# Manual de Usuario

PFace202

Reconocimiento Facial y
Palma touch de 4.3

# DECLARACIÓN IMPORTANTE

Gracias por elegir nuestro producto. Lea este manual detenidamente para evitar daños en el dispositivo antes de su uso. Le recordamos que a través del uso adecuado, puede experimentar buenos efectos y velocidad de verificación.
Ninguna parte de este documento puede ser reproducida, copiada o transmitida por ningún medio sin el previo consentimiento por escrito de nuestra compañía.

Los productos descritos en este manual pueden contener software perteneciente a nuestra empresa o licenciatarios que poseen derechos de autor. Derechos de autor, exclusivo, por, modificar, extraer, descompilar, desensamblar, decodificar, aplicar ingeniería inversa, alquilar, transferir, sublicenciar software en cualquier forma u otra conducta que infrinja el copyright del software, excluyendo los casos con prohibición de tal limitación por las leyes aplicables

Debido a la actualización del producto, nuestra compañía no promete la consistencia del manual con los productos reales, y no asume ninguna responsabilidad por cualquier problema que surja de la discrepancia entre los parámetros técnicos reales y este manual. El manual está sujeto a cambios sin previo aviso.

# ACERCA DE ESTE MANUAL

• Este manual presenta el funcionamiento de las interfaces de usuario de 4.3 pulgadas y las funciones del menú Palm Attendance Terminal. Para la instalación, consulte Asistencia de Palm de 4.3 pulgadas Terminal Guía de inicio rápido.

• No todos los dispositivos tienen la función con ★ , Varia el producto real.

• Las imágenes de este manual pueden no ser consistentes con las de su producto;
la exhibición del producto real prevalecerá.

## 1. Introducción

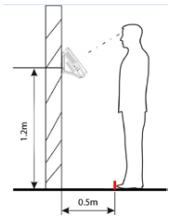
Este producto es una terminal de control de acceso y tiempo y asistencia, que se puede conectar con cerradura eléctrica, sensor de puerta, alarma y botón de salida, etc.
Con el último algoritmo de identificación de palma / huella digital y tecnología optimizada, puede contener 600 plantillas de palma y hasta 2,000 plantillas de huellas digitales sin dividirse en grupos.
Al comunicarse a través de Wi-Fi, TCP / IP y un cliente USB, garantiza una conexión y transferencia de datos fluidas. La increíble velocidad de verificación y el proceso de operación intuitivo lo hacen popular.
Elaboradamente diseñado y finamente procesado, combina perfectamente con su oficina.

| | |
|---|---|
| **PANTALLA** | Pantalla táctil de 4.3 pulgadas |
| | |
| **CAPACIDAD** | Capacidad de la palma: 600 (estándar) |
| | Capacidad de huella digital: 2,000 |
| | Capacidad de cara: 1200 |
| **CAPACIDAD EN TARJETAS** | ID 10,000 (Opcional) |
| **CAPACIDAD DE EVENTOS** | 100 |
| **COMUNICACIÓN** | TCP/IP WIFI |
| **FUNCIONES ESTÁNDAR** | Cambio automático de estado, consulta de autoservicio |
| | Botón de salida, bloqueo de la puerta, 12V de SALIDA, alarma |
| | Código de trabajo, Entrada T9, ID de usuario de 9 dígitos, DST, Timbre programado |
| | SMS, sensor de puerta, Wiegand HACIA FUERA |
| **FUNCIONES OPCIONALES** | Tarjeta de identificación, Mifare, tarjeta HID, 3G, módulo de batería, ADMS, RS485 |
| | lector, Impresora RS232 |
| **FUENTE DE ALIMENTACIÓN** | 12V / 3A |
| **VELOCIDAD DE VERIFICACIÓN** | < 1 seg |
| **TEMPERATURA DE OPERACIÓN** | 0-45 ° C |
| **HUMEDAD DE FUNCIONAMIENTO** | 20%-80% |

## 2. Notas de Orientación

### 2.1 Posición de pie, expresión facial y postura.

*** Posición de pie recomendada**




La distancia entre una persona y el dispositivo es recomendado es 0.5 metros (rango de altura aplicable de 1.5-1.8 metros).

*** Expresión Facial y Postura**

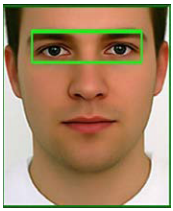


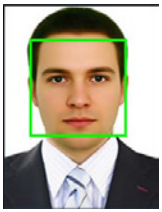


Nota: Durante el enrolamiento y verificación, mantenga la expresión facial y la postura natural

### 2.2 Posición de pie, expresión facial y postura.

Durante la inscripción, debe avanzar o retroceder para asegurarse de que sus ojos estén dentro del marco verde. Durante la comparación, asegúrese de que la cara se muestre en el centro de la pantalla y se encuentra dentro del marco verde



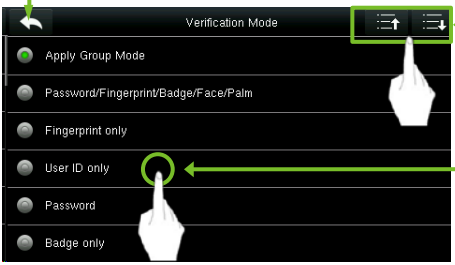
Se recomienda que muestre la cara en el medio de la pantalla y enfoque los ojos dentro del marco verde de acuerdo con la indicación.

## 2.3 Estado de Iconos

| ÍCONO | NOMBRE | DESCRIPCIÓN |
|---|---|---|
| | intensidad de la Célula | Los iconos de estado indican si se encuentra dentro de la cobertura de la red móvil celular, con más barras verdes que indican una señal más fuerte. |
| | | G: indica que la red móvil actual es la red GPRS, a través de la cual el dispositivo accede a Internet. |
| | | E: indica que la red EDGE (GSM) del operador está disponible, a través de la cual el dispositivo accede a Internet. |
| | | W: indica que la red móvil actual es la red WCDMA, a través de la cual el dispositivo accede a Internet |
| | | H: indica que la red móvil actual es la red HSDPA, a través de la cual el dispositivo accede a Internet. |
| | | T: indica que la red móvil actual es la red TD-SCDMA, a través de la cual el dispositivo accede a Internet. |
| | | 1X: indica que la red móvil actual es la red CDMA 1X, sobre la cual el dispositivo accede a Internet. |
| | | 3G: indica que la red 3G UMTS (GSM) o EV-DO (CDMA) del operador está disponible. |
| | | Indica que no hay una red móvil disponible. |
| | Timbre | Indica que ha configurado el timbre. |
| | | Indica el desarmado de la alarma. |
| | Ethernet | Indica que la conexión a Ethernet se ha establecido. |
| | | indica que la red Ethernet está desconectada. |
| | Servidor ADMS | La conexión entre el dispositivo y el servidor ADMS es exitosa. |
| | | La conexión entre el dispositivo y el servidor ADMS ha fallado. |
| | | Los datos de comunicación de ADMS están transmitiendo. |
| | SMS | Hay mensajes cortos públicos. |
| | Señal Wi-Fi | La conexión Wi-Fi es normal. |
| | | La conexión Wi-Fi falla. |

## 2.4 Operaciones Touch

### 2.4.1 Operaciones Básicas




**Devolver y guardar**

**Re Pág. y Av Pág.**
Nota: Si la lista no tiene mucho contenido y el menú puede mostrarse completamente cuando presiona **Re Pág**. una sola vez, solo la tecla **AvPág** se muestra aquí.

Puede seleccionar una opción solo grabando la línea donde está esta opción de menú, y el sistema regresa automáticamente a la interfaz anterior.

Nota: Durante las operaciones, después de registrar o modificar la información del usuario o establecer los parámetros, debe tocar Volver / Guardar para que la configuración surta efecto. Si se agota el tiempo de espera y no hay operaciones en la interfaz, el sistema regresa a la interfaz principal sin guardar el registro, la modificación de la información del usuario ni la configuración de los parámetros.

### 2.4.2 Teclado Suave

**Teclado digital**


**Área de visualización de contenido**

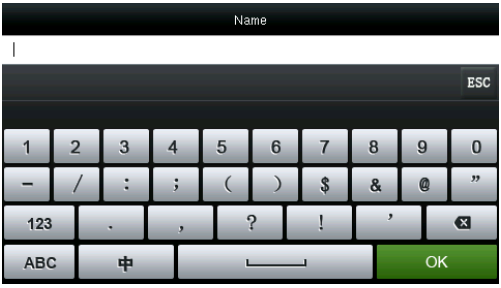
**Borrar la entrada anterior**

**Confirmar el comando**

**Tecla de retorno**

**Teclado Alfabético**


**Teclado Alfanumérico**




## 2.5 Verificación

Verificación de huella digital 1:N
En este método de verificación de huellas, se verifica una huella dactilar recogida por el sensor con todas las huellas dactilares almacenadas en el dispositivo.

Para ingresar al modo de verificación de huellas digitales. El dispositivo distingue automáticamente la verificación de rostro y huella digital, simplemente presionando el dedo sobre el colector. Deberá ser el modo de autenticación de huellas dactilares.

Utilice la forma correcta de presionar la huella digital en el sensor de huellas dactilares (para obtener la información detallada)


**Verificación Exitosa**


**Verificación Fallida**

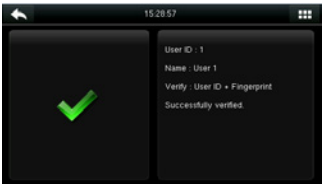
**Verificación de huellas 1:1**

Según este método de verificación de huellas dactilares, una huella dactilar recogida por el sensor se verifica con la huella digital correspondiente a la identificación de usuario introducida. Utilice este método cuando se encuentre dificultad en la verificación de huellas dactilares 1: N

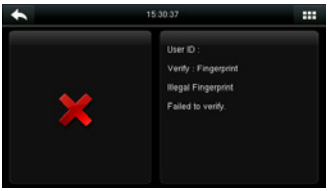
Presione en la pantalla para ingresar al modo de verificación 1: 1


1. Ingrese su id y presione OK


2. Presione su Huella para verificación

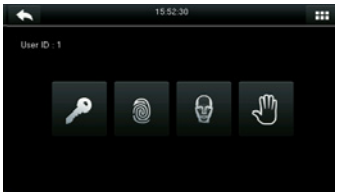



3. Verificación exitosa




4. Verificación fallida

Si ha registrado varios modos de verificación, aparecerá la siguiente interfaz después de ingresar su ID y toque [OK].




Toca el icono de Huella digital para acceder la interfaz de verificación de huella digital


Presione su dedo sobre el escáner de huellas digitales para escanear su huella digital para verificarla. El resultado se muestra como arriba.

Nota: si ha registrado solo su huella dactilar, accederá a la interfaz de verificación de huellas dactilares directamente después de ingresar su ID. Si se ha registrado en varios modos de verificación, se mostrarán los iconos de los modos de verificación registrados, como se muestra en la figura anterior. Como contraseña, huella dactilar, cara y palma.

### 2.5.2 Asistencia basada en la cara

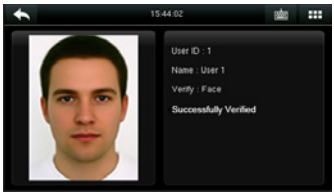
Método de reconocimiento 1: N de cara

Compare la imagen facial capturada por la cámara con todos los datos faciales en el dispositivo.

• El dispositivo diferencia automáticamente entre los modos de verificación de rostro y huella digital.

Coloque su cara dentro del área de captura de la cámara (sin que se coloque su dedo en el escáner de huellas digitales), y el dispositivo automáticamente realiza la detección en el modo de verificación de rostros.


Realice la comparación de la manera correcta en la interfaz principal



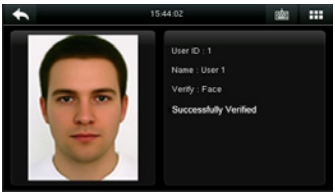

Verificación exitosa

**Método de reconocimiento 1: 1 de cara**

Compare la imagen facial capturada con la imagen facial asociada con la ID de usuario ingresada.
Nota: Si se indica "No hay datos registrados" después de que el usuario ingrese la ID y presione [OK], el usuario correspondiente a esta ID no existe

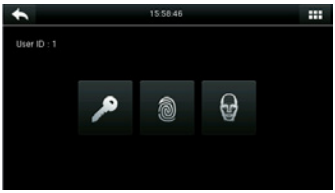

1. Ingrese la ID de usuario en la interfaz principal usando el teclado y luego presione [OK]


2. Compare su cara




3. Verificación aprobada. Si la verificación falla durante 20 segundos consecutivos, el sistema volverá a la interfaz principal.

Si ha registrado varios modos de verificación, aparecerá la siguiente interfaz después de ingresar su ID y toque [OK].



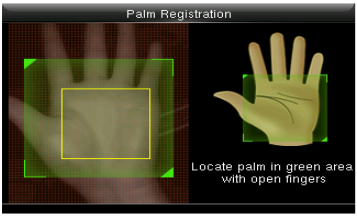

Toca el ícono de la cara para acceder a la verificación de la cara.


El resultado de la verificación se muestra como arriba.

Nota: si ha registrado solo su rostro, accederá a la interfaz de verificación de caras directamente después de ingresar su ID. Si se ha registrado en múltiples modos de verificación, se mostraran los íconos de los modos de verificación registrados, como se muestra en la figura anterior con contraseña, huella digital y rostro.

### 2.5.3 Modo de verificación de palma

El dispositivo compara la palma actual con la palma de los usuarios en el dispositivo. Use la forma correcta de inscribirse y verificar.



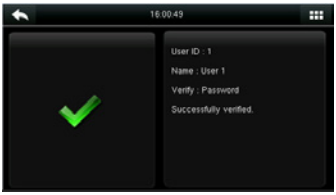
### 2.6.4 Modo de verificación por Contraseña

Con este método de verificación, la contraseña ingresada se verifica con la contraseña del usuario ingresado.

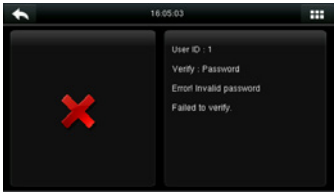
**Toque el botón [1: 1] en la interfaz principal para ingresar al modo de verificación 1: 1**


1. Ingrese la ID de usuario y presione [OK]


2. Ingrese la contraseña y presione [OK].

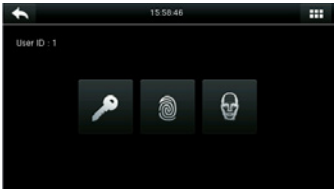



3. Verificación exitosa




4. Verificación fallida

Si ha registrado varios modos de verificación, aparecerá la siguiente interfaz después de ingresar su ID y toque [OK].



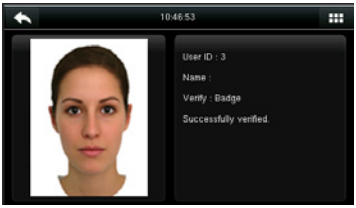

Toca el ícono de la tecla para acceder a la verificación de contraseña.


El resultado de la verificación se muestra como arriba.

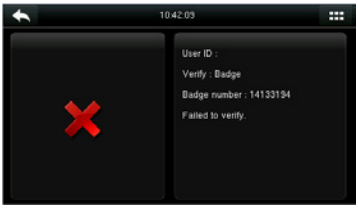
Nota: si ha registrado solo su rostro, accederá a la interfaz de verificación de caras directamente después de ingresar su ID. Si se ha registrado en múltiples modos de verificación, se mostraran los íconos de los modos de verificación registrados, como se muestra en la figura anterior con contraseña, huella digital y rostro.

