ZKTeco

# MANUAL DE USUARIO

## ProBio & ProFAC
## Dispositivos de Control de Acceso

Green Label

# Acerca de este manual

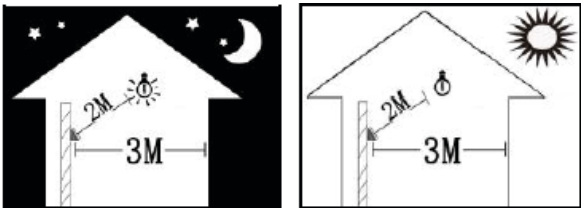
- Este documento describe las funciones del menú, y la interfaz de usuario de la serie de productos  con reconocimiento facial. Las funciones marcadas con * son opcionales en algunos dispositivos.
- Para obtener información no consignada en este documento, por favor consulte el manual de instalación, la guía rápida o al personal técnico de su región.

# Contenido

# Notas de Orientación

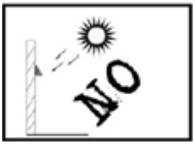
## 1.1 Funcionamiento del Dispositivo

**1) Posición recomendada de Instalación:**

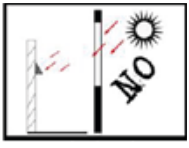



✓Posición de instalación recomendada (como se muestra en la figura de la izquierda): Instalar el dispositivo en el interior, que esté a tres metros de la ventana y la puerta, y dos metros lejos de la lámpara, con iluminación ambiental de 0 ~ 800 LUX.

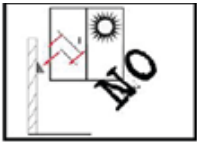
**2) Diferentes posiciones que afectan su funcionamiento:**



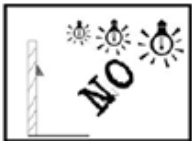

La exposición cercana a la luz de la lámpara (Interior)




Luz solar directa (Al aire libre)




La luz del sol oblicua a través de la ventana (Interior)




La luz solar directa a través de la ventana (Interior)

**Nota:** El valor de la iluminación ambiental como referencia es de 0~800 LUX.

10 Lux

Mas de 1200 Lux

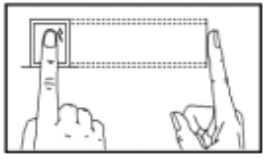

50-800 Lux

# Notas de Orientación

## 1.2 Método para colocar la huella digital.

Es recomendable utilizar el dedo índice, dedo medio, o dedo anular, evitar el uso del dedo pulgar o del meñique.

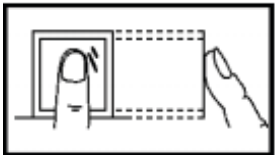
**1. Forma correcta de colocar la huella digital:**



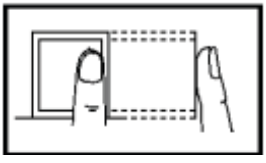
Presione el dedo horizontalmente en el sensor de huellas digitales; el centro de la huella digital se debe colocar en el centro del sensor.

**2. Formas incorrectas de colocar la huella digital:**

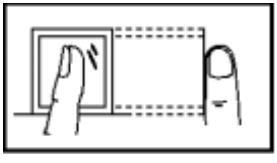
Vertical



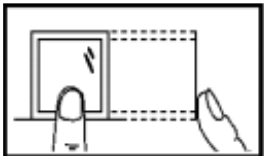
A los lados



Inclinado



Demasiado abajo



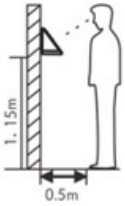
Utilice el método correcto para colocar las huellas digitales para el registro y la verificación. Nuestra empresa no asume la responsabilidad por el mal desempeño de la verificación causado por la operación incorrecta del usuario. Los derechos a la interpretación final y modificación están reservados.

# Notas de Orientación

## 1.3 Precauciones para el uso del dispositivo de reconocimiento facial

### 1. Recomendación de la ubicación

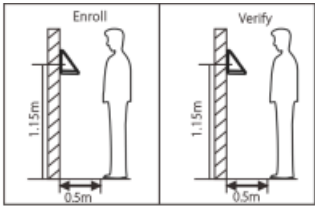
Para usuarios con alturas entre 1.80 m y 1.50 m, se recomienda instalar el dispositivo a 1.15 m por encima del suelo (puede ser modificado de acuerdo a la altura de cada usuario).



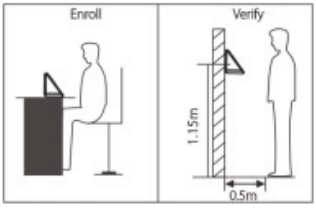

### Posición recomendada para el registro y la verificación

Procedimientos recomendados (como se muestra en la imagen de la derecha):

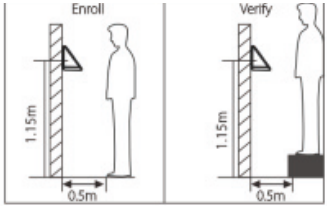
Durante los procedimientos de registro y verificación, la posición del dispositivo no se debe cambiar para evitarla mala precisión de la verificación. Si es necesario puede mover el dispositivo, pero su altura vertical no debe ser cambiada.




### Factores que afectan la precisión de la verificación Posición recomendada para el registro y la verificación

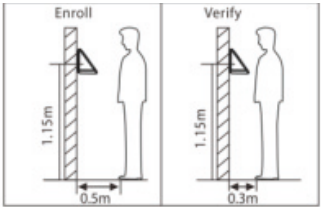



Posturas diferentes de registro y verificación

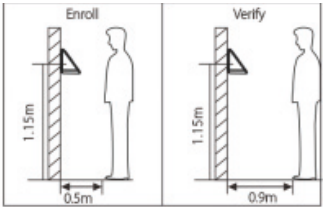



Alturas diferentes de registro y verificación

# Notas de Orientación

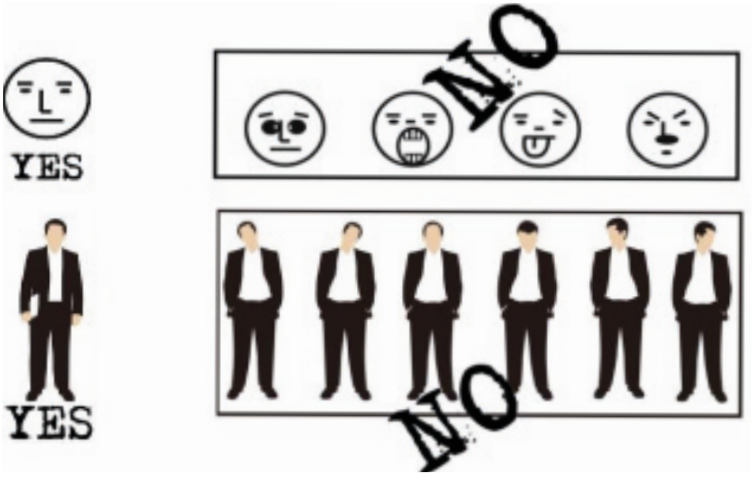



Posturas diferentes de registro y verificación




Distancias diferentes de registro y verificación

**2. Expresiones faciales y postura**




**Nota:** Durante el registro y la verificación, mantenga una expresión y una postura natural.

# Notas de Orientación

**3. Registro y Verificación**

a. Durante el registro, se requiere ajustar la parte superior del cuerpo para colocar de forma correcta los ojos en el recuadro verde de la pantalla.

b. Durante la verificación, se requiere colocar su rostro en el centro de la pantalla y ajustar su cara en el marco verde.

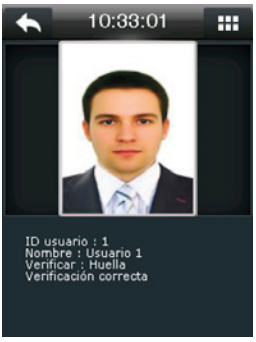
## 1.4 Modos de Verificación

### 1.4.1 Verificación de huellas digitales 1:N

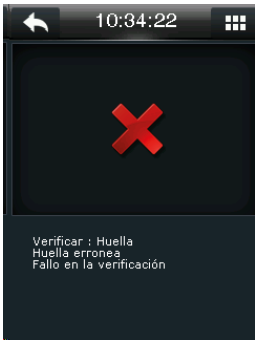
En el método de verificación de huellas digitales 1:N, la huella digital que es leida por el sensor, se verifica con todas las huellas digitales almacenadas en el dispositivo.

**Nota:** Utilice el modo correcto para colocar la huella digital en el sensor (para obtener instrucciones detalladas, consulte 1.2 Método para colocar la huella digital)

# Notas de Orientación




Verificación exitosa

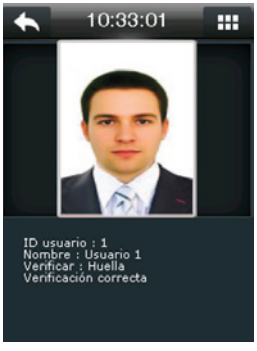



Verificación fallida

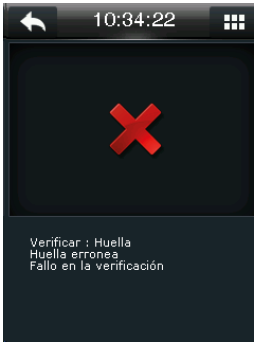
### 1.4.2 Verificación de huellas digitales 1:1

Bajo este método de verificación de huellas digitales, la huella digital que es leida por el sensor, se verifica con la huella digital correspondiente a la del ID del usuario introducido. Por favor, use este método cuando se encuentren dificultades con la identificación 1:N


Pulse para introducir el ID de usuario y ponga la huella digital




Verificación exitosa




Verificación fallida

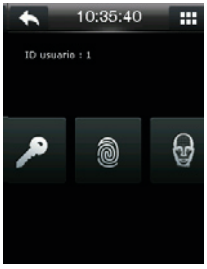
# Notas de Orientación

**Nota:** Cuando el dispositivo muestra "por favor presione el dedo nuevamente" coloque de nuevo el dedo en el sensor de huellas digitales. Si la verificación falla aún después de dos intentos, volverá a la interfaz inicial

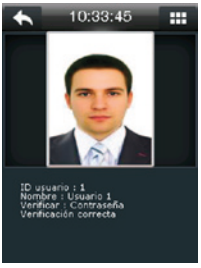
### 1.4.3 Verificación con contraseña

En este método de verificación, la contraseña introducida se verifica con la contraseña del ID de usuario introducido.

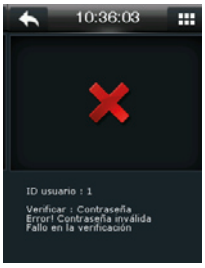

Pulse para introducir el ID de usuario




Pulse el icono de la llave para introducir la contraseña




Verificación exitosa

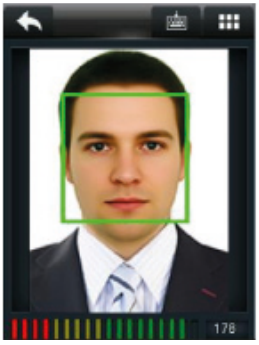



Verificación fallida

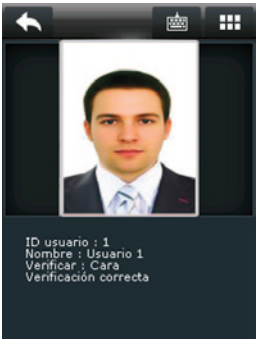
### 1.4.4 Verificación de asistencia con rostro 1:N

En este método, la imagen facial capturada por la cámara se compara con todos los datos faciales en el dispositivo.

# Notas de Orientación



Llevar a cabo la comparación de la forma correcta en la interfaz principal

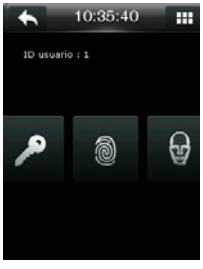



Verificación exitosa

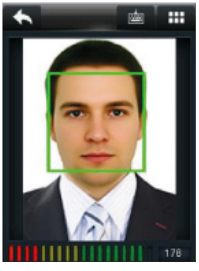
### 1.4.5 Verificación de asistencia con rostro 1:1

En este método, la imagen facial capturada se compara con la imagen facial asociada con el ID de usuario introducido.


Pulse para introducir el ID de usuario




Pulse el icono del rostro



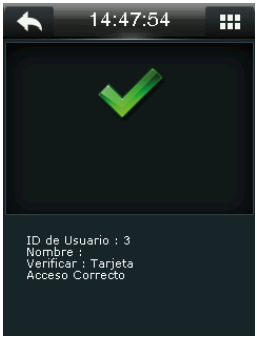
Comparación de rostros correcta

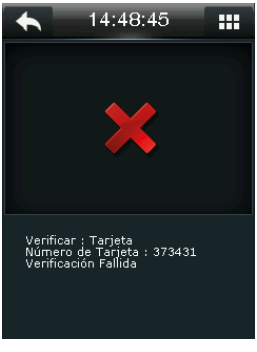

Verificación exitosa

### 1.4.6 Verificación de tarjeta

**Nota:** La función de la tarjeta es opcional, solamente los productos con un módulo de tarjeta incorporado incluyen función de verificación con tarjeta. Por favor pónganse en contacto con soporte técnico si lo necesita.

1. Deslice la tarjeta por encima del lector de tarjetas (la tarjeta debe estar registrada)
2. Verificación exitosa
3. Verificación fallida




## 1.5 Interfaz Inicial

# Notas de Orientación

**1. Fecha y hora:** Se muestra la fecha actual del dispositivo: 1. Fecha y hora.

**2. Timbre:** Hay una alarma establecida para el dispositivo si aparece este icono.

**3. Conexión de red:** Se muestra el estado de la conexión de red del dispositivo.

**4. Alarma tamper:** El botón de alarma de sabotaje depende si aparece este icono, y la posible causa es "una instalación incorrecta" o "desmontaje ilegal".

**5. Entrada auxiliar:** Este icono aparece cuando el terminal de entrada auxiliar del dispositivo está conectado a un dispositivo auxiliar.

**6. Tiempo:** Se muestra la hora actual del dispositivo. Los formatos 12 horas y 24 horas son compatibles. Los usuarios pueden personalizar el estilo de la interfaz principal. Para más detalles, consulte Personalizar opciones 8.

**7. Menú:** Pulse este icono para acceder al menú principal. Si los administradores se establecen para el dispositivo, debe pasar la verificación del administrador antes de acceder al menú principal.

**8. Verificación 1: 1 (teclado en pantalla):** Pulse la tecla para entrar en la interfaz para introducir un ID de usuario en modo de verificación 1: 1. Después de introducir un ID de usuario, pulse [OK] y continuar la relación de verificación 1: 1 de acuerdo a las indicaciones que aparecen en la interfaz.

