Introducir contraseña + Enter
2. El terminal emite la locución "**Confirmación de clave de acceso correcta"**
3. Pulsar 9+Enter **(2 veces)**
4. El terminal emite la locución **"Borrar todos los usuarios,operación correcta, el sistema vuelve a modo de verificación.**
5. El terminal volverá a estado de reposo y genera la locución **"Por favor, registre la tarjeta de administrador"**
6. Todos los usuarios registrados,incluido el administrador,se borran en este proceso,tambien se pierde la contraseña de acceso del teclado USB.

8. USO DE LA MEMORIA USB

El terminal admite una memoria USB, la cual se conecta a través del cable **USB TipoA-Hembra/Mini- USB** de color gris incluido con el mismo.

El usuario puede descargar fichajes y usuarios asi como importar los usuarios y actualizar el Firmware.

El menú de gestión de la memoria USB se compone de 4 opciones: **Descarga de fichajes, descarga de usuarios, carga de usuarios y actualización de Firmware.**

Para activar la memoria USB una vez conectada,esperar 10 segundos y pasar la tarjeta de administrador, se genera la locución **"descarga de fichajes,por favor acerque la tarjeta de administración para confirmación"**

Si no acercamos la tarjeta, el terminal pasará de forma automática al siguiente menú, generando la locución **descarga de usuarios,por favor acerque la tarjeta de administración para confirmación"**

Una vez el terminal haya efectuado las 4 opciones del menú, si no se pasa la tarjeta de administrador, volverá a modo de verificación (reposo)

Para confirmar la opción del menú que queramos usar, pasar la tarjeta de administrador y el terminal generará la locución **"operación correcta"**y pasará al siguiente menú hasta finalizar.

Nota: Los archivos que se almacenan en la memoria USB son de extension.dat

Es recomendable emplear memorias USB de un máximo de 8 GB

Las actualizaciones de Firmware, no deben hacerse a discreción ya que esto puede causar un daño irreversible al terminal,pues el Firmware está diseñado para cada equipo de forma específica.

9. BOTÓN DE SABOTAJE (TAMPER)

El botón de sabotaje del terminal, consiste en un imán alojado en la parte posterior del mismo y fijado a la chapa metálica.

Este mecanismo tiene como finalidad 2 usos.

1.Reconocer una alarma: Si se intenta desmontar el terminal de la pared, se genera una señal de alarma, la cual puede ser reproducida por una sirena, conectada al mismo terminal.

2.Restaurar los valores de fábrica: Con el terminal alimentado,abrir la parte posterior y separar el imán junto con la tapa metélica del mismo, se escuchará un "click" conforme se activa la señal de alarma.

Esperar 30 segundos, acercar y separar el imán 3 veces. (Tras cada acercamiento y separación se ha de escuchar un beep). Una vez se produzca el tercer beep, el terminal se reinicia.

Nota:Este reset elimina,el número de terminal,contraseña del teclado y contraseña de comunicación, dirección IP y RS485.

Este proceso no elimina los usuarios ni el administrador, este proceso se ha de hacer de forma manual.