### 2.6.5 Modo de verificación por Tarjeta ★

El modo de tarjeta es opcional, solo equipos biométricos equipados con este módulo pueden cumplir esta función

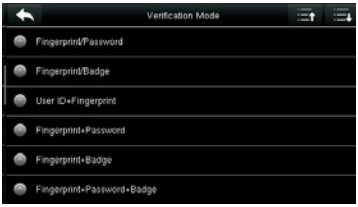



Verificación exitosa




Verificación fallida, mostrara una ventana si la tarjeta no está registrada

Con el fin de satisfacer las necesidades de algunas ocasiones de control de acceso con alta seguridad y teniendo en cuenta la diversidad del control de acceso, el dispositivo proporciona una amplia gama de modos de verificación, que se pueden combinar según sea necesario para usuarios individuales y grupos de usuarios. El dispositivo admite 21 modos de verificación de combinaciones, como se muestra en la siguiente figura.



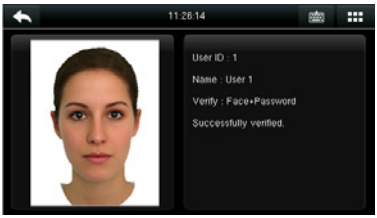

Nota! "/" Significa "o" y "&" significa "y"

En el modo de verificación combinada, debe registrar la información de verificación requerida; de lo contrario, la verificación puede fallar. Por ejemplo, si el usuario A usa el registro de huellas digitales pero el modo de verificación es PW, este usuario nunca pasará la verificación.
Lo siguiente toma Face & Password como ejemplo para presentar el modo de verificación de combinación.

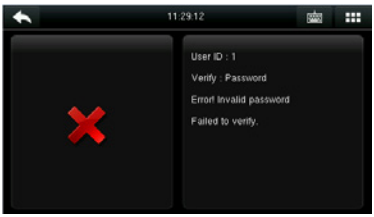
• Coloque su cara dentro del área de captura de la cámara, y el dispositivo automáticamente realiza la detección en el modo de verificación de cara


1. Proceso de verificación de rostro


2. La interfaz de entrada de contraseña aparece una vez que pasa la verificación. Ingrese la contraseña y toque [OK].




3. Verificación de contraseña y rostro exitoso




4. Verificación fallida de contraseña y rostro

Nota: La verificación combinada solo está disponible si se seleccionan los modos de verificación correspondientes durante el registro del usuario.

## 3. Menú Principal

Cuando el dispositivo está en modo de espera, presione para abrir el menú principal.



| ICONO DEL MENÚ | DESCRIPCIÓN |
|---|---|
| User Admin | Información básica de usuarios registrados, que incluye identificación de usuario, rol de usuario, huella dactilar, Tarjeta ★ (ID, tarjeta MiFare y HID son opcionales), contraseña, rostro, palma y función de control de acceso. |
| Rol de Usuario | Para establecer las funciones del usuario para acceder al menú y cambiar la configuración. |
| Comunicación | Para establecer los parámetros relacionados de la comunicación entre el dispositivo y la PC, incluidos los parámetros de Ethernet, como la dirección IP,etc. Com. Serie, conexión de PC, red inalámbrica, configuración de Cloud Server y configuración de salida de Wiegand |
| Sistema | Para configurar los parámetros relacionados del sistema y actualizar el firmware, incluidos el ajuste de fecha y hora, la asistencia, la cara, el parámetro de la palma y los parámetros de la huella digital y el restablecimiento de la configuración de fábrica. |
| Personalización | Esto incluye la pantalla de la interfaz, Sonido, la Sirena externa, el modo de tecla de estado de verificación y la configuración de la tecla de acceso directo. |
| Adm. Datos | Eliminar datos, hacer copias de seguridad de datos, restaurar datos, etc. |
| Control de acceso | Esto incluye establecer los parámetros de la cerradura. |
| Adm. USB | Para transferir datos como datos de usuario y registros de asistencia desde el disco USB al software compatible u otros dispositivos. |
| Asistencia | Para buscar los registros almacenados en el dispositivo después de una verificación exitosa |
| Impresión | Para configurar la información y las funciones de impresión (si la impresora está conectada al dispositivo) |
| Mensaje corto | Para establecer mensajes cortos públicos o privados, que son leídos por objetos especificados dentro del tiempo especificado después de la asistencia, lo que facilita la transmisión de información |

| | |
|---|---|
| Código de trabajo | Para marcar diferentes categorías de trabajo, facilitar el control de asistencia del usuario |
| Auto test | Para probar automáticamente las diferentes funciones del módulo, incluida la pantalla LCD, sonido, teclado, sensor de huellas dactilares, prueba de RTC de la cara y el reloj |
| Info. Sistem. | Para probar automáticamente las diferentes funciones del módulo, incluida la pantalla LCD, sonido, teclado, sensor de huellas dactilares, prueba de RTC de la cara y el reloj |

Nota: Si no hay un súper administrador disponible en el dispositivo, cualquiera puede acceder al menú de operaciones presionando . Después de configurar un administrador en el dispositivo, el administrador debe realizar la autenticación de identidad para acceder al menú. Un usuario puede acceder al menú solo después de la autenticación de identidad exitosa. Para fines de seguridad del dispositivo, se recomienda registrar a un administrador cuando el dispositivo se utiliza por primera vez. Para operaciones específicas, consulte la sección 3.3 Configuración de la función de usuario.

## 4. Agregar un Usuario

Toque Nuevo usuario en la interfaz del menú principal.


Presione Nuevo Usuario


Toca Página abajo para ver otras opciones

### 4.1 Ingrese una ID de usuario

El dispositivo asigna automáticamente identificadores de usuario para el personal, comenzando desde 1 y así sucesivamente. La identificación del usuario también se puede ingresar manualmente

**Seleccionar ID de usuario**


Nota:
1. Por defecto, un ID de usuario contiene de 1 a 9 dígitos. Para ampliar la longitud, consulte a nuestro personal de soporte técnico.
2. Durante el registro inicial, puede modificar su ID, que no se puede ser modificado después del registro.
3. Si se muestra "ID ya existe", se refiere a que ya se utilizó este ID. Por favor ingrese un ID distinto.

**Presione OK para confirmar**

### 4.2 Ingrese el nombre de usuario

**Seleccionar rol de usuario**


Ingrese su nombre y toque Aceptar para guardar


La entrada del nombre es completada

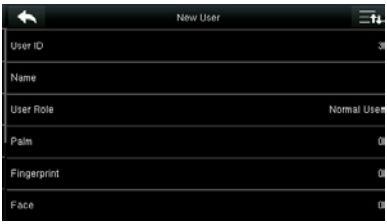
Nota: Predeterminadamente, un nombre de usuario contiene 1-12 caracteres. Para más detalles, consulte la sección 1.7.2 Teclado

## 4.3 Establecer el rol del usuario

Hay dos tipos de funciones otorgadas respectivamente a dos tipos de usuarios: el usuario y el administrador. Al usuario solo se le otorgan los derechos de verificación facial, de huellas dactilares, de palma o de contraseña, mientras que al administrador se le concede el acceso al menú principal para varias operaciones además de tener todos los privilegios otorgados al usuario.

**Toca, rol del usuario**

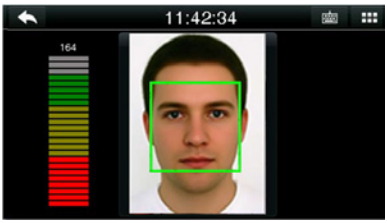

**Seleccionar rol de usuario**




**La selección de rol de usuario está completa**

Si la función del usuario seleccionado es Súper Admin, la autenticación de identidad debe realizarse para el acceso al menú principal. El proceso de autenticación depende del modo de autenticación que el súper administrador haya registrado. El siguiente es un ejemplo de acceso al menú principal como el súper administrador mediante la autenticación de la cara.

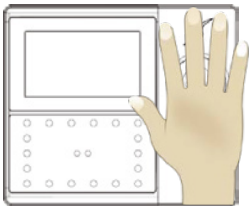

**Presione ▦ para la interfaz principal**




**Coloque su cara delante de la cámara para autenticación**

## 4.4 Enrolar la palma

Como enrolar correctamente la palma

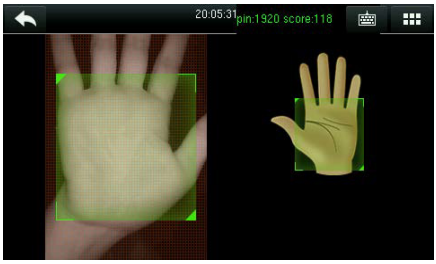


Coloque su palma en el área de recolección multimodal de la palma, de modo que la palma se coloque paralela al dispositivo.

Asegúrese de mantener espacio entre tus dedos.

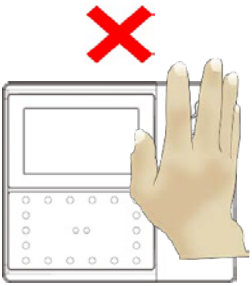
Durante la inscripción, ubique su palma en el centro de la pantalla y siga las indicaciones de voz "Enfoque el centro de la palma, dentro del recuadro verde". El usuario debe avanzar y retroceder para ajustar la posición de la palma durante el registro de la palma.

**Verificación**



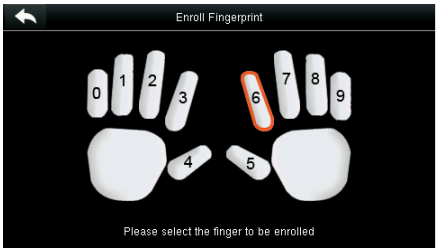

Coloque su palma en el área verde paralela al dispositivo con espacio entre los dedos.

**Gestos de palma incorrectos**

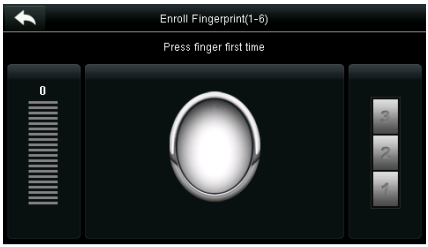


## 4.5 Enrolar una Huella Dactilar

**Presiona Huella Dactilar**

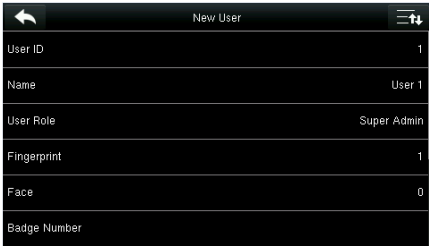



**1. Toca para seleccionar un dedo para el registro de huellas dactilares**



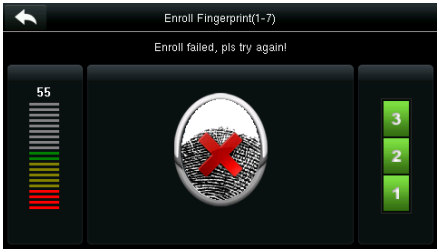

**2. Presione el mismo dedo en el escáner de huellas digitales por tres veces consecutivas como se le solicite**


**3. Registro exitoso.**

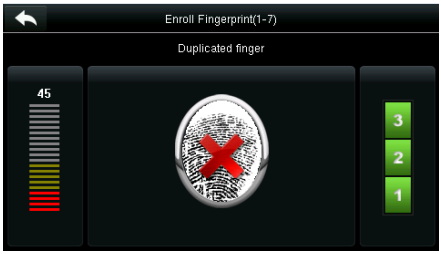



**4. El sistema vuelve automáticamente a la interfaz de Nuevo Usuario.**

Si el registro de la huella digital falla, aparece el siguiente mensaje



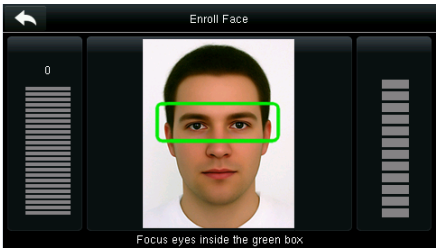

**Registro de huella digital fallido.**
**Necesita registrar una huella digital nuevamente.**



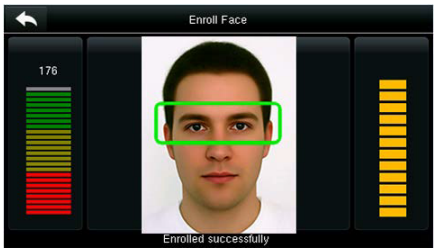

**Si se indica "Huella digital duplicada", esta huella digital ya se ha registrado.**

Nota: Para registrar otra huella dactilar, vuelva a la interfaz de usuario nuevo, toque Fingerprint nuevamente y repita los pasos anteriores para seleccionar otro dedo para el registro de la huella digital

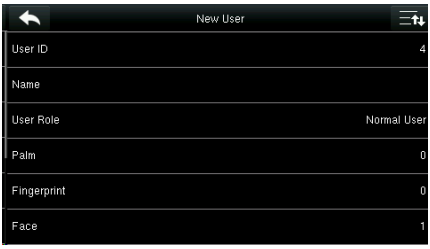
## 4.6 Enrolar una Cara



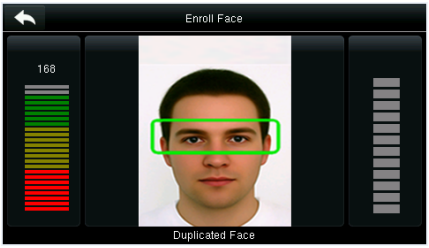

**Siga las indicaciones de la voz y la interfaz para moverse hacia adelante y hacia atrás y colocar sus ojos dentro del marco verde.**




**Registro de cara exitoso**



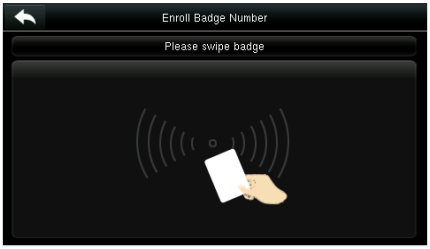

El sistema vuelve automáticamente a la interfaz de Nuevo Usuario.



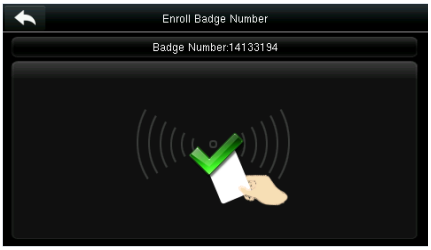

Si se registra una cara duplicada, el sistema indica: “Cara duplicada”.

## 4.7 Enrolar una Tarjeta ★

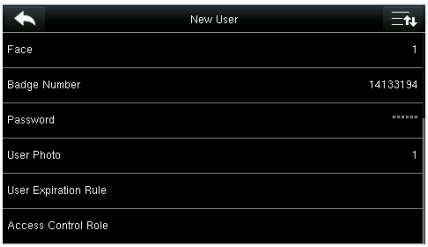
Toca Tarjetas




Coloque su tarjeta de identificación debajo del colector de huellas digitales.




Registro de tarjeta exitoso.

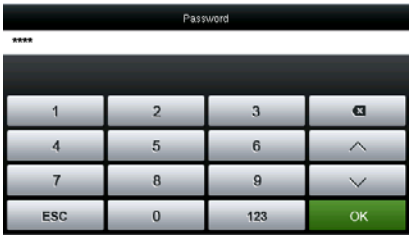



El sistema vuelve automáticamente a la interfaz de Nuevo Usuario.

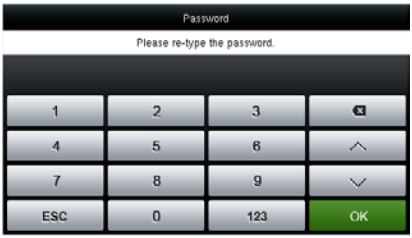

Nota: si la tarjeta ha sido enrolada, Indicara “Tarjeta Duplicada”.