# Menú Principal




**Gestión de usuarios:** Para gestionar la información básica de los usuarios registrados, incluyendo el ID de usuario, nombre de usuario, privilegio de usuario, huella digital, rostro, (ID y tarjetas MIFARE son opcionales), la contraseña y foto del usuario.

**Privilegio de usuario:** Para configurar los permisos de usuario para acceder al menú y cambiar los ajustes.

**Comunicación:** Para establecer los permisos relacionados para permitir la comunicación entre el dispositivo y la PC, incluyendo parámetros de Ethernet, tales como dirección IP, etc., comunicación serial, conexión para PC, ADMS y configuración Wiegand.

**Sistema:** Para establecer los parámetros relacionados con el sistema y actualizar el firmware, incluyendo ajustes de fecha y hora, los registros de acceso, los parámetros de del rostro, los parámetros de huellas digitales y restablecer la configuración de fábrica.

**Personalizar:** Esto incluye la visualización de la interfaz, la configuración de la voz y el sonido del timbre.

**Gestión de datos:** Para la eliminación de los datos incluidos los registros de acceso, privilegio de administrador, protectores de pantalla y así sucesivamente, hacer copias de seguridad y restaurar datos eliminados.

# Menú Principal

**Control de acceso:** Para establecer los parámetros de las cerraduras y de los dispositivos de control de acceso, incluidos reglas de tiempo, días de festivos, verificación combinada y antipassback.

**Gestión USB:** Para la transferencia de datos, tales como datos de usuario y los registros de acceso desde el puerto USB al software de apoyo u otros dispositivos.

**Asistente de búsqueda:** Para buscar los registros almacenados en el dispositivo después de la verificación exitosa.

**Pruebas:** Para probar automáticamente diferentes funciones del módulo, incluyendo la pantalla LCD, voz, sensor de huellas digitales, reloj, cámara.

**Sistema de Información:** Para comprobar la capacidad e información del dispositivo y del firmware.

# Configuración de Fecha/Hora




En la pantalla principal, pulse > **Sistema**> **Fecha/Hora** para ingresar a la interfaz de configuración de fecha/hora. Incluye formato de fecha, formato de hora 12/24 y horario de verano.

Al restablecer la configuración de fábrica, **el formato** de fecha puede ser restaurado de al siguiente formato: (AAAA-MM-DD).

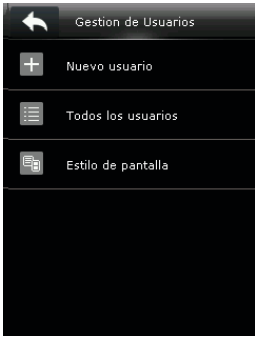
**Nota:**

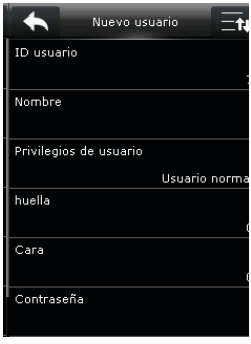
Al restablecer los ajustes de fábrica, no se restaurará la fecha/hora del dispositivo (si la fecha/hora se ajusta a 18:30 el 1 de enero de 2020, después que los ajustes se restablecen, la fecha / hora se quedará a las 18:30 en Enero 1, 2020.)

# Gestión de Usuarios

## 4.1 Agregar Usuarios

Incluyendo la adición de administrador y usuarios normales al dispositivo.


En la interfaz inicial, presione > **Gestión de Usuarios** >**Nuevo Usuario** para entrar en la interfaz de **Nuevo Usuario**. Los ajustes incluyen la introducción de ID de usuario, el nombre, la elección de privilegio de usuario (Administrador / Usuario normal), su registro de huellas digitales, rostro y número de identificación. (Tarjeta de identificación y MIFARE son opcionales), el establecimiento de contraseña, mostrar fotografía de usuario y asignación de su privilegio de acceso.

**Agregar un Administrador:** Elija "Administrador" en [**Privilegios de usuario**], quién está autorizado para operar todas las funciones en el menú.
Como se muestra a continuación, el usuario con el ID de usuario 1 es un administrador:

**Agregar a un usuario normal:** Elija "Usuario normal" en [Privilegios de usuario]. Cuando se establece el administrador, el resto de los usuarios sólo pueden utilizar la huella digital, contraseña o tarjeta para la verificación; cuando el administrador aún no está establecido, los usuarios normales pueden operar todas las funciones en el menú.

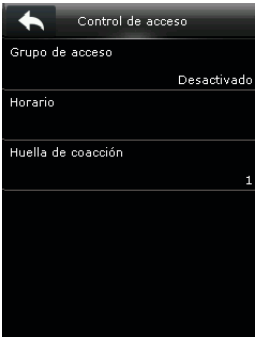
**Contraseña:** El dispositivo acepta contraseñas de 1 a 8 dígitos.

**Nota:**

1. El equipo asigna automáticamente el ID de usuario para los usuarios en secuencia, pero estos pueden ser modificados manualmente.
2. El dispositivo es compatible con IDs de usuario de entre 1 a 9 dígitos.

## 4.2 Configuraciones de Control de Acceso

La opción de control de acceso de los usuarios es para configurar el acceso a la puerta que controla el dispositivo,, incluyendo el establecimiento de grupos de acceso, horarios y la gestión de la huella digital de amago.



# Gestión de Usuarios

**Grupos de Acceso:** Para asignar los usuarios a diferentes grupos de control de acceso para la gestión. Por defecto, los nuevos usuarios pertenecen al Grupo 1 y pueden ser reasignados a otros grupos. El número de grupos válidos oscila de 1 a 99.

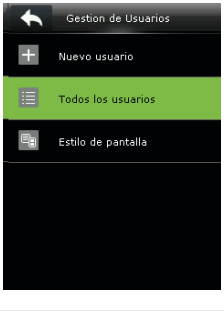
**Horario:** Seleccionar los horarios para el acceso del usuario. Los horarios se establecen bajo el menú de Control de Acceso y como máximo se permiten 50 horarios. El tiempo efectivo de la apertura de la puerta será la suma de los horarios seleccionadas.

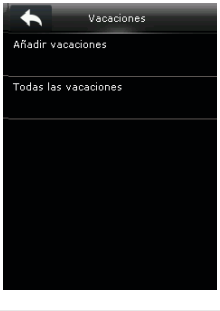
**Huella de Amago:** El usuario puede elegir uno o más dedos para registrarlos como huella de amago o coacción. Cuando ese dedo sea verificado se activará la alarma de amago.


**Ejemplo:** Entre esas huellas digitales registradas (6, 7), elija la huella 7 como la huella digital de coacción.

## 4.3 Buscar Usuarios

Ingrese el ID del usuario en la lista [Todos los usuarios] para buscarlo

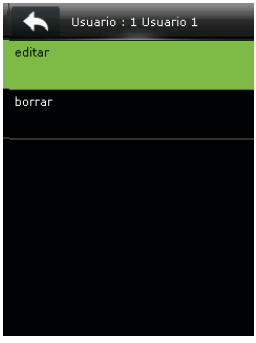


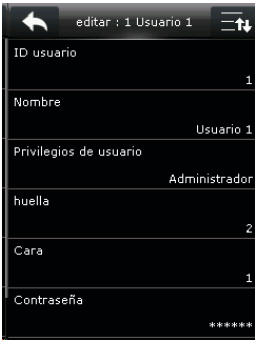




# Gestión de Usuarios

En la interfaz inicial, presione > **Gestión de Usuarios** > para entrar a la interface **Todos los Usuarios.** Escriba un ID de usuario en la caja de búsqueda, y el usuario correspondiente se mostrará. La figura anterior muestra las interfaces de búsqueda de un usuario con el ID de usuario "1".

## 4.4 Editar Usuario



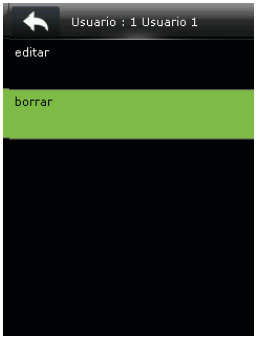

Después de elegir un usuario en 4.3 Buscar Usuarios, pulse [Editar] para entrar en la interfaz de edición de usuario.

O en la interfaz inicial pulse > Gestión de Usuarios > Todos los usuarios> seleccione un usuario de la lista > > Editar para acceder a la interfaz de edición del usuario.

El método de operación de edición de usuarios es la misma que de agregar usuarios, pero el nombre de usuario no se puede editar.

# Gestión de Usuarios

## 4.5 Eliminar Usuario



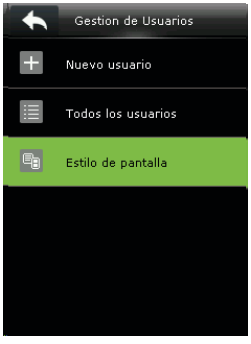


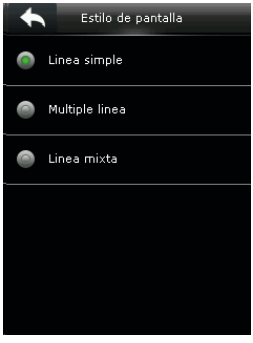
Después de elegir un usuario en 4.3 Buscar Usuarios, pulse [M/OK] para entrar en la interfaz de eliminar usuario.

O en la interfaz inicial pulse > **Gestión de Usuarios** > **Todos los usuarios**> seleccione un usuario de la lista > **Eliminar** para acceder a la interfaz de eliminación de usuario. Seleccione la información del usuario que desea eliminar o eliminar el usuario

**Nota:** El elemento correspondiente a ser eliminado sólo aparecerá cuando el usuario haya registrado huella digital, contraseña o foto de usuario.

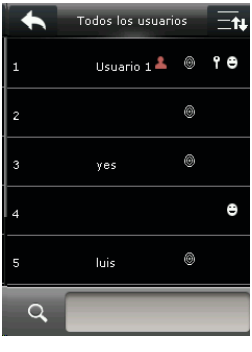
## 4.6 Estilo de Visualización del Usuario

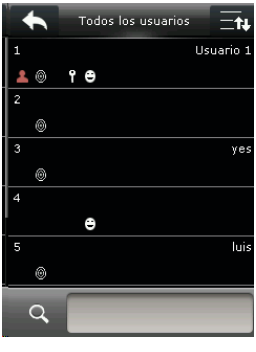




En la interfaz inicial pulse > **Gestión de Usuarios** > **Estilo de Visualización** para entrar a la interfaz de ajuste de estilo.

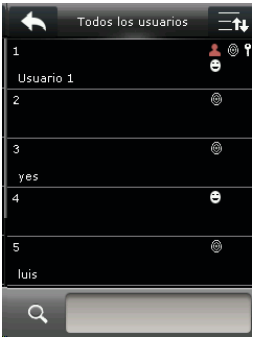
Varios estilos de visualización se muestran a continuación:




Estilo de línea única




Estilo de línea única



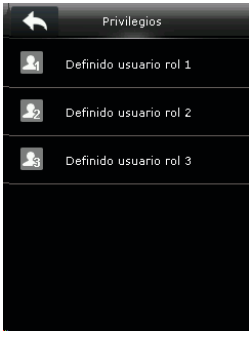

Línea mixta

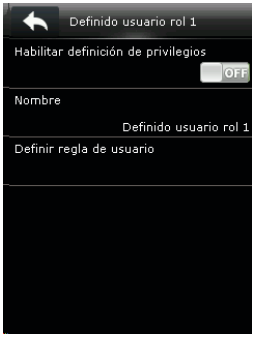
# Privilegios de Usuario

Configure los permisos que tiene cada usuario para operar los menús (se pueden definir un máximo de 3 perfiles de privilegios). Cuando se habilitan los privilegios definidos por el usuario, se pueden asignar los permisos adecuados a cada usuario en [Gestión de Usuario]> [Nuevo usuario]> [Privilegios de usuario].

**Privilegio:** El Administrador tiene que asignar diferentes permisos a los nuevos usuarios. Para evitar el establecimiento de permisos para cada usuario de uno en uno, puede definir los privilegios de usuario para categorizar diferentes niveles de permisos en la gestión de usuarios.

## 5.1 Habilitación de Privilegios de un Usuario

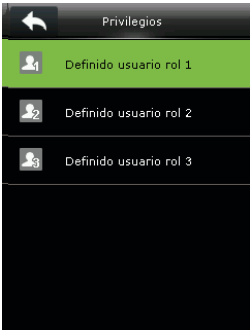

En la pantalla inicial, pulse > Privilegios > Privilegio Definido por Usuario 1 (2/3) > Habilitar definición de Privilegio Definido.

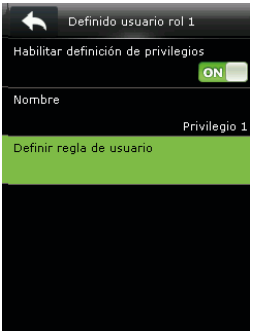
Después de habilitar los privilegios definidos, puede comprobar que los privilegios han sido habilitados en [Gestión de usuario.]> [Nuevo usuario]> [Privilegio de Usuario].

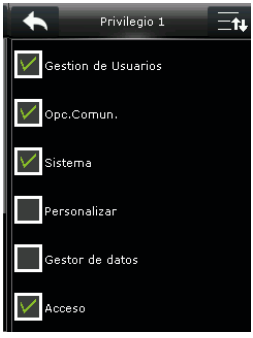
**Nota:** Se requiere al menos un administrador registrado para habilitar los privilegioS de usuario, de lo contrario el dispositivo le pedirá "Por favor registre un administrador primero".

# Privilegios de Usuario

## 5.2 Asignación de Privilegios




En la pantalla inicial, pulse > Privilegios > Privilegio Definido por Usuario 1 (2/3) > Definir Privilegio De Usuario para acceder a la interfaz de definición de privilegio de usuarios 1 (2/3).

# Ajustes de Comunicación

## 6.1 Configuración Ethernet




En la interfaz principal, pulse > Comunicación inicial > Ethernet, para entrar en la interfaz de configuración de Ethernet.

Los parámetros que aparecen a continuación son los valores predeterminados de fábrica, por favor, ajústelos de acuerdo a la situación real de la red.

Dirección IP: 192.168.1.201

Máscara de red: 255.255.255.0

Puerta de enlace: 0.0.0.0

DNS: 0.0.0.0

Puerto de comunicación TCP: 4370

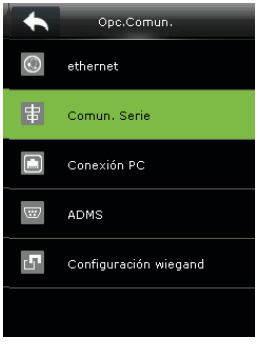
**DHCP:** Dynamic Host Configuration Protocol, que es asignar dinámicamente direcciones IP a los clientes a través del servidor. Si DHCP está habilitado, la IP no se puede ajustar manualmente.

