



# Manual de Usuario

## Equipos de Control de Acceso con Reconocimiento de Vena

Julio 2015

## Acerca de este manual

Este documento describe al usuario las interfaces y las funciones del menú de la serie de productos del reconocimiento de vena. Este documento puede ser usado en combinación con el software Access 3.5. Para la instalación del producto, vea por favor la guía de inicio.

- Las imágenes en éste manual quizá no sean iguales a las del producto pero la pantalla del producto actual prevalecerá.
- ★ Significa que solo algunos dispositivos están equipados con ésta función. Los productos actuales prevalecerán.

## Declaración importante

Gracias por haber elegido nuestro producto. Por favor lea este manual cuidadosamente para evitar daños al dispositivo antes de usarlo. Le recordamos que a través del uso adecuado, podrás experimentar buenos resultados y rápida verificación.

Ni una parte de este documento es extraída, copiada o transmitida de algún medio sin previo consentimiento de nuestra compañía.

Los productos descritos en este manual pueden contener software de nuestra compañía o licencias con derechos de autor. A menos que sea permitido, no puede copiar, distribuir, modificar, extraer, descompilar, desembalar, decodificar, ingeniería inversa, rentar, transferir, sub-licenciar dicho software en cualquier forma o realizar otro tipo de comportamiento infringirá en los derechos de autor del software, exclusivo de los casos de prohibición de cualquier limitación por las leyes aplicables.

Debido a la actualización del producto, nuestra compañía no promete la consistencia del manual con los productos actuales y no asume responsabilidades por alguna disputa derivada de la discrepancia entre los parámetros técnicos actuales y de este manual. El manual está sujeto a cambio sin previo aviso.

# CONTENIDO

<b>1. NOTAS DE ORIENTACIÓN.....</b>	<b>1</b>
1.1 Funciones del producto.....	1
1.2 Modos de enrolamiento y verificación de reconocimiento de vena y huella digital ★.....	2
1.3 Método para presionar la huella ★.....	4
1.4 Uso de la pantalla táctil.....	5
1.5 Modos de verificación.....	5
1.5.1 Verificación de reconocimiento de vena y huella digital ★.....	5
1.5.2 Verificación de contraseña.....	7
1.5.3 Verificación de tarjeta ★.....	8
1.5.4 Verificación combinada.....	9
1.5.5 Verificación combinada para desbloquear.....	9
1.6 Apariencia del producto y bloques de la terminal.....	11
1.6.1 Apariencia del producto.....	11
1.6.2 Bloques de la terminal.....	12
1.7 Interface inicial.....	12
<b>2. MENÚ PRINCIPAL.....</b>	<b>13</b>
<b>3. GESTIÓN DE USUARIO.....</b>	<b>15</b>
3.1 Agregar usuarios.....	15
3.1.1 Agregar ID de usuario.....	16
3.1.2 Agregar un nombre.....	17
3.1.3 Privilegio de usuario.....	17
3.1.4 Registrar vena del dedo y huella digital.....	18
3.1.5 Enrolar número de tarjeta ★.....	19
3.1.6 Enrolar contraseña.....	20
3.1.7 Establecer el Nivel de Control de Acceso.....	21
3.2 Todos los Usuarios.....	22
3.2.1 Consultar un Usuario.....	23
3.2.2 Editar/Borrar un Usuario.....	23
3.3 Estilo de la pantalla.....	25
<b>4. PRIVILEGIO DE USUARIO.....</b>	<b>26</b>
<b>5. CONFIGURACIÓN DE COMN.....</b>	<b>28</b>
5.1 Comunicación de Ethernet.....	28
5.2 Comunicación de Comn. Serial.....	29
5.3 Conexión a PC.....	30
5.4 Configuración Wiegand.....	31
5.4.1 Entrada Wiegand.....	31
5.4.2 Salida Wiegand.....	33
5.4.3 Formato de Tarjeta para Detección Automática.....	34

<b>6 CONFIGURACIÓN DE SISTEMA.....</b>	<b>34</b>
6.1 Configurar Fecha/Hora.....	35
6.2 Configuración de Registros de Acceso ★.....	35
6.3 Configuración de Parámetros FV&FP★.....	36
6.4 Restablecer a Configuración de Fábrica.....	37
6.5 Actualización USB.....	37
<b>7 CONFIGURACIÓN PERSONALIZADA.....</b>	<b>38</b>
7.1 Configurar Interface de Usuario.....	38
7.2 Configuración de Voz.....	40
7.3 Configuración de Sirena.....	41
7.3.1 Nuevo Tiempo de Sirena.....	41
7.3.2 Todos los Tiempos de Sirena.....	43
<b>8 GESTIÓN DE DATOS.....</b>	<b>43</b>
8.1 Borrar Datos.....	44
8.2 Respalidar Datos.....	45
8.3 Restaurar Datos.....	47
<b>9 CONTROL DE ACCESO.....</b>	<b>47</b>
9.1 Configuración de las Opciones de Control de Acceso.....	48
9.2 Configuración de Horarios.....	49
9.3 Configuración de Dias Festivos.....	51
9.3.1 Agregar Dia Festivo.....	52
9.3.2 Todos los horarios de Timbre.....	53
9.4 Configuración de Verificación Combianda.....	53
9.5 Configuración Anti-passback.....	55
<b>10 GESTIÓN USB.....</b>	<b>56</b>
10.1 Descargar USB.....	57
10.2 Cargar de la USB.....	57
<b>11 BUSQUEDA DE ASISTENCIA.....</b>	<b>58</b>
<b>12AUTOPRUEBA.....</b>	<b>59</b>
<b>13 INFORMACIÓN DE SISTEMA.....</b>	<b>60</b>
<b>APÉNDICES.....</b>	<b>62</b>
Apéndice 1 Instrucción de la Operación de Entrada de Texto .....	62
Apéndice 2 USB.....	64
Apéndice 3 Introducción Wiegand.....	64
Apéndice 3.1 Introducción Wiegand 26.....	65
Apéndice 3.2 Introducción Wiegand 34.....	67
Apéndice 4 Configuración Anti-passback.....	68
Apéndice 5 Declaración Sobre los Derechos de Privacidad.....	70
Apéndice 6 Descripción del Uso Amigable al Medio Ambiente.....	72

# 1. Notas de Orientación

No exponer el dispositivo directamente a los rayos del sol, porque la luz fuerte tiene un impacto dañino en el colector de imagen de vena. La temperatura de funcionamiento en el dispositivo tiene rangos desde 0°C a 40°C y junto con la disipación de calor del dispositivo, puede comprometer su rendimiento, que se traduce en un reposo más lento. Si el dispositivo debe ser utilizado al aire libre, en una vivienda o en un equipo que irradia calor, es recomendable.

La altura de instalación recomendada (distancia vertical desde el suelo al timbre de la puerta) el dispositivo estaría a 1,4mts. basado en el grupo de usuarios con la altura que va de 1.55mts. a 1.75mts. La altura de instalación puede ajustarse con base a la altura promedio de los usuarios para que el usuario pueda registrarse.

## 1.1 Funciones del Producto

- **Funciones Especiales (Aplicación Lógica de Firmware)**

### 1. Función de reconocimiento de vena

La tecnología de identificación de reconocimiento de vena es una nueva tecnología la cual cuenta con características de diversidad biológica. Ésta reconoce identidades utilizando imágenes de la distribución de venas en los dedos y tiene las características de unidad, estabilidad, alto nivel de exactitud en la identificación y anti-clasificación.

La función de reconocimiento de vena soporta enrolamiento, borrado, verificación y descarga y subida de plantillas vía USB, disco o software.

### 2. Control de Acceso de Usuario

Un control de acceso lógico que se adapta a un controlador tiene las siguientes funciones:

- (1) Configuración de fechas de usuarios válidos
- (2) Configuración de periodos de tiempo efectivo
- (3) Soporta múltiples métodos de verificación de usuario
- (4) Configuración de periodos de tiempo efectivo para las puertas
- (5) Configuración de periodos de tiempo para abrir puertas
- (6) Configuración de periodos de tiempo para días festivos
- (7) Configuración de la primera tarjeta para apertura normal
- (8) Configuración de periodos de tiempo para anti-passback
- (9) Configuración de entrada y salida para anti-passback
- (10) Mantener registros de control de acceso del controlador
- (11) Soporta entrada auxiliar
- (12) Soporta las funciones del dispositivo maestro y esclavo Weigand

### 3. Función Memoria USB

Puede descargar los datos del usuario y control de acceso a una memoria USB y subir los datos de usuario e imágenes de publicidad de la memoria USB al dispositivo.

### 4. Comunicación a través de RS485 ó Ethernet

Los comunica el dispositivo con el software Access 3.5 sobre el protocolo RS485 o Ethernet (TCP/IP).

## 1.2 Modos de Enrolamiento y Verificación de Reconocimiento de Vena y Huella Digital ★

**Nota:** Mientras enrolle una vena, el dispositivo también registra la huella digital del dedo seleccionado.

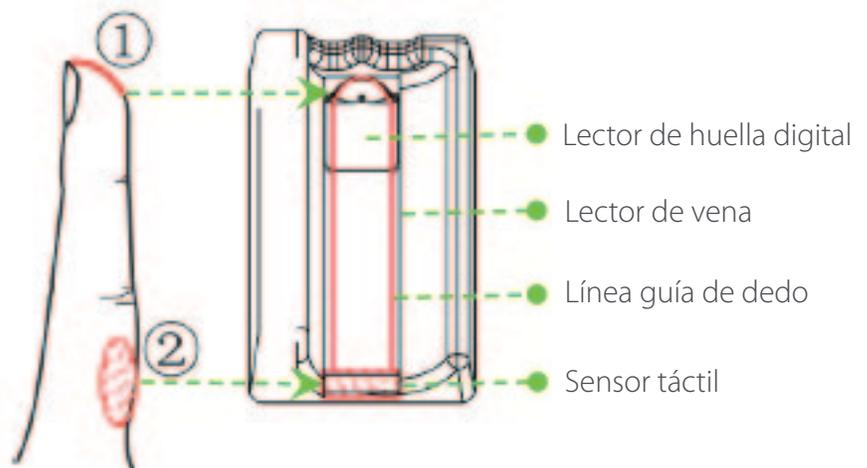
### 1. Dedos recomendados: dedo índice y dedo medio.



### 2. Colocación del dedo

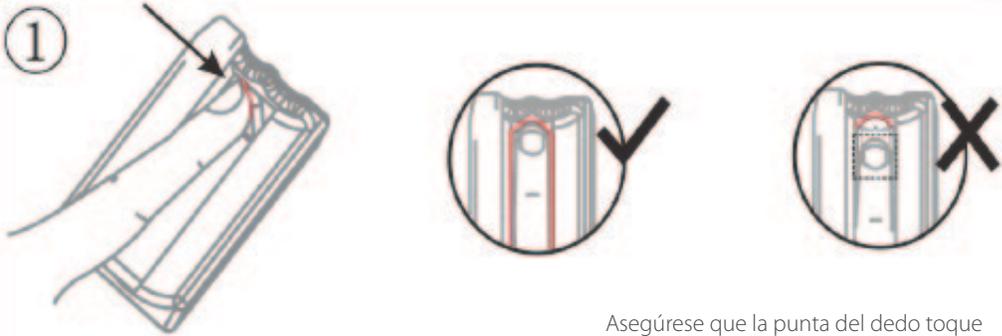
**1.** Tocar el frontal anterior del dispositivo, presione el dedo uniformemente contra el lector de manera que éste perciba la vena y la huella digital.

**2.** Cuando la yema del dedo haga contacto con el sensor, el lector comenzará a reconocer la vena y la huella digital.



### 3. Procedimiento de Verificación de Vena

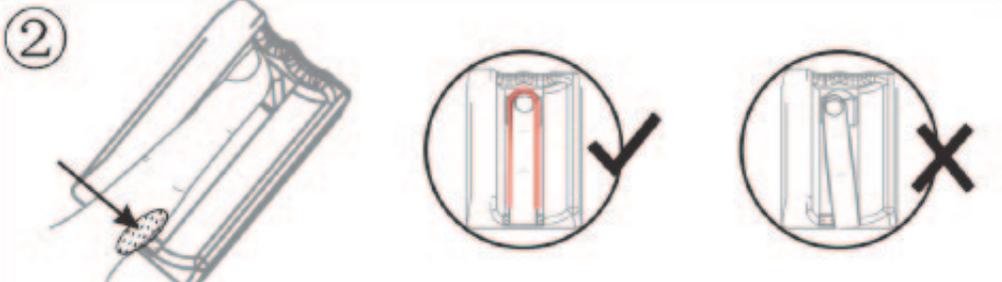
①



Asegúrese de que la punta del dedo toque el extremo del lector de imagen y presione uniformemente la yema del dedo contra el lector.