## 4.8 Enrolar una Contraseña

**Toca Contraseña**

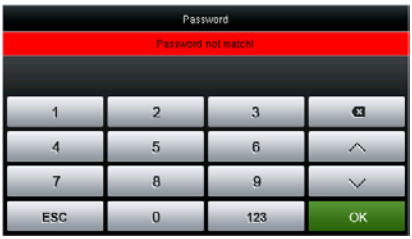



**1. Ingrese la contraseña y toque OK.**




**2. Ingresa la contraseña nuevamente y toca OK.**


**Si el registro es exitoso el sistema vuelve automáticamente a la interfaz de Nuevo Usuario.**

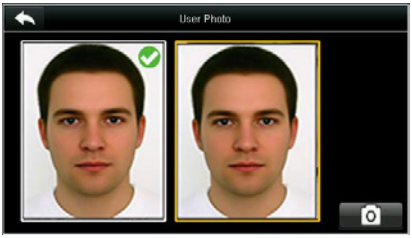



**Si las dos contraseñas ingresadas son distintas, se mostrara "Contraseña no Coincide".**

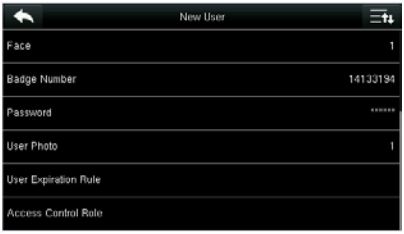
## 4.9 Enrolar una Foto

Cuando un usuario registrado con una imagen pasa la autenticación, se muestra la imagen del usuario registrado.

**Toca Foto de Usuario**




**Toca el ícono de la cámara para tomar una foto.**




**Una vez que la toma de fotografía es completada, el sistema vuelve a la interfaz de Nuevo Usuario.**

Nota: Una vez que se completa el registro facial, el sistema toma una foto automáticamente. Si no desea registrar una imagen de usuario, la imagen tomada automáticamente por el sistema se usa de forma predeterminada.

## 4.10 Configuración de los Privilegios de Control de Acceso

Puede establecer a qué grupo pertenece un usuario, el modo de verificación de acceso, si registrar una huella digital de amago y si se debe utilizar el período de tiempo del grupo. De forma predeterminada, el permiso de desbloqueo se concede a los usuarios recién inscritos

**Toca Rol de Control de Acceso**


### 4.10.1 Grupo de Acceso

Grupo de acceso: seleccione el grupo perteneciente. De forma predeterminada, un usuario recién inscrito pertenece al grupo uno.


**Ingrese el grupo perteneciente y toque OK.**


**El sistema vuelve a la interfaz de Control de acceso.**

### 4.10.2 Modo de Verificación

**Toca modo de verificación**


**Seleccione un modo de verificación.**

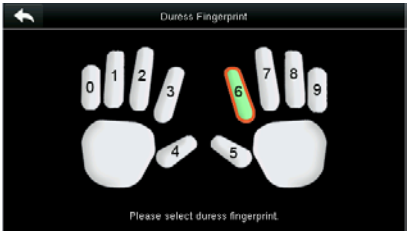

**El sistema vuelve a la interfaz de Control de acceso.**

Nota: Un usuario puede seleccionar Aplicar modo de grupo. Es decir, el usuario puede verificarse mediante el modo de verificación del grupo al que pertenece este usuario o mediante el uso de un modo de verificación individual. Para obtener detalles sobre la configuración del grupo, consulte la sección 10.4 Configuración del grupo de acceso.

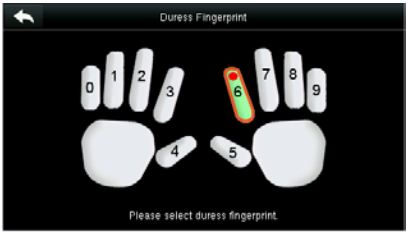
### 4.10.3 Huella Digital de Amago

Una huella dactilar registrada en el dispositivo está especialmente especificada como una huella digital de amago. En cualquier caso, se genera una alarma de amago cuando una huella dactilar coincide con una huella digital de amago. Después de que se cancela una huella digital de amago, la huella dactilar no se elimina y el dedo correspondiente todavía se puede usar para la comparación normal.

**Toca Huella de Amago**




**Seleccione una Huella de amago.**




**Si la selección tiene éxito. Toca el botón Volver.**


**El sistema vuelve a la interfaz de Control de acceso.**

Nota:
1. La huella digital de amago seleccionada debe ser una huella dactilar registrada.
2. Si no desea utilizar una huella dactilar de amago, acceda al mismo menú durante la edición del usuario

### 4.10.4 Aplicar período de tiempo grupal

Elija si desea aplicar el período de tiempo del grupo para este usuario, sí de forma predeterminada. Si no se aplica el período de tiempo del grupo, debe establecer el tiempo de desbloqueo para este usuario. En este momento, el período de tiempo de este usuario no afecta el período de tiempo de ningún otro miembro de este grupo.


**1. Toque Período de tiempo 1.**


**2. Ingrese el número del período de tiempo y toque OK.**


Nota: Se pueden configurar un total de 50 períodos de tiempo en el dispositivo y se pueden establecer tres períodos de tiempo para cada usuario. Para más detalles, vea 10.2 Configuraciones de horario.

**3. Seleccione el período de tiempo 2 y 3 de la misma manera e ingrese los números del período de tiempo.**

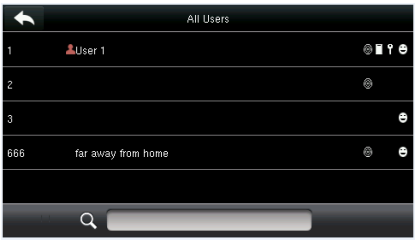
Nota: Después de registrar los datos anteriores, toque para regresar a la interfaz de Nuevo usuario. Para modificar los datos registrados, toque el menú correspondiente para volver a registrarse. Para guardar los datos registrados, toque .

Si el menú se deja desatendido dentro del tiempo de espera, el sistema vuelve a la interfaz principal y la información registrada no se guarda.

## 5. Gestión de usuarios

Presione **Admin. De usuarios** en la interfaz del menú principal.

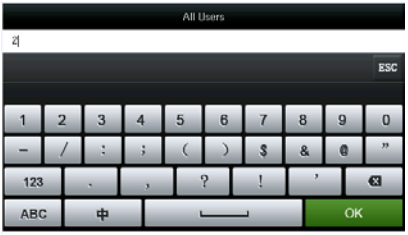

**Toque todos los usuarios.**



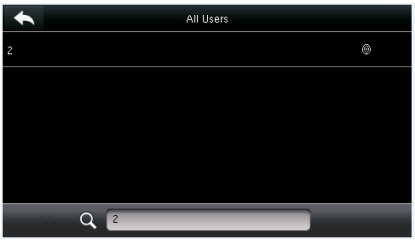

**Se muestra la interfaz, "Todos los usuarios".**

Nota: Los usuarios están ordenados por nombre, con  indica que es súper administrador.

### 5.1 Buscar Usuario




**Toque la barra de búsqueda en la lista de usuarios e ingrese la palabra clave.**

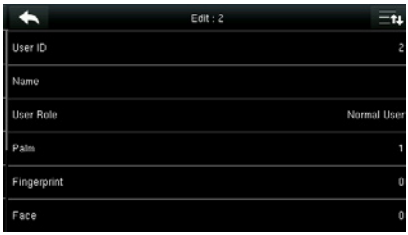



**El sistema encuentra automáticamente a los usuarios relacionados con la palabra clave ingresada.**

Nota: La palabra clave puede ser ID, apellido, nombre de pila o nombre completo.

### 5.2 Editar Usuario


**Elija un usuario de la lista y toque Editar.**

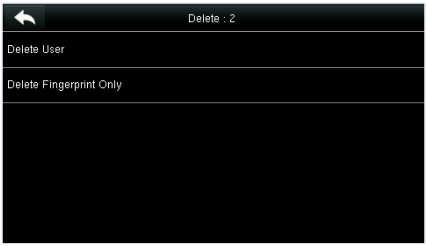



**Se muestra la interfaz Editar usuario.**

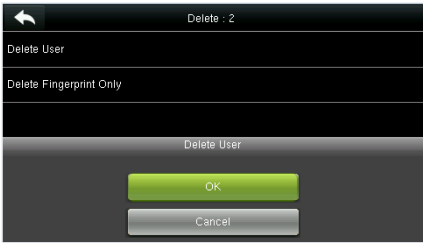
Nota: La operación de edición de un usuario es la misma que la de agregar un usuario, excepto que la ID no se puede modificar al editar un usuario.

## 5.3 Eliminar un Usuario

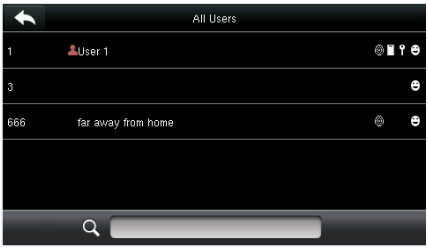

**Elija un usuario de la lista y toque Eliminar.**




**Se muestra la interfaz Eliminar usuario. (Toca Página abajo para ver más información).**



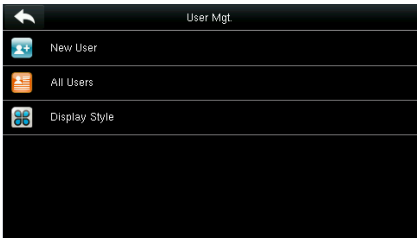

**Seleccione la información del usuario para ser borrada y toque OK.**




**El usuario se borró exitosamente y ya no se muestra en la lista.**

Nota:
1. Al eliminar un usuario, puede optar por eliminar información parcial, como el privilegio o la huella digital del usuario. Si selecciona Eliminar usuario, se borrará toda la información de este usuario.
2. Una vez que se eliminan los privilegios del súper administrador, el súper administrador se convierte en un usuario común, sin privilegios de súper administrador

## 5.4 Estilo de visualización del usuario




**1. Toque Mostrar estilo en la interfaz de Gestión del usuario.**


**2. El estilo predeterminado es Single Line. (Línea sencilla).**


**3. La figura anterior muestra todos los usuarios en el estilo de línea múltiple.**


**4. La figura anterior muestra todos los usuarios en el estilo de línea mixta.**

## 6. Rol de usuario

Establece los derechos de usuario para operar el menú (se puede establecer un máximo de 3 roles).

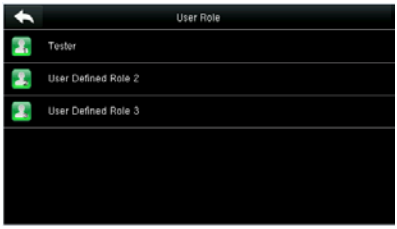
**Toca Rol de usuario en la interfaz del menú principal.**


**1. Toque cualquier elemento para establecer un rol definido.**


**2. Toque Habilitar rol definido para habilitar este rol definido.**


**3. Toque Nombre para ingresar el nombre del rol.**


**4. El sistema vuelve a la interfaz de Función definida por el usuario.**

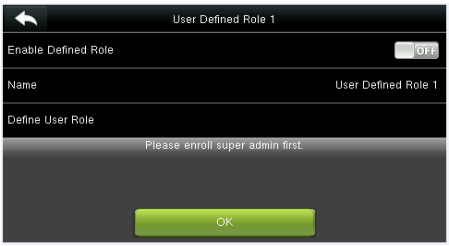




**5. Pulse Definir rol de usuario para asignar privilegios a la función.**

**6. La definición del rol es completada.**

La asignación de privilegios se completa. Toca **Regresar**

Nota: Durante la asignación de privilegios, el menú principal está a la izquierda y sus submenús a la derecha. Solo necesita seleccionar las funciones en los submenús. Si no hay un súper administrador registrado en el dispositivo, aparecerá el siguiente mensaje después de tocar Habilitar función definida.



# 7. Configuración de comunicación

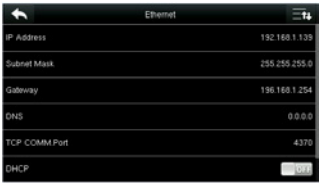
Incluyendo los parámetros de Ethernet como la dirección IP, la comunicación en serie, la conexión de PC, los ajustes ADMS ★ y Wiegand, etc.

Toque [Com] en la interfaz del menú principal.


## 7.1 Configuraciones de Ethernet

Incluyendo los parámetros de Ethernet como la dirección IP, la comunicación en serie, la conexión de PC, los ajustes ADMS y Wiegand, etc.

**Toca Ethernet en la interfaz de configuración de comunicación.**





| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Dirección IP** | El valor predeterminado de fábrica es192.168.1.201, ajústelos según la situación real de la red |
| **Mascara de red** | El valor predeterminado de fábrica es 255.255.255.0, ajústelos según la situación real de la red |
| **Puerta de Enlace** | El valor predeterminado de fábrica es 0.0.0.0, ajústelos según la situación real de la red |
| **DNS** | El valor predeterminado de fábrica es 0.0.0.0, ajústelos según la situación real de la red |
| **Puerto TCP** | El valor predeterminado de fábrica es 4370, ajústelos según la situación real de la red |
| **DHCP** | Dynamic Host Configuration Protocol, que es asignar dinámicamente direcciones IP para los clientes a través del servidor. Si DHCP está habilitado, IP no se puede configurar manualmente |
| **Mostrar en Barra de estatus** | Para establecer si se muestra el icono de red en la barra de estado |

## 7.2 Configuración de Comunicación Serial

Para establecer la comunicación con el dispositivo a través de un puerto en serie (RS232 / RS485), debe realizar las configuraciones del puerto serie.

**Toque Com. Serial en la Interfaz de configuración de comunicación**

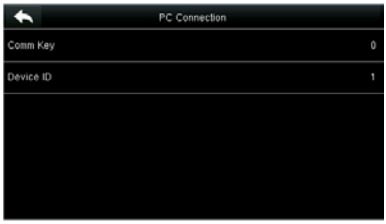


| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **RS232** | Para conectar a impresora |
| **RS485** | Para conectar lector 485 |
| **Baudrate/Baudios** | La velocidad de la comunicación con una PC; hay 5 opciones de velocidad en baudios: 115200 (predeterminado), 57600, 38400, 19200 y 9600. Cuanto mayor es la velocidad en baudios, más rápida es la velocidad de comunicación, pero también menos confiable. En general, se puede usar una tasa de baudios más alta cuando la distancia de comunicación es corta; cuando la distancia de comunicación es larga, elegir una velocidad en baudios más baja sería más confiable |
| Nota: Si se utiliza un puerto serie RS485 para la comunicación con el dispositivo, la velocidad en baudios del puerto serie no debe ser de 9600 bps | |

## 7.3 Conexión a pc

Para mejorar la seguridad de los datos, es necesario configurar "Comm Key" clave de comunicación, para la comunicación entre el dispositivo y la PC.
Si se establece una clave de comunicación en el dispositivo, se debe ingresar la contraseña de conexión correcta cuando el dispositivo está conectado al software de la PC, de modo que el dispositivo y el software se puedan comunicar.

**Toque Conexión de PC en la Interfaz de configuración de comunicación.**

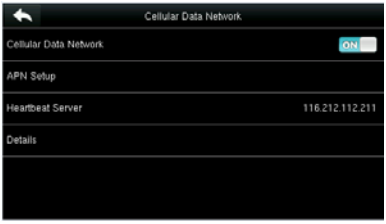



| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Clave de comunicación** | Clave de comunicación: la contraseña predeterminada es 0 (sin contraseña). Comm Key puede tener 1 ~ 6 dígitos y oscila entre 0 ~ 999999. |
| **ID. De dispositivo** | Número de identidad del dispositivo, que varía entre 1 ~ 254. Si el método de comunicación es RS232 / RS485, se requiere ingresar esta ID de dispositivo en la interfaz de comunicación del software |

## 7.4 Red de datos celulares ★

Cuando el dispositivo se aplica en una red de acceso telefónico, asegúrese de que el dispositivo esté dentro de la cobertura de las señales de la red móvil (GPRS / 3G). Además, debe conocer el APN utilizado y el número de acceso.