**Visualización en la barra de estado:** Para establecer si se muestra el icono de red en la barra de estado.

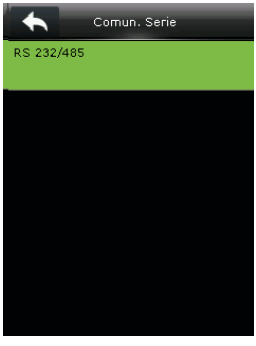
# Ajustes de Comunicación

## 6.2 Comunicación Serial


En la interfaz [Comunicación], y haga clic en la opción [Comunicación Serial].

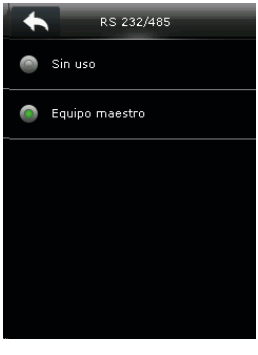



Seleccione Comunicación serial




Seleccione RS232 / 485


Seleccione RS485




Seleccione RS485 como la función de "unidad maestra" o desactive RS485

**Nota:** Cuando se utiliza RS485 como la función de "unidad maestra", el dispositivo actuará como "unidad maestra", y puede ser conectado al lector de huellas digitales RS485.

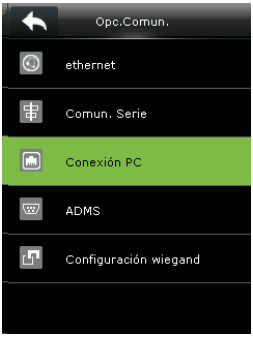
# Ajustes de Comunicación

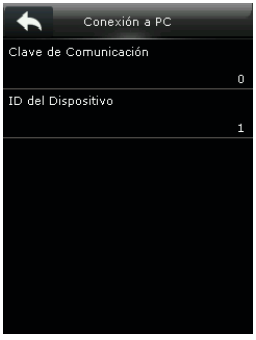
## 6.3 Conexión de PC

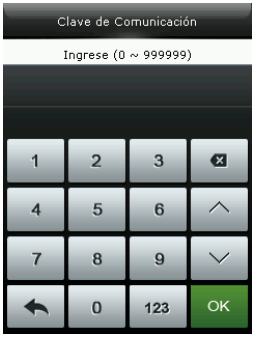
**• Clave de Comunicación**

Para mejorar la seguridad de los datos, la clave de comunicación entre el dispositivo y el PC necesita ser establecido.

Si una clave de comunicación se configura en el dispositivo, la clave correcta de conexión necesita ser ingresada cuando el dispositivo esté conectado al software de PC, de manera que el dispositivo y el software se puedan comunicar..



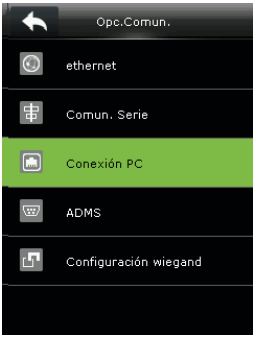



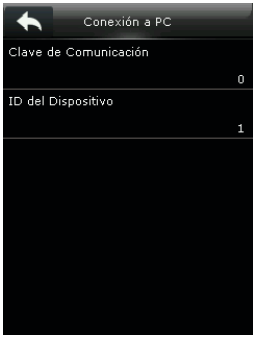

En la interfaz, pulse > Comunicación > Conexión PC> Clave de comunicación para entrar en la interfaz de configuración de la clave de comunicación

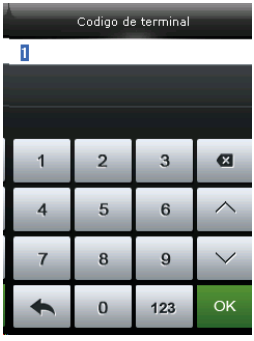
**Clave de comunicación:** La clave por defecto es 0 (sin clave). La clave de comunicación puede ser de 1 ~ 6 dígitos y se extiende entre 0 ~ 999999.

# Ajustes de Comunicación

• **Configuración del ID del dispositivo**
Si el método de comunicación es RS232 / RS485, se requiere la introducción de este código en la interfaz del software de comunicación.



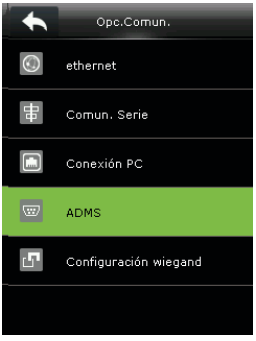

En la interfaz inicial, pulse > Comunicación > Conexión PC > Código del Terminal para entrar en la interfaz de configuración del ID del dispositivo.

**ID del dispositivo:** el número de identificación del dispositivo, que oscila entre 1 ~ 254.

## 6.4 Configuración del ADMS

Ajustes utilizados para la conexión con el servidor ADMS, como la dirección IP y el puerto de configuración, etc.

# Ajustes de Comunicación






En la pantalla inicial, pulse [M / OK]> Comunicación > ADMS para entrar a la interface de configuración del servidor ADMS. Cuando esté conectado con éxito el servidor ADMS, la interfaz principal mostrará el ícono .

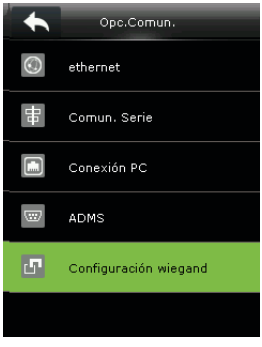
**Habilitar el nombre de dominio:** Cuando esta función está activada, el dominio de nombre http: //... serán utilizados, tales como http://www.XXX.com. XXX indica el nombre de dominio cuando este modo está activado; Cuando este modo está desactivado, introduzca el formato de dirección IP en XXX.

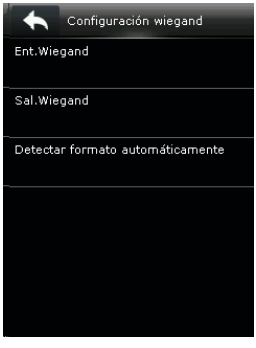
**Dirección del servidor:** la dirección IP del servidor ADMS.

**Puerto del servidor:** puerto utilizado por el servidor ADMS.

**Habilitar Servidor Proxy:** Método de habilitar proxy. Para habilitar el proxy, configurar la dirección IP y número de puerto del servidor proxy. Introduciendo el IP proxy y el servidor será la misma

## 6.5 Configuración Wiegand

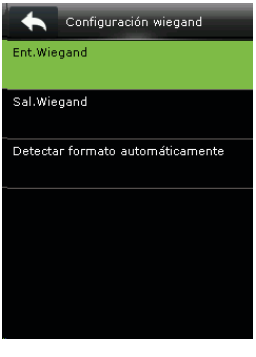



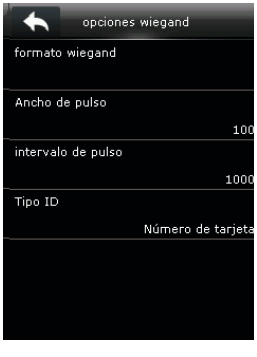




En la interfaz, pulse > Comunicación > Configuración Wiegand, para entrar en la interfaz inicial de configuración Wiegand.

### 6.5.1 Entrada Wiegand

El conector de entrada Wiegand es compatible con lector de tarjetas, también es posible conectar el dispositivo como un dispositivo maestro a otro dispositivo (dispositivo esclavo), formando un sistema maestro / esclavo.





Pulse [Entrada Wiegand] para entrar en la interfaz de entrada Wiegand.

# Ajustes de Comunicación

**Formato Wiegand:** El dispositivo soporta los siguientes formatos: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a y Wiegand 50. El estado "Sin Usar" significa que ese formato no está siendo utilizado.

**Ancho de Pulso (us):** El ancho de pulso enviado por medio de Wiegand. El valor predeterminado es de 100 microsegundos, pero puede ser ajustado dentro de un rango de 20 a 100.

**Intervalo de Pulso (us):** El valor predeterminado es de 100 microsegundos, pero puede ser ajustado en dentro de un rango de 200 a 20.000.

**Tipo de ID:** Contenido de entrada incluido en la señal de entrada Wiegand. El ID de Usuario o Número de Tarjeta puede ser elegido.

**Definiciones de los formatos Wiegand:**

| Formato Wiegand | Definición |
|---|---|
| Wiegand26 | ECCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste de 26 bits de código binario. El 1er bit es el bit de paridad par de los bits del 2º al 13º, mientras que el bit 26º es el bit de paridad impar del 14º al 25º. Los bits del 2º al 25º son los del número de tarjeta. |
| Wiegand26a | ESSSSSSSSCCCCCCCCCCCCCCCCO<br>Consiste de 26 bits de código binario. El 1er bit es el bit de paridad par de los bits del 2do al 13ro, mientras que el bit 26 es el bit de paridad impar de los bits del 14to al 25to. Los bits del 2do al 9no son los códigos del sitio y los bits del 10mo al 25to son los números de tarjeta. |
| Wiegand 34 | ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste de 34 bits de código binario. El 1er bit es el bit de paridad par del 2do al 17mo bit, mientras que el 34to bit es el bit de paridad impar del 18vo al 33er bit. Los bits del 2do al 25to son el número de tarjeta. |
| Wiegand 34a | ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste de 34 bits de código binario. El 1er bit es el bit de paridad par del 2do al 17mo bit, mientras que el 34to bit es el bit de paridad impar del 18vo al 33er bit. Los bits del 2do al 19no son el código del sitio, mientras que del 10mo al 25to bit son el número de tarjeta. |

# Ajustes de Comunicación

| | |
|---|---|
| Wiegand 36 | OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME<br>Consiste de 36 bits de código binario. El 1er bit es el bit de paridad impar del 2do al 18vo bit, mientras que el 36to bit es el bit de paridad par del 19no al 35to bit. Los bits del 2do al 17mo son el código del dispositivo, los bits del 18vo al 33er son el número de tarjeta, y los bits 34to y 35to son el código del fabricante. |
| Wiegand 36a | EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO<br>Consiste de 36 bits de código binario. El 1er bit es el bit de paridad par del 2do al 18vo bit, mientras que el 36to bit es el bit de paridad impar del 19no al 35to bit.<br>Los bits del 2do al 19no son el código del dispositivo y del 20mo al 35to bit son el número de tarjeta. |
| Wiegand 37 | OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE<br>Consiste de 37 bits de código binario. El 1er bit es el bit de paridad impar del 2do al 18vo bit, mientras que el 37mo bit es el bit de paridad par del 19no al 36to bit.<br>Del 2do al 4to bit son el código del fabricante, del 5to al 16to son el código del sitio y del 21ro al 36to son el número de tarjeta. |
| Wiegand 37a | EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO<br>Consiste de 37 bits de código binario. El 1er bit es bit de paridad par del 2do al 18vo bit, mientras que el 37mo bit es el bit de paridad impar del 19no al 35to bit.<br>Del 2do al 4to bit son el código del fabricante, del 5to al 14to bit son el código del dispositivo, del 15to al 20mo bit son el código del sitio, y del 21er al 36to bit son el número de tarjeta. |
| Wiegand 50 | ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 50 bits de código binario. El 1er bit es el bit de paridad par del 2do al 25to bit, mientras que el 50mo bit es el bit de paridad impar del 26to al 49no bit. Del 2do al 17mo bit son el código del sitio y del 18vo al 49 son el número de tarjeta |

**Nota:**
**C** denota el número de tarjeta, **E** el bit de paridad par, **O** el bit de paridad impar, **f** código del dispositivo, **M** código de fabricante, **P** paridad par y **S** código de sitio.

### 6.5.2 Salida Wiegand

El conector de salida Wiegand compatible con SRB, o conecte el dispositivo como un dispositivo esclavo de otro dispositivo (el maestro), formando un sistema maestro / esclavo.



Pulse [Salida Wiegand] para entrar en la interfaz de salida Wiegand.

**SRB:** Seleccione [ON] para activar la función de SRB (caja relevadora de seguridad), mientras que la elección [OFF] puede desactivar la función.

**Formato Wiegand:** Consulte las definiciones de los formatos Wiegand soportados por el sistema en el punto 5.4.1; el actual formato es determinado por los bits de salida Wiegand.

**Bits de Salida Wiegand:** Cantidad de bits de los datos Wiegand. Después de elegir la opción [Bits de Salida Wiegand], el dispositivo utilizará la cantidad de bits establecidos para encontrar el formato Wiegand adecuado.
Por ejemplo, si son seleccionados el 26Bit/Wiegand26, 34Bit/Wiegand34a, 36Bit/Wiegand36, 37Bit/Wiegand 37a y 50Bit/Wiegand 50; pero los bits de salida Wiegand están establecidos en 36, el formato 36-Bit Wiegand36 es adoptado.

**ID Fallido:** Está definido como el valor de salida de la verificación de usuario fallida. El formato de salida depende de la configuración del [Formato Wiegand]. El rango predeterminado es de 0 a 65535.

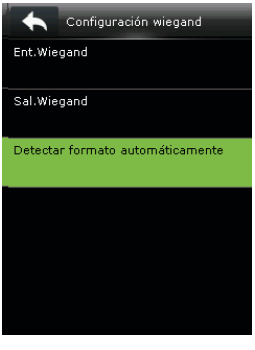
**Código de Sitio:** Es similar al ID del dispositivo, excepto porque este puede ser establecido manualmente y puede repetirse en varios dispositivos.

**Ancho de Pulso (us):** El ancho de pulso enviado por medio de Wiegand. El valor predeterminado es de 100 microsegundos, pero puede ser ajustado dentro de un rango de 20 a 100.

**Intervalo de Pulso (us):** El valor predeterminado es de 100 microsegundos, pero puede ser ajustado en dentro de un rango de 200 a 20.000.
Tipo de ID: Contenido de salida incluido en la señal de salida Wiegand. El ID de Usuario o Número de Tarjeta puede ser elegido.

### 6.5.3 Detección Automática del tipo de Tarjeta

La [Detección Automática del Tipo de Tarjeta] es una función que permite la rápida detección del tipo de tarjeta y su formato correspondiente. Varios formatos de tarjetas están preestablecidos en el dispositivo. Después de deslizar la tarjeta, el sistema detectará los diferentes números de tarjeta de acuerdo a cada formato; el usuario sólo requiere escoger el ítem equivalente al actual número de tarjeta, y establecer el formato como el formato Wiegand para el dispositivo. Esta función aplica también a la función de lectura de tarjetas y lector Wiegand auxiliar.



En la interfaz inicial, pulse > Comunicación > Configuración> Detectar Formato Automáticamente para entrar en la interfaz.

# Ajustes de Comunicación

**Procedimiento de operación:**

1. Después de entrar a la interfaz de [Detectar Formato Automáticamente] deslize la tarjeta de identificación por encima del lector de tarjetas (en el dispositivo local o lector de tarjetas auxiliar), la interfaz mostrará los formatos Wiegand detectados automáticamente y los números de las tarjetas analizadas.