Asegúrese que la punta del dedo toque el extremo del lector de imagen. De otra manera, las imágenes de la vena y de la huella digital no se copiarán correctamente.

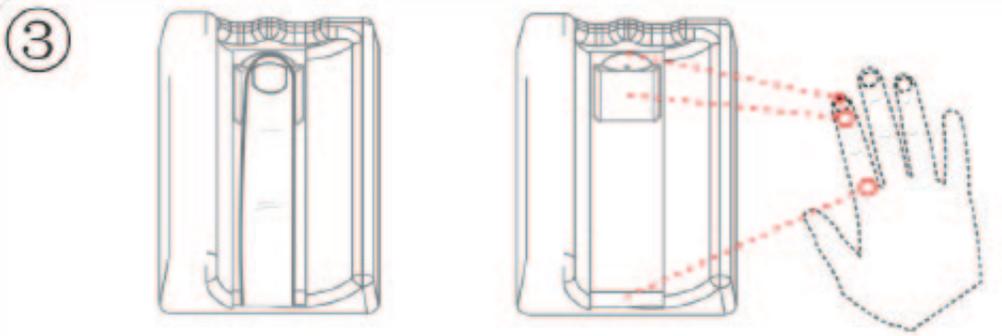
②



Poner el dedo a lo largo de la línea guía, manténgalo en medio, haciendo contacto con la yema del dedo y el sensor.

Las imágenes de la vena y de la huella digital no serán guardadas si el dedo está inclinado

③



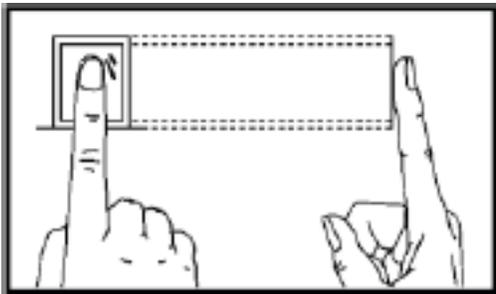
Después de que la yema del dedo haga contacto con el sensor, el lector empezará a leer la imagen de la vena.  
Mantenga el dedo en el lugar hasta oír un "Bip" después de esto podrá alejar el dedo.

- Estire su mano naturalmente sin fuerza.
- Estire su dedo y no trate de doblarlo o girarlo.
- No necesita presionar con fuerza el dedo contra el lector

### 1.3 Método para presionar la huella digital★

Es recomendable usar el dedo índice, dedo medio o dedo anular; evitar usar el dedo pulgar o el meñique.

#### 1. Forma correcta de presionar la huella digital



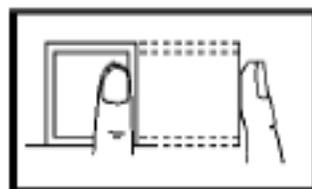
Presiona horizontalmente el dedo en el sensor; colocando la huella en el centro del sensor.

#### 2. Formas incorrectas de presionar la huella digital

**Vertical**



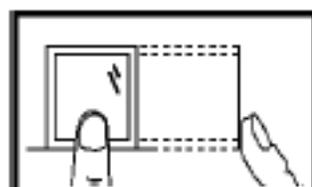
**Lados**



**Inclinado**



**Demasiado abajo**



## 1.4 Uso de la Pantalla Táctil

Puede dar clic en la pantalla táctil o en alguna diapositiva usando la yema del dedo. Si utiliza la punta del dedo o la uña del dedo puede ocasionar algún daño.



De clic en el botón  para mover la pantalla arriba/abajo o arrastre el scroll derecho.



## 1.5 Modos de Verificación

### 1.5.1 Verificación de Reconocimiento de Vena y Huella Digital★

#### ► Verificación 1:N

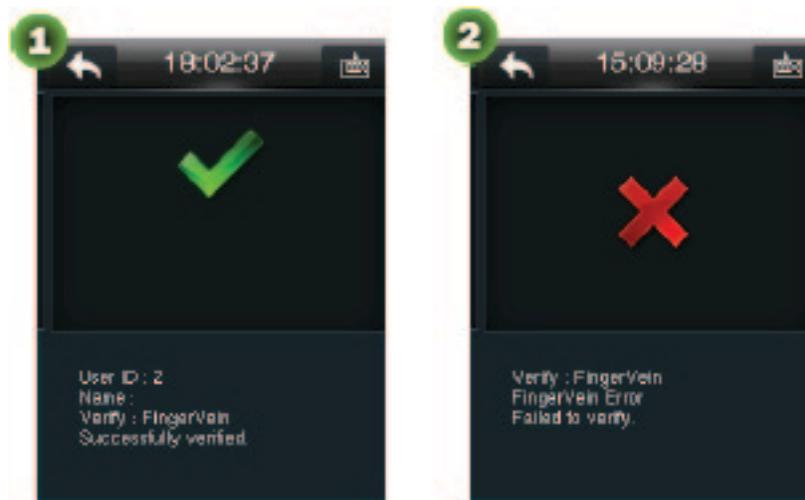
La imagen de vena y la huella digital guardada en el lector es comparada con todas las imágenes de vena y huellas en el dispositivo.

1. El dispositivo detecta automáticamente la vena u otro modo de verificación. Cuando el dedo tiene contacto con el sensor de vena, el dispositivo empieza en modo de verificación de vena y de huella digital.

(Nota: para la posición del sensor de reconocimiento de vena, vea 1.6.1 "Apariencia del producto")

2. Presione el dedo en el lector correctamente. Para más detalles, vea 1.2 "Modos de Enrolamiento y Verificación de Reconocimiento de Vena y Huella Digital"

3. Después de que el dispositivo genera el sonido "Bip", retire el dedo. Si la verificación es exitosa, el dispositivo reproducirá una voz diciendo "Gracias" y "Acceso Correcto" desplegado en la pantalla. Si la verificación falla, el dispositivo reproducirá una voz diciendo "Por favor intente de nuevo" y "Acceso denegado" desplegado en la pantalla.



### ► Verificación 1:1

La imagen de vena y la huella digital, recogida actualmente por el lector se comparan con las imágenes asociadas con el ID de usuario introducida a través del teclado. Este modo es usado cuando es difícil la verificación con vena o huella digital.

1. En la interface inicial, dar clic en para entrar al ID de usuario.
2. Ingrese el ID de usuario y dar clic en OK (ver imagen 2) para entrar en la interface y seleccionar el modo de verificación.

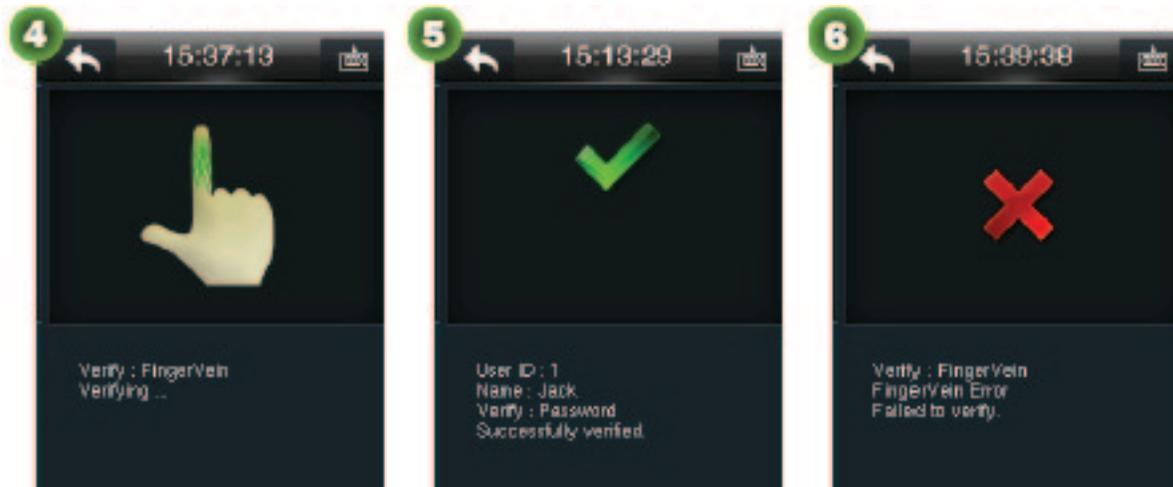
**Nota:** Si aparece "Sin datos", el ID de usuario no existe.

3. Haga clic en el icono verificador de vena (vea la imagen 3) y entrará a la interface 1:1 de verificación de vena.



4. Presione el dedo en el lector correctamente. Para más detalles, ver 1.2 “Modos de Enrolamiento y Verificación de Reconocimiento de Vena y Huella Digital”.

5. Después de que el dispositivo genera el sonido “Bip”, retire el dedo. Si la verificación es exitosa, el dispositivo reproducirá una voz diciendo “Gracias” y “Acceso Correcto” desplegado en la pantalla (ver **imagen 5**). Si la verificación falla, el dispositivo reproducirá una voz diciendo “Por favor intente de nuevo” y “Acceso denegado” desplegado en la pantalla (ver **imagen 6**).



### 1.5.2 Verificación de Contraseña

1. En la interface inicial, dar clic en  para entrar al ID de usuario.

2. Ingrese el ID de usuario y dar clic en OK (ver imagen 2) para entrar en la interface y seleccionar el modo de verificación.

**Nota:** Si aparece “Sin datos”, el ID de usuario no existe.

3. Haga clic en el icono (vea la **imagen 3**) y entrará a la interface de verificación de contraseña.



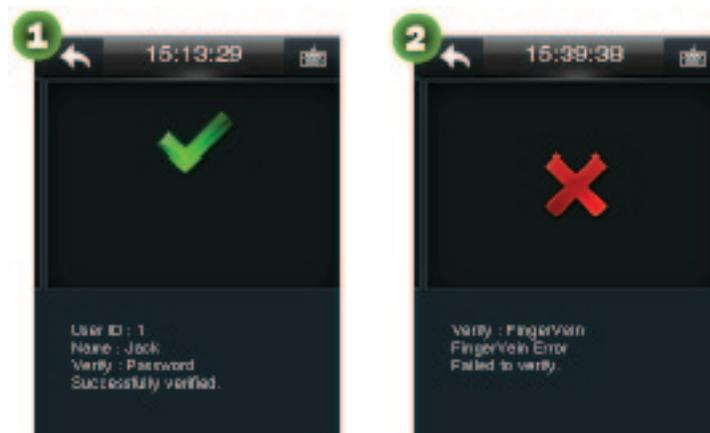
4. En la interface de la pantalla, ingrese la contraseña y de clic en **OK**. Si la verificación es exitosa, el dispositivo reproducirá una voz diciendo "Gracias" y "Acceso Correcto" desplegado en la pantalla. Si la verificación falla, el dispositivo reproducirá una voz diciendo "Por favor intente de nuevo" y "Acceso denegado" desplegado en la pantalla.



### 1.5.3 Verificación de Tarjeta★

1. La función de tarjeta es opcional. Solo los productos que integran módulo de tarjeta tienen la función de verificación con tarjeta. Algunos dispositivos soportan tarjetas Mifare como tarjetas ID.

2. Si la verificación es exitosa, el dispositivo reproducirá una voz diciendo "Gracias" y "Acceso Correcto" desplegado en la pantalla. Si la verificación falla, el dispositivo reproducirá una voz diciendo "Por favor intente de nuevo" y "Acceso denegado" desplegado en la pantalla.



### 1.5.4 Verificación de Tarjeta

El dispositivo soporta verificación combinada, como reconocimiento de vena y contraseña, el dispositivo necesita verificar la contraseña/vena después de que el usuario pasa la verificación de vena y contraseña. Tomar la verificación de vena y contraseña por ejemplo. Supongamos que el usuario primero realiza la verificación de vena.

1. Presione el dedo en el lector correctamente. Para más detalles, vea 1.2 “Modos de enrolamiento y verificación de reconocimiento de vena y huella digital”
2. Después de que el dispositivo genera el sonido “Bip”, retire el dedo. Y se pasa al reconocimiento de vena, la interface de verificación de contraseña como se ve en la pantalla (ver **imagen 2**).



3. Ingrese la contraseña correcta y haga clic en OK. Cuando la contraseña pase la verificación, aparecerá en la pantalla “Acceso Correcto” (ver imagen 4).

**Nota:** El usuario puede usar estos modos de verificación si los necesita. Para más especificaciones, vea 9.1 “Configuración de las Opciones de Control de Acceso”.