**Toque Red de Datos Celulares en la Interfaz de configuración de comunicación**




| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Red de Datos Celulares** | Para habilitar la red móvil |
| **Configuración APN** | Para establecer la información de APN, como el número de acceso, el nombre de usuario y la contraseña |
| **Servidor Heartbeat** | Para detectar el estado de conexión de la red móvil. El terminal envía periódicamente paquetes ICMP al servidor de heartbeat para detectar si el terminal está en línea. Cuando el terminal está fuera de línea, el dispositivo realiza automáticamente la conexión de acceso telefónico nuevamente. Por lo tanto, al configurar el servidor de heartbeat, asegúrese de que el servidor de heartbeat se pueda conectar y permanecer en línea de manera estable por un período prolongado. Nota: Generalmente, el cliente puede establecer la dirección del servidor de heartbeat como la dirección del servidor ADMS. |
| **Detalles** | Para ver la información sobre la conexión de red móvil, como el modo de red, el operador, la dirección IP, los datos recibidos y los datos enviados. |

### 7.4.1 Configuración de APN

**Toque Configuración de APN en la interfaz de Red de Datos Celulares**


| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **APN** | (Access Point Name)Nombre del punto de acceso, proporcionado por el operador y no admitido en la red CDMA. |
| **Número de Marcado** | Número de la red de datos móviles |
| **Nombre de usuario y contraseña** | Para verificar si el usuario tiene el privilegio de usar esta red |

### 7.4.2 Detalles

**Toca Detalles en la interfaz de datos Celulares**

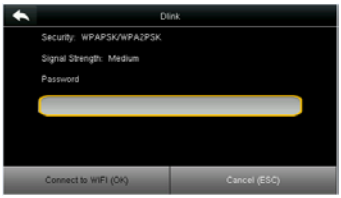

Se muestra la información sobre la conexión del dispositivo

## 7.5 Configuración de Wi-Fi

Wi-Fi es la abreviatura de Wireless Fidelity. El dispositivo proporciona un módulo de Wi-Fi, que puede integrarse en el la placa base del dispositivo o conectarse externamente, para permitir la transmisión de datos a través de Wi-Fi y establecer un entorno de red inalámbrica.

Wi-Fi está habilitado en el sistema de manera predeterminada. Si no necesita usar la red Wi-Fi, puede presionar el botón ON para desactivar Wi-Fi.


**1. Cuando Wi-Fi está habilitado, toca el buscador de red**



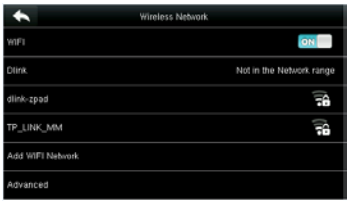

**2. Toque el cuadro de ingreso de contraseña, para ingresar la contraseña y toque "Conectar a Wi-Fi (OK)."**


**3. Conectando**


**4. Conexión exitosa, el estado se muestra en la barra de iconos.**

### 7.5.1 Agregando una red Wi-Fi

Si la red Wi-Fi deseada no está en la lista, puede agregar la red Wi-Fi manualmente.



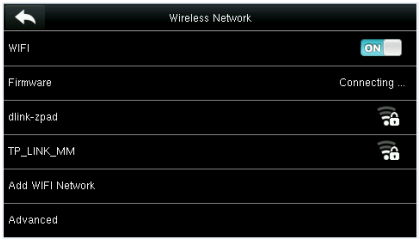

**Toca Página abajo y agrega red Wi-Fi.**


**Ingrese los parámetros de la red Wi-Fi. (La red agregada debe existir)**

Después de agregar, encuentre la red Wi-Fi agregada en la lista y conéctese a la red de la manera anterior

### 7.5.2 Opciones avanzadas

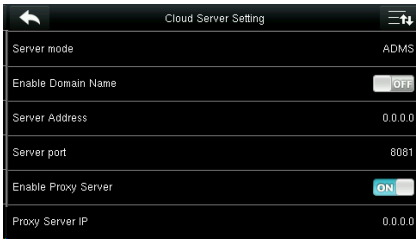
Esto se usa para configurar los parámetros de la red Wi-Fi




| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **DHCP** | Abreviatura de Dynamic Host Configuration Protocol, que implica la asignación de direcciones IP dinámicas a los clientes de la red. |
| **Dirección IP** | Dirección IP de la red Wi-Fi |
| **Máscara de red** | Máscara de subred de la red Wi-Fi |
| **Puerta de enlace** | Dirección de la puerta de enlace de la red Wi-Fi |

### 7.6 Configuración del Servidor Cloud

Configuración utilizada para conectarse con el servidor de la nube. Toque Conexión de PC en la Interfaz de configuración de comunicación.




| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Habilitar nombre de dominio** | Cuando esta función está habilitada, se utiliza el modo de nombre de dominio http: // ..., como http://www.XXX.com. XXX denota el nombre de dominio cuando este modo está activado; cuando este modo está desactivado, ingrese el formato de dirección IP en XXX. |
| **Dirección del Servidor** | Dirección IP de la red Wi-Fi |
| **Puerto del Servidor** | Puerto utilizado por el servidor ADMS |
| **Habilitar Servidor Proxy** | Método para habilitar el proxy. Para habilitar el proxy, configure la dirección IP y el número de puerto del servidor proxy. |

## 7.7 Configuración de Wiegand

Para establecer los parámetros de salida de Wiegand, toque Configuración de Wiegand en la Interfaz de configuración de comunicación.


Toque Salida Wiegand en la interfaz de configuración de Wiegand.



| DETALLE DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Formato Wiegand** | Los usuarios pueden seleccionar los formatos estándar de Wiegand integrados en el sistema. Aunque se admiten múltiples opciones, el formato real está determinado por los bits de salida de Wiegand |
| **Bits de salida** | Número de bits de datos de Wiegand. Después de elegir [bits de salida Wiegand], el dispositivo utilizará el número de bits establecido para encontrar el formato Wiegand adecuado en [Formato Wiegand].<br><br>Por ejemplo, si se selecciona Wiegand26, Wiegand34a, Wiegand36, Wiegand37a o Wiegand50 en formato Wiegand, pero los bits de salida de Wiegand se establecen en 36, el formato Wiegand36 entra en vigencia. |
| **ID fallido** | Se define como el valor de salida de la verificación de usuario fallida. El formato de salida depende de la configuración [Formato Wiegand]. El valor predeterminado oscila entre 0 y 65535 |
| **Código de sitio** | Es similar a la ID del dispositivo, excepto que se puede configurar de forma manual y repetible con diferentes dispositivos. El valor predeterminado oscila entre 0 y 256. |
| **Ancho de pulso (µs)** | El ancho de pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, que se puede ajustar dentro del rango de 20 a 100 microsegundos |
| **Intervalo del pulso (µs)** | El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos |

| Tipo de ID | Contenido de salida después de una verificación exitosa. Identificación de usuario o número de tarjeta puede ser elegida. |
|---|---|
| **Definiciones de varios formatos generales de Wiegand:** | |
| **FORMATO WIEGAND** | **DEFINICIÓN** |
| **Wiegand 26** | ECCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste en 26 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 13º, mientras que el bit 26º es el bit de paridad impar de los bits 14º a 25º. Los bits 2 a 25 son el número de tarjeta |
| **Wiegand 26a** | ESSSSSSSSCCCCCCCCCCCCCCCCO<br>Consiste en 26 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 13º, mientras que el bit 26º es el bit de paridad impar de los bits 14º a 25º. Los bits 2º a 9º son el código del sitio, mientras que los bits 10º a 25º son el número de la tarjeta. |
| **Wiegand 34** | ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste en 34 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 17º, mientras que el bit 34º es el bit de paridad impar de los bits 18º a 33º. Los bits 2 a 25 son el número de tarjeta. |
| **Wiegand 34a** | ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste en 34 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 17º, mientras que el bit 34º es el bit de paridad impar de los bits 18º a 33º. Los bits 2º a 9º son el código del sitio, mientras que los bits 10º a 25º son el número de la tarjeta. |
| **Wiegand 36** | OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME<br>Consiste en 36 bits de código binario. El 1er bit es el bit de paridad impar de los bits 2º a 18º, mientras que el bit 36º es el bit de paridad par de los bits 19º a 35º. Los bits 2º a 17º son el código del dispositivo, los bits 18º a 33º son el número de la tarjeta, el terminal de asistencia de Palm de 34,3 pulgadas y los bits del 34º al 35º son el código del fabricante. |
| **Wiegand 36a** | EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO<br>Consiste en 36 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 18º, mientras que el bit 36º es el bit de paridad impar de los bits 19º a 35º. Los bits 2º a 19º son el código del dispositivo, y los bits 20º a 35º son el número de la tarjeta |
| **Wiegand 37** | OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE<br>Consiste en 37 bits de código binario. El 1er bit es el bit de paridad impar de los bits 2º a 18º, mientras que el bit 37º es el bit de paridad par de los bits 19º a 36º. Los bits 2º a 4º son el código del fabricante, los bits 5º a 16º son el código del sitio, y los bits 21º a 36º son el número de la tarjeta |
| **Wiegand 37a** | EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO<br>Consiste en 37 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 18º, mientras que el bit 37º es el bit de paridad impar de los bits 19º a 35º. Los bits 2º a 4º son el código del fabricante, los bits 5º a 14º son el código del dispositivo, los códigos 15º a 20º son el código del sitio, y los bits 21º a 36º son el número de la tarjeta |
| **Wiegand 50** | ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO<br>Consiste en 50 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 25º, mientras que el bit 50º es el bit de paridad impar de los bits 26º a 49º. Los bits 2º a 17º son el código del sitio, y los bits 18º a 49º son el número de la tarjeta. |

C denota número de tarjeta, E indica bit de paridad par, O indica bit de paridad impar, F indica código de dispositivo, M indica código de fabricante, P denota bit de paridad, y S denota código de sitio

# 8. Configuraciones del sistema

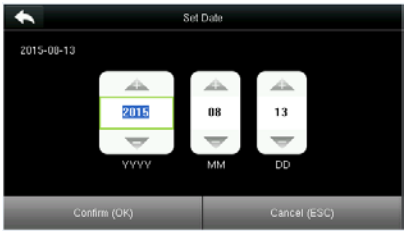
Establecer los parámetros del sistema relacionados para maximizar el rendimiento del dispositivo.

**Toque [Sistema] en la interfaz del menú principal.**

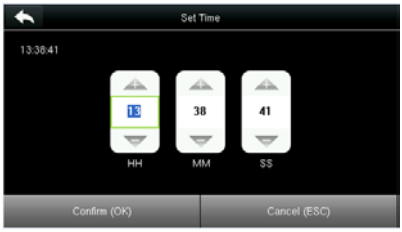

## 8.1 Configuraciones de fecha / hora

Toque fecha / hora en la interfaz del sistema


**1. Toque Establecer fecha.**

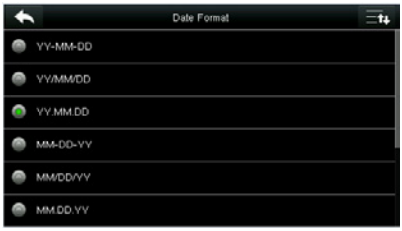



**2. Presione Re Pág y Av Pág para configurar el año, mes y día, y luego presione Confirmar (OK)**




**3. Toque Establecer hora en la interfaz de fecha y hora y presione Re Pág y Av Pág para configurar la hora, los minutos y los segundos.**


**4. Toque Hora de 24 horas para elegir si desea habilitar este formato.**




**5. Pulse Formato de fecha en la interfaz Fecha y hora para seleccionar el formato de visualización de la fecha**

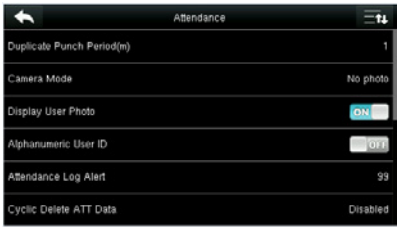

**6. Pulse "Horario de verano" para elegir si desea habilitar el horario de verano.**


**7. Seleccione un modo de ahorro de luz diurna.**


**8. Configure cuándo comenzar y finalizar el horario de verano.**

## 8.2 Parámetros de asistencia

Presiona Asistencia en la interfaz del sistema




| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Periodo de marcaje duplicado** | Dentro de un período de tiempo establecido (unidad: minutos), los registros de asistencia duplicados no serán reservados (el rango de valores va de 1 a 999999 minutos) |
| **Modo cámara** | Para establecer si tomar y guardar imágenes en la verificación; aplicable a todos los usuarios. Los siguientes 5 modos están incluidos:<br><br>Sin imagen: no se toma ninguna fotografía en la verificación del usuario.<br>Tome la foto, no guarde: la foto se toma pero no se guarda en la verificación.<br><br>Tomar foto y guardar: la foto se toma y se guarda en la verificación<br><br>Guarde en la verificación exitosa: la foto se toma y se guarda en verificación exitosa<br><br>Guardar en la verificación fallida: la foto se toma y se guarda en la verificación fallida |
| **Mostrar imagen de usuario** | Para configurar la imagen del usuario para que se muestre cuando un usuario aprueba la verificación. Gírelo [ON] para visualizar la imagen del usuario y [OFF] para desactivarlo. |
| **ID de usuario alfanumérico** | Ya sea para soportar las letras en la identificación del empleado. |
| **Alerta de registro de asistencia** | Cuando el almacenamiento restante sea menor que el valor establecido, el dispositivo alertará automáticamente a los usuarios sobre la información de almacenamiento restante. Se puede deshabilitar o establecer en un valor entre 1 y 9999 |
| **Eliminación cíclica de datos de ATT** | El número de registros de asistencia se puede eliminar de una vez cuando se alcanza el máximo de almacenamiento. Se puede deshabilitar o establecer en un valor de 1 a 999. |
| **Eliminación cíclica de Fotos de ATT** | El número de imágenes de asistencia se puede eliminar de una vez cuando se alcanza el máximo almacenamiento. Se puede deshabilitar o establecer en un valor de 1 a 99. |
| **Confirmar el retraso de la pantalla** | Es el tiempo que se visualizará la interfaz de información de verificación después de la verificación. El valor varía de 1 a 9 segundos |
| **Intervalo de Detección de Rostros** | Para establecer el intervalo de comparación de rostros según sea necesario, dentro del rango de 0-9 s |
| **Guardar registro de verificación ilegal** | Para establecer si las verificaciones fallidas, como las causadas por el acceso en Horarios de horario no válidos o Verificación combinada ilegal, se guardarán cuando la función de control de acceso avanzado esté activada. |
| **Regla de expiración** | Si se habilita la regla de caducidad. En caso afirmativo, realice la configuración de vencimiento, que incluye: retener la información del usuario y no guardar el registro de asistencia; retener información del usuario y guardar el registro de asistencia; y borrar información del usuario |

## 8.3 Parámetros faciales

Toque Cara en la interfaz del sistema.


| FRR | FAR | UMBRAL DE CONCIDENCIA | |
|---|---|---|---|
| | | 1:N | 1:1 |
| Alto | Bajo | 85 | 80 |
| Medio | Medio | 82 | 75 |
| Bajo | Alto | 80 | 70 |

| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Umbral de coincidencia 1: 1** | En el Método de verificación 1: 1, solo cuando la similitud entre la cara de verificación y las caras registradas del usuario es mayor que este valor, la verificación puede tener éxito. El rango de valores válidos es 70-120, con un umbral más grande que conduce a una menor tasa de error y una mayor tasa de rechazo, y viceversa |
| **Umbral de coincidencia 1:N** | En el método de verificación 1: N, solo cuando la similitud entre la cara de verificación y todas las caras registradas es mayor que este valor, la verificación puede tener éxito. El rango de valores válidos es de 80-120, con un umbral más grande que conduce a una menor tasa de error y una mayor tasa de rechazo, y viceversa. |
| **Detecta la cara falsa** | Cuando esta función está habilitada, el dispositivo elimina automáticamente la cara falsa |
| **Exposición** | Este parámetro se utiliza para establecer el valor de exposición de la cámara. |
| NOTA: El ajuste incorrecto de los parámetros de Exposición y Calidad puede afectar gravemente el rendimiento FFR del terminal. Ajuste el parámetro de Exposición solo bajo la guía del personal de servicio postventa de nuestra empresa. | |