2. Seleccione el elemento correspondiente al número de tarjeta como el [formato Wiegand] del dispositivo, que es el formato Wiegand para la lectura de este tipo de tarjeta.


**Nota:** Si el dispositivo no incluye un lector de tarjetas ID, es necesario conectar un lector de tarjetas auxiliar a través de la entrada Wiegand.

# Configuración del sistema

## 7.1 Configuración de registros de acceso




En la interfaz inicial, pulse > Sistema > Configuración de Registros de Acceso para acceder a la interfaz de Configuración de registros de acceso.

**Modo de cámara:** Para establecer si se debe tomar y guardar fotos en la verificación; aplicable a todos los usuarios. Los 5 modos siguientes se incluyen:

**1. Sin foto:** No se toma foto en la verificación del usuario.
**2. Tomar foto, sin salvar:** La foto se toma pero no se guarda en la verificación.
**3. Tomar foto y guardar:** La foto se toma y se guarda en la verificación.
**4. Guardar en la verificación exitosa:** La foto se toma y se guarda en la verificación exitosa.
**5. Guardar en verificación fallida:** La foto se toma y se guarda en la verificación fallida.

**Mostrar Foto de Usuario:** Configurar la fotografía de los usuarios para que aparezca cuando un usuario pasa la verificación. Colocarlo en [ON] para mostrar la foto de usuario y [OFF] para desactivarlo.

**Alerta de Espacio Insuficiente:** Cuando la capacidad de registros de acceso restantes es menor que el valor predeterminado, el dispositivo genera automáticamente un mensaje que indica la capacidad disponible para registros. Usted puede configurarlo para establecer un valor que oscile entre 1 y 9999 registros.

**Borrar Eventos Antiguos:** Establecer el número de registros de acceso que se eliminarán cuando la cantidad de registros llegue a su capacidad máxima permitida. El valor predeterminado es desactivado. Se puede establecer un valor que va de 1 a 999.

**Limpieza cíclica de fotos de Asistencia:** El número de fotos de asistencia autorizados a borrar en el momento en que se alcanza el máximo de almacenamiento. Se puede desactivar o establecer en un valor que oscile entre 1 y 99.

**Limpieza cíclica de fotos de la lista negra:** El número de fotos de la lista negra que se permiten sean eliminadas en el momento en que se alcanza el máximo de almacenamiento. Se puede desactivar o establecer un valor que oscile 1 y 99.

**Duración de Pantalla de Confirmación:** permite establecer la duración para mostrar mensajes de resultados de la verificación. El rango permitido es de 1-9 segundos.

## 7.2 Parámetros de Rostro

En la pantalla inicial, pulse > Sistema> Rostro, para entrar en la interfaz.

**Umbral de la verificación 1:1:** Bajo el método de verificación 1:1, la verificación tiene éxito sólo cuando la similitud entre la cara y la cara a los usuarios registrados es mayor que el valor del umbral.

**Umbral 1: N** Bajo el método de verificación 1: N, la verificación tiene éxito sólo cuando la similitud entre los rostros que se verifican y todos los rostros registrados es mayor que el valor umbral.

**Umbral Recomendado:**

| Tasa de rechazo por error | Tasa de error de cálculo | Umbral de Coincidencia | |
|---|---|---|---|
| | | 1:N | 1:1 |
| Alto | Bajo | 85 | 80 |
| Medio | Medio | 82 | 75 |
| Bajo | Alto | 80 | 70 |

**Detección de Rostros Falsos:** Para establecer si desea detectar rostros falsos. Activar [Detectar Rostro Falso], el dispositivo detectará los rostros falsos durante el registro y la verificación, de manera que no se puede registrar o verificar con éxito.

**Calidad:** La calidad del umbral al capturar la imagen facial. Cuando la calidad de la imagen es mayor que este valor, el dispositivo recibe esta imagen facial y comienza el procesamiento del algoritmo, de lo contrario, el dispositivo filtra esta imagen facial. El valor por defecto es 80 (o dentro de 50-150).

**Nota:** Los ajustes incorrectos de la exposición y calidad afectan gravemente el funcionamiento del dispositivo. Si es necesario ajustar los parámetros, por favor, siga las instrucciones de nuestro personal de servicio post-venta para las operaciones.

## 7.3 Parámetros de Huella Digital



En la interfaz, pulse > Sistema> Huella digital, para entrar en la interfaz de configuración de la huella digital.

• **Umbral de Verificación 1:1:** Examina la similitud entre la huella de verificación actual y la plantilla de la huella registrada por el usuario (almacenada en el dispositivo). El valor preestablecido es 15, pero usted puede modificarlo dentro de un rango de 10 a 35. Cuando la similitud alcance el nivel establecido, la verificación es exitosa. Entre más alto sea el umbral más bajo es el error de cálculo y más alto el índice de rechazo, y viceversa.

• **Umbral de Verificación 1:N:** Examina la similitud entre la huella de verificación actual y todas las plantillas de huellas almacenadas en el dispositivo. El valor preestablecido es 35, pero usted puede modificarlo dentro de un rango de 25 a 45. Cuando la similitud alcance el nivel establecido, la verificación es exitosa. Entre más alto sea el umbral más bajo es el error de cálculo y más alto el índice de rechazo, y viceversa.

# Configuración del sistema

• **Umbrales de verificación recomendados:**

| Tasa de rechazo por error | Tasa de error de cálculo | Umbral de Coincidencia | |
|---|---|---|---|
| | | 1:N | 1:1 |
| Alto | Bajo | 45 | 25 |
| Medio | Medio | 35 | 15 |
| Bajo | Alto | 25 | 10 |

**Sensibilidad del sensor de huellas::** Para ajustar la sensibilidad al momento de capturar las huellas digitales. Se recomienda utilizar el nivel predeterminado "Medio". Cuando el ambiente está seco y provoca que la detección de huellas dactilares sea lenta, se puede establecer el nivel "Alto" para elevar la sensibilidad; cuando el ambiente es húmedo, por lo que es difícil identificar la huella digital, se puede establecer el nivel de "Bajo".

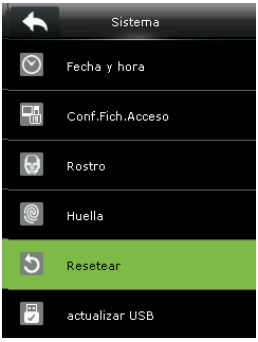
**Detección de dedo vivo:** Para detectar si se trata de una huella digital falsa. Habilitar [Detección de dedo vivo], en el dispositivo y detectará la huella digital falsa durante el registro y la verificación, por lo que no podrá ser verificado correctamente.

**Número de Intentos 1:1:** La contraseña de verificación de los usuarios puede ser olvidada o ha pulsado de manera inadecuada el dedo durante la verificación. Para reducir el proceso de tener que introducir el ID de usuario, se le permite volver a intentar; el número de reintentos puede ser de 1 ~ 9 veces.

**Imagen de la huella:** Para establecer si se muestra la imagen de la huella en la pantalla durante el registro o la verificación. Hay cuatro opciones disponibles: Mostrar al registrar, mostrar al verificar, mostrar siempre, Ninguno.

## 7.4 Restablecer configuraciones de fábrica

Restablecer datos como la configuración de comunicación o de sistema a la configuración de fábrica.



En la interfaz, pulse > Sistema> Restablecer> OK para terminar los ajustes de restablecimiento.
Restablecer los parámetros incluyendo las opciones de control de acceso, instalación de antipassback, el establecimiento de la comunicación (es decir, la configuración de Ethernet, Comunicaciones en serie, conexión a la PC y configuración Wiegand), Personalizar (voz, sonido del teclado, volumen y tiempo de espera para el modo de reposo) etcétera.

| Parámetros | Valores de Fábrica |
|---|---|
| Opciones de control de acceso | Tiempo de apertura 5 segundos<br>Retraso del sensor de la puerta: 10 segundos |
| | Tipo de puerta del sensor: normalmente abierto (NO)<br>Modo de verificación: Contraseña / huella digital / Rostro<br>Puertas disponibles por periodo de tiempo: 1<br>Período de tiempo: Ninguno<br>Usar como maestro: Dentro<br>Salida Aux / bloqueado de tiempo abierto: 255 segundos<br>Ajuste del tipo de salida auxiliar: Alarma de puerta abierta<br>Alarma Altavoz: OFF |

# Configuración del sistema

| | |
|---|---|
| Dirección de Antipassback | Sin antipassback |
| Ethernet | Dirección IP: 192.168.1.201<br>Máscara de red: 255.255.255.0<br>Puerta de enlace: 0.0.0.0 |
| Conexión a la PC | Clave Comunicación: 0<br>ID de dispositivo: 1 |
| Configuraciones Wiegand | Wiegand ID del modelo de entrada / salida: ID de usuario<br>ancho de pulso: 100 US<br>intervalo de pulso: 1000 us |
| El tiempo de inactividad para la presentación de diapositivas | 30 Seg |
| Tiempo de espera para entrar en modo reposo | 30 minutos |
| Tiempo de espera de los menús en las pantallas | 60 seg |
| Teclado rápido | Encendido |
| Mensajes de voz | Encendido |
| Volumen | 70 |

**Nota:** Al restablecer la configuración de fábrica, la información de usuario, la fecha y hora no se verán afectados. Por ejemplo, si la fecha y hora del dispositivo se fijan a 18:30 el 1 de enero de 2020, la fecha y la hora permanecerán sin cambios después de restablecer los ajustes de fábrica.

## 7.5 Actualización por USB



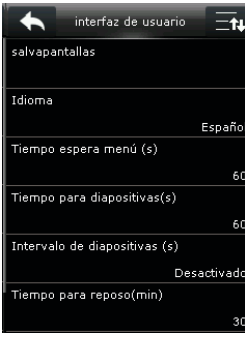
Inserte la unidad USB con el archivo de actualización en el puerto USB del dispositivo, y en la interfaz, pulse > Sistema> Actualización por USB, para completar la operación de actualización del firmware.

Si necesita archivo de actualización, por favor, póngase en contacto con nuestro soporte técnico. La actualización del firmware no se recomienda en circunstancias normales.

# Ajustes de Personalización

## 8.1 Configuración de la interfaz de usuario






En la pantalla inicial, pulse > Personalizar> Interfaz de usuario Para configurar la interfaz de usuario.

**Fondos:** Permite seleccionar el fondo de la pantalla principal, se pueden encontrar fondos de pantalla de varios estilos en el dispositivo.

**Idioma:** Seleccione el idioma del dispositivo según lo requiera.

**Tiempo de espera del menú (s):** Cuando no se realiza ninguna operación en la interfaz de menú y el tiempo supera el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. Se puede desactivar o establecer el valor desde 60 ~ 99.999 segundos.

**NOTA:** Si se elige la opción [Desactivado], el sistema no vuelve a la interfaz de menú, incluso cuando no se realiza ninguna operación. Desactivar esta función no se recomienda debido al alto consumo de energía y la inseguridad.

**Tiempo de Espera para Diapositivas (s):** Cuando no se realiza ninguna operación en la interfaz inicial y el tiempo supera el valor establecido, se mostrará una presentación de diapositivas. Se puede desactivar (ajustar a "Ninguna") o configurar el tiempo desde 3 ~ 999 segundos.

**Intervalo de diapositivas:** Se refiere al intervalo entre diferentes diapositivas. Se puede desactivar o establecer tiempo de 3 ~ 999 segundos.

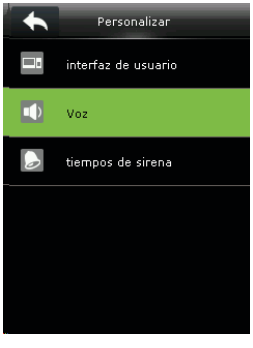
# Ajustes de Personalización

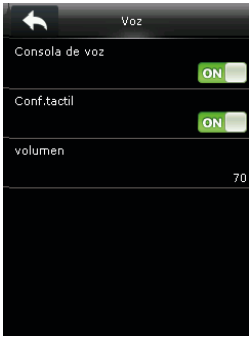
**Tiempo de inactividad para modo reposo:** Cuando no se realiza ninguna operación en el dispositivo, el dispositivo entrará en modo de reposo. Pulse cualquier tecla o coloque el dedo para desactivar el modo de espera. Puede desactivar esta función, o establecer el valor de 1 ~ 999 minutos. Si se desactiva esta función, el dispositivo no entrará en el modo de reposo.

**NOTA:** No se recomienda desactivar esta función debido a la cantidad de energía que utiliza.

**Estilo de la pantalla principal:** Seleccione el estilo de la pantalla principal.

## 8.2 Configuración de voz


En la pantalla inicial, pulse > Personalizar> Voz, para acceder a la interfaz de configuración de voz.

**Avisos de voz:** Seleccione esta opción si desea activar los mensajes de voz durante la operación. El valor predeterminado es modo [ON], lo que indica que la instrucción de voz ya está activado. Y el icono [OFF] indica que mensaje de voz está desactivada.

**Todo del Teclado:** Seleccione si desea habilitar el sonido mientras toca la pantalla. El valor predeterminado es [ON], lo que indica que la función está habilitada. El icono [OFF] indica que está desactivado.

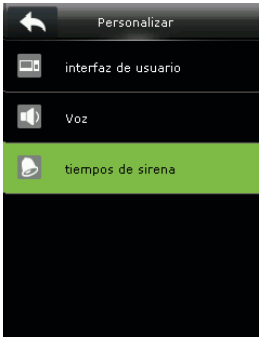
**Volumen:** Ajuste el volumen de los mensajes del dispositivo. El valor por defecto es de 70. Pulse la tecla [+] para aumentar el volumen, pulse la tecla [-] para disminuir el volumen.

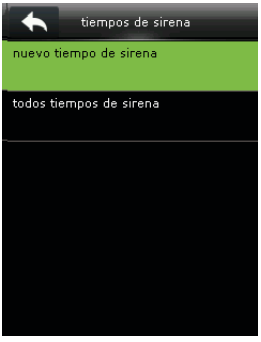
# Ajustes de Personalización

## 8.3 Configuración del timbre

Muchas empresas optan por utilizar un timbre para indicar cuando inicia el tiempo de trabajo y cuando termina. Al llegar a la hora programada para el timbre, el dispositivo reproducirá el tono seleccionado automáticamente hasta que se pasa el tiempo del sonido.

### 8.3.1 Agregar un nuevo timbre





En la pantalla inicial, pulse > Personalizar> Timbre> Nuevo timbre, para entrar a la interfaz de configuración

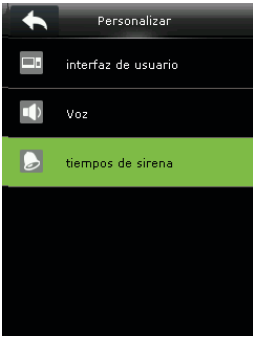
**Estado del timbre:** [ON] es para permitir que suene el timbre, mientras que [OFF] es para deshabilitarlo.