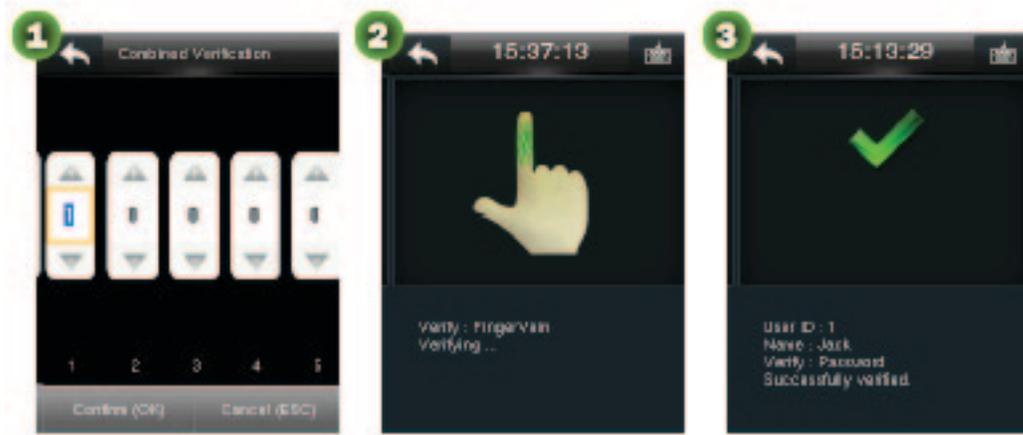
### 1.5.5 Verificación Combinada por Desbloqueo

#### **Notas:**

- ① Para más detalles sobre cómo poner verificación combinada por desbloqueo, vea 9.4 “Configuración de Verificación Combinada”.
- ② En la interface de añadir/editar del usuario, el administrador puede especificar el grupo al que pertenece y añadir un usuario al grupo de desbloqueo. Para detalles de métodos de operación, vea 3.1.7 “Establecer el Nivel de Control de Acceso”.

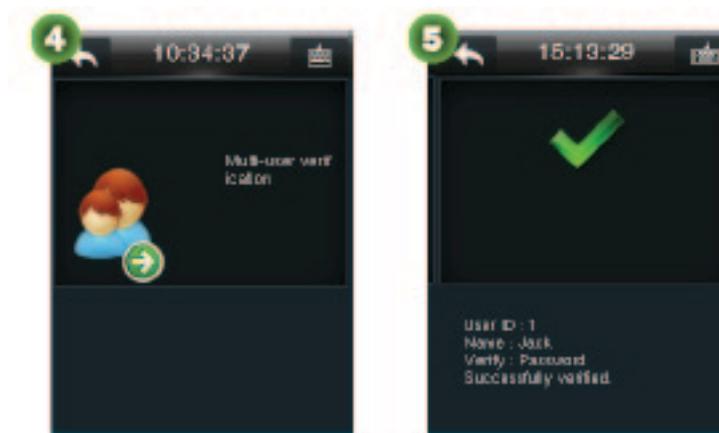
Por ejemplo, agregue una combinación de desbloqueo requiriendo simultaneas verificaciones del grupo 1 y grupo 2 (vea **imagen 1**) y agregue usuarios a los grupos para desbloquear.

Suponga que el usuario con ID 1 pertenece al grupo 1 y el usuario con ID 2 pertenece al grupo 2.



1. El usuario con ID 1 presione el dedo correctamente en el lector. Para más detalles, vea 1.2 "Modos de enrolamiento y verificación de reconocimiento de vena y huella digital".

2. Después de que el dispositivo genera el sonido "Bip", retire el dedo. Y se pasa al reconocimiento de vena (vea imagen 3), la pantalla del dispositivo mostrará "Verificación Multi-Usuario" (vea imagen 4).

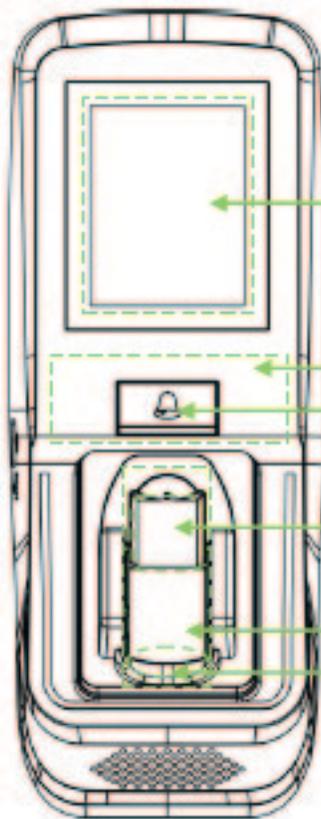


3. El usuario con ID 2 presione el dedo correctamente en el lector. Después de que el dispositivo genera el sonido "Bip", retire el dedo. Si la verificación es exitosa, el dispositivo reproducirá una voz diciendo "Gracias" y "Acceso Correcto" desplegado en la pantalla.

## 1.6 Apariencia del Producto y Bloques de la Terminal

### 1.6.1 Apariencia del Producto

#### ● Vista frontal del dispositivo de vena y huella digital



Pantalla Táctil

Área de aproximación de tarjeta

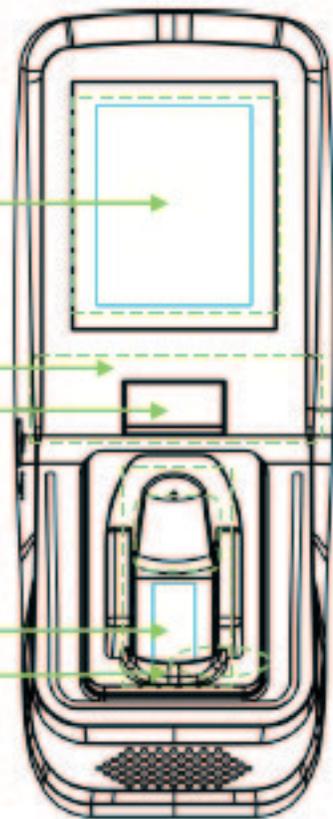
Indicador, timbre de puerta

Lector de huella

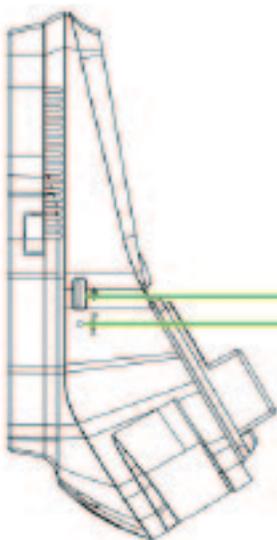
Lector de vena

Sensor de lector de vena

#### Vista frontal del dispositivo de vena



#### ● Vista lateral

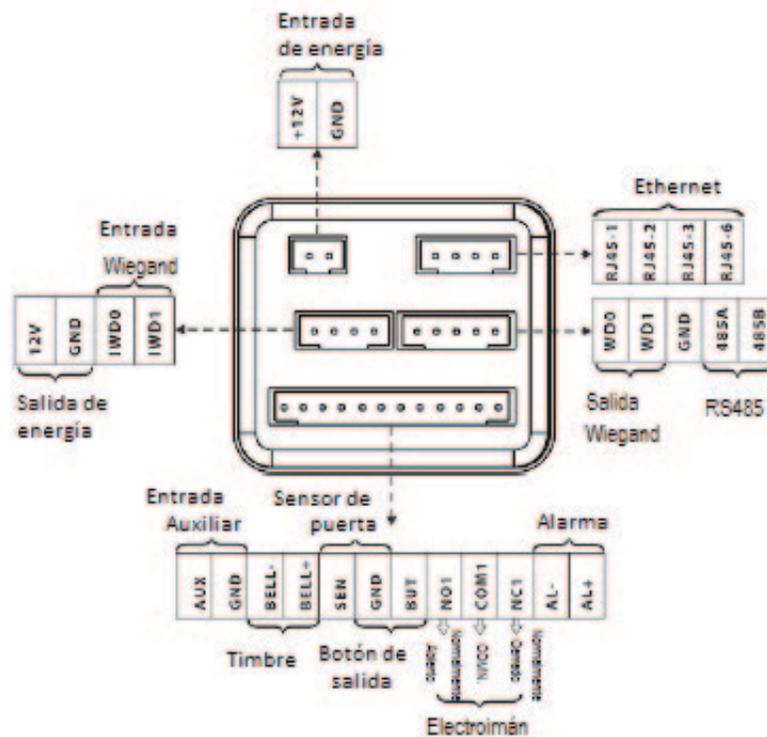


Puerto USB

Botón de Reset

**Botón de reset:** Después de que el dispositivo es prendido por 30 segundos, pulse el botón usando una herramienta afilada de extremo con un diámetro de menos de 2mm para resetear el dispositivo.

## 1.6.2 Bloque de la Terminal



Entrada de alimentación: Use el adaptador de energía standard. El voltaje es de DC 12V y la corriente no debe ser menor a 3A. No debe usar otro suministro de energía para evitar daños al dispositivo.

Puerto Ethernet: Es una interfaz de red, la cual el dispositivo se puede conectar a una red mediante un conmutador, router o cubo.

Puerto de entrada auxiliar: Conecte una alarma de humo para recibir la señal de alarma.

## 1.7 Interfaz Inicial

1. **Fecha:** Fecha actual del dispositivo.
2. **Señal de Alarma:** Si se muestra este ícono se ha configurado una alarma para el dispositivo.
3. **Señal de conexión de red:** Estado de la conexión de red del dispositivo.
4. **Alarma de desmontaje:** El botón de desmontaje de alarma depende si este ícono aparece en la pantalla y posiblemente la causa es "instalación inadecuada" o "desmontaje ilegal".
5. **Salida auxiliar:** Éste ícono es desplegado cuando la entrada auxiliar de la terminal está conectada a un dispositivo auxiliar y se dispara la condición de la entrada auxiliar.
6. **Hora:** La hora actual del dispositivo es desplegada. Se puede configurar en 12 hrs. y en 24 hrs. Puede personalizar el estilo del menú principal.

7. **Menú:** Presione el ícono para entrar al menú. Si se ha establecido un administrador para el dispositivo, debería pasar la verificación de éste antes de acceder al menú.

8. **1:1 Verificación (teclado en pantalla):** Presione la clave para entrar a la interfaz introduciendo la ID de un usuario en el modo de verificación 1:1. Después dar clic en OK y completar la verificación 1:1 de acuerdo a las indicaciones en la interfaz.

## 2. Menú Principal

En la interfaz inicial, dar clic  para entrar al menú principal (ver **imagen 2**). Dar clic en  para desplazarse hacia abajo de la pantalla (ver **imagen 3**) para mostrar el contenido.



Estos son los 12 sub-menús debajo del menú principal.

<b>Gestión de Usuarios</b>	Es para establecer a un usuario administrador, busca información de usuario (incluido ID de usuarios, privilegios de usuario, imágenes de vena, huellas digitales, números de tarjeta★, contraseñas y niveles de control de acceso) y agregar, consultar, modificar o eliminar tal información.
<b>Privilegio de Usuario</b>	Sirve para establecer privilegios de usuario para acceder al menú y cambiar configuración.
<b>Comn.</b>	Se usa para establecer parámetros relacionados a la comunicación entre el dispositivo y la PC, incluyendo parámetros de Ethernet tales como dirección de IP etc., comunicación serial, conexión a PC y configuraciones Wiegand
<b>Sistema</b>	Para establecer el sistema relacionado con parámetros y actualización de firmware, incluyendo hora, archivos de control de acceso, parámetros de reconocimiento de vena y huella digital así como factores de restauración de ajustes de fábrica, de modo que el dispositivo cumple hasta el máximo en funciones y pantalla.
<b>Personalizar</b>	Esto incluye la pantalla de interfaz, voz, timbre, estado de verificación, modo de teclado y configuración de tecla de acceso directo.
<b>Gestión de Datos</b>	Para eliminar datos de asistencia, todos los datos, privilegios del super-administrador o protectores de pantalla, etc.
<b>Control de Acceso</b>	Establecer los parámetros del bloqueo de control y dispositivos de acceso de control, incluyendo parámetros para acceso de control, normas de tiempo, días festivos, desbloqueo combinado y anti-passback.
<b>USB</b>	Puede transferir datos como datos de usuario y asistencia, registros de la USB en el software de soporte o de otro dispositivo.
<b>Búsqueda de Asistencia</b>	Para consultar los archivos salvados en el dispositivo después de la verificación.
<b>Auto-prueba</b>	Automáticamente realiza pruebas de las diferentes funciones de los módulos, incluyendo el LCD, voz, teclado, sensor de huella digital, cámara★ y prueba del tiempo real en el reloj.
<b>Información del Sistema</b>	Comprueba la capacidad del dispositivo, información del firmware y del dispositivo.