## 8.4 Parámetros de huellas dactilares

Toque Huella digital en la interfaz del sistema.


| FRR | FAR | UMBRAL DE CONCIDENCIA | |
|---|---|---|---|
| | | 1:N | 1:1 |
| Alto | Bajo | 45 | 25 |
| Medio | Medio | 35 | 15 |
| Bajo | Alto | 25 | 10 |

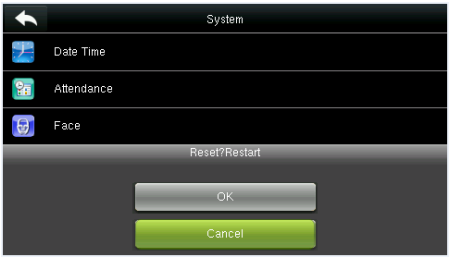
| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Umbral de coincidencia 1: 1** | En el Método de verificación 1: 1, solo cuando la similitud entre la huella digital de verificación y la huella digital registrada del usuario es mayor que este valor, la verificación puede tener éxito. |
| **Umbral de coincidencia 1:N** | En el Método de Verificación 1: N, solo cuando la similitud entre la huella digital de verificación y todas las huellas digitales registradas es mayor que este valor, la verificación puede tener éxito. |
| **Sensibilidad del sensor FP** | Para establecer la sensibilidad de la colección de huellas dactilares. Se recomienda utilizar el nivel predeterminado "Medio" (cuando el entorno está seco, lo que resulta en una detección lenta de la huella digital, puede establecer el nivel en "Alto" (para aumentar la sensibilidad, cuando el ambiente es húmedo, lo que dificulta identificar la huella digital) , puede establecer el nivel en "Bajo". |
| **1: 1 veces de reintento** | Tiempos de reintento de 1: 1: en Verificación 1: 1 o Verificación de contraseña, los usuarios pueden olvidar la huella dactilar registrada o la contraseña, o presionar el dedo incorrectamente. Para reducir el proceso de reingreso de la identificación de usuario, se permite volver a intentarlo |
| **Imagen de huella digital** | Para establecer si mostrar la imagen de la huella digital en la pantalla en el registro o verificación. Hay cuatro opciones disponibles:<br>Mostrar para inscribirse: para mostrar la imagen de la huella digital en la pantalla solo durante el registro.<br><br>Mostrar para coincidencia: para mostrar la imagen de la huella digital en la pantalla solo durante la comparación.<br><br>Mostrar para inscribirse y combinar: para mostrar la imagen de la huella digital en la pantalla durante el registro y la comparación.<br><br>No mostrar para inscribirse o coincidir: no mostrar la imagen de la huella digital en ningún caso |

## 8.5 Parámetros de Palma

Toque Parámetro Palm en la interfaz del sistema y seleccione el umbral correspondiente, solo cuando la similitud entre la cara verificadora y todas las caras registradas sea mayor que este valor la verificación puede tener éxito y el umbral más grande conduce a una menor tasa de error y mayor tasa de rechazo

## 8.6 Restablecer la configuración de fábrica

Restablezca los datos como la configuración de comunicación y la configuración del sistema a la configuración de fábrica.
Toca Restablecer en la interfaz del sistema.




## 8.7 Actualización USB

Con esta opción, el firmware del dispositivo se puede actualizar utilizando el archivo de actualización en un disco USB. Antes de realizar esta operación, asegúrese de que el disco USB esté insertado correctamente en el dispositivo y contenga el archivo de actualización correcto.
Si no se inserta ningún disco USB, el sistema le da la siguiente instrucción después de tocar USB Upgrade en la interfaz del sistema.


NOTA: Si se necesita un archivo de actualización, comuníquese con soporte técnico. La actualización del firmware no se recomienda bajo circunstancias normales.

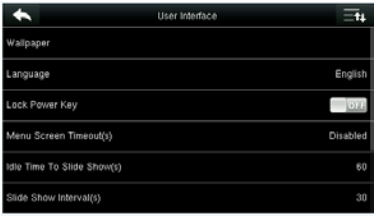
# 9. Configuración de personalización

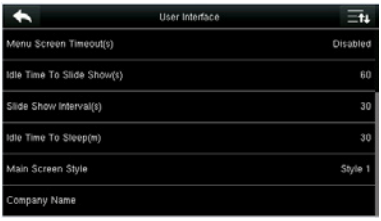
Realice configuraciones relacionadas de la interfaz de usuario, voz, calendario y opciones de estado de perforación, y personalice teclas de método abreviado.

Toque [Personalizar] en la interfaz del menú principal


## 9.1 Configuración de interfaz de usuario

Puede personalizar el estilo de visualización de la interfaz de inicio.




| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Protector de pantalla** | Seleccione el fondo de pantalla de la pantalla principal según sea necesario, puede encontrar fondos de pantalla de varios estilos en el dispositivo |
| **Idioma** | Seleccione el idioma del dispositivo según sea necesario |
| **Bloquear la tecla de encendido** | Para establecer si bloquear la tecla de encendido. Cuando esta función está habilitada, al presionar la tecla de encendido no funciona. Cuando esta función está desactivada, el sistema se apaga después de presionar la tecla de encendido durante tres segundos. |
| **Tiempo de espera de la pantalla del menú** | Cuando no hay ninguna operación en la interfaz del menú y el tiempo excede el valor establecido, el dispositivo saldrá automáticamente a la interfaz inicial. Puede desactivarlo o establecer el valor a 60 ~ 99999 segundos. |
| **Tiempo de inactividad para mostrar diapositivas** | Cuando no hay ninguna operación en la interfaz inicial y el tiempo excede el valor establecido, se mostrará una presentación de diapositivas. Se puede deshabilitar (establecer en "Ninguno o establecer en 3 ~ 999 segundos. |
| **Intervalo de presentación** | Esto se refiere al intervalo entre mostrar diferentes imágenes de presentación.<br>Se puede desactivar o establecer en 3 ~ 999 s. |
| **Tiempo de inactividad para suspender** | Cuando no hay ninguna operación en el dispositivo y se alcanza el tiempo de espera establecido, el dispositivo entrará en el modo de espera. Presione cualquier tecla o dedo para cancelar el modo en espera. Puede desactivar esta función o establecer el valor en 1 ~ 999 minutos. Si esta función se gira a [Disabled], el dispositivo no entrará en el modo de espera. |
| **Estilo de pantalla principal** | Elegir la posición y las formas del reloj y la clave de estado |

## 9.2 Configuraciones de voz

Toque la interfaz de usuario en la interfaz Personalizar


| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Mensaje de voz** | Seleccione si desea habilitar las indicaciones de voz durante el funcionamiento, presione [ON] para habilitarlo |
| **Indicar al Toque** | Seleccione si desea activar la voz del teclado mientras presiona el teclado, presione [ON] para habilitarlo |
| **Volumen** | Configura el volumen del dispositivo. |

## 9.3 Configuraciones de Timbres

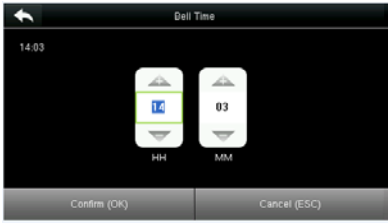
Muchas empresas optan por utilizar la campana para indicar el tiempo de servicio y fuera de servicio. Al llegar a la hora programada para el timbre, el dispositivo reproducirá el tono de llamada seleccionado automáticamente hasta que pase la duración del timbre.

### 9.3.1 Agregar un Timbre

Toque los horarios de timbre  en la interfaz Personalizar


**1. Toque Nuevo horario de campana**

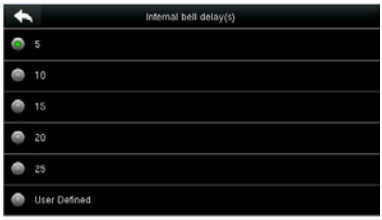

**2. Toque el estado de la campana para habilitar el estado de la campana**




**3. Configure la hora de la campana**


**4. Establecer Repetir.**


**5. Seleccione un tono**




**6. Seleccione la campana interna**

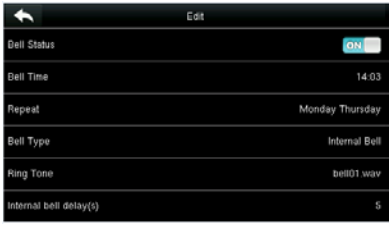

**7. Regrese a la interfaz de Programaciones de Bell y toque Todas las programaciones de Campana**


**8. Las campanas agregadas se muestran en una lista.**

### 9.3.2 Editar una campana

En la interfaz de Todos los horarios de Bell, toca el elemento de la campana que se va a editar.

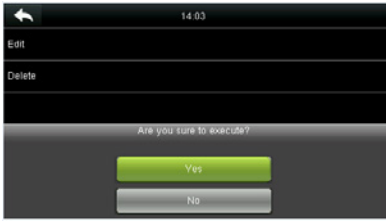

**Tocar Editar.**




**El método de edición es el mismo que el de una nueva**

### 9.3.3 Eliminar una campana

En la interfaz de Todos los horarios de Bell, toca un elemento de campana para eliminar.




**Toca Eliminar y selecciona [Sí] para eliminar la campana.**


**La campana se elimina con éxito.**

## 9.4 Configuraciiones de Estados de Perforación

Toque las opciones de estados de golpe en la interface personalizable.



| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Estado del marcaje** | Seleccione un modo de estado de marcaje, que puede ser:<br>**Desactivado:** para desactivar la función de verificación de la tecla de estado. La clave de estado de perforación establecida en el menú Asignaciones de teclas de acceso directo dejará de ser válida.<br><br>**1. Modo manual:** para cambiar manualmente la tecla de estado de verificación, y la tecla de estado de perforación desaparecerá después de comprobar el tiempo de espera del estado.<br><br>**2. Modo automático:** después de elegir este modo, configure el tiempo de conmutación de la tecla de estado de verificación en las asignaciones de teclas de acceso directo; cuando se alcanza el tiempo de conmutación, la tecla de estado de perforación configurada cambiará automáticamente.<br><br>**Modo manual y automático:** en este modo, la interfaz principal mostrará la tecla de estado de verificación de conmutación automática, mientras tanto admite la tecla de estado de verificación de cambio manual. Después del tiempo de espera, la tecla de estado de verificación de cambio manual se convertirá en la tecla de estado de verificación de conmutación automática.<br><br>**Modo manual fijo:** después de que la tecla de estado de verificación se conmuta manualmente, la tecla de estado de verificación permanecerá sin cambios hasta que se cambie manualmente la próxima vez.<br><br>**Modo fijo:** solo se mostrará la clave de estado de comprobación fija y no se podrá cambiar. |
| **Periodo de tiempo de verificación** | El tiempo de espera de la visualización del estado de verificación. El valor oscila entre 5 ~ 999 segundos |
| **Estado de Asistencia Obligatoria** | Si se debe seleccionar un estado de asistencia durante la verificación |

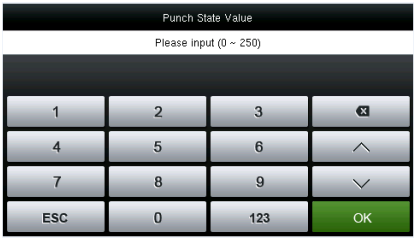
## 9.5 Configuraciones de teclas de acceso directo

Las teclas de acceso directo se pueden definir como teclas de estado de perforación o tecla de función de menú. Cuando el dispositivo se encuentra en la interfaz principal, presionar la tecla de acceso directo configurada mostrará el estado de asistencia o ingresará a la interfaz de operación del menú.

Toque Asignaciones de teclas de acceso directo en la interfaz Personalizar.


**1. Toque la tecla de método abreviado que se va a establecer.**

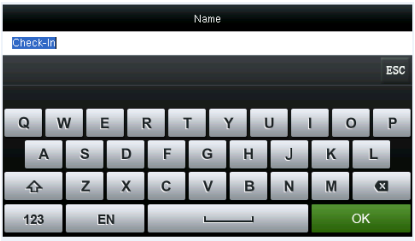

**2. Se muestra la interfaz de configuración de la tecla de acceso directo. Nombre de la clave correspondiente, ver sección 1.5 Interfaz inicial).**



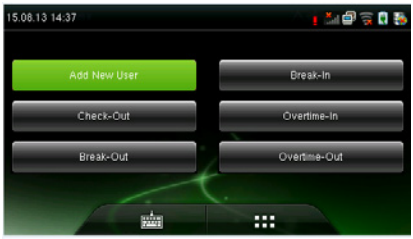

**3. Establezca el valor de estado (rango de valores 0-250).**


**4. Configure la función correspondiente para esta tecla táctil**


**5. Establezca el nombre de la clave de estado.**




**6. Personaliza e ingresa un nombre**



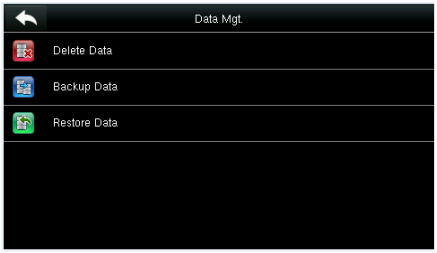

**7. Toque la interfaz principal para mostrar el menú contextual.**

Toque el estado de asistencia para hacer un cambio. Toque la función para acceder rápidamente a la configuración de la función. (Presione F1 New User "Nuevo usuario" para acceder rápidamente a este menú).

# 10. Gestión de datos

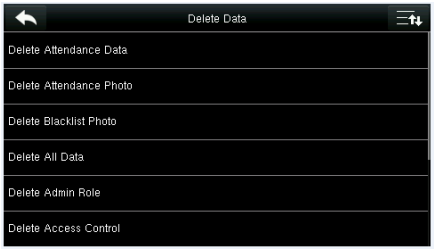
Para administrar datos en el dispositivo, que incluye eliminar datos, hacer copias de seguridad de datos y restaurar datos.

Toca Gestión de datos en la interfaz del menú principal




## 10.1 Eliminar datos

Toca Eliminar datos en la interfaz de gestión de datos.

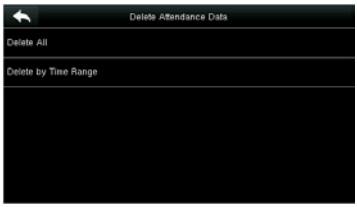




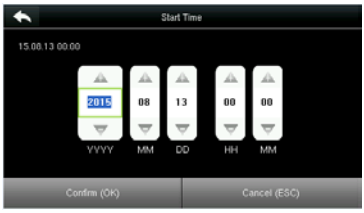
| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Eliminar datos de asistencia** | Para eliminar todos los datos de asistencia en el dispositivo |
| **Borrar foto de asistencia** | Para eliminar todas las imágenes de asistencia de los usuarios en el dispositivo. |
| **Eliminar lista negra** | Para eliminar todas las imágenes de la lista negra en el dispositivo, lo que significa que las imágenes se tomaron después de las verificaciones fallidas |
| **Eliminar todos los datos** | Para eliminar toda la información del usuario, huellas dactilares y registros de asistencia, etc. |
| **Eliminar rol de administrador** | Para hacer que todos los administradores se conviertan en usuarios normales. |
| **Eliminar el control de acceso** | Para eliminar todos los datos de acceso. |
| **Eliminar imagen de usuario** | Para eliminar todas las imágenes de usuario en el dispositivo. |

| | |
|---|---|
| **Eliminar fondo de pantalla** | Para eliminar todos los fondos de pantalla en el dispositivo |
| **Eliminar protectores de pantalla** | Para eliminar todos los protectores de pantalla en el dispositivo. |
| **Borrar respaldo de Datos** | Para elimitar todos respaldos de datos de seguridad |

Nota: Al eliminar el registro de asistencia, la imagen de asistencia o la imagen de la lista negra, puede seleccionar Eliminar todo o Eliminar por intervalo de tiempo. Cuando se selecciona Eliminar por intervalo de tiempo, debe establecer el intervalo de tiempo para la eliminación de datos.