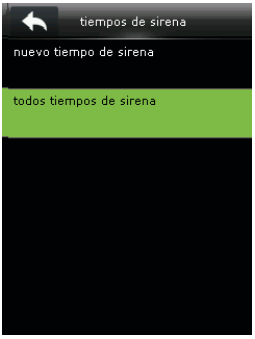
**Hora de timbre:** El timbre inicia automáticamente cuando se alcanza la hora especificado.

**Repetir:** Para establecer si se desea repetir el timbre de lunes a domingo.
Timbre: Seleccionar sonido.

**Tono de del timbre:** Para ajustar la duración del timbre. Los rangos de los valores a partir de 1 ~ 999 segundos.

### 8.3.2 Editar timbre

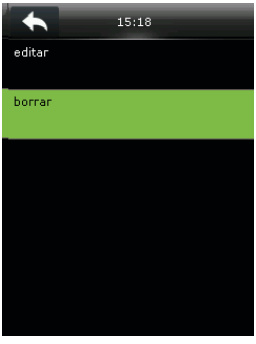


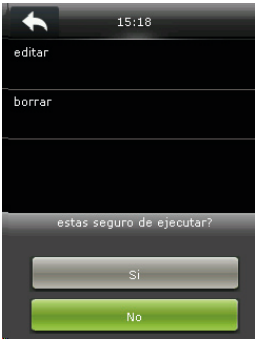





En la pantalla inicial, pulse > Personalizar> Timbre > Todos los timbres> elija un timbre> Editar, para entrar en la interfaz de edición.

### 8.3.3 Eliminar timbre




En la pantalla inicial, pulse > Personalizar> Timbre > Todos los Timbres > elija timbre> Eliminar, para entrar en la interfaz Eliminación.

# Gestión de Datos

## 9.1 Eliminar datos

Para gestionar los datos en el dispositivo, que incluye eliminar registros de acceso, eliminar todos los datos, eliminar privilegio de administrador y eliminar fondo de pantalla, etc.




En la pantalla inicial, pulse > Gestión de Datos.> Borrar datos, para entrar en la interfaz y eliminar valores.

**Eliminar registros de acceso:** Para borrar todos los registros de acceso guardados en el dispositivo o eliminar registros de acceso en un rango de tiempo especificado.

**Eliminar fotos:** Para eliminar todas las fotografías de asistencia guardados en el dispositivo o eliminar fotos de asistencia en un rango de tiempo especificado.

**NOTAS:**

1. Sólo si [Modo cámara] se selecciona "Capturar y guardar" o "Guardar en verificación exitosa", las fotos de asistencia se pueden guardar en el dispositivo después de la verificación exitosa.

2. En la interfaz inicial, , pulse > Sistema > Configuración de registros de acceso> Modo de cámara, para seleccionar "Capturar y guardar" o "Guardar en verificación exitosa".

**Eliminar fotos de la lista negra:** Para eliminar todas las fotografías de la lista negra guardadas en el dispositivo o borrar las fotos de la lista negra en un rango de tiempo especificado, las fotos de lista negra son las fotos tomadas después de las verificaciones fallidas.

**Notas:**

1. Sólo si [Modo cámara] se selecciona como "Capturar" o "Guardar en la verificación fallida" las fotos de lista negra se guardarán en el dispositivo después de cada verificación fallida.

2. En la interfaz inicial, pulse > Sistema > Configuración de registros de acceso > Modo cámara, para seleccionar "Capturar y guardar" o "Guardar en la verificación fallida".

**Eliminar todos los datos:** Para eliminar toda la información del usuario, huellas dactilares, rostro y el registro de accesos, etc.

**Eliminar privilegios de administrador:** Para que todos los administradores sean usuarios normales.

**Eliminar Control de acceso:** Para borrar todos los registros de acceso.

**Eliminar foto de usuario:** Para eliminar todas las fotos de los usuarios en el dispositivo. Para los detalles de subir una foto de usuario, consulte 16.3 Subir imágenes.

**Eliminar Fondo:** Para eliminar fondos de pantalla seleccionados o todos los que hay en el dispositivo.

**Procedimiento de operación:**
1. Pulse [Eliminar fondo de pantalla] para entrar en la interfaz de Eliminar fondo de pantalla.

# Gestión de Datos



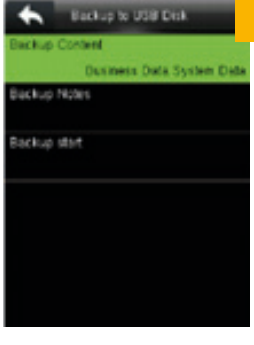
2. Pulse [ / ] para cambiar la visualización del fondo de pantalla y [Eliminar imagen seleccionada] para borrar la imagen seleccionada, o pulse [borrar todas las imágenes] para borrar todas las imágenes.

**Eliminar Protectores de Pantalla:** Para eliminar el protector de pantalla seleccionado o todos los que hay en el dispositivo. (Para los detalles de subir protectores de pantalla, por favor vaya al punto 16.3 Subir imágenes.)

## 9.2 Copia de Seguridad

Copia de seguridad en el dispositivo o en un una unidad USB

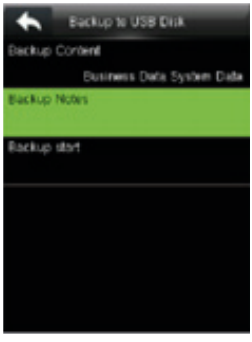




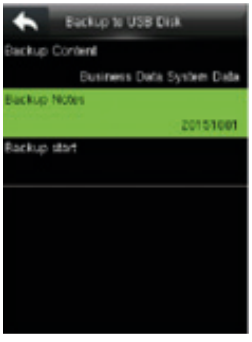



En la pantalla inicial, pulse > Gestión de datos> Copia de seguridad de datos> Copia de seguridad en disco USB, para entrar en la interfaz de configuración de la copia de seguridad.

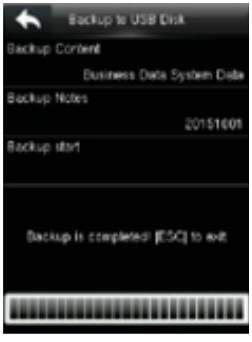
# Gestión de Datos




Presione [Guardar Contenido] para elegir el tipo de datos que desea respaldar.



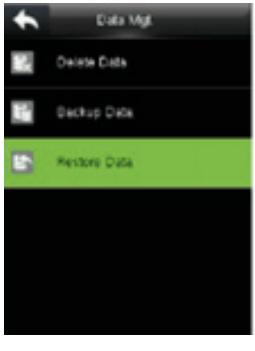

Presione [Iniciar Respaldo] y espere un momento.

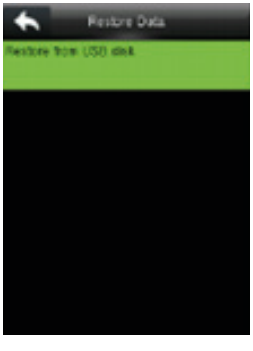


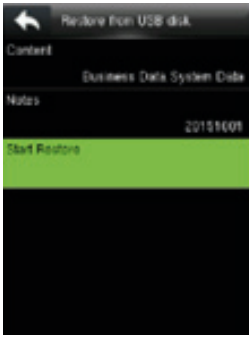

Respaldo completo

## 9.3 Restaurar Datos

Para restaurar los datos guardados en el dispositivo o en una unidad externa.




En la pantalla inicial, pulse ⊞ > Gestión de datos> Restaurar datos> Restaurar desde disco USB, para acceder a la interfaz.

# Control de acceso

La opción de control de acceso se utiliza para definir las los horarios, días de festivos, verificación combinada así como los parámetros relacionados al control de la cerradura y otros dispositivos.



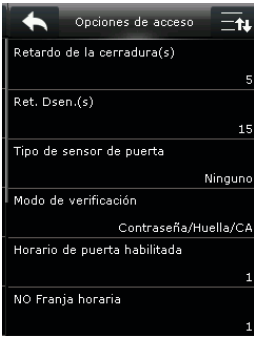
**Para tener acceso, el usuario registrado deberá cumplir las siguientes condiciones:**

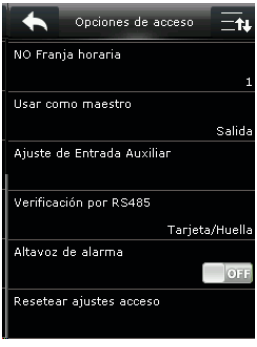
1. El tiempo de acceso del usuario deberá coincidir con los horarios de acceso permitidos para cualquier otro usuario del mismo grupo

2. El grupo del usuario debe estar dentro de la combinación de acceso combinada (cuando hay otros grupos en la misma combinación de acceso, se requiere la verificación de los miembros de esos grupos para poder abrir la puerta).

En la configuración predeterminada, los nuevos usuarios se asignan automáticamente en el primer grupo de acceso, con el horario [1] y el combo de acceso "1", se configuran en estado desbloqueado.

## 10.1 Configuración de Control de Acceso




En la pantalla inicial, pulse > Control de Acceso> Opciones de control de acceso para entrar en la interfaz de configuración.

**Retardo de la Cerradura (s):** Período de tiempo que permanece desbloqueada la puerta (desde la apertura de la puerta hasta el cierre automático) después de que la cerradura electrónica recibe una señal de apertura desde el dispositivo (el valor varía de 1 a 10 segundos).

**Retardo del sensor de puerta (s):** Cuando se abre la puerta, el sensor de la puerta se comprueba después de un período de tiempo; si el estado del sensor es incompatible con el modo de sensor de la puerta se disparará una alarma.
Este periodo de tiempo es la retardo del sensor de puerta (rangos de los valores de 1 a 255 segundos).

**Tipo de sensor de puerta:** Incluye Ninguno, normalmente abierto (NA) y normalmente cerrado (NC). Ninguno significa que el sensor de la puerta no está en uso; Normalmente abierto significa que la puerta se abre cuando está encendido; Normalmente cerrado significa que la puerta está cerrada está encendido.

**Modo de verificación:** Seleccione el modo de verificación para abrir la puerta, incluida la contraseña / huella digital / rostro, solo huella digital, sólo ID de usuario, sólo contraseña, etc.

# Control de acceso



**Nota:**

1. "/" Significa "o". "&" significa "y".

2. En un modo de verificación combinado, la información de verificación correspondiente debe registrarse en primer lugar. Por ejemplo: cuando el usuario se registra solo una huella digital, y el [Modo de Verificación] se establece como "contraseña y rostro", el usuario A no pasará la verificación.

**Horario de Puerta Disponible:** Asignar horarios a los usuarios para la apertura de la puerta.

**Horario NO:** Para establecer horarios de normalmente abierto, de modo que la puerta siempre está desbloqueado durante este período.

**Utilizar como maestro:** Mientras se realiza la configuración de los dispositivos como maestro y esclavo, se debe configurar el dispositivo como Entrada o Salida.

**Salida:** Un registro de verificación en el dispositivo maestro es un registro de salida.

**Entrada:** Un registro de verificación en el dispositivo maestro es un registro de entrada en el registro.

**Configuración de entrada auxiliar:** Para fijar la salida aux / Horario de Puerta Disponible, y configuración del tipo de salida auxiliar para el dispositivo con conector auxiliar. La configuración del tipo de salida auxiliar incluye Ninguno, Abrir Puerta, Activar Alarma, y Abrir Puerta & Activar Alarma.

# Control de acceso

**Modo de verificación por RS485:** Es el modo de verificación utilizado por el dispositivo cuando es la unidad maestra. Esta opción sólo se muestra si se ha activado la función del lector RS485. Puede activarlo siguiendo estos pasos: En la interfaz inicial, pulse > Comunicación> Comunicación serial> RS232 / 485> RS485> unidad maestra.

**Alarma de altavoz:** Cuando se activa la [Alarma Altavoz], el altavoz emite una alarma cuando el dispositivo está siendo desmantelado

**Restablecer configuración de acceso:** Para restablecer los parámetros de retardo de cerradura de la puerta, retardo del sensor de la puerta, Tipo de Sensor de Puerta, modo de verificación, Horario de Puerta Disponible, Horario NO, la configuración de entrada auxiliar, alarma de altavoz, dirección de antipassback. Sin embargo, el contenido de [Borrar Datos de Acceso] en [Gestión de datos] no se verá afectado.

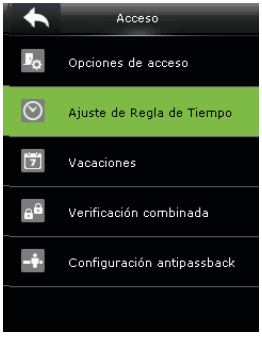
| **Parámetros de Acceso** | **Valores de Fábrica** |
|---|---|
| Retardo de bloqueo de la cerradura | 5 Segundos |
| Retraso del sensor de la puerta | 10 Segundos |
| Tipo de sensor de puerta | Normalmente abierto (NA) |
| Modo de verificación | Contraseña / huella digital / rostro |
| Horario de Puerta Disponible | 1 |
| Horario NO | Ninguna |
| Salida auxiliar / bloqueo de tiempo abierto | 255 Segundos |
| Configuración del tipo de salida auxiliar | Alarma de puerta abierta |
| Alarma de altavoz | Apagado |
| Dirección del antipassback | Sin antipassback |

**Nota:** Después de que el dispositivo está conectado al software, la "multi-verificación" no es visible, se puede restablecer la configuración de acceso en el sistema de control de acceso del dispositivo y después ir a Gestión de Datos > Eliminar Control de Acceso para hacerlo visible.

# Control de acceso

## 10.2 Ajustes de Horario

El horario es la unidad de tiempo mínima de los ajustes de control de acceso; se pueden establecer un máximo de 50 horarios en el sistema. Cada Horario consiste de 7 secciones de tiempo (una semana) y 3 secciones de días festivos, y cada sección de tiempo es el tiempo válido dentro de 24 horas.
Usted puede establecer un máximo de 3 periodos de tiempo para cada sección de tiempo. La relación entre estos periodos de tiempo es "O". Cuando un tiempo de verificación cae dentro de cualquiera de estos periodos de tiempo, la verificación es válida. El formato del periodo de tiempo es HH:MM-HH:MM en el sistema de 24 horas con precisión de minutos.





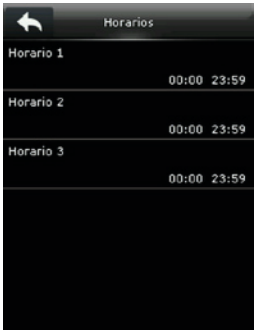

En la pantalla inicial, pulse > Control de Acceso> Ajustes de Horario, para entrar en la interfaz de ajustes de Horario. El número predeterminado de la regla de tiempo es el No. 1 (válido todo el día), y puede ser editado.