10. APÉNDICE

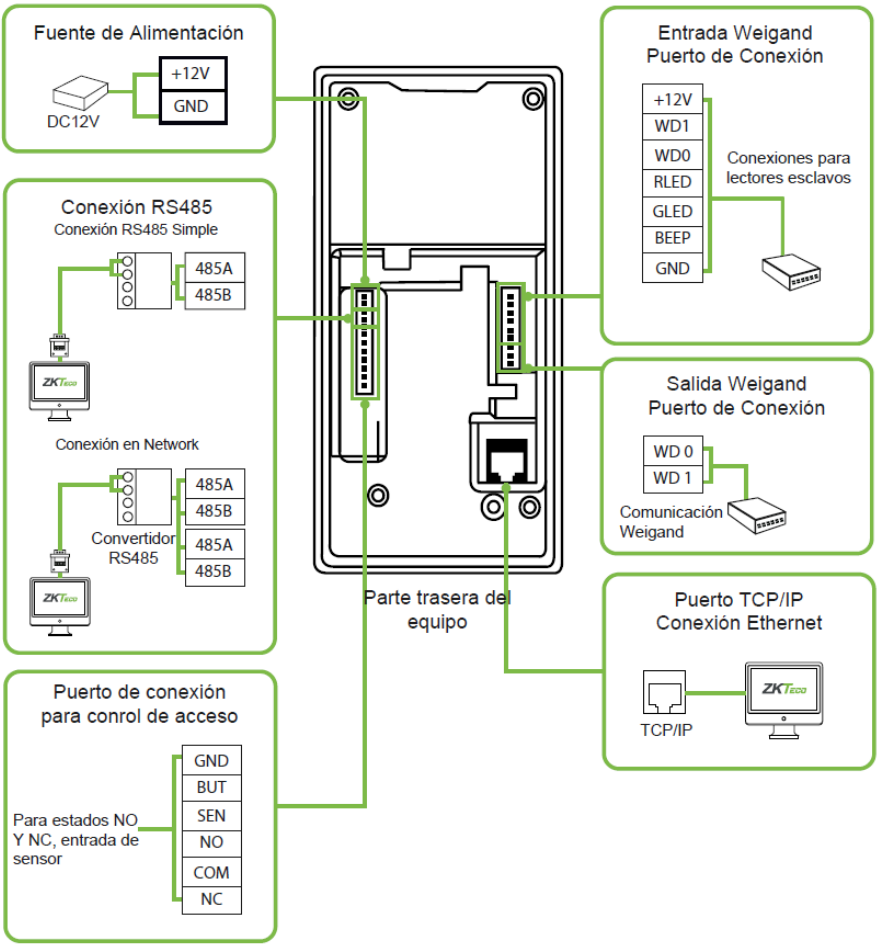
10.1 Características Técnicas

En la tabla siguiente se muestran las carácteristicas técnicas del terminal

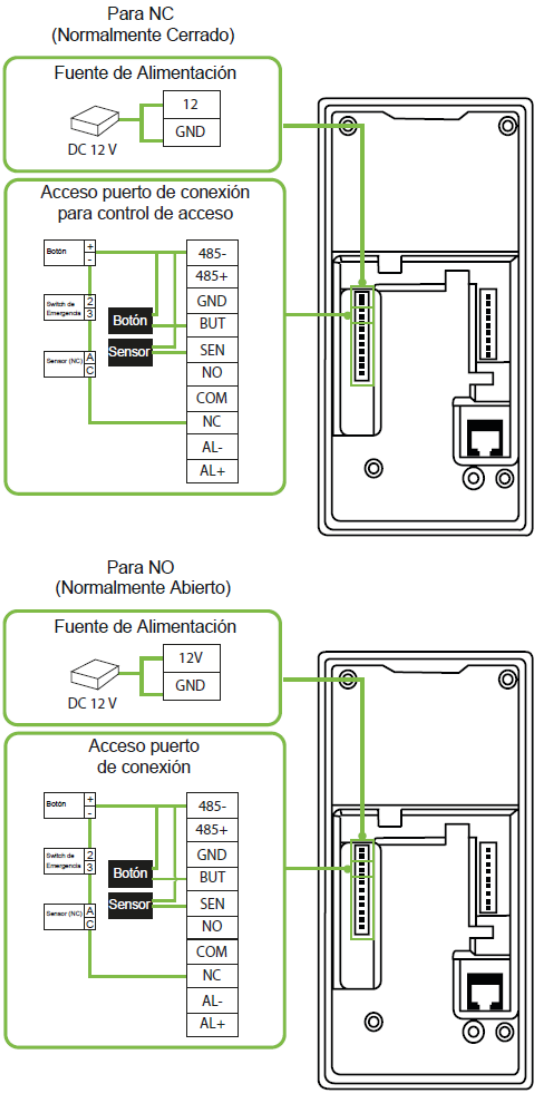
Alimentación	12V 3A
Función	Control de acceso, estado de puerta/alarma/bloqueo/pulsador de control de acceso
	1 entrada Wiegand y 1 salida Wiegand
Usuarios	10000 (Huella o tarjeta)
Registros	Hasta 100000
Capacidad (huellas/tarjetas)	1500 Huellas /10000 tarjetas
Modo de verificacion	Tarjeta (Mifare) o huella
Communicaciones	TCP/IP, RS485, USB
Altavoz	Mensaje de voz
LED	Bi-color (rojo/verde)
Teclado	Teclas válidas: 0-9, Enter, Esc.

10.2 Diagrama de conexiones 1

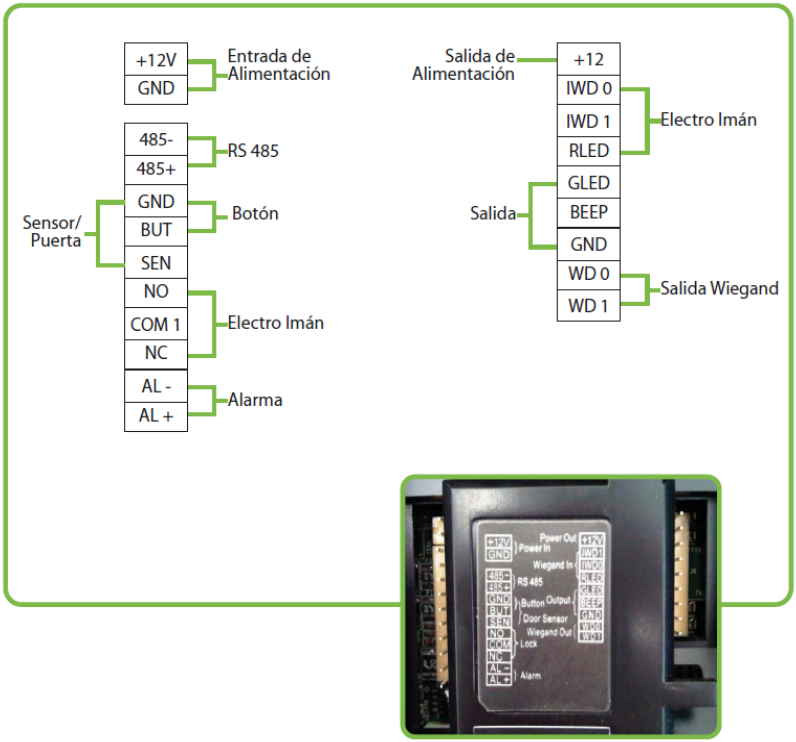
Diagrama de cableado para la conexión de puntos de alimentación y comunicación



10.3 Diagrama de conexiones 2



10.4 Diagrama de conexiones 3



10.5 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.

Golmar Sistemas de Comunicación S.A.

Silici, 13
Polígono Industrial Famades
08940 Cornellá de Llobregat
Barcelona, España

Teléfono y Fax

Teléfono: 902 511 910
Fax: 905 511 960

Online

Email: golmar@golmar.es
Web: golmar.es