**Seleccione Eliminar por rango de tiempo**




**Establezca el rango de tiempo y toque Confirmar (OK).**

## 10.2 Copia de seguridad de datos

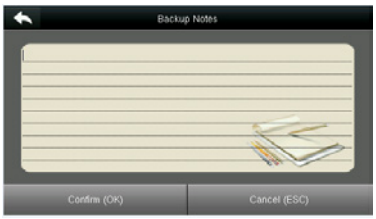
Para hacer una copia de seguridad de los datos comerciales o datos de configuración en el dispositivo o Memoria USB.

Toque Datos de copia de seguridad en la Interfaz de gestión de datos.


**1. Seleccione Copia de seguridad en el dispositivo**


**2. Toque Contenido de respaldo.**


**3. Seleccione el contenido de la copia de seguridad.**




**4. Haga una observación de respaldo. (Este paso es opcional)**


**5. Toque Inicio de copia de seguridad y la copia de seguridad se realiza correctamente.**

## 10.3 Restauración de datos

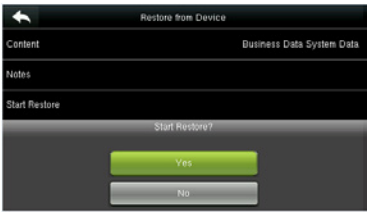
Para restaurar los datos en el dispositivo o Memoria Usb al dispositivo.

Toque Restaurar datos en la interfaz de gestión de datos.


**1. Toque Restaurar desde dispositivo.**


**2. Toca Contenido.**


**3. Seleccione el contenido de datos que se restaurará**



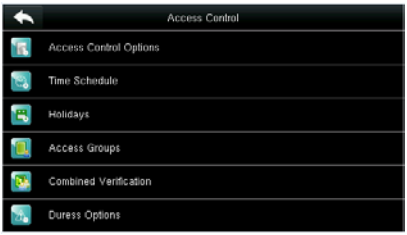

**4. Toque Iniciar restauración y seleccione Sí para confirmar la restauración.**

NOTA: las operaciones de Restaurar desde dispositivo son las mismas que las de Restaurar desde USB.
Cuando elija guardar datos en un disco USB, asegúrese de que el disco USB esté correctamente enchufado en el dispositivo y contenga los datos correspondientes para restaurar

# 11. Control de acceso

La opción de control de acceso se usa para configurar el horario, las vacaciones, los grupos de acceso, la verificación combinada, etc., los parámetros relacionados para que el dispositivo controle el bloqueo y otros dispositivos.

Toque [Control de acceso] en la interfaz del menú principal.




Para obtener acceso, el usuario registrado debe cumplir con las siguientes condiciones:
1. El tiempo de acceso del usuario cae dentro de la zona horaria personal del usuario o la zona horaria del grupo.
2. El grupo de usuarios debe estar en el combo de acceso (cuando hay otros grupos en el mismo combo de acceso, también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).
En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria de grupo predeterminada y el combo de acceso como "1 (, y se configura en el estado de desbloqueo.

## 11.1 Configuración de opciones de control de acceso

Para establecer los parámetros del bloqueo de control del equipo y el equipo relacionado.

Toque Opciones de control de acceso en la interfaz de Control de acceso.



| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Retardo de bloqueo de puerta** | El período de tiempo de desbloqueo (desde la apertura de la puerta hasta el cierre automático) después de que la cerradura electrónica recibe una señal abierta enviada desde el dispositivo (el valor oscila entre 0 y 10 segundos). |
| **Retardo del sensor de puerta** | Cuando se abre la puerta, el sensor de la puerta se revisará después de un período de tiempo; si el estado del sensor de la puerta no coincide con el del sensor de puerta, se activará la alarma. El período de tiempo es el retraso del sensor de la puerta (el valor varía de 0 a 255 segundos). |
| **Tipo de sensor de puerta** | Incluye normalmente abierto, normalmente cerrado y No. No significa que el sensor de puerta no está en uso; Normalmente abierto significa que la puerta se abre cuando la electricidad está encendida; Normalmente cerrado significa que la puerta está cerrada cuando la electricidad está encendida. |
| **Retardo de la alarma de la puerta** | Cuando el estado del sensor de la puerta no es coherente con el del tipo de sensor de puerta, la alarma se activará después de un período de tiempo; este período de tiempo es el retardo de la alarma de la puerta (el valor va de 1 a 999 segundos). |
| **Reintentar tiempos para alarma** | Cuando el número de verificación fallida alcanza el valor establecido (el rango de valores va de 1 a 9 veces), la alarma se disparará. Si el valor configurado es Ninguno, la alarma no se activará después de la verificación fallida. |

| | |
|---|---|
| **Período de tiempo NC** | Para establecer el período de tiempo para el modo Normalmente cerrado, para que nadie pueda obtener acceso durante este período. |
| **Periodo de tiempo NO** | Para establecer el período de tiempo para Normalmente abierto, para que la puerta siempre esté desbloqueada durante este período. |
| **Lector RS485** | |
| **Vacaciones válidas** | Para establecer si los ajustes de Periodo de tiempo NC o Periodo de tiempo NO son válidos en el período de tiempo de vacaciones establecido. Elija [ACTIVADO] para habilitar el período de ajuste CN o NO en feriado. |
| **Alarma de altavoz (Tamper)** | Cuando [Alarma de altavoz] está habilitado, el altavoz emitirá una alarma cuando el dispositivo se desmantele. |
| **Restablecer configuración de acceso** | Para restaurar los parámetros de control de acceso |
| **Observaciones** | Después de configurar el Período de tiempo NC, cierre bien la puerta, de lo contrario la alarma podría activarse durante el Período de tiempo NC |

## 11.2 Configuraciones de horario

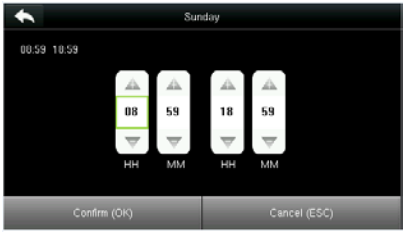
Horario es la unidad de tiempo mínima de configuración de control de acceso; como máximo 50 Horarios pueden configurarse para el sistema. Cada Horario consta de 7 secciones de tiempo (una semana), y cada sección de tiempo es el tiempo válido dentro de las 24 horas.

Toque horario en la interfaz de Control de acceso.


**1. Toque el cuadro de entrada de la Zona horaria de búsqueda.**


**2. Ingrese el número de la zona horaria (50 en total) para buscar.**


**3. Toque la fecha en la que se requiere la configuración de zona horaria.**



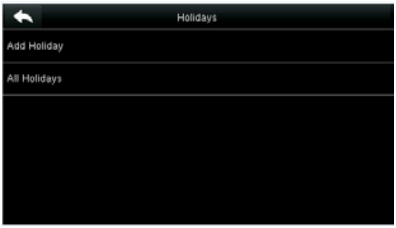

**4. Presione Arriba y Abajo para configurar la hora de inicio y finalización, y luego presione Confirmar (OK).**

Nota:
1. Horario de tiempo válido: 00:00 ~ 23:59 (todo el día válido) o cuando el tiempo de finalización es mayor que la hora de inicio.
2. Horario de tiempo no válido: cuando el tiempo de finalización es menor que la hora de inicio.
3. La zona horaria predeterminada 1 indica que el sistema está abierto todo el día.

## 11.3 Configuración de vacaciones

El concepto de vacaciones y festival se introduce en el control de acceso. En días festivos o fiestas, es posible que se requiera un tiempo de control de acceso especial, pero cambiar el tiempo de control de acceso de todos es muy tedioso. Por lo tanto, se puede configurar el tiempo de control de acceso en días festivos y festivales, que se aplica a todo el personal.
Si se establece el tiempo de control de acceso en festividades y festivales, el período de apertura de festivos y festivales está sujeto al período de tiempo establecido aquí.

Toque Vacaciones en la interfaz de Control de acceso




### 11.3.1 Añadir nuevas vacaciones

Toca Agregar vacaciones en la interfaz de Vacaciones


**Establecer parámetros de vacaciones**


**Los días festivos agregados se muestran en una lista**

### 11.3.2 Editar vacaciones

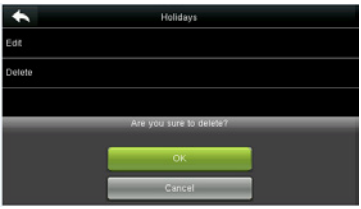
En la interfaz de Vacaciones, toque para seleccionar un elemento para modificar.


**Toca [Editar].**


**Después de la eliminación, esta festividad ya no se muestra en Todos los días festivos**

### 11.3.3 Borrar vacaciones

En la interfaz de Vacaciones, toque para seleccionar un elemento para modificar y tocar borrar.




**Toca OK para confirmar la eliminación.**

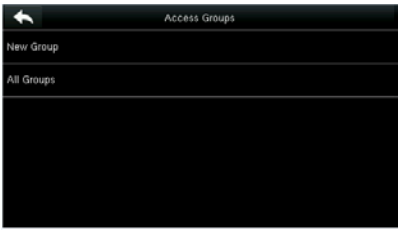

**Después de la eliminación, esta festividad ya no se muestra en Todos los días festivos.**

## 11.4 Configuración de grupos de acceso

Agrupar es administrar usuarios en grupos.

La zona horaria predeterminada de los usuarios del grupo está configurada para ser la zona horaria del grupo, mientras que los usuarios pueden establecer su zona horaria personal. Cuando el modo de verificación de grupo se solapa con el modo de verificación del usuario, prevalecen los modos de verificación del usuario. Cada grupo puede establecer 3 zonas horarias como máximo, siempre que una de ellas sea válida, el grupo se puede verificar con éxito. De forma predeterminada, el usuario recién inscrito pertenece al Grupo de acceso 1 y también se puede asignar a otro grupo de acceso.

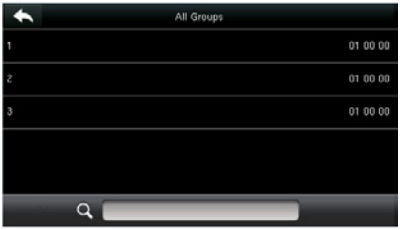
Toque Grupos de acceso en la interfaz de Control de acceso




### 11.4.1 Agregar nuevo grupo

Toque Nuevo grupo en la interfaz de Grupos de acceso.


**Establecer los parámetros del grupo de acceso.**

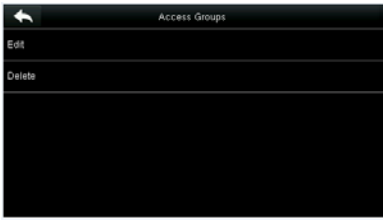



**Los grupos de acceso agregados se muestran en una lista. Puede buscar rápidamente grupos por número**

Nota:
1. El sistema tiene un grupo de acceso predeterminado numerado 1, que no se puede eliminar, pero se puede modificar.
2. Un número no puede ser modificado nuevamente después de ser configurado.
3. Cuando las vacaciones se establecen como válidas, el personal de un grupo puede abrir la puerta solo cuando el período de tiempo del grupo se solapa con el período de vacaciones.
4. Cuando el feriado se establece como no válido, el tiempo de control de acceso del personal de este grupo es no afectado por las vacaciones

### 11.4.2 Editar grupo

En la interfaz Todos los grupos, toque para seleccionar el elemento del grupo de acceso que se modificará.

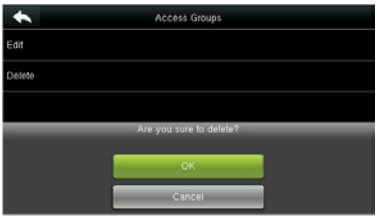



**Toca [Editar].**


**Modificar los parámetros del grupo de acceso.**

### 11.4.3 Eliminar un grupo

En la interfaz Todos los grupos, toque para seleccionar el elemento del grupo de acceso que se va a modificar y toque Eliminar.



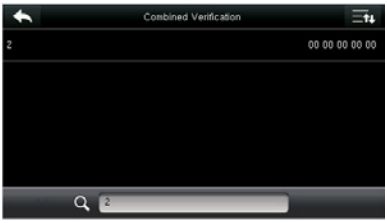

**Toca OK para confirmar la eliminación.**


**El grupo de acceso eliminado ya no es mostrado en Todos los grupos.**

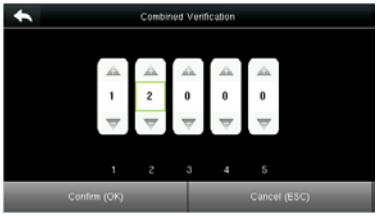
### 11.5 Configuraciones de verificación combinadas

Combine dos o más miembros para lograr la verificación múltiple y mejorar la seguridad. Toque la verificación combinada en la interfaz de control de acceso


**1. Toque la combinación de desbloqueo que se establecerá o toque la barra de búsqueda e ingrese un número de combinación de desbloqueo para encontrar la combinación específica**




**2. Toque este elemento de combinación de desbloqueo.**



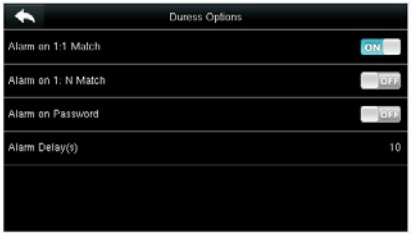

Nota: En una verificación combinada, el rango del número de usuario es: 0 ≤ N ≤ 5. Si necesita eliminar una combinación de desbloqueo, configure directamente todos los dígitos del número de combinación. Si necesita modificar una combinación, toque directamente elemento de combinación correspondiente para volver a establecer la configuración.

**3. Toque Arriba y Abajo para ingresar el número de combinación, y luego presione [Confirmar (OK)].**

## 11.6 Configuraciones de opciones de amago

Cuando los usuarios se encuentren bajo amago, seleccione el modo de alarma de amago, el dispositivo abrirá la puerta como de costumbre y enviará la señal de alarma.

Toque Opciones de amago en la interfaz de control de acceso



| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **coincidencia Alarma en 1: 1** | En el estado [ON], cuando un usuario usa el Método de verificación 1: 1 para verificar cualquier huella digital registrada, se activará la alarma. En el estado [OFF], no se disparará ninguna señal de alarma |
| **Coincidencia Alarma 1: N** | En el estado [ON], cuando un usuario usa el Método de verificación 1: N para verificar cualquier huella digital registrada, se activará la alarma. En el estado [OFF], no se activará ninguna señal de alarma |
| **Alarma en la contraseña** | IEn el estado [ON], cuando un usuario usa el método de verificación de contraseña, se activará la alarma. En el estado [OFF], no se disparará ninguna señal de alarma. |
| **Retardo de alarma** | Cuando se dispara la alarma de coacción, el dispositivo enviará la señal de alarma después de 10 segundos (predeterminado); el tiempo de retardo de la alarma se puede cambiar (el rango de valores va de 1 a 999 segundos). |

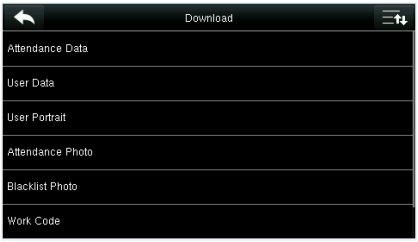
## 12. Administrador USB

Puede importar la información del usuario, la plantilla de huellas dactilares y los datos de asistencia en la máquina para comparar el software de asistencia con un disco USB, o importar la información del usuario y las huellas dactilares a otros dispositivos de huellas digitales para realizar una copia de seguridad.