**• Editar Ajustes de Horario**

Un administrador puede editar ajustes de horario según sea necesario. El funcionamiento detallado es el siguiente:

# Control de acceso


Introduzca un número de Horario (como "2"), el horario (2) se localizará automáticamente, seleccione una sección de tiempo (como "lunes").




Seleccione el "periodo de tiempo 1/2/3"


Configure la "hora de inicio" y la "hora de finalización" según sea necesario.

**Nota:**

1. Cuando la hora de finalización es previa a la hora de inicio (por ejemplo, 23:57 - 23:56), esto significa el cierre de todo el día. Cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 00:00 ~ 23:59), esto quiere decir que este período de tiempo es válido.

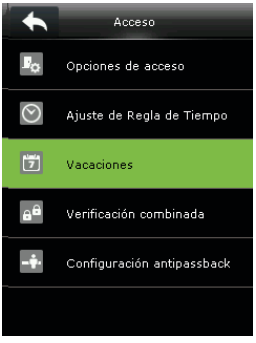
2. Periodo válido de tiempo: 00: 00-23: 59 (Válido todo el día) o cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 08:00 - 23:59).

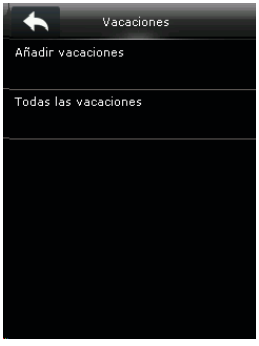
3. Por defecto, el Ajuste de Horario 01 indica la apertura de día completo (00:00 - 23:59).

# Control de acceso

## 10.3 Configuración de Días Festivos

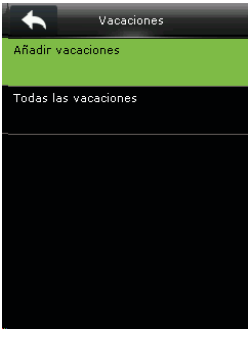
Usted puede agregar días festivos al dispositivo de control de acceso y establecer los periodos de tiempo para dichos días festivos según sea necesario.



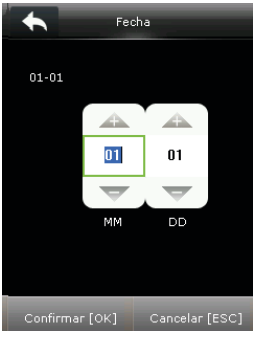

En la pantalla inicial, pulse > Control de Acceso> Días festivos, para entrar en la interfaz de configuración.

### 10.3.1 Agregar Días Festivos




Presione [Añadir días festivos]


Presione [Fecha]




Establecer fecha

**No.:** El dispositivo asigna automáticamente un número a un día festivo. El número varía de 1 a 24.

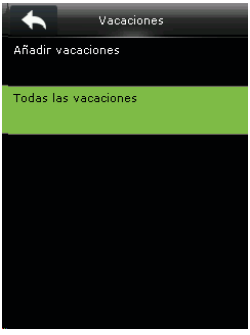
**Fecha:** Establecer la fecha del día festivo.

**Tipo de día festivo:** Puede clasificar el día festivo en 3 tipos (1/2/3). El horario válido para cada tipo de día festivo se puede editar en la interfaz de Ajustes de Horario. Para más detalles sobre editar horarios, consulte la sección 10.2 Ajustes de Horario.



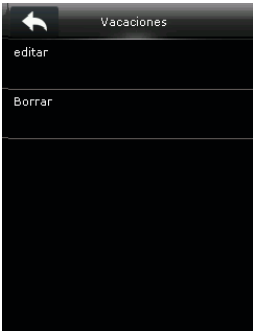

**Repetir:** El modo predeterminado de repetir es encendido [ON].
Para días festivos fijos cada año, por ejemplo, Año Nuevo que es el 1 de enero, la opción Repetir se puede establecer.
Para los días festivos no fijos de cada año, por ejemplo, el Día del Padre es el tercer domingo de junio, las fechas específicas son inciertos y la opción Repetir puede ser desactivado en [OFF].
Por ejemplo, cuando la fecha de un día festivo se establece el 1 de enero de 2010 y el tipo de día festivo se ajusta a los día festivo tipo 1, el control de acceso el 1 de enero se llevará a cabo de acuerdo con los ajustes de horario del tipo de día festivo 1 en lugar de los ajustes del periodo de tiempo del viernes.

### 10.3.2 Todos los Días Festivos




Presione [Todos los días festivos]


Presione [Seleccione un día festivo]




Edite o elimine el día festivo

**Nota:**

Los métodos para editar o borrar un día festivo son los mismos que los de editar o borrar un usuario. Para más detalles, ver 4.4 Modificar un usuario y 4.5 Eliminar un usuario

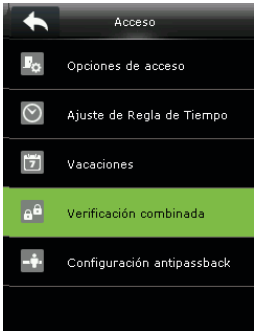
## 10.4 Configuración de verificación combinada.

Combinar dos o más grupos de acceso para lograr una verificación combinada. y mejorar la seguridad.

En la verificación combinada., el rango de un número de usuario es: 0 = N = 5; todos los usuarios pueden pertenecer a un mismo grupo, o pertenecer a 5 grupos diferentes como máximo.

**Nota:** Los grupos de acceso se establecen cuando la adición de usuario (en la interfaz, pulse ▦ > Gestión de usuario.> Nuevo usuario> Privilegio de Acceso > Grupo de Acceso, para establecer el número de grupo de acceso al que pertenece el usuario agregado), el número de grupo de acceso varía de 1 a 99.

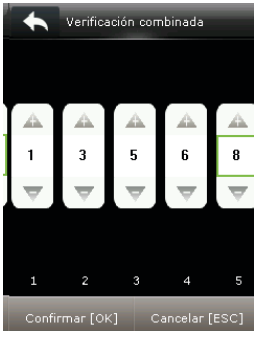
# Control de acceso



En la pantalla inicial, pulse > Control de Acceso> Verificación Combinada., para entrar en la interfaz de configuración.

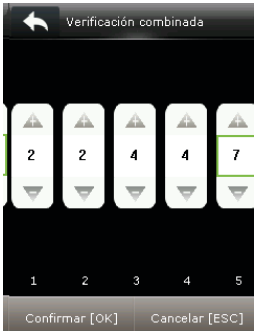
**Por ejemplo:**



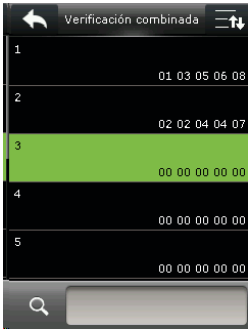
Como en la imagen anterior, la verificación combinada 1 se compone de cinco miembros procedentes de cinco grupos diferentes: --- grupo de acceso 1/3/5/6/8, respectivamente.

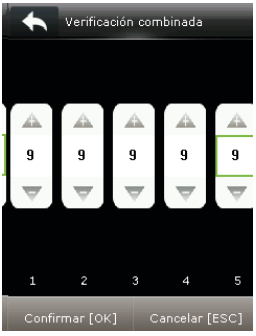
# Control de Acceso

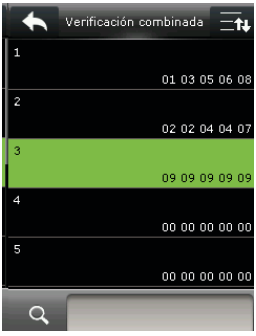





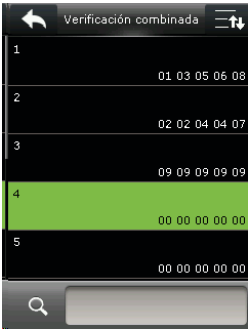
Como en la imagen anterior, la verificación combinada 2 se compone de cinco miembros procedentes de tres grupos diferentes: Dos miembros de los grupos de Acceso 2, dos de acceso grupo 4, y uno de acceso a grupo 7.

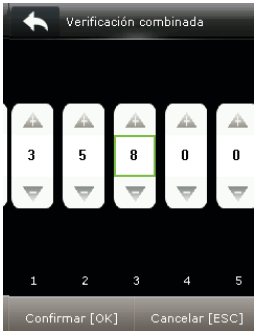


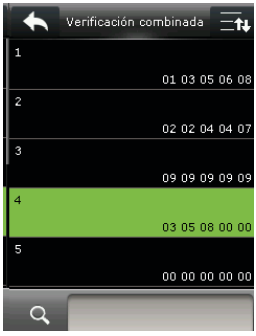




Como en la imagen anterior, la  verificación combinada 3 se compone de cinco miembros, y todos ellos vienen de acceso grupo 9.



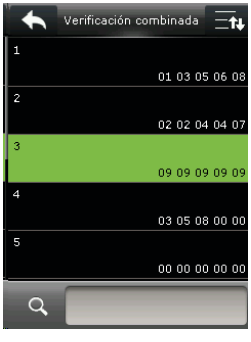



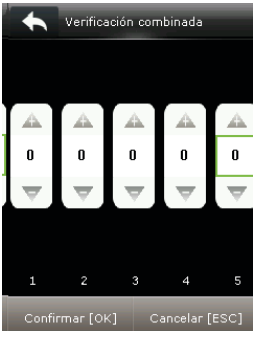




Como en la imagen anterior, la multi-verificación 4 se compone de tres miembros procedentes de tres grupos diferentes –Grupo de acceso 3, 5, 8, respectivamente.

**Eliminación de una multi-verificación**
Para eliminar una multi-verificación, ajustar todos los números del grupo de acceso a 0.

Por ejemplo, para eliminar la verificación combinada 3, consulte las siguientes figuras:





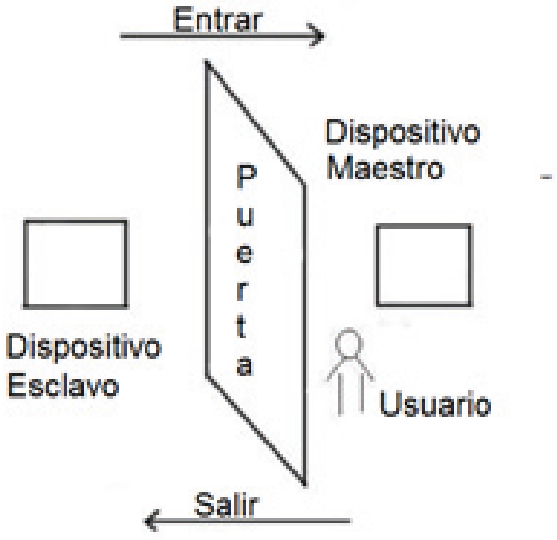
Si todos los números de los grupos de acceso en la verificación combinada 3 se establecen en 0, se borrará.

### 10.5 Antipassback

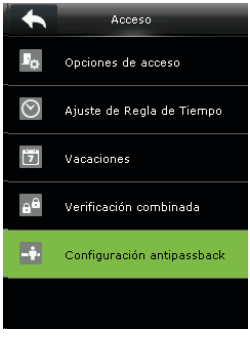
Para evitar que una persona que sigue a un usuario consiga acceder sin verificación, lo cual resulta en un problema de seguridad, los usuarios pueden activar la función Anti-Passback. Bajo esta función el registro de entrada debe coincidir con el registro de salida para poder abrir una puerta.

Esta función requiere de 2 dispositivos trabajando juntos: Uno instalado dentro de la puerta (dispositivo maestro) y otro instalado fuera de la puerta (dispositivo esclavo). Ambos dispositivos se comunican a través de una señal Wiegand.

El formato Wiegand y el tipo de salida (ID de Usuario/Número de Tarjeta) de ambos dispositivos debe ser consistente.



# Control de Acceso






En la interfaz inicial, pulse > Control de Acceso> Configuración inicial antipassback, para acceder a la interfaz de configuración Antipassback. Seleccione Dirección antipassback.

**Sin Antipassback:** La función Anti-Passback está desactivada, lo que significa que la verificación, ya sea en el dispositivo maestro o esclavo, puede abrir la puerta. Los registros de acceso no se guardan.

**Salida con Antipassback:** Después de que el usuario registre una salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrar entradas libremente.

**Entrada con Antipassback:** Después de que el usuario registre una entrada, sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrar salidas libremente.

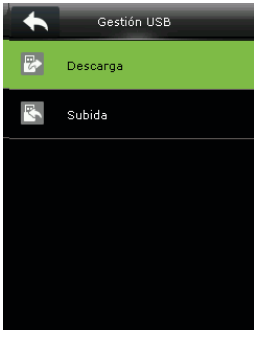
**Entrada / Salida Antipasssback:** Después de que un usuario entre / salga, sólo si el último registro es un registro de salida el usuario puede entrar nuevamente, o si es un registro de entrada el usuario puede salir; de lo contrario, se activará la alarma.

# Exportar a la USB

Los datos de usuario, foto del usuario, los registros de acceso y otros datos se pueden exportar al software correspondiente para su procesamiento a través de una unidad USB, o importar los datos de usuario al dispositivo mediante el uso de USB.

**Nota:** Antes de cargar / descargar datos desde / hacia el disco USB, inserte el disco USB en la ranura USB.

## 11.1 Exportar a la USB



En la pantalla inicial, pulse > Gestión USB> Descarga para entrar en la interfaz.

**Descarga de registros de acceso:** Para descargar los registros de acceso de un periodo de tiempo específico en la USB.

**Datos del Usuario:** Para descargar toda la información del usuario y las huellas digitales del dispositivo en la USB.

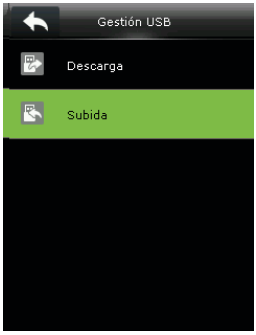
**Foto del usuario:** Para descargar todas las fotos de los usuarios del dispositivo en la USB.

**Fotos de asistencia:** Para descargar las fotos de los asistentes en un de horario especificado desde el dispositivo a la USB.

**Lista negra de fotos:** Para descargar fotos de la lista negra (fotos tomadas después de una verificación fallida) en un período de tiempo especificado desde el dispositivo a la USB.

# Exportar a la USB

## 11.2 Importar desde USB



En la interfaz inicial, pulse ▦ > Gestión USB > Subida, para entrar en la interfaz.