Cuando no se establece a un administrador, cualquiera puede acceder al menú principal dando clic en . Después de que un administrador se establece, el usuario debe pasar la verificación de la identidad del administrador antes de entrar al menú.

Por motivo de seguridad, es recomendable que un administrador se registre cuando el dispositivo es usado por primera vez.

### 3. Gestión de Usuario

La información básica registrada del usuario en el dispositivo incluye el ID de usuario, nombre, privilegios de usuario, imagen de vena y huella digital★, contraseñas, números de tarjeta ★ y niveles de control de acceso. Ésta información está sujeta a cambio debido a cambios personales y por lo tanto el dispositivo soporta operaciones como agregar, borrar, consultar y modificar.



#### 3.1 Agregar un Usuario

En la interfaz **Gestión de Usuario**, de clic en **Nuevo Usuario** y de clic en  para desplazarse hacia abajo para ver el contenido. (Nota: Usted puede dar clic en  para regresar arriba.)



**ID de Usuario:** Ingrese un ID de usuario. Por defecto, soporta de 1-9 caracteres. Un carácter chino, ocupan dos caracteres.

**Nombre:** Ingrese un nombre de usuario. Por defecto, soporta de 1-24 caracteres. Un carácter chino, ocupa dos caracteres.

**Privilegios de Usuario:** Establecer privilegios de usuario. El valor por defecto es **Usuario Normal**. Puede escoger al **Super Admin**. Un usuario normal solamente puede usar la verificación por vena, huella digital ★ tarjeta★ o contraseña, mientras que un administrador tiene todas las funciones del usuario normal y acceso al menú principal.

**FV&FP ★:** Enrolar con reconocimiento de vena y huella digital. Índice y dedo medio son los recomendados. Contraseña: Enrolar con contraseña. Por defecto, soporta de 1-8 dígitos.

**Número de Tarjeta ★:** Enrolar un número de tarjeta.

**Nivel de Control de Acceso:** Establece los niveles de acceso de los usuarios.

### 3.1.1 Agregar ID de Usuario

El dispositivo automáticamente asigna un ID al usuario, a partir de 1. Si usa un número de dispositivo asignado, omite este paso.

1. En la interfaz **Nuevo Usuario**, haga clic en **ID de usuario**.



**Tips:** Enrole ID's de usuarios que no puedan ser modificados.

2. En la interfaz que se muestra, ingrese un ID de un usuario que este registrado y de clic en **OK** para salvar la configuración y regrese a la interfaz **Nuevo Usuario**. Si se muestra "Ya existe ID de usuario", esto indica que este ID ya ha sido usado.

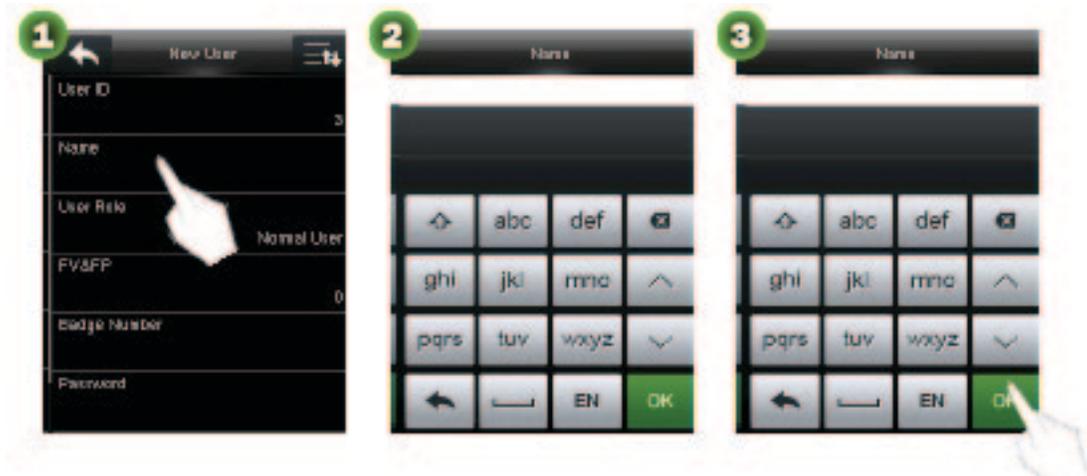
**Tips:** Por defecto, los ID's de usuario soportan de 1-9 dígitos. Para extender dígitos, consulte a nuestros representantes de ventas o a nuestro personal de soporte.

### 3.1.2 Agregar un Nombre

Ingrese un nombre de usuario utilizando el método de entrada T9 con el teclado.

1. En la interfaz Nuevo Usuario, haga clic en Nombre.
2. En la interfaz que se muestra, ingrese un nombre de usuario ya registrado. Haga clic para seleccionar las letras.

Para la operación de la interfaz del teclado, vea Apéndice 1 Instrucción de la Operación de Entrada de Texto.



3. Después de ingresar el nombre, haga clic en OK para salvar y regrese a la interfaz Nuevo Usuario. Si da clic en, el dispositivo regresará a la interfaz del nivel superior sin salvar la información.

Tips: Por defecto, soporta de 1-24 caracteres para el nombre. Un carácter chino, ocupa dos caracteres.

### 3.1.3 Privilegios de Usuario

El dispositivo soporta dos privilegios de usuario: Usuario Normal y Super Admin.

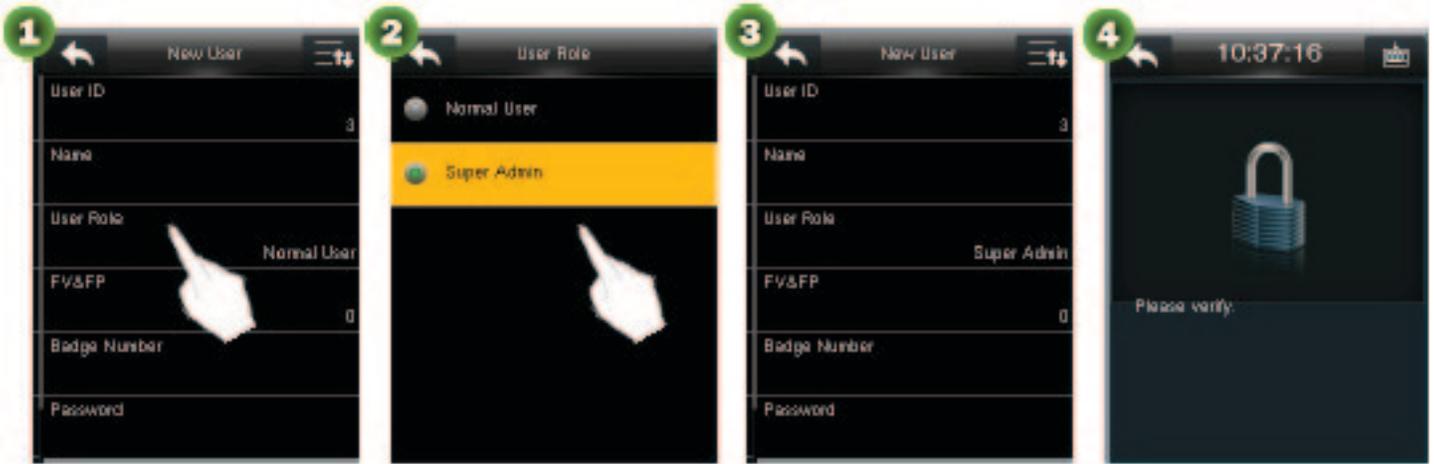
**Super Admin.:** Un Super Administrador permite realizar operaciones en todos los menús.

**Usuario Normal:** Cuando se establece un administrador, un usuario normal solo puede usar reconocimiento de vena (huella digital★), contraseñas o tarjetas★ para verificación. Cuando no se ha establecido administrador, un usuario normal tiene permitido realizar operaciones en todos los menús.

**Definir Privilegios de Usuarios:** Después de establecer un super administrador, puede definir los Privilegios de Usuario y asignar que operación tiene derecho a realizar. El Usuario Definido tiene los derechos del usuario normal, como la verificación vía vena (huella digita★), contraseña y tarjeta.

Indica que el usuario actual es un administrador.

1. En la interfaz **Nuevo Usuario**, haga clic en **Privilegios de Usuario**.



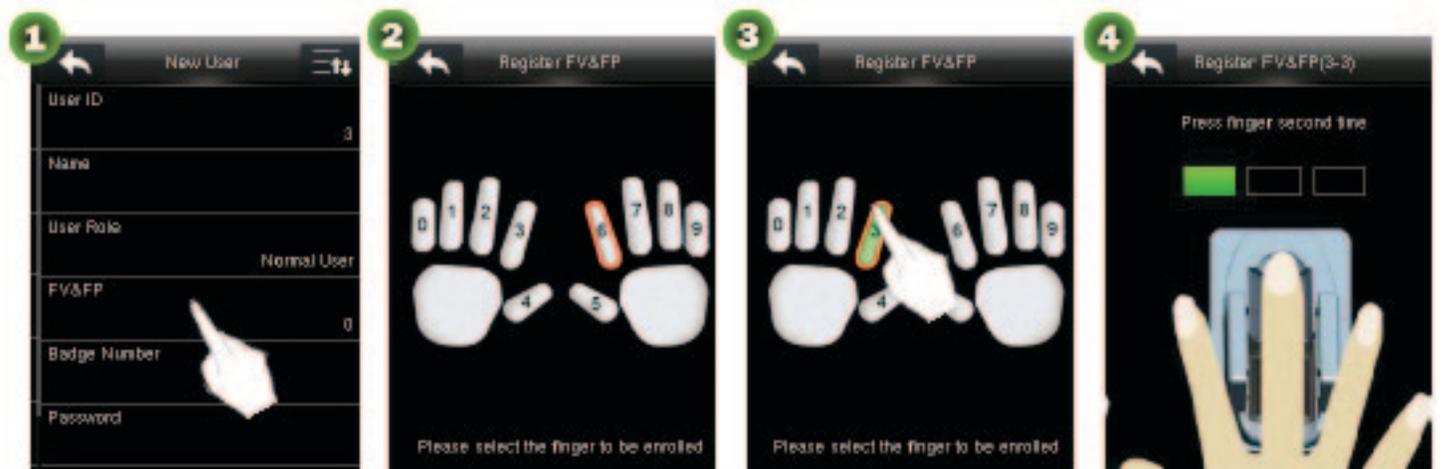
2. Seleccione los privilegios que necesita. Después, regrese a la interfaz **Nuevo Usuario**.

**Nota:** Después de añadir al super administrador, necesita pasar la verificación del mismo antes de acceder al menú principal.

### 3.1.4 Privilegios de Usuario

**Nota:** Mientras enrole una vena, el dispositivo registrará la huella del dedo seleccionado.

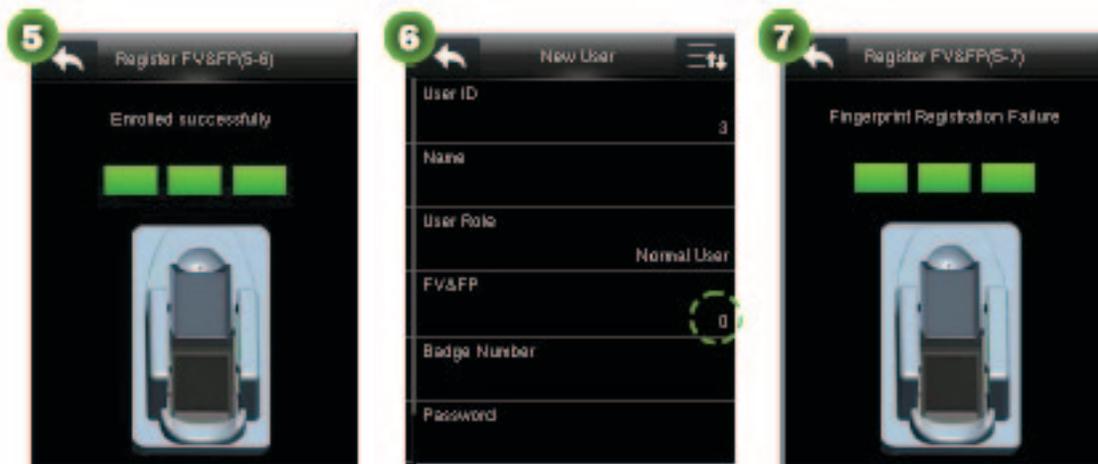
1. En la interfaz de **Nuevo Usuario**, de clic en **FV&FP** para entrar a la interfaz **Registro de FV&FP** (ver imagen 2).