Antes de cargar / descargar datos desde / hacia el disco USB, primero inserte el disco USB en la ranura USB.
Toque Administrador USB en la interfaz del menú principal


### 12.1 Descarga de USB

En la interfaz de USB Manager, toca Descargar.



| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Datos de asistencia** | Para descargar los datos de asistencia en el período de tiempo especificado en el disco USB. |
| **Datos del usuario** | Para descargar toda la información del usuario y las huellas dactilares del dispositivo al USB |
| **Retrato de usuario** | Descargue todas las imágenes del usuario del dispositivo en un disco USB. |
| **Foto de asistencia** | Para descargar todas las imágenes de asistencia desde el dispositivo al disco USB. |
| **Imagen de lista negra** | Para descargar todas las fotos de la lista negra (imágenes tomadas después de verificaciones fallidas) desde el dispositivo al disco USB |
| **Código de trabajo** | Para guardar el código de trabajo en el dispositivo en un disco USB. |
| **Mensaje Corto** | Para descargar el mensaje corto configurado en el dispositivo a un disco USB. |

## 12.2 Carga de USB

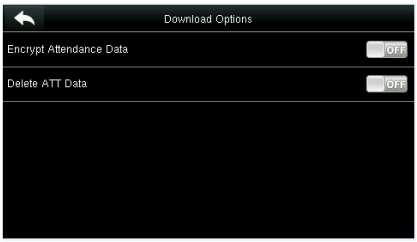
En la interfaz de USB Manager, toque Cargar.


| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Subir datos de usuario** | Para cargar toda la información del usuario y las huellas dactilares del disco USB en el dispositivo. |
| **Cargar imagen de usuario** | Para cargar la imagen JPG nombrada después de un código de trabajo en el disco USB del dispositivo. Durante la carga, puede seleccionar Subir imagen actual o Cargar todas las imágenes. La imagen se muestra después de la autenticación exitosa.<br>Durante la carga, debe crear una carpeta llamada "imagen" o "picture" en el directorio raíz del disco USB y colocar la imagen del usuario en este directorio. Se admite un máximo de 2000 imágenes y cada imagen no puede superar los 20 KB. Las imágenes se nombran en el formato de X.jpg, de las cuales X indica la identificación del usuario real y debe estar en formato JPG. |
| **Cargar código de trabajo** | Para cargar códigos de trabajo en el disco USB al dispositivo. |
| **Subir mensaje corto** | Para cargar mensajes cortos guardados en el disco USB al dispositivo. |

| | |
|---|---|
| **Cargar protector de pantalla** | Para cargar todos los protectores de pantalla del disco USB en el dispositivo. Puede elegir Cargar la imagen seleccionada o Cargar todas las imágenes. Las imágenes se mostrarán en la interfaz principal del dispositivo después de la carga. Durante la carga, debe crear una carpeta llamada "publicidad" o "advertise" en el directorio raíz del disco USB y colocar las imágenes publicitarias en este directorio. Se admite un máximo de 20 imágenes y cada imagen no puede superar los 30 KB. El nombre y el formato de la imagen no están limitados, con formatos como jpg, png y bmp compatibles |
| **Cargar fondo** | Para cargar todos los fondos de pantalla del disco USB en el dispositivo. Puede elegir Cargar la imagen seleccionada o Cargar todas las imágenes. Las imágenes se mostrarán en la pantalla después de cargarlas. Durante la carga, debe crear una carpeta llamada "fondo de pantalla" o "walpaper" en el directorio raíz del disco USB y colocar las imágenes del fondo de pantalla en este directorio. Se admite un máximo de 20 imágenes y cada imagen no puede superar los 30 KB. El nombre y el formato de la imagen no están limitados, y se admiten formatos como jpg, png y bmp |
| **Nota** | El tamaño de una sola imagen de usuario o imagen de asistencia no supera los 10 KB, y el dispositivo puede guardar un total de 10.000 imágenes de usuarios e imágenes de asistencia.<br>El tamaño óptimo de una imagen de protector de pantalla o fondo de pantalla es de 640 * 480. |

### 12.3 Configuración de opciones de descarga

En la interfaz de administración de USB, toque Descargar opciones

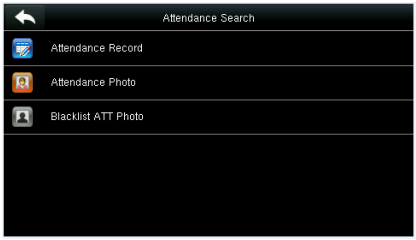



| OPCIÓN DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Cifrar datos de asistencia** | Durante la carga y descarga, los datos de asistencia están encriptados. |
| **Eliminar datos ATT** | Después de una descarga exitosa, los datos de asistencia en el dispositivo se eliminan. |

## 13. Búsqueda de asistencia

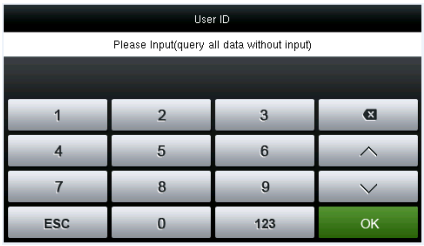
Cuando los usuarios verifican con éxito, los registros de asistencia se guardan en el dispositivo. Esta función permite a los usuarios verificar los registros de asistencia.

Toque Búsqueda de asistencia en la interfaz del menú principal




El proceso de consultar las imágenes de asistencia y las imágenes de la lista negra es el mismo que el de consultar los registros de asistencia. El siguiente es un ejemplo de consulta de registros de asistencia.

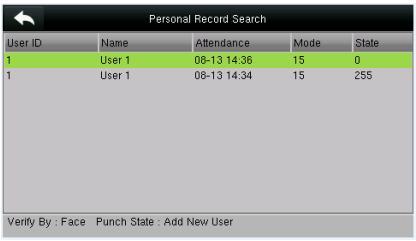
En la interfaz de Registro de asistencia, toque Registro de asistencia.




**1. Ingrese la identificación de usuario que se va a buscar y toque OK. Al marcar OK sin ingresar un ID de usuario, se buscan los registros de asistencia.**


**2. Seleccione el rango de tiempo para la consulta del registro de asistencia de todos los empleados.**


**3. La búsqueda de registros tiene éxito. Toca el registro**

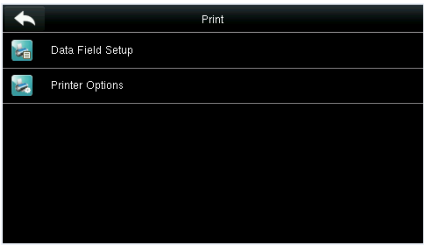



**4. La figura de arriba muestra los detalles de este registro**

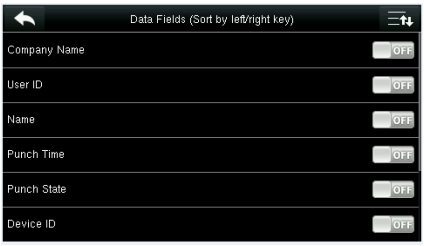
## 14. Configuraciones de impresión

Los dispositivos con función de impresión pueden imprimir registros de asistencia cuando se conecta una impresora (esta función es opcional y solo se puede equipar en algunos productos).

Toque [Imprimir] en la interfaz del menú principal.




**Toque Configuración del campo de datos en la interfaz de impresión.**




**Presione ON / OFF para activar / desactivar los campos que se deben imprimir.**


Presione ON / OFF para activar / desactivar la función de corte de papel.

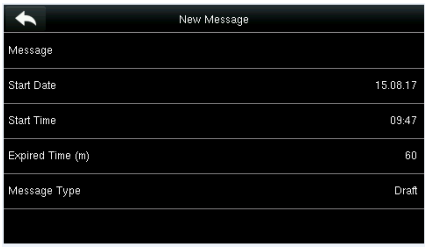
Nota: para activar la función de corte de papel, es necesario conectar el dispositivo con una impresora con función de corte de papel, de modo que la impresora corte los papeles de acuerdo con la información de impresión seleccionada al imprimir.

## 15. Mensaje corto.

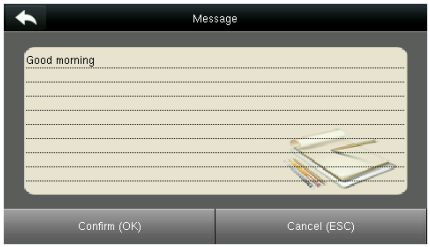
SMS es similar a un aviso. El operador puede editar el contenido del aviso por adelantado y convertirlo en SMS que se muestra en la pantalla. SMS incluye SMS comunes y SMS individuales. Si se establece un SMS común, se mostrará en la columna de información en la parte superior de la interfaz en espera en el tiempo especificado. Si se configura un SMS individual, el empleado que puede recibir SMS puede ver los SMS después de una asistencia exitosa.

### 15.1 Agregar un nuevo mensaje corto

1. Ingresar el contenido: ingrese el contenido de un mensaje corto con un método de entrada.

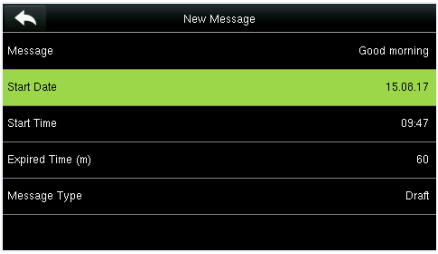



**Seleccione Fecha de inicio y presione OK.**

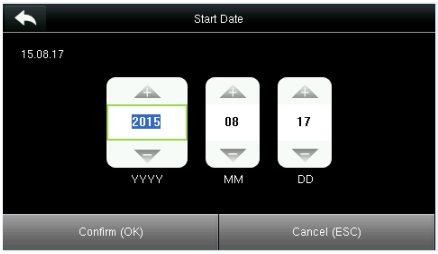



**Ingrese el contenido y presione OK para guardar el contenido ingresado y salir.**

2. Configuración de la fecha y hora de inicio: la fecha y hora en que el mensaje corto se vuelve válido




**Seleccione Fecha de inicio y presione OK..**




**Presione las teclas numéricas en el teclado para ingresar la fecha y presione OK.**

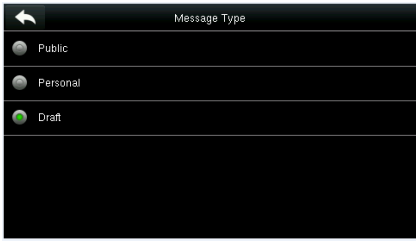
3. Establecer el tiempo vencido (m) SMS aparece en el tiempo efectivo. Después del tiempo efectivo, no aparecerá.}

Nota: Para mensajes cortos públicos, el período efectivo es también el período de visualización. Para mensajes cortos privados, debe establecer un período de visualización después de establecer un período efectivo. Es decir, el período de visualización de un mensaje corto privado se puede ver cuando ingresa o sale durante el período de vigencia del mensaje.

4. Establecer tipo de mensaje

**Público:** los SMS pueden ser vistos por todos los empleados.
**Personal:** SMS dirigido solo a personas.
**Borrador:** SMS preestablecidos, sin diferencia de SMS individuales o SMS comunes

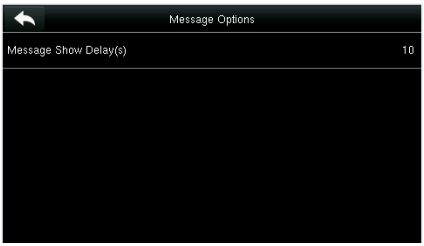

**Seleccione Tipo de mensaje y presione OK para confirmar**




**Presione ▼ para seleccionar un tipo y presione OK para**

### 15.2 Opciones de mensaje

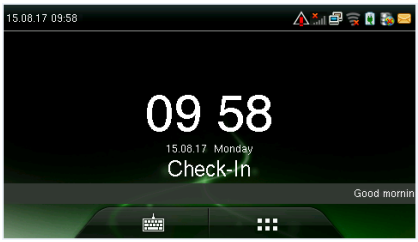
Establezca el tiempo de Retraso para Mostrar mensaje personal en la interfaz inicial.



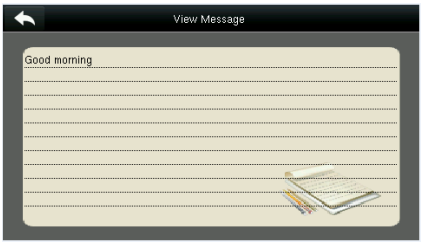


### 15.3 Ver los mensajes públicos y mensaje personal

Después de configurar un mensaje público corto, el ícono de mensaje corto se muestra en la esquina superior derecha de la interfaz principal, y el contenido público de mensajes cortos se muestra en el modo de desplazamiento a continuación.
El contenido de un mensaje corto personal se muestra después de la autenticación de usuario exitosa.



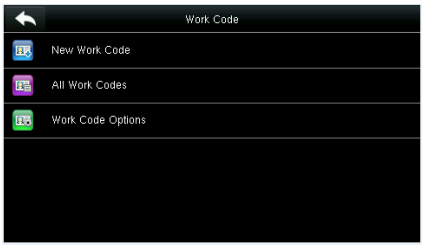

**El mensaje corto público se muestra en la parte inferior de la interfaz.**




**El mensaje corto personal se muestra después de la autenticación de usuario exitosa.**

## 16. Código de trabajo

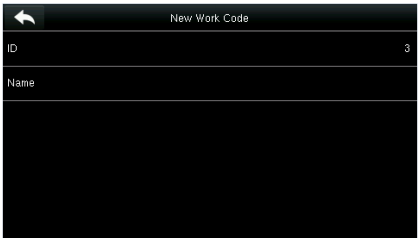
Los salarios de los empleados están sujetos a sus registros de asistencia. Los empleados pueden participar en diferentes tipos de trabajo que pueden variar con los períodos de tiempo. Considerando que los salarios varían según los tipos de trabajo, el terminal FFR proporciona un parámetro para indicar el tipo de trabajo correspondiente para cada registro de asistencia para facilitar una comprensión rápida de las diferentes situaciones de asistencia durante el manejo de los datos de asistencia..



## 16.1 Agregar un código de trabajo

No. : un código digital del código de trabajo.
Etiqueta: El significado del código de trabajo.

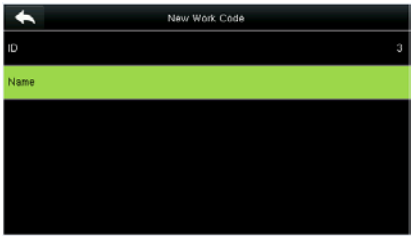
1. Editando un ID



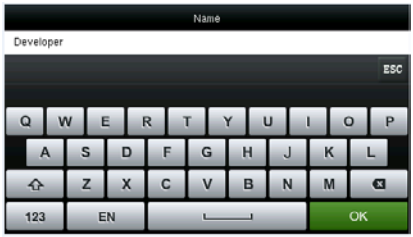

**Seleccione ID**


**Presione las teclas numéricas para asignar un número entre 1 ~ 99999999.**

2. Editando un nombre

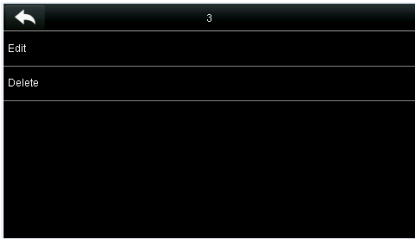



**Seleccione Nombre.**




**Presione * para seleccionar un método de entrada e ingrese un nombre**

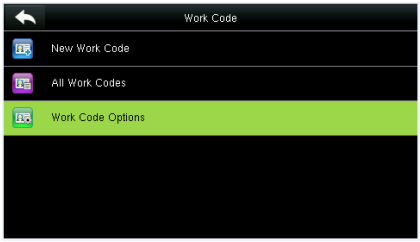

**Ver la información sobre todos los códigos de trabajo.**



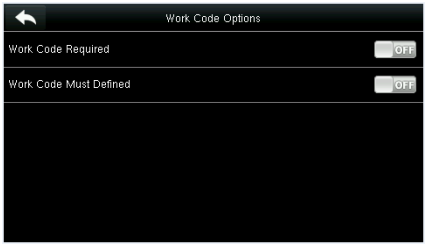

**Edite o elimine un código de trabajo.**

## 16.2 Lista de todos los códigos de trabajo

Puede ver, editar y eliminar códigos de trabajo en Todos los códigos de trabajo. El proceso de edición de un código de trabajo es el mismo que el de agregar un código de trabajo, excepto que no se permite modificar la ID.