**Datos del usuario:** Si desea cargar todos los datos de usuario y las huellas digitales desde la USB al dispositivo.

**Foto del usuario:** Para subir fotos de los usuarios desde la USB al dispositivo. Seleccione [Subir imagen seleccionada] o [Cargar todas las Fotos], para más detalles consulta 16.3 Subir Imágenes

**Protector de pantalla:** Para cargar los protectores de pantalla desde la USB al dispositivo. Puede elegir [Subir imagen seleccionada] o [Subir todas las imágenes]. Las imágenes se mostrarán en la pantalla principal del dispositivo después de la carga (para las especificaciones de los protectores de pantalla, consulte 16.3 Subir Imágenes).

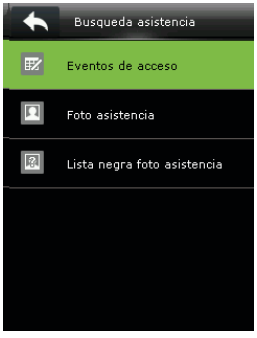
**Fondo de pantalla:** Para subir imágenes de fondo de la USB al dispositivo. Puede elegir [Subir imagen seleccionada] o [Subir todas las imágenes]. Las imágenes se mostrarán en la pantalla después de la carga (para las especificaciones de fondos de pantalla, consulte 16.3 Subir Imágenes)

# Buscar Registros

Cuando los usuarios son verificados con éxito, los registros se guardan en el dispositivo. Esta función permite a los usuarios comprobar sus registros de acceso, la foto de asistencia y las fotos en la lista negra.

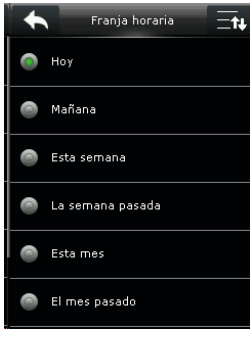
## 12.1 Buscar registros de acceso


Presione ▦ y seleccione [Busqueda Asistencia]

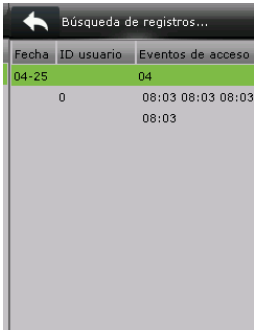



Presione [Eventos de acceso]

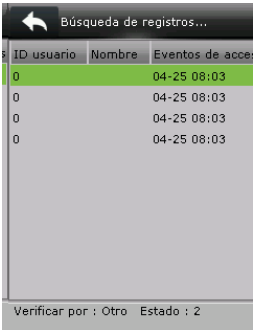

Digite su ID de usuario [deje en blanco para consultar todo]




Elija el intervalo de tiempo en el que se debe buscar



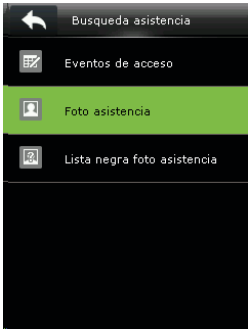

Total de registros de acceso en el rango de tiempo seleccionado




Registros detallados de acceso

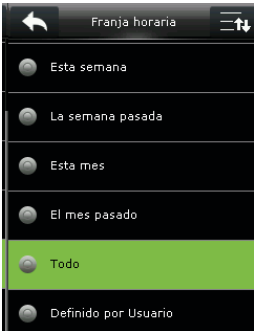
# Buscar Registros

## 12.2 Buscar Fotos de Asistentes




Presione [Foto asistencia]


Digite su ID de usuario (deje en blanco para consultar todo)

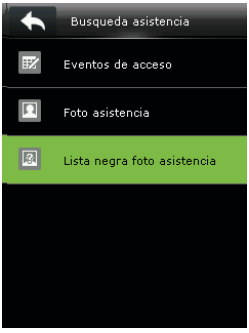



Elije el rango de tiempo en el que se debe buscar

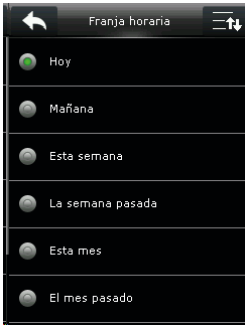

A continuación se mostrarás las fotos de asistencia correspondientes al periodo seleccionado

# Buscar Registros

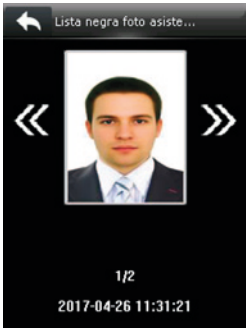
## 12.3 Buscar Fotos de la Lista Negra




Presione [Lista negra foto asistencia]




Elija el intervalo de tiempo en el que se debe buscar




A continuación, se muestran las fotos de asistencia correspondientes

# Pruebas

Para realizar pruebas automáticamente y saber si todos los módulos del dispositivo funcionan correctamente, incluyendo el LCD, voz, sensor de huellas digitales, cámara y RTC (reloj en tiempo real).



En la pantalla inicial, pulse > Pruebas, para entrar en la interfaz de pruebas.

**Probar Todo:** Para probar LCD, voz, sensor de huellas digitales, cámara y RTC. Durante el test.

**Probar LCD :** Para probar el efecto de la exhibición de la pantalla LCD mediante la visualización a todo color, blanco puro y negro puro para comprobar si la pantalla muestra los colores correctamente.

**Probar Voz:** El dispositivo comprueba automáticamente si los archivos de voz almacenados en el dispositivo están completos y la calidad de la voz es buena.

**Probar Sensor Huella:** Para probar el sensor de huellas digitales pulsando huella digital para comprobar si la imagen de la huella obtenida es clara. Cuando se pulsa la huella digital en el sensor, la imagen se visualiza en la pantalla.

**Probar Cámara:** Para probar si la cámara funciona correctamente mediante la comprobación de las fotos tomadas son claras para su uso.

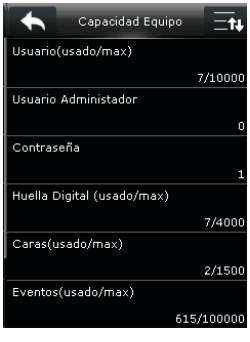
**Probar Reloj RTC:** Para probar el reloj de tiempo real. El dispositivo realiza pruebas para saber si el reloj funciona correctamente y marca con precisión el cronómetro. Pulse la pantalla para empezar a contar el tiempo, y presione la pantalla de nuevo para dejar de contar, para comprobar si el cronómetro cuenta el tiempo con precisión.

# Información del Sistema

Compruebe la capacidad de datos, información del dispositivo y del firmware.




En la pantalla inicial, pulse ▦ > Información del Sistema para acceder a la información de interfaz del sistema.




Capacidad del Dispositivo


Información del dispositivo


Información del firmware

# Información del Sistema

**Capacidad del dispositivo:** Muestra el número de usuarios registrados, administradores, contraseñas, huellas digitales, rostro, tarjetas , registros de asistencia, fotos, lista negra de fotos de usuario.

**Información del dispositivo:** Para visualizar el nombre del dispositivo, número de serie, la dirección MAC, el algoritmo de la huella digital, el algoritmo de reconocimiento facial, información de la plataforma, la versión de MCU, fabricante y fecha de fabricación.

**Información de Firmware:** Para visualizar la versión del firmware, bio service, push service y dev service.

**Nota:** La pantalla de la capacidad del dispositivo, información del dispositivo y la información del firmware en la interfaz información del sistema de los diferentes productos pueden variar; el producto real prevalecerá.

# Solución de Problemas

**• El sensor de huellas digitales no es capaz de leer y verificar la huella de forma efectiva.**

➢ Comprobar si el dedo está mojado, o el sensor de huellas dactilares está húmedo o polvoriento.

➢ Limpiar el dedo y el sensor de huellas digitales y volver a intentarlo.

➢ Si el dedo está demasiado seco, soplarle y volver a intentarlo.

**• "Horario Inválido" aparece después de la verificación.**

➢ Contactar al administrador para comprobar si el usuario tiene el privilegio de acceder dentro de ese horario.

**• La verificación tuvo éxito, pero el usuario no puede abrir la puerta.**

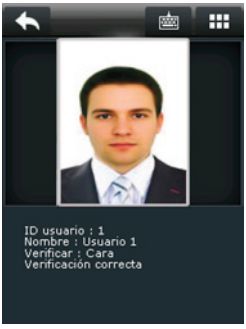
➢ Compruebe si el cableado de la cerradura es correcto.

**• La alarma de sabotaje se activó.**

➢ Compruebe si el dispositivo y la placa posterior fijan entre sí; si no, el interruptor de sabotaje en la parte posterior del dispositivo se activará y sonará una alarma, se mostrará un ícono en la esquina superior derecha de la interfaz. Sólo cuando [alarma de altavoz] (Control de acceso> Opciones de Control de Acceso> Alarma de altavoz) está en [ON] elevará la alarma de altavoz.

## 16.1 Función de identificación con foto

Cuando la función de identificación con foto está activada, y el usuario pasa la verificación, no sólo la información de ID de usuario y el nombre aparecerán, sino también la foto registrada por el usuario o guardada en la unidad USB se mostrarán.




**Nota:** Habilite la opción [**Mostrar foto de Usuario**] (en la interfaz, pulse [**M/OK**]> **Sistema**> **Configuración de registros de acceso**> **Foto usuario en pantalla**, y active la opción [Mostar Foto de usuario]) de forma que se muestre la foto del usuario después de cada verificación exitosa.

**[Procedimiento de operación]**

1. Si se utiliza una foto de usuario tomada por el dispositivo, la foto se mostrará justo después de la verificación del usuario.

2. Si se utiliza una foto de usuario de una USB, el procedimiento de funcionamiento es el siguiente:

(1) Crear una carpeta llamada "photo" en la USB y guardar la foto del usuario en el archivo.

(2) El formato de la foto debe ser JPG, y el archivo debe ser nombrado como el ID de usuario. Por ejemplo: la foto correspondiente al usuario con el ID del 154 debe ser nombrado como 154.jpg.

(3) Inserte la USB en el puerto USB del dispositivo y entre a Gestión USB> Cargar> Foto de usuario para subir fotos de los usuarios. La foto entonces se mostrará después de la verificación del usuario.

**Notas:**

(1) El nombre de la foto debe estar dentro de 9 dígitos.

(2) El tamaño de la foto debe ser inferior a 15kb.

(3) La fotografía recién cargada sustituirá a la foto original del usuario.

(4) Al descargar foto del usuario, entre a Gestión USB> Cargar> Foto de usuario, un archivo denominado como "foto" se creará en la USB de forma automática, en la que se guardarán todas las fotos de usuario descargados.

## 16.2 Wiegand: Introducción

El protocolo wiegand26 es un protocolo estándar de control de accesos desarrollada por el Subcomité de control de acceso estándar afiliado a la Asociación de la Industria de Seguridad (SIA).

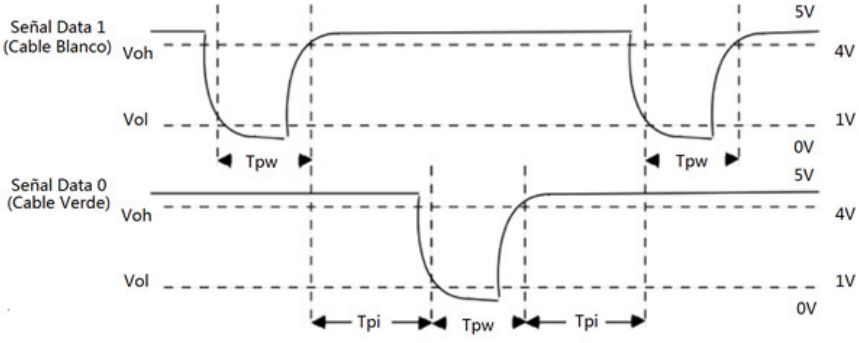
El protocolo define el puerto entre el lector de tarjetas y un controlador que son ampliamente utilizados en el control de acceso, seguridad y otras industrias relacionadas. Esto ha estandarizado el trabajo de los diseñadores y fabricantes de lectores de tarjetas controladoras. Los dispositivos de control de acceso producidos por nuestra empresa también se aplican este protocolo.

**Señal Digital:** La figura 1 muestra el diagrama de secuencia del lector de tarjetas enviando la señal digital en bits al controlador. El Wiegand en este diagrama sigue el protocolo estándar de control de acceso SIA (Asociación de la Industria de la Seguridad, por sus siglas en inglés), que tiene como objetivo un lector de tarjetas Wiegand de 26 bits (Con una duración de pulso de 20 µs. a 100 µs y un salto de frecuencia de 200 µs a 20 ms). Las señales Data 1 y data 0 son de alto nivel (Superior que VOH), hasta que el lector de tarjetas está listo para enviar un flujo de datos. El lector de tarjetas envía un pulso asíncrono bajo (menor que VOL), transmitiendo flujo de datos vía Data 1 y Data 0 a la caja de control de acceso (Como en la onda de sierra en la figura1). Los pulsos de Data 1 y Data 0 no se superponen o sincronizan. La figura 1 muestran el ancho de pulso mínimo y máximo (Pulso consecutivo) y el tiempo de salto de frecuencia (El tiempo entre dos pulsos) permitidos por la serie de terminales de control de acceso de huella digital.

Tabla 1: Duración de Pulso

| Símbolo | Definición | Valores Normales del Lector de Tarjetas |
|---|---|---|
| Tpw | Ancho de Pulso | 100 µs |
| Tpi | Intervalo de Pulso | 1ms |

Figura 1: Diagrama de Secuencia




### 16.2.1 Wiegand26, Introducción.

Composición del formato Wiegand 26: 2 bit de paridad y 24-bit de contenido de salida (ID de usuario o número de tarjeta). El código binario 24-Bit puede indicar 16 777 216 (0-16 777 215) diferentes valores.

| 1 | 25 | 26 |
|---|---|---|
| Bit de Paridad Par | ID de Usuario/ Número de Tarjeta | Bit de Paridad Impar |

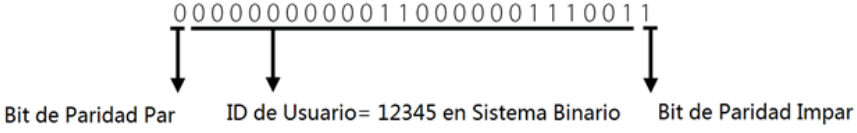
# Apendice

La siguiente tabla describe los campos:

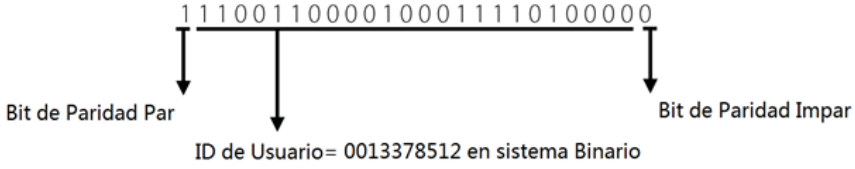
| | |
|---|---|
| Bit de Paridad Par | El bit de paridad par es determinado por los bit 2~13. Si ahí hay un número par de 1's, el bit de paridad par es 0. Si hay un número impar de 1's, el bit de paridad par es 1. |
| ID de Usuario/ Número de tarjeta<br>(Bit 2 a través de bit 25) | El ID de usuario/Número de tarjeta (Código de tarjeta, 0-16777215) y el bit 2 indica el bit más significativo (MSB) |
| Bit de Paridad Impar | El bit de paridad impar es determinado por los bit 14~25. Si ahí hay un número par de 1's, el bit de paridad impar es 1. Si hay número impar de 1's, el bit de paridad impar es 0. |

Ejemplo: Un usuario con el ID 12345 tiene el número de tarjeta 0013378512 y el ID de fallo es establecido en 1.