2. En la interfaz que se muestra en la pantalla, de clic en el dedo que enrolará la huella o la vena (ver imagen 3).

3. Presione el mismo dedo en el lector por tres veces consecutivas de acuerdo a las indicaciones en el dispositivo (ver imagen 4). Para más detalles, vea 1.2 “Modos de enrolamiento y verificación de reconocimiento de vena y huella digital”.

Después de que se coloca el dedo tres veces, el dispositivo arrojará el mensaje “Acceso correcto” en la pantalla (ver imagen 5) y el dispositivo regresará a la interfaz de **Nuevo Usuario** y mostrará el número de registros de vena y huella (ver imagen 6). Si el registro es fallido, se mostrará en la pantalla el mensaje “Registro Fallido” (ver imagen 7). Continuar el registro, repita los pasos 2 y 3.



### Notas:

- ① Durante el enrolamiento de vena y huella, generará el sonido “Bip” así el lector indicará que se ha registrado con éxito.
- ② Para un mejor enrolamiento de venas y de huellas, retire el dedo después de que el registro sea exitoso (después del sonido “Bip” generado) y continúe presionando el dedo nuevamente.

### 3.1.5 Agregar una tarjeta ★

1. En la interfaz **Nuevo Usuario**, de clic en **Tarjeta Numérica** entrará en la interfaz Enrolamiento con tarjeta numérica (ver **imagen 2**).
2. Deslizar una tarjeta encima del área. Para detalles acerca del área de deslizamiento de tarjeta, vea 1.6.1 “Apariencia del producto”.
3. Después de que la tarjeta es leída correctamente, el número aparecerá en la pantalla (ver **imagen 3**) el dispositivo retornará a la interfaz **Nuevo Usuario** (ver **imagen 4**).



**Nota:** Algunos dispositivos soportan tarjetas Mifare como tarjetas ID.

### 3.1.6 Agregar una contraseña

1. En la interfaz **Nuevo Usuario**, dar clic en Contraseña.
2. En la pantalla aparecerá un teclado, ingresar la contraseña y dar clic en OK (ver **Imagen 2**)

**Tips:** Por defecto, soporta contraseñas de 1-8 dígitos.

3. Ingrese nuevamente la contraseña y de clic en OK guarde la contraseña (ver **imagen 3**). Después de que se guarda satisfactoriamente, el dispositivo regresará a la interfaz de Nuevo Usuario (ver **imagen 4**).



#### Notas:

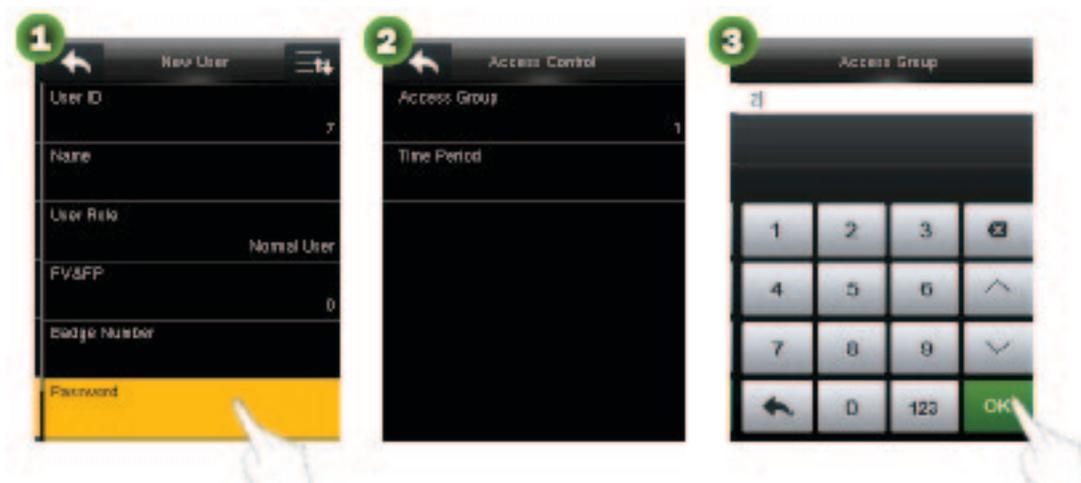
- ① Las contraseñas ingresadas en los pasos 2 y 3 deben ser iguales. De otra manera aparecerá un mensaje en la pantalla.
- ② Si ingresa una contraseña diferente, necesita regresar al paso 2 e ingresarla nuevamente



### 3.1.7 Agregar una contraseña

En la interfaz **Nuevo Usuario**, de clic en **Control de Acceso** y entre (ver imagen 2).

El nivel de control de acceso es usado para ajustar el nivel de apertura de la puerta para cada usuario, incluyendo el grupo de acceso y periodos de tiempo.



- **Configuración para un grupo de acceso**

Establezca al grupo de usuarios que pertenecen a este grupo, para facilitar el desbloqueo de la configuración de combinación. Un grupo válido de números oscila de 0 a 99999999.

① En la interfaz **Control de Acceso**, de clic en **Grupo de Acceso**.

② Introduzca el número del grupo a la que pertenece el usuario y de clic en **OK** (ver imagen 3) guarde la configuración y regrese a la interfaz **Control de Acceso**.

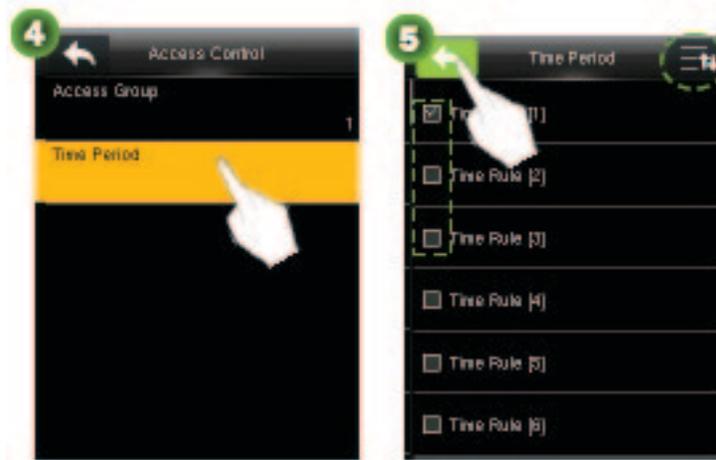
- **Configuración de periodo de tiempo**

Seleccione las reglas de horario para el usuario. Las reglas de horario estarán debajo del menú **Control de Acceso** y soporta máximo 50 reglas de tiempo. El período de tiempo efectivo del usuario de apertura de la puerta es la suma de las reglas de tiempo seleccionadas.

① En la interfaz **Control de Acceso**, de clic en **Periodo de Tiempo** (ver imagen 4).

De clic  para deslizarse arriba/debajo de la pantallas para ver más opciones.

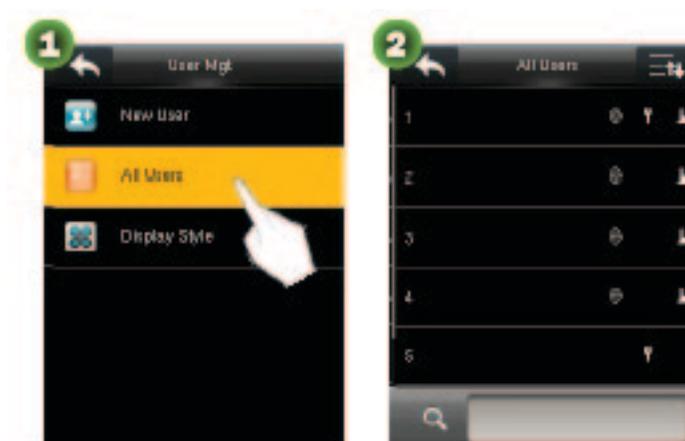
② En la lista de reglas de horario, de clic y seleccione una regla de horario (puede seleccionar varias y el símbolo  indica que la regla de horario está seleccionada), de clic  (ver imagen 5) guarde la configuración y regrese a la interfaz previa.



### 3.2 Todos los Usuarios

En la interfaz **Gestión de Usuarios**, de clic en **Todos los Usuarios** y entre a la interfaz (ver imagen 2).

Puede consultar al administrador, edite o elimine usuarios.



: Indica que el usuario actual es un super administrador.

: Indica que la huella del usuario está guardada.

: Indica que el número de tarjeta del usuario está guardado.

: Indica que la contraseña del usuario está guardada.

: Indica que la vena del usuario está guardada.

**Tips:** La información de todos los usuarios registrados aparecerá de acuerdo al Estilo de Pantalla preestablecido. Para más detalles acerca del Estilo de Pantalla, vea 3.3 “Estilo de la pantalla”.

### 3.2.1 Consultar un Usuario

Usted puede consultar un usuario por nombre o ID de usuario. El funcionamiento detallado es como se muestra:

1. De clic en la opción consultar (ver **imagen 1**) entre a la interfaz como se muestra en la **Imagen 2**.
2. Entre en consultar condición, de clic en **OK** (ver **imagen 4**).



### 3.2.2 Editar/Eliminar un Usuario

En la interfaz Todos los Usuarios, de clic en un usuario (ver **imagen 1**) entre en la interfaz como se muestra en la **Imagen 2**.

- **Editar Usuario**

Haga clic en **Editar** (ver **imagen 3**) entre a **Nuevo Usuario** (ver **imagen 4**).

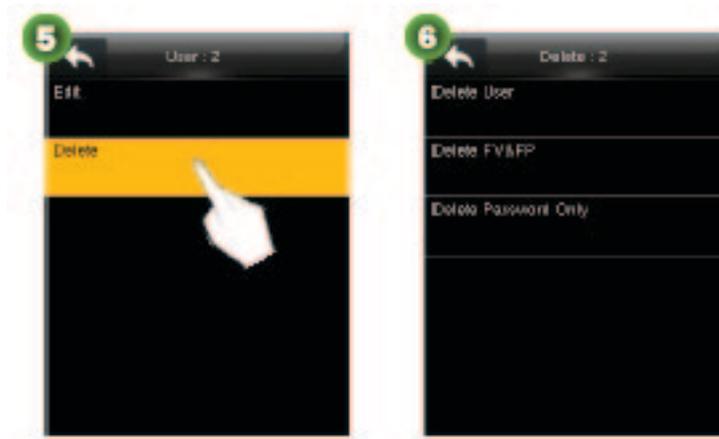


2. Modificar la información del usuario, dar clic guarde la configuración y regrese a la interfaz previa.  
Nota: El método de edición de un usuario es la misma que la de añadir un usuario y no se describe aquí.

## ● **Borrar un Usuario**

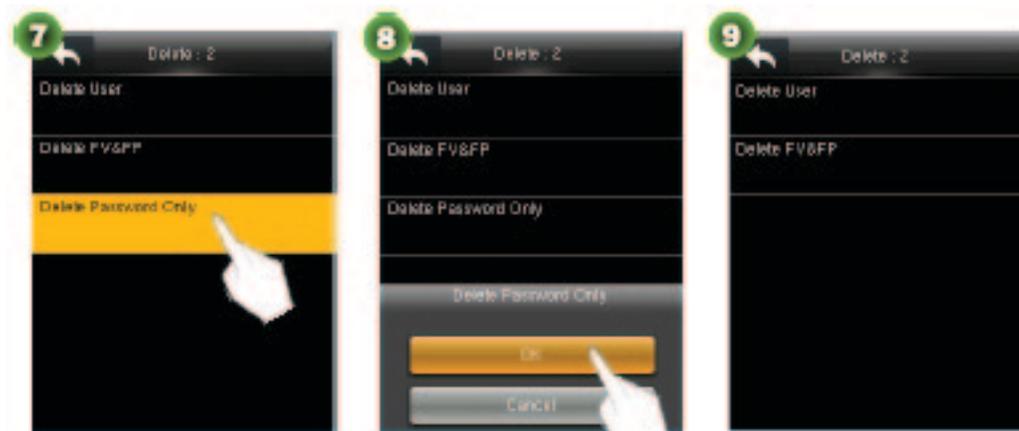
1. De clic en Borrar (**imagen 5**) entre en la interfaz como se muestra en la **Imagen 6**. Los artículos de las operaciones se muestran de acuerdo con la información registrada.

**Ejemplo:** Si la contraseña del usuario no está registrada, el objeto **Solo Borrar Contraseña** no se muestra.



Los siguientes son usos de Solo Eliminar Contraseña como un ejemplo. La operación es descrita como sigue:

2. Dar clic en Solo Eliminar Contraseña (ver **imagen 7**) y aparecerá un cuadro de diálogo en la pantalla (ver **imagen 8**).



3. Dar clic en **OK** para borrar toda la contraseña o dar clic en **Cancelar** para cancelar la operación.

#### Notas:

- ① Cuando se borra un usuario, el dispositivo borra toda la información del usuario, incluyendo la vena y la huella digital★, contraseña y tarjeta ★.
- ② Cuando borra solo un privilegio de usuario, el dispositivo cambia el privilegio de usuario a Usuario Normal.
- ③ Después el privilegio del último super administrador es borrado, todas las funciones definidas por el usuario se convierten en no disponibles.

### 3.3 Estilo de Pantalla

1. En la interfaz **Gestión de Usuarios**, dar clic en **Estilo de Pantalla** para entrar en la interfaz **Estilo de Pantalla** como se muestra en la **Imagen 2**.

**Tips:** El estilo de la pantalla por defecto es **Línea Sola**.



2. En la interfaz **Estilo de Pantalla**, usted puede seleccionar **Línea Sola**, **Línea Múltiple** o **Línea Mixta** para la pantalla de información de usuario.



## 4. Privilegio de Usuario

Usted puede definir los privilegios y asignar niveles de operación a privilegios en **Privilegio de Usuario**.



Las funciones definidas por el usuario se establecen como sigue:

En la lista **Privilegio de Usuario**, seleccione un privilegio a editar (ver **Imagen 3**) para entrar a la interfaz **Privilegio Definido por Usuario** (ver **imagen 4**).

**Nota:** Las funciones definidas por usuario pueden ser añadidas solo después del super administrador. De otra manera, aparecerá un cuadro de diálogo como se muestra en la **Imagen 5**.

- **Habilitar Privilegio Definido**

El valor por defecto es  OFF indica que la función está deshabilitada. De clic y arrastre el ícono para cambiar  ON y  OFF éste icono  ON significa que la función está activada.

- **Nombre**

Establezca un nombre para el privilegio. De clic en **Nombre** para entrar a la interfaz **Nombre** (ver **imagen 7**). Ingrese un nombre utilizando el método de entrada T9 y haga clic en **OK** (ver **imagen 8**) para salvar la configuración y regresar a la interfaz previa (ver **imagen 9**).

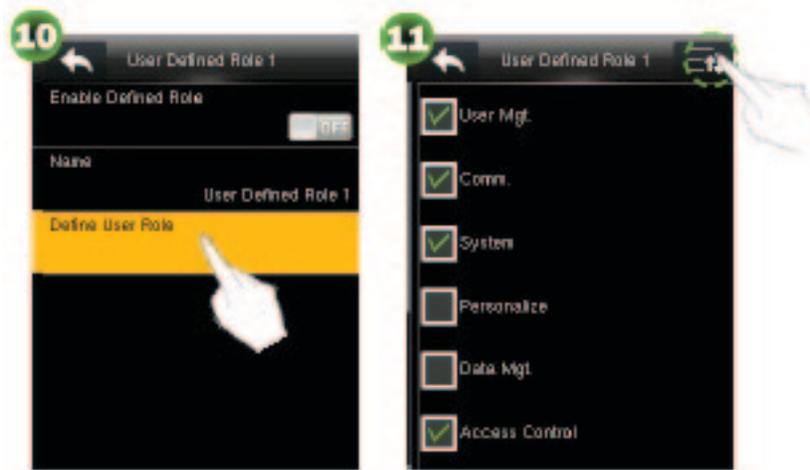
Para detalles acerca de como ingresar un nombre, ver Apéndice 1 Instrucción de la Operación de Entrada de Texto.



## ● Definir Privilegio de Usuario

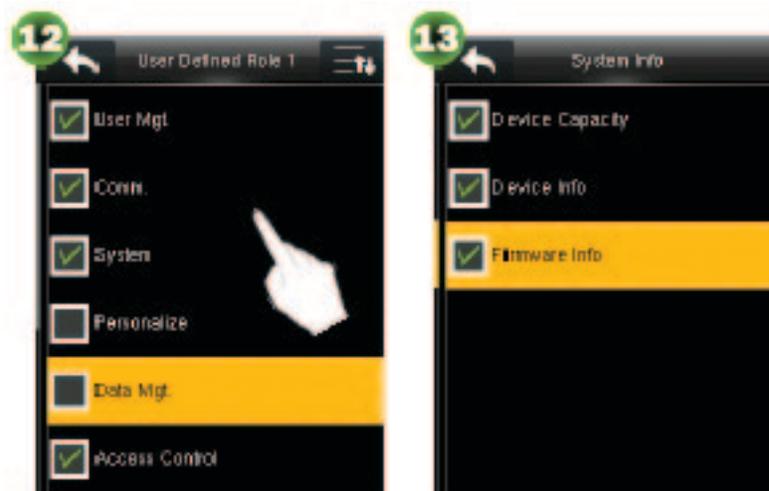
Para asignar el nivel de operación para un privilegio, siga los siguientes pasos:

1. Haga clic en **Definir Privilegio de Usuario** para entrar a la interfaz como se muestra en la **Imagen 11**, de clic en  para deslizarse hacia debajo de la pantalla para ver el contenido.



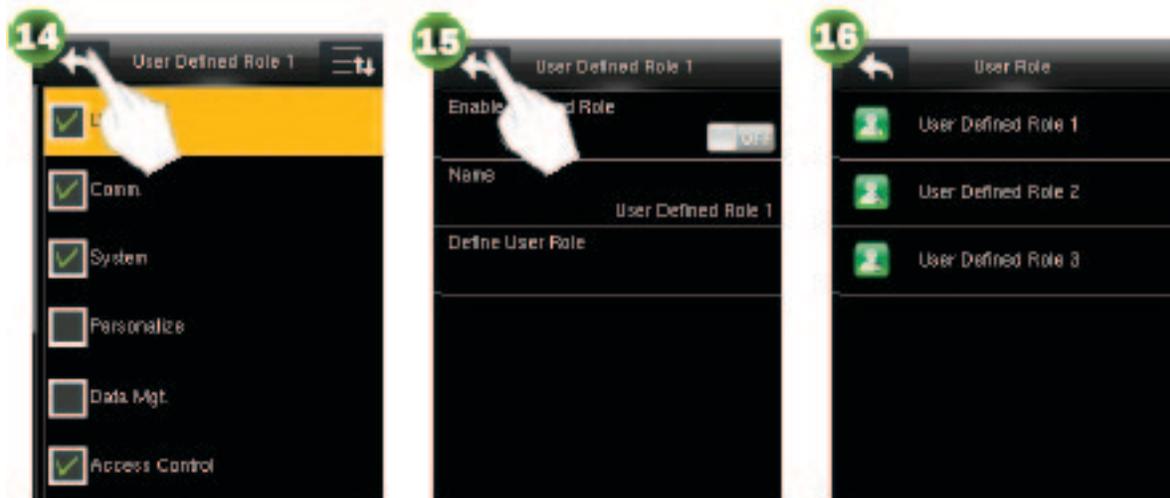
2. Asignar nivel de operación para el privilegio (el símbolo  indica la opción seleccionada).

**Tips:** Haga clic en un nivel primario (ver **imagen 12**) para entrar a la interfaz de selección de nivel (ver **imagen 13**).



3. Después configurar, haga clic en  (ver **imagen 14**) guardar la configuración y regresar a la interfaz **Definir Privilegio de Usuario**.

4. En la interfaz **Definir Privilegio de Usuario**, haga clic en  (ver **imagen 15**) guarde la configuración y regrese a la interfaz **Privilegio de Usuario**.



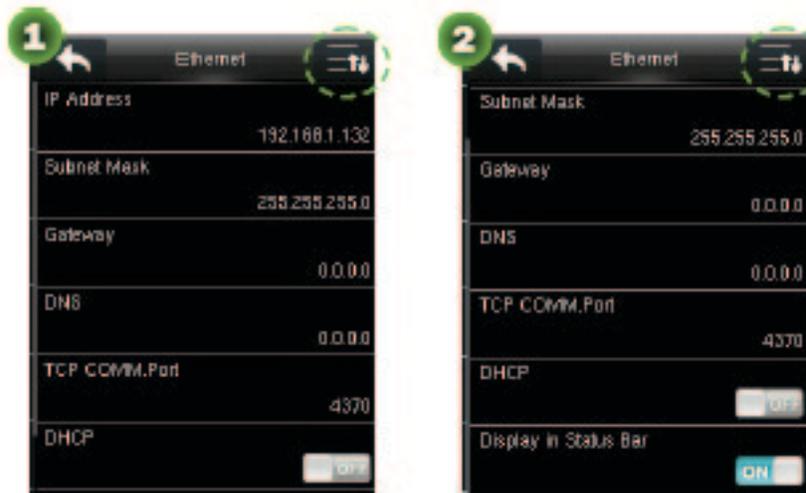
## 5. Configuración de Comunicación



Establezca los parámetros para la comunicación entre el dispositivo y una PC, incluyendo la dirección IP, puerta de entrada, máscara subred, velocidad de transmisión, número de dispositivo y contraseña de conexión.

### 5.1 Configuración de Ethernet

En la interfaz **Conn.**, haga clic en **Ethernet** para entrar a la interfaz **Ethernet**, y haga clic en  para deslizarse debajo de la pantalla para ver el contenido. (**Nota:** Usted puede dar clic en  de nuevo para deslizarse hacia arriba de la pantalla).



Los parámetros que se muestran abajo son los valores por defecto, por favor ajústelos de acuerdo a la situación actual de la red.

**Dirección IP:** 192.168.1.201

**Máscara Subred:** 255.255.255.0

**Puerta de Entrada:** 0.0.0.0

**DNS:** 0.0.0.0

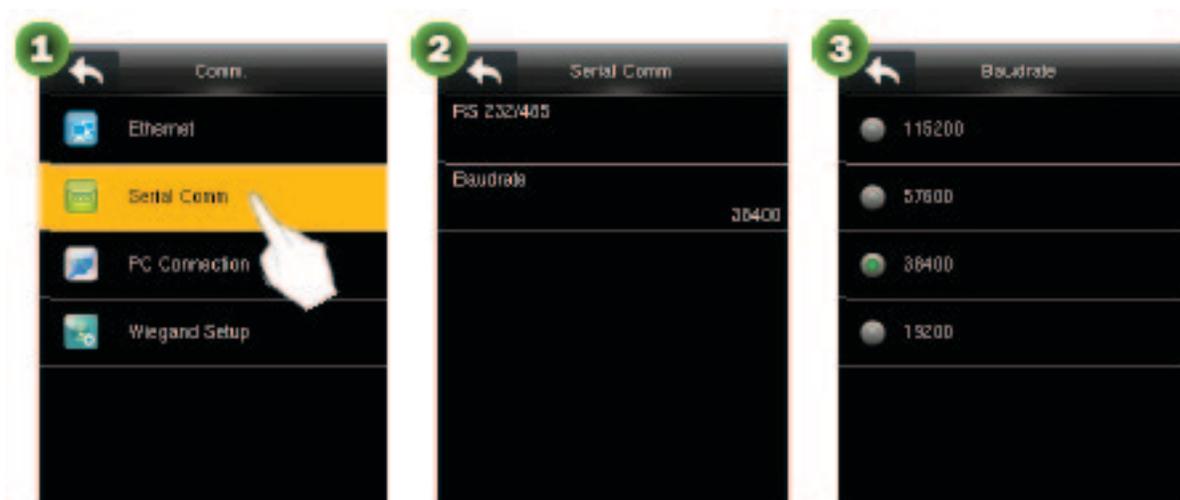
**Puerto TCP Comn:** 4370

**DHCP:** La dirección IP es asignada dinámicamente para clientes vía servidor.

**Pantalla en la Barra de Estado:** Para establecer si se muestra el ícono de red en la barra de estado.

## 5.2 Configuración de Comunicación Serial

Hacer clic en **Comunicación Serial** para entrar a la interfaz.



Cuando el dispositivo se comunica con una PC en modo serial, compruebe las siguientes configuraciones.

**RS232/485:** si habilita RS485 para comunicación. El valor por defecto es  OFF y  ON para cambiar entre  OFF y  ON

**Velocidad de transferencia:** La velocidad para la comunicación con PC; hay 5 opciones para la velocidad de transferencia: 115200 (por defecto), 57600, 38400 y 19200. Cuanto mayor es la velocidad de transferencia, es más rápida la comunicación, pero también la menos segura. En general, una mayor velocidad de transferencia puede ser usada cuando la distancia de comunicación es más corta; cuando la distancia de comunicación es más larga, puede seleccionar una velocidad de transferencia menor para que sea más segura.

### 5.3 Conexión a PC

Para mejorar la seguridad de datos, necesita establecer **Llave de Comunicación** para la comunicación entre el dispositivo y PC. Si una **Clave de comunicación** es establecida en el dispositivo, la contraseña correcta de conexión necesita ser ingresada cuando el dispositivo esté conectado con el software y la PC, así el dispositivo y el software podrán comunicarse.



- **Configuración de Clave de Comunicación**

**Clave de Comunicación:** La clave por defecto es 0 (no contraseña). Entrar a la interfaz **Clave de Comunicación**, ingrese la contraseña, haga clic en OK (Imagen 3) guarde la configuración y regrese a la interfaz **Conexión PC**.

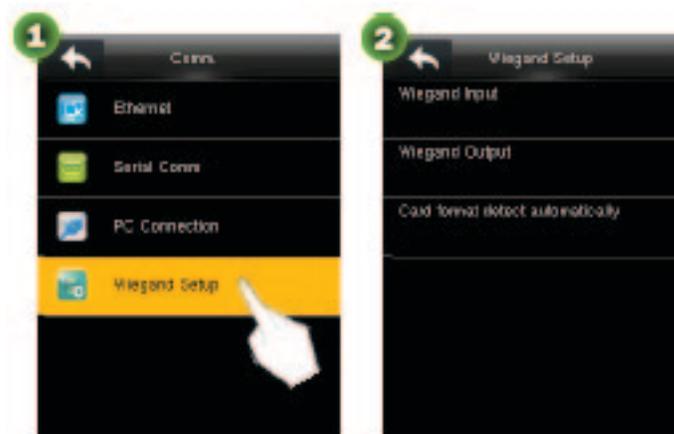
**Nota:** La Clave de Comunicación puede tener de 1-6 dígitos y rangos de 0-999999.

- **Configuración de ID de Dispositivo**

Establezca la ID del dispositivo. El valor por defecto es 1. Hacer clic en **ID de Dispositivo** para entrar en la interfaz, ingresar el ID y hacer clic en **OK** (ver imagen4) para salvar la configuración y regrese a la interfaz **Conexión PC**.

**Nota:** El número de identidad del dispositivo tiene un rango de 1 a 254. Para la comunicación serial RS235, el número de identidad del dispositivo necesita ser introducido en la interfaz de comunicación del software.

## 5.4 Configuración Wiegand



### 5.4.1 Entrada Wiegand

Establezca el formato de Wiegand del lector conectado externamente.



**Formato Wiegand:** El usuario puede escoger entre los formatos Wiegand integrados: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a y Wiegand 50.

**No usar.** El valor no usado con este número de bits no es usado. La tabla siguiente describe todos los formatos.

**Ancho de Pulso (us):** La amplitud del pulso enviado por Wiegand. El valor por defecto es de 100 microsegundos, la cual puede ser ajustada dentro del rango de 20 a 100 microsegundos.

**Intervalo de Pulso (us):** EL valor por defecto es de 1000 microsegundos , el cual puede ser ajustado dentro del rango de 200 a 20000 microsegundos.

**Tipo de ID:** El contenido de entrada incluido en la señal de entrada Wiegand. La ID de Usuario o Tarjeta Numérica puede ser elegida.

## Definiciones de Formatos Wiegand:

Formato Wiegand	Definición
Wiegand 26	ECCCCCCCCCCCCCCCCCCCCCO Consiste de 26 bits en código binario. El 1° bit es el bit de paridad par del 2° bit al 13° bit, mientras que el 26° bit es el bit de paridad impar del 14° al 25° bit. Del 2° al 25° bit son el número de tarjeta.
Wiegand 26a	ESSSSSSSCCCCCCCCCCCCCCO Consiste de 26 bits en código binario. El 1° bit es del bit de paridad par del 2° al 13° bit, mientras el 26° bit es el bit de paridad impar del 14° al 25° bit. Del 2° bit al 9° bit son el código de serie, mientras que del 10° al 25° bit son el número de tarjeta.
Wiegand 34	ECCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits en código binario. El 1° bit es el bit de paridad del 2° al 17° bit, mientras que el 34° bit es impar del 18° al 33° bit. Del 2° al 25° bit son el número de tarjeta.
Wiegand 34a	ESSSSSSSCCCCCCCCCCCCCCCCCCO Consiste de 34 bits en código binario. El 1° bit es el bit de paridad par del 2° al 17° bit, mientras el 34° bit es el bit de paridad impar del 18° al 33° bit. Del 2° al 9° bit es el código de serie, mientras del 10° al 25° bit son el número de tarjeta.
Wiegand 36	OFFFFFFFFFCCCCCCCCCCCCMME Consiste de 36 bits en código binario. El 1° bit es el bit de paridad impar del 2° al 18° bit, mientras el 36° bit es el bit de paridad par del 19° al 35° bit. Del 2° al 17° bit son el código del dispositivo, del 18° al 33° bit son el número de tarjeta y el 34° y 35° bit son el código del fabricante.
Wiegand 36a	EFFFFFFFFFCCCCCCCCCCCCCO Consiste de 36 bits en código binario. El 1° bit es el bit de paridad par del 2° al 18° bit, mientras que el 36° bit es el bit de paridad impar del 19° al 35° bit. Del 2° al 19° bit son el código del dispositivo y del 20° al 35° bit con el número de tarjeta.
Wiegand 37	OMMMSSSSSSSSSSSCCCCCCCCCCCCCCE Consiste de 37 bits en código binario. El 1° bit es el bit de paridad impar del 2° al 18° bit, mientras el 37° bit es el bit de paridad par del 19° al 36° bit. Del 2° al 4° bit son el código del fabricante, del 5° al 16° bit es el código de sitio y del 21° al 36° son el número de tarjeta.
Wiegand 37a	EMMMFFFFFFFSSSSSCCCCCCCCCCCCCCO Consiste de 37 bits en código binario. El 1° bit es el bit de paridad par del 2° al 18° bit, mientras el 37° bit es el bit de paridad impar del 19° al 35° bit. Del 2° al 4° bit es el código del fabricante, del 5° al 14° bit son el código del dispositivo, del 15° al 20° bit son el código del sitio y el 21° al 36° bit son el número de tarjeta.
Wiegand 50	ESSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCO Consiste de 50 bits en código binario. El 1° bit es el bit de paridad par del 2° al 25° bit, mientras el 50° bit es el bit de paridad impar del 26° al 49° bit. Del 2° al 17° bit son el código de sitio y del 18° al 49° bit son el número de tarjeta.

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

### 5.4.2 Salida Wiegand



**Formato Wiegand:** El usuario puede seleccionar el formato de Wiegand estándar incluidos en el sistema. Vea las definiciones de todos los tipos de los formatos Wiegand en 5.4.1 Entrada Wiegand. Soporta múltiples opciones, pero el formato actual es el determinado de los Bits de Salida Wiegand.

**Bits de Salida Wiegand:** El número de datos de bits Wiegand. Después de elegir **[Bits de Salida Wiegand]**, el dispositivo usará el número de serie de bits para encontrar el formato Wiegand adecuado en **[Formato Wiegand]**.

Por ejemplo, si seleccionamos 26-bit Wiegand26, 34-bit Wiegand34a, 36-bit Wiegand36, 37-bit Wiegand37a y 50-bit Wiegand50 pero los bits de salida Wiegand tienen un número de serie de 36, el Wiegand36 36-bit es asumido.

**ID Fallido:** Es definido como el valor de salida de la verificación fallida del usuario. El formato de salida depende de la configuración **[Formato Wiegand]**. El valor por defecto tiene rangos de 0 a 65535.

**Código de Sitio:** Es similar al ID del dispositivo a excepción de que tiene que ser ingresado manualmente y repetible con diferentes dispositivos. El valor por defecto tiene rangos de 0 a 256.

**Ancho de Pulso (us):** La amplitud del pulso enviado por Wiegand. El valor por defecto es de 100 microsegundos, la cual puede ser ajustada dentro del rango de 20 a 100 microsegundos.

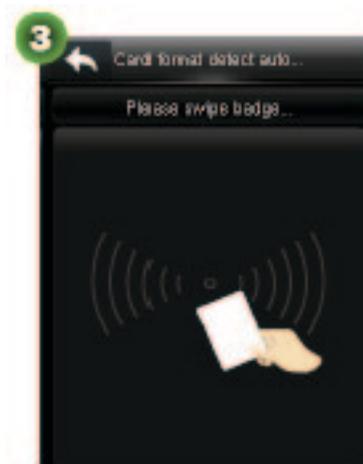
**Intervalo de Pulso (us):** EL valor por defecto es de 1000 microsegundos, el cual puede ser ajustado dentro del rango de 200 a 20000 microsegundos.

**Tipo de ID:** El contenido de entrada incluido en la señal de entrada Wiegand. La ID de Usuario o Tarjeta Numérica puede ser elegida.

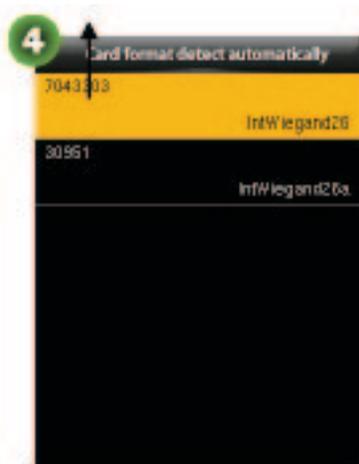
### 5.4.3 Formato de Tarjeta para Detección Automática

[Formato de Tarjeta para Detección Automática] con el propósito de usar asistencia con el detector de tarjeta y con el formato correspondiente. Varios formatos de tarjeta son preestablecidos en el dispositivo. Después de que desliza la tarjeta, el sistema deberá detectarla como número de tarjeta diferente de acuerdo a cada formato; el usuario solo requiere elegir la opción equivalente al número actual de tarjeta y establecer el formato así como el formato Wiegand para el dispositivo. Ésta función es aplicable al lector de tarjeta y al lector auxiliar Wiegand.

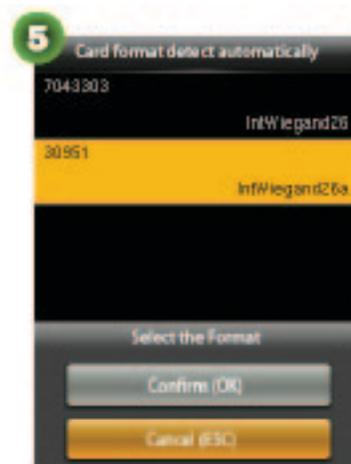
Número de tarjeta obtenido basado en el formato de análisis IntWiegand26



Después de entrar a la detección automática, deslizar la tarjeta en el área indicada (en este dispositivo o lector).



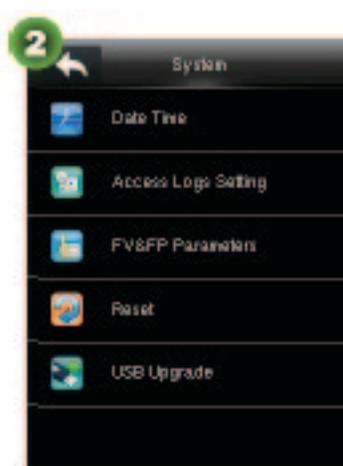
El formato Wiegand y el número de tarjeta preestablecido será detectado automáticamente.



Seleccione el número consistente con el número de tarjeta actual y el formato correspondiente es el formato Wiegand el cual se debe seleccionar para la lectura de este tipo de tarjeta.

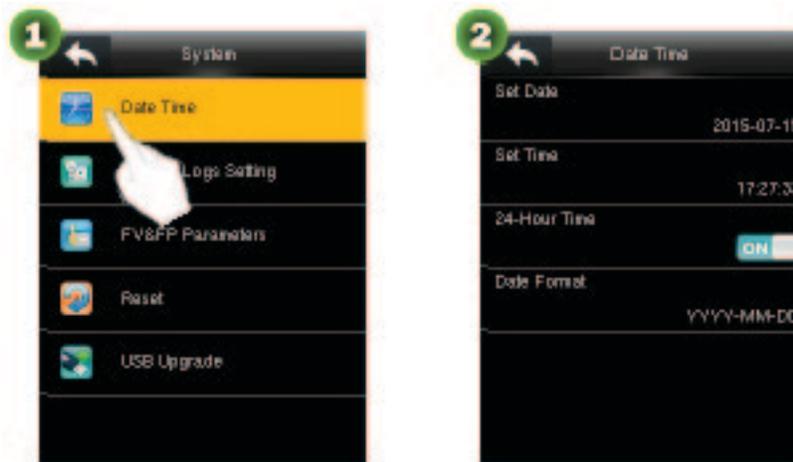
## 6. Configuración del Sistema

Establecer los parámetros del sistema, incluyendo fecha y hora, registro de acceso ★, parámetros de registro de vena, configuración de restauración de fábrica y actualización de USB, así éste dispositivo cumple con las necesidades de usuario a las funciones de máximo alcance y pantalla.



## 6.1 Configuración de Fecha/Hora

Establezca la fecha y la hora en el dispositivo

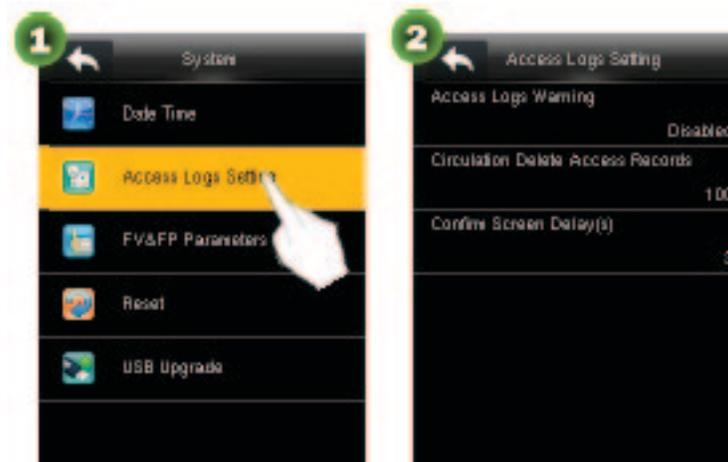


**Fecha y Hora:** Establezca la fecha y la hora en el dispositivo.

**Hora 24-Horas:** Establezca un formato de visualización para la hora en la interfaz principal. Seleccione ON para que la hora se visualice en sistema de 24-horas o seleccione OFF para que la hora se visualice en sistema de 12-horas.

**Formato de Fecha:** Establezca el formato de fecha que se muestra en todas las interfaces del dispositivo.

## 6.2 Configuración de Registros de Acceso ★



**Acceso a Registros de Advertencia:** Cuando la capacidad de registro excedente es menor que el valor preestablecido, el dispositivo automáticamente generará un mensaje indicando la capacidad del registro restante. Usted puede establecer Deshabilitado o establecer un valor que va de 1 a 999.

**Borrar Registros de Acceso:** Establezca el número de entradas de registro y puede ser borrado en el momento en el que existan registros y excedan la capacidad de número de entradas. El valor por defecto es Deshabilitado. Usted puede establecer un valor que va de 1 a 999.

**Confirmar Retardos de Pantalla:** Establecer la duración para mostrar el mensaje de verificación de resultados. El valor válido es de 1-9.

### 6.3 Configuración de Parámetros FV&FP★



**1:1 Verificación del Umbral:** Establecer el similar entre la imagen de vena actualmente registrada y la imagen de registro en el dispositivo en el modo de verificación 1:1. El valor por defecto es 60 y puede establecer un valor de 55 a 75. Cuando el alcance es similar al nivel establecido, la verificación es correcta. Cuanto mayor es el umbral, menor es el rango de error y más alto es el rechazo y viceversa.

**1:N Verificación del Umbral:** Establecer el similar entre la imagen de vena actualmente registrada y la imagen de registro en el dispositivo en el modo de verificación 1:N. El valor por defecto es 70 y puede establecer un valor de 65 a 85. Cuando el alcance es similar al nivel establecido, la verificación es correcta. Cuanto mayor es el umbral, menor es el rango de error y más alto es el rechazo y viceversa.

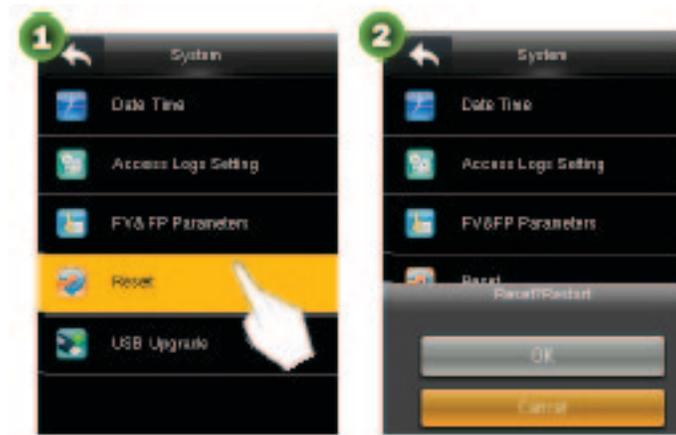
#### Verificación del Umbral Recomendada:

Tasa de Rechazo	Rango de Error	Verificación del Umbral	
		1:N	1:1
Alto	Alto	85	75
Medio	Medio	70	60
Bajo	Alto	65	55

**Modo FV&FP:** La verificación es correcta cuando ambas, la vena y la huella digital, tienen la verificación correcta.

## 6.4 Restablecer a Configuración de Fábrica

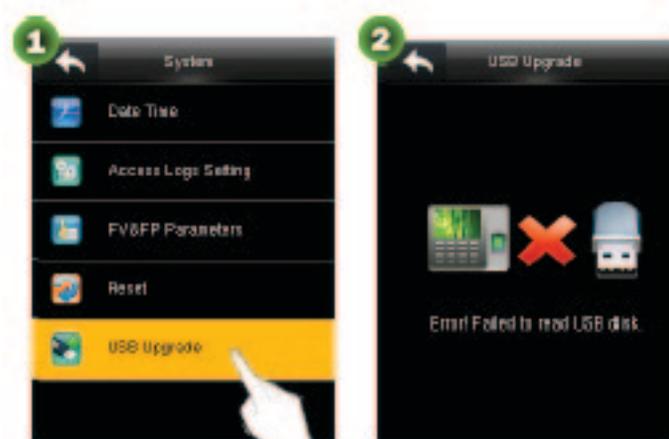
Restaurar datos como son la configuración de comunicación y configuración del sistema a configuración de fábrica.



**Nota:** Después de restaurar, la información del usuario en el dispositivo y en la interfaz de configuración de acceso no se elimina.

## 6.5 Actualización USB

Esta función permite la actualización del firmware con un archivo de actualización en una USB. Inserte una USB en el puerto USB y de clic en **Actualización USB** y actualice el firmware.



## Nota:

- ① Si no es insertada la USB, aparecerá un mensaje en la pantalla como se muestra en la **Imagen 2**.
- ② Si un archivo necesita una actualización, por favor póngase en contacto con nuestro soporte técnico. La actualización de Firmware no es recomendada bajo circunstancias normales.

## 7. Configuración Personalizada



### 7.1 Configurar Interface de Usuario

Usted puede configurar el estilo de pantalla en la interfaz principal.

En la interfaz **Personalizar**, haga clic en **Interfaz de Usuario** para entrar a la interfaz y hacer clic en  para deslizar en la pantalla para ver el contenido. (Nota: Puede hacer clic en  para deslizar hacia arriba de la pantalla.)



- **Protector de Pantalla**

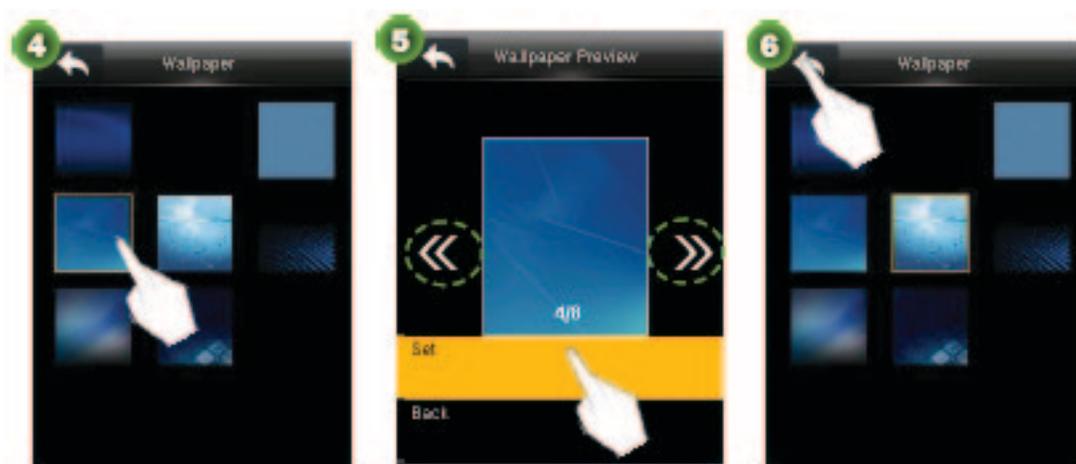
Seleccionar el protector de pantalla de la pantalla principal según sea necesario, usted puede encontrar varios estilos de protector de pantalla en el dispositivo. Las indicaciones detalladas son las siguientes:

1. Haga clic en **Protector de Pantalla**

2. De clic en una imagen (**Imagen 4**) para entrar en la interfaz de **Vista Previa de Protector de Pantalla**.

3. Ocho protectores de pantalla están almacenadas en el dispositivo. Seleccione una, haga clic  y después de clic en **Establecer** (**Imagen 5**). Después configure el dispositivo y regrese a la interfaz Protector de Pantalla.

De clic  (**Imagen 6**) para salvar la configuración y regrese a la **Interfaz de Usuario**.



- **Idioma:** Seleccione el idioma requerido para el dispositivo.

- **Menú Pantalla en Tiempo de Espera**

Cuando no se está realizando alguna operación en la interfaz del menú y el tiempo excede el valor establecido, el dispositivo automáticamente saldrá a la interfaz inicial. Usted puede deshabilitarlo o establecer el valor de 60-99999 segundos.

- **Tiempo de Inactividad en la Pantalla**

Cuándo no se está realizando alguna operación en la interfaz inicial y el tiempo excede el valor establecido, una serie de diapositivas se mostrará. Puede deshabilitarlo (establecer "Ninguno") o establecerlo de 3-999 segundos.

- **Intervalos de Diapositivas**

Se refiere al intervalo de mostrar las diferentes diapositivas. Puede deshabilitarlo o establecer un valor de 3-999 segundos.

- **Tiempo de Inactividad para el Apagado de Pantalla**

Cuándo no se está realizando alguna operación en el dispositivo y se establece el apagado de pantalla, el dispositivo entrará al modo standby. Presione cualquier tecla o dedo para cancelar éste modo. Usted puede deshabilitar esta función o establecer el valor de 1-999 minutos. Si se recurre a ésta función [Deshabilitado], el dispositivo no entrará en modo standby.

- **Menú Estilo de Pantalla**

La operación es detallada a continuación:

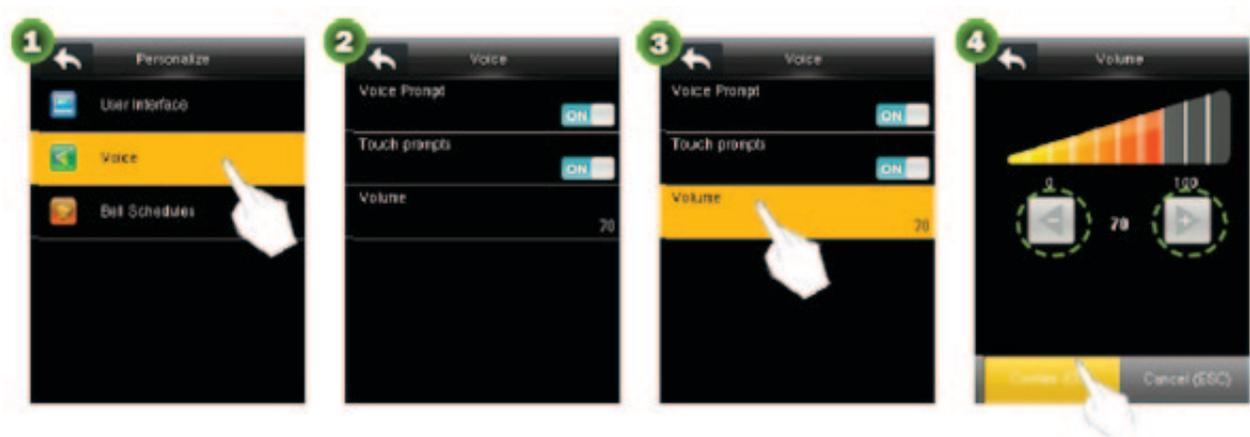
1. De clic en **Menú Estilo de Pantalla** para entrar a la configuración de la interfaz.

2. Haga clic en  para deslizarse y seleccionar el estilo, de clic en establecer (Imagen 8). Después configure, el dispositivo retornará a la interfaz **Protector de Pantalla**.



## 7.2 Configuración de Voz

De clic en **Voz** para entrar a la interfaz.



**Consola de Voz:** Seleccione si desea activar los mensajes de voz durante la operación. El valor por defecto es **ON**, indica que el mensaje de voz está habilitado. Usted puede dar clic para deslizar entre **ON** y **OFF**. El ícono **OFF** indica que el mensaje de voz está deshabilitado.