**Seleccione Opciones de código de trabajo.**

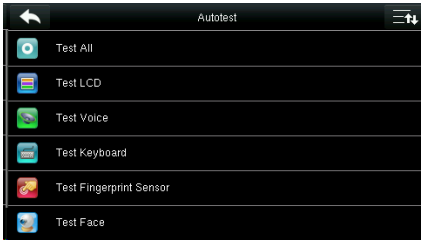



**Presione ON / OFF para encender o apagar.**

## 17. Autotest

Para probar automáticamente si todos los módulos en el dispositivo funcionan correctamente, que incluyen la pantalla LCD, la voz, el teclado, el sensor de huellas digitales, la cámara y el RTC (reloj en tiempo real).

En la interfaz inicial, presione [Autotest] para ingresar a la interfaz de Autotest

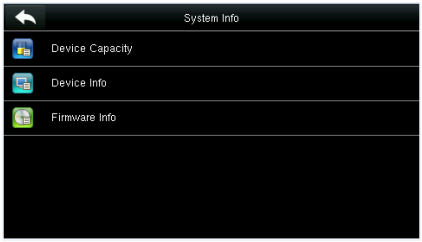



| DETALLES DEL MENÚ | DESCRIPCIÓN |
|---|---|
| **Prueba de LCD** | Para probar el efecto de visualización de la pantalla LCD, visualice a todo color, blanco puro y negro puro para comprobar si la pantalla muestra los colores correctamente. |
| **Prueba de Voz** | El dispositivo prueba automáticamente si los archivos de voz almacenados en el dispositivo están completos y la calidad de la voz es buena. |
| **Prueba de Sensor de huellas** | Para probar el sensor de huellas digitales, presione la huella digital para verificar si la imagen de la huella dactilar recopilada es clara. Al presionar la huella digital en el sensor, la imagen se mostrará en la pantalla. |
| **Prueba de cámara** | Para comprobar si la cámara funciona correctamente, verificando las imágenes tomadas está claras para su uso. |
| **Prueba de Reloj RTC** | Para probar el reloj en tiempo real. El dispositivo prueba si el reloj funciona correctamente y con precisión al marcar el cronómetro. Toque la pantalla para iniciar el tiempo de conteo, y presiónelo nuevamente para detener el conteo, para ver si el cronómetro cuenta el tiempo con precisión. |

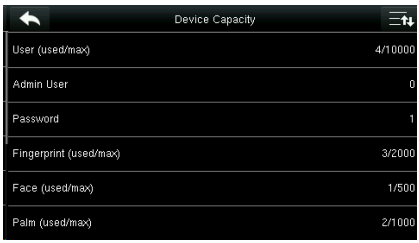
## 18. Información del sistema

Verifique la capacidad de datos, el dispositivo y la información de firmware.

Toque [Información del sistema] en la interfaz del menú principal

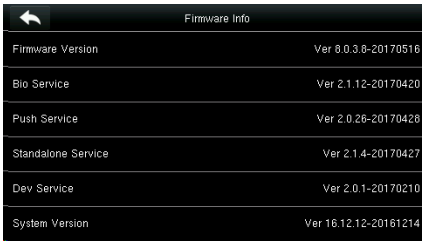



**1. En la interfaz de Información del sistema, toque un elemento de información para ser examinado..**




**2. Vea la información de capacidad de datos, y presione Página abajo para ver otra información..**


**3. Vea la información del dispositivo y presione Página abajo para ver otra información.**




**4. Vea la información del firmware del dispositivo**

## Apéndice 1 Introducción a Wiegand

El protocolo Wiegand26 es un protocolo estándar sobre control de acceso desarrollado por el Subcomité de control de acceso afiliado a la Security Industry Association (SIA). Es un protocolo utilizado para el puerto y la salida del lector de tarjetas IC sin contacto.

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

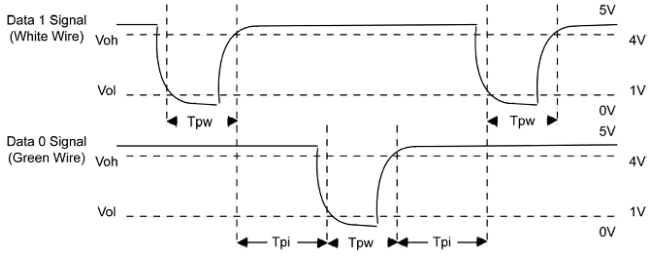
### Señal digital

La figura 1 muestra el diagrama de secuencia del lector de tarjetas que envía la señal digital en bits al controlador de acceso. El Wiegand en este diagrama sigue el protocolo estándar de control de acceso SIA, que se dirige al lector de tarjetas Wiegand de 26 bits (con un tiempo de pulso dentro de los 20us a 100us y un tiempo de salto de pulso de 200us y 20ms). Las señales Data1 y Data0 son de alto nivel (mayor que Voh) hasta que el lector de tarjetas esté listo para enviar una secuencia de datos. El lector de tarjetas envía un pulso asíncrono de bajo nivel (menor que el volumen), transmitiendo el flujo de datos a través del cable Data1 o Data0 para acceder a la caja de control (como la onda de diente de sierra en la figura 1). Los pulsos Data1 y Data0 no se superponen ni sincronizan. La Figura 1 muestra el ancho de pulso máximo y mínimo (pulsos sucesivos) y el tiempo de salto de pulso (el tiempo entre dos pulsos) permitido por los terminales de control de acceso de huellas digitales de la serie F.

**Tabla1: Tiempo de pulso**

| Señal | Definición | Valor típico del lector de tarjetas |
|---|---|---|
| Tpw | Ancho de pulso | 100 µs |
| Tpi | intervalo del pulso | 1 ms |

**Figura 1: diagrama de secuencia**




Los formatos Wiegand de 26 y 34 bits se describen de la siguiente manera:
El sistema tiene un formato Wiegand integrado de 26 bits. Presione [Formato Wiegand], y seleccione "Estándar Wiegand 26 bits".
La composición del formato Wiegand de 26 bits contiene 2 bits de paridad y 24 bits para los contenidos de salida ("ID de usuario" o "Número de tarjeta"). El código binario de 24 bits representa hasta 16,777,216 (0-16,777,215) valores diferentes

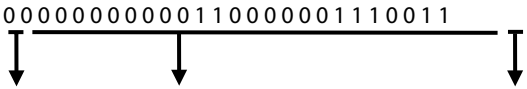
| 1 | 2 | 25 26 |
|---|---|---|
| Paridad par | ID de usuario/ número de tarjeta | Paridad impar |

**Definición de campos:**

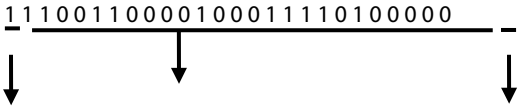
| Campo | Significado |
|---|---|
| Paridad par | Juzgado del bit 2 al bit 13. El bit de paridad par es 1 si el personaje tiene un número par de 1 bit; de lo contrario, el bit de paridad par es 0. |
| ID de usuario / Número de Tarjeta (bit 2-bit 25) | ID de usuario /Número de Tarjeta Codigo de tarjeta, 0-16777215<br>El bit 2 es el bit más significativo (MSB). |
| Bit de paridad impar | Juzgado del bit 14 al bit 25. El bit de paridad impar es 1 si el personaje tiene un número par de 1 bit; de lo contrario, el bit de paridad impar es 0 |

Por ejemplo, para un usuario con el ID de usuario de 12345, el número de tarjeta registrada es 0013378512 y el ID fallido está establecido en 1.

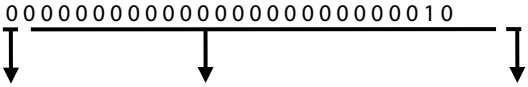
1. Cuando la salida se establece en "ID de usuario", la salida de Wiegand es la siguiente al momento de la verificación exitosa:




2. Cuando la salida se establece en "Número de tarjeta", la salida de Wiegand es la siguiente al momento de la verificación exitosa:




3. La salida de Wiegand es la siguiente al fallo de verificación:




Nota: si el contenido de salida excede el alcancepermitido para el formato Wiegand, los últimos bits serán adoptados y los primeros bits se descartan automáticamente. Por ejemplo: el usuario ID 888 888 888 is 110 100 111 110 110 101 111 000 111 000 en formato binario. Wiegand26 solo soporta 24 bits, esto es, si solo emite los ultimos 24 bits, y los primeros 6 bits "110 100" son automaticamente descartados.

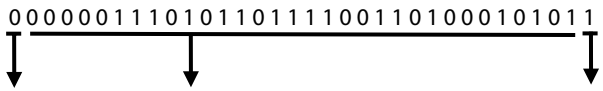
## Wiegand 34

El sistema tiene un formato Wiegand incorporado de 34 bits. Presione [Formato Wiegand], y seleccione "Estándar Wiegand 34 bits".
La composición del formato Wiegand de 34 bits contiene 2 bits de paridad y 32 bits para los contenidos de salida ("ID de usuario" o "Número de tarjeta"). El código binario de 32 bits representa hasta 4,294,967,296 (0-4,294,967,295) valores diferentes.

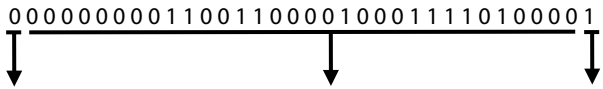
| 1 | 2 | 33 34 |
|---|---|---|
| Paridad par | ID de usuario/ número de tarjeta | Paridad impar |

| Campo | Significado |
|---|---|
| Paridad par | Juzgado del bit 2 al bit 17. El bit de paridad par es 1 si el personaje tiene un número par de 1 bit; de lo contrario, el bit de paridad par es 0. |
| ID de usuario / Número de Tarjeta (bit 2-bit 25) | ID de usuario /Número de Tarjeta Codigo de tarjeta 0–4,294,967,295<br>El bit 2 es el bit más significativo (MSB). |
| Bit de paridad impar | Juzgado del bit 18 al bit 33. El bit de paridad impar es 1 si el personaje tiene un número par de 1 bit; de lo contrario, el bit de paridad impar es 0 |

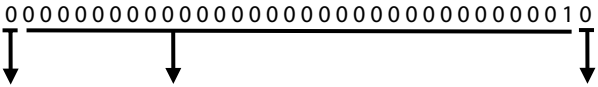
Por ejemplo, para un usuario con la ID de usuario de 123456789, el número de tarjeta registrada es 0013378512 y la ID fallida está establecida en 1. 1. Cuando la salida está configurada en "ID de usuario", la salida de Wiegand es la siguiente después de una verificación exitosa:




2. Cuando la salida se establece en "Número de tarjeta", la salida de Wiegand es la siguiente al momento de la verificación exitosa




3. La salida de Wiegand es la siguiente al fallo de verificación:



## Apéndice 2 Función de impresión

Observaciones: solo algunos modelos admiten la función de impresión.
Instrucción de función
Esta función solo admite el puerto serie pero no la impresión de puerto paralelo. El contenido de impresión se envía a través del formato RS232; la información de verificación saldrá cada vez al puerto en serie. La impresión está disponible si se conecta una impresora, o se puede usar un hiper terminal para leer el contenido de salida.

| | |
|---|---|
| Conexión entre el dispositivo e impresora | Dispositivo Impresora<br>TXD <-----> RXD<br>RXD <-----> TXD<br>GND <-----> FG |
| Orden de línea de pin RS232 |  |

[Operación]
1. En la interfaz inicial, presione [M / OK]> Comm. > Serial Comm> Baudrate, y elija 19200 como la velocidad en baudios.
2. En la interfaz inicial, presione [M / OK]> Imprimir.

Nota:
1. La velocidad en baudios del dispositivo y la impresora (hiper terminal) debe ser consistente.
2. Si el formato de impresión predeterminado no es satisfactorio, puede comunicarse con nuestra empresa para personalizar otros formatos.

## Apéndice 3 Declaración sobre los Derechos Humanos y la Privacidad

Queridos clientes:

Gracias por elegir los productos biométricos híbridos diseñados y fabricados por nosotros. Como proveedor de renombre mundial de tecnologías y servicios biométricos, prestamos mucha atención al cumplimiento de las leyes relacionadas con los derechos humanos y la privacidad en todos los países, mientras realizamos constantemente investigación y desarrollo
Por la presente hacemos las siguientes declaraciones:
1. Todos nuestros dispositivos de reconocimiento de huellas dactilares para uso civil solo recopilan los puntos característicos de las huellas dactilares en lugar de las imágenes de huellas dactilares, y, por lo tanto, no implican problemas de privacidad.
2. Los puntos característicos de las huellas dactilares recopiladas por nuestros productos no pueden utilizarse para restaurar las imágenes originales de huellas dactilares y, por lo tanto, no implican problemas de privacidad.
3. Nosotros, como proveedores de equipos, no seremos responsables legalmente, directa o indirectamente, de las consecuencias que surjan debido al uso de nuestros productos.
4. Para cualquier disputa relacionada con los derechos humanos o la privacidad al usar nuestros productos, por favor
contacte a su empleador directamente
Nuestros productos de huellas dactilares para uso policial o herramientas de desarrollo respaldan la recolección de las imágenes originales de huellas dactilares. En cuanto a si dicho tipo de recolección de huellas dactilares constituye una violación de su privacidad, comuníquese con el gobierno o el proveedor del equipo final. Nosotros, como fabricante del equipo original, no seremos legalmente responsables por ninguna infracción que surja de ello
La ley de la República Popular China tiene las siguientes regulaciones con respecto a la libertad personal:

1. Se prohíbe el arresto, detención o registro ilegal de ciudadanos de la República Popular China; se prohíbe la violación de la privacidad individual.
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 la privacidad de la correspondencia de los ciudadanos de la República Popular de China están protegidas por la ley

Por último, insistimos una vez más en que la biometría, como tecnología avanzada de reconocimiento, se aplicará en muchos sectores, incluidos el comercio electrónico, la banca, los seguros y los asuntos jurídicos. Cada año, personas de todo el mundo sufren grandes pérdidas debido a la inseguridad de las contraseñas. Los productos biométricos ofrecen una protección adecuada para su identidad en un entorno de alta seguridad

## Apéndice 4 Uso amigable con el medio ambiente

## Descripción

El Período de Uso Amigable con el Medio Ambiente (EFUP) marcado en este producto se refiere al período de seguridad del tiempo en que el producto se utiliza bajo las condiciones especificadas en las instrucciones del producto sin fugas de sustancias nocivas y dañinas.
El EFUP de este producto no cubre las partes consumibles que deben reemplazarse regularmente, como baterías, etc. El EFUP de las baterías es de 5 años

**Nombres y Concentración de Sustancias o Elementos Tóxicos y Peligrosos**

| **Nombre de partes** | **Sustancias o elementos tóxicos y peligrosos** | | | | | |
|---|---|---|---|---|---|---|
| | Pb | Hg | Cd | Cr6+ | PBB | PBDE |
| Resistor de chip | x | o | o | o | o | o |
| Chip condensador | x | o | o | o | o | o |
| Chip inductor | x | o | o | o | o | o |
| Diodo de chip | x | o | o | o | o | o |
| Componentes ESD | x | o | o | o | o | o |
| Zumbador | 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 peligrosa contenida en todo el material homogéneo los materiales para esta parte están por debajo del requisito de límite en SJ / T11363-2006.
×: indica que esta sustancia tóxica o peligrosa contenida en al menos uno de los materiales homogéneos para esta parte está por encima del requisito de límite en SJ / T11363-2006.
Nota: el 80% de las piezas de este producto están fabricadas con materiales no peligrosos para el medio ambiente. Las sustancias peligrosas o elementos contenidos no pueden ser reemplazados con materiales respetuosos con el medio ambiente en la actualidad debido a limitaciones técnicas o económicas.

www.zkteco.com

www.zktecolatinoamerica.com