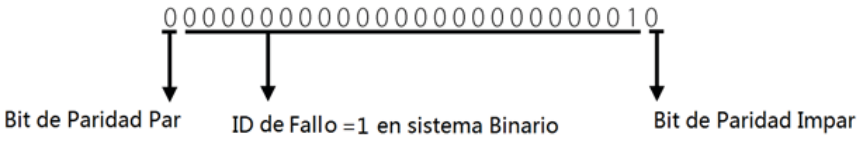
(1). Cuando el contenido de salida es establecido para ID de Usuario, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:



(2). Cuando el contenido de salida es establecido para número de tarjeta, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:




(3). Cuando la verificación falla, la salida Wiegand del sistema es la siguiente:




**Nota:** Cuando el contenido de salida esté por encima del rango predeterminado del formato Wiegand, los últimos bit son reservados y los primeros bits son descartados. Por ejemplo, si un ID de usuario es 888 888 888 que es 110 100 111 110 110 101 111 000 111 000 en sistema binario, los últimos 24 bits (111 110 110 101 111 000 111 000) son emitidos y los primeros 6 bits (110 100) son descartados porque el formato Wiegand 26 sólo soporta 24 bits de salida de contenido.

### 16.2.2 Wiegand34, Introducción

Composición del formato Wiegand 34: 2 bit de paridad y 31 bit de salida de contenido (Id de Usuario o número de tarjeta). Los 32 bits en código binario pueden indicar 4 294 967 296 (0-4 294 297 295) diferentes valores.

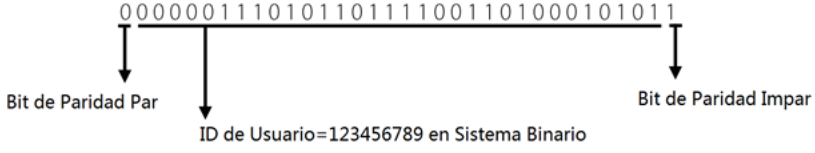
| 1 | 2 33 | 34 |
|---|---|---|
| Bit de Paridad Par | ID de Usuario/ Número de Tarjeta | Bit de Paridad Impar |

La siguiente tabla describe los campos:

| | |
|---|---|
| Bit de Paridad Par | El bit de paridad par es determinado por los bit 2~17. Si ahí hay un número par de 1's, el bit de paridad par es 0. Si hay un número impar de 1's, el bit de paridad par es 1. |
| D de Usuario/ Número de tarjeta<br>(Bit 2 a través de bit 25 | El ID de usuario/Número de tarjeta (Código de tarjeta, 0-4 294 967 295) y el bit 2 indica el bit más significativo (MSB) |
| Bit de Paridad Impar | El bit de paridad impar es determinado por los bit 18~33. Si ahí hay un número par de 1's, el bit de paridad impar es 1. Si hay número impar de 1's, el bit de paridad impar es 0. |

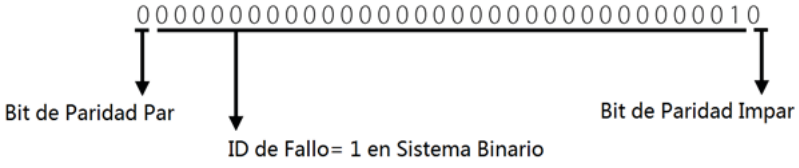
Ejemplo: Un usuario con el ID 123456789 tiene el número de tarjeta 0013378512 y el ID de fallo es establecido como 1.

(1). Cuando el contenido de salida es establecido para ID de usuario, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:



(2). Cuando el contenido de salida es establecido para número de tarjeta, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:


(3). Cuando la verificación falla, la salida Wiegand del sistema es la siguiente:




## 16.3 Reglas para subir Imágenes

**1. Foto de usuario:** Se necesita crear una carpeta llamada "photo" en la unidad USB y agregar las fotos de usuario dentro de esa carpeta. La capacidad es de 3000 imágenes, que cada uno de ellos no exceda de 15k. El nombre de la imagen es x.jpg (x es el ID de usuario real, máx. 9 dígitos). El formato de la foto debe ser JPG.

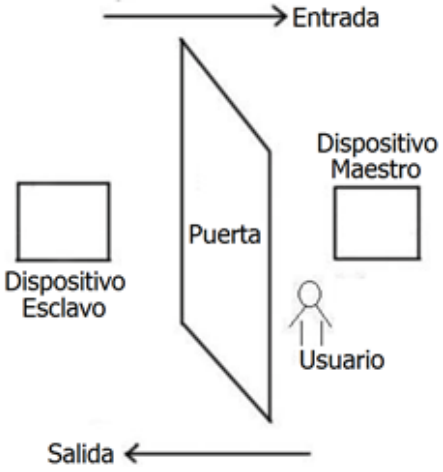
**2. Protector de Pantalla:** Se necesita crear una carpeta llamada "advertise" en la unidad USB y agregar las fotos a usar como protectores de pantalla dentro de esa carpeta.

**3. Fondo de pantalla:** Se necesita crear una carpeta llamada "wallpaper" en la unidad USB y agregar las fotos a usar como fondos de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes con cada uno de ellos no superior a 30k. Nombre y formato de imagen no están restringidas.

**Nota:** Cuando cada foto de usuario y foto de asistencia no exceden 10Kb, el dispositivo puede guardar un total de 10000 fotos de usuario y de asistencia (considerando la capacidad real del dispositivo, se recomienda ampliamente agregar a lo mucho 5000 fotos de usuario y de asistencia.

### 16.4 Configuración del Antipassback

Para evitar que algunas personas sigan a los usuarios para ingresar por una puerta sin autorización, la función Antipassback puede ser establecida. Los registros de entrada deben coincidir con los de salida para abrir la puerta. Esta función requiere que dos dispositivos trabajen juntos: Uno es instalado en el lado de adentro de la puerta (Dispositivo Maestro) y el otro es instalado en la parte de afuera (Dispositivo Esclavo). Los dos dispositivos se comunican por medio de señal Wiegand. El formato Wiegand y el tipo de salida (ID de usuario/Tarjeta) adoptado por los dispositivos Esclavo y Maestro deben coincidir.



**[Principio de Funcionamiento]**

El dispositivo maestro soporta la señal de entrada Wiegand y el dispositivo esclavo soporta la señal de salida Wiegand. Después que el puerto de salida Wiegand del dispositivo esclavo es conectado al puerto de entrada Wiegand del dispositivo maestro, la señal Wiegand emitida por el dispositivo esclavo no puede contener el ID del dispositivo y los ID de usuarios enviados al maestro deben existir en el dispositivo maestro. Esto significa que la información del usuario en el dispositivo esclavo, soportando la función Antipassback debe corresponder a la información del usuario en el dispositivo maestro.

**[Descripción de las Funciones]**

El dispositivo detecta el Antipassback basado en el último registro entrada/ Salida de los usuarios. El registro entrada debe coincidir con el último registro Salida. El dispositivo soporta Antipassback de Salida, Antipassback de Entrada y Antipassback de Entrada/Salida.

Cuando el Antipassback de Salida es establecido para un usuario en el dispositivo maestro, el último registro del usuario debe ser un Entrada si el usuario necesita hacer Entrada/out libremente. De lo contrario, el usuario no puede hacer el Salida y la petición de Salida es rechazada por el Antipassback. Por ejemplo; si el primer reciente registro del usuario es un Entrada, el segundo registro puede ser un Entrada o un Salida pero el tercer registro debe ser basado en el segundo, asegurando que el Entrada coincida con el Salida.

**Nota:** Si el usuario no tiene un registro previo, sólo puede registrar entrada.

# Apendice

Cuando el **Anti-Passback de Entrada** es establecido para un usuario en el dispositivo maestro, el último registro del usuario debe ser una salida si el usuario necesita hacer entrada/salida libremente. De lo contrario, el usuario no puede hacer una entrada y la petición de los usuarios es rechazada debido al Anti-Passback.

**Nota:** Si un usuario no tiene registro previo, sólo puede hacer Salida.

Cuando el Anti-Passback de Entrada/Salida es establecido en el dispositivo maestro, si el último registro del usuario es una Salida el siguiente registro debe ser un Check –in y viceversa; para que el usuario pueda realizar el próximo entrada/salida sin problemas. Esto significa, que los registros de entrada y Salida deben coincidir siempre.

**[Descripción de la Operación]**

(1). Selección del Modelo

Dispositivo Maestro: Dispositivos que soportan la función Wiegand de entrada, excepto el lector F10.

Dispositivo Esclavo: Dispositivos que soportan la función de salida Wiegand.

(2). Configuraciones del Menú

**Dirección del Anti-Passback**

Las opciones de dirección del Anti-Passback incluyen Anti-Passback de Entrada/Salida, Anti-Passback de Salida, Anti-Passback de Entrada y No Anti-Passback.

- Anti-Passback de Salida: Sólo si el último registro es una Entrada el usuario puede realizar la Salida de nuevo.
- Anti-Passback de Entrada: Sólo si el último registro es una Salida el usuario puede hacer Entrada de nuevo.

(3). Modificar el Formato de Salida Wiegand del Dispositivo

Cuando dos dispositivos se comunican entre sí, sólo las señales Wiegand que no se contentan el ID del Dispositivo son aceptables. En el dispositivo usted puede utilizar la opción Menú Principal>> configuración Wiegand o acceda al Software y elija las opciones Configuración Básica >> Gestión de Dispositivos >> Wiegand y establezca los parámetros Definir Formato para Wiegand 26-bits o Wiegand26 Sin ID de Dispositivo.

(4). Registro de Usuario

Los ID de los usuarios deben existir en ambos dispositivos (esclavo y maestro) y deben coincidir.  Por lo tanto, los usuarios deben ser registrados en los dos dispositivos.

(5). Descripción del Cableado

Los dispositivos esclavo y maestro se comunican entre sí por medio de Wiegand y el cableado es el siguiente:

| Dispositivo Maestro | Dispositivo Esclavo |
|---:|---|
| IWD0 | WD0 |
| IWD1 | WD1 |
| GND | GND |

## 16.5 Declaración de Derechos Humanos y de Privacidad

Apreciado consumidor:

Gracias por elegir las soluciones diseñadas y fabricadas por el equipo ZK. Como proveedor líder en el mercado de productos y soluciones biométricas, nos esforzamos por cumplir los estatutos relacionados con los derechos humanos & privacidad de cada país. Por esta razón consignamos en este documento la siguiente información:

1. Todos dispositivos de reconocimiento de huella digital ZKTeco para uso civil, sólo recogen puntos característicos de las huellas digitales, no imágenes como tal. Gracias a esto no se suscitan problemáticas que involucren o violen la privacidad de los usuarios.
2. Los puntos característicos de las huellas digitales recolectadas por nuestros dispositivos no pueden ser utilizadas para reconstruir la imagen original de la huella.
3. ZKTeco como proveedor de los equipos, no se hace legalmente responsable directa o indirectamente por ninguna consecuencia generada debido al uso de nuestros productos.
4. Por cualquier inconveniente que involucre los derechos humanos o la privacidad de los mismos cuando se utilicen nuestros productos, por favor contacte directamente a su empleador directamente.

Nuestros otros equipos de huella digital de uso policíaco u herramientas de desarrollo, pueden proporcionar la función de recolección de las imágenes originales de las huellas digitales de los ciudadanos. Cuando considere que este tipo de recolección de huellas infringe su privacidad, por favor contacte al gobierno local o al proveedor final. ZKTeco como el fabricante original de los equipos, no se hace legalmente responsable de ninguna infracción generada por esta razón.

**Nota:** Las siguientes son regulaciones ligadas a las leyes de la República popular de China acerca de la libertad personal:

# Apendice

1. Detención, reclusión o búsqueda ilegal de ciudadanos de la República Popular de China es una violación a la intimidad de la persona, y está prohibida.

2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.

3. El hogar de los ciudadanos de la República Popular de China es inviolable.

4.La libertad y privacidad correspondiente a los ciudadanos de la República Popular de China están protegidos por la ley.

Recalcamos que la biometría, como avanzada tecnología de reconocimiento, será aplicada en diversos sectores; incluyendo el comercio electrónico, sistemas bancarios, aseguradoras y cuestiones legales. Cada año alrededor del mundo, una gran cantidad de personas sufren inconvenientes causados por la inseguridad de las contraseñas.

En la actualidad, el reconocimiento de huellas digitales es utilizado para una protección adecuada de la identidad de las personas brindando un ambiente de alta seguridad en todo tipo de empresa.

# Descripción Medio Ambiental

El EFUP (Periodo de Uso Amigable con Medio Ambiente, por sus siglas en inglés) marcado en este producto, se refiere al periodo de seguridad en el cual el producto es utilizado bajo las condiciones establecidas en las instrucciones del mismo, sin riesgo de fuga de sustancias nocivas o perjudiciales.

El EFUP de este producto no cubre las partes consumibles que necesiten ser reemplazadas regularmente, como por ejemplo, las baterías. El EFUP de las baterías es de 5 años.

| Nombre y concentración de sustancias o elementos nocivos | | | | | | |
|---|---|---|---|---|---|---|
| Nombre de las piezas | Sustancias o elementos nocivos | | | | | |
| | Pb | Hg | Cd | Cr6+ | PBB | PBDE |
| Resistencia | X | O | O | O | O | O |
| Condensado | X | O | O | O | O | O |
| Inductor | X | O | O | O | O | O |
| Diodo | X | O | O | O | O | O |
| Componentes ESD | X | O | O | O | O | O |
| Buzzer | 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 tóxica o nociva está presente en todos los materiales homogéneos de esta pieza, por debajo de los límites requeridos en SJ/T11363-2006.

X: Indica que esta sustancia tóxica o nociva está presente en al menos uno de los materiales homogéneos de esta pieza, por encima de los límites requeridos en SJ/T11363-2006.

Nota: El 80% de las partes de este producto están fabricadas con materiales ecológicos. Las sustancias o elementos nocivos contenidos, no pueden ser reemplazados por materiales ecológicos por razones técnicas o restricciones económicas.

Green Label

www.zkteco.com

www.zktecolatinoamerica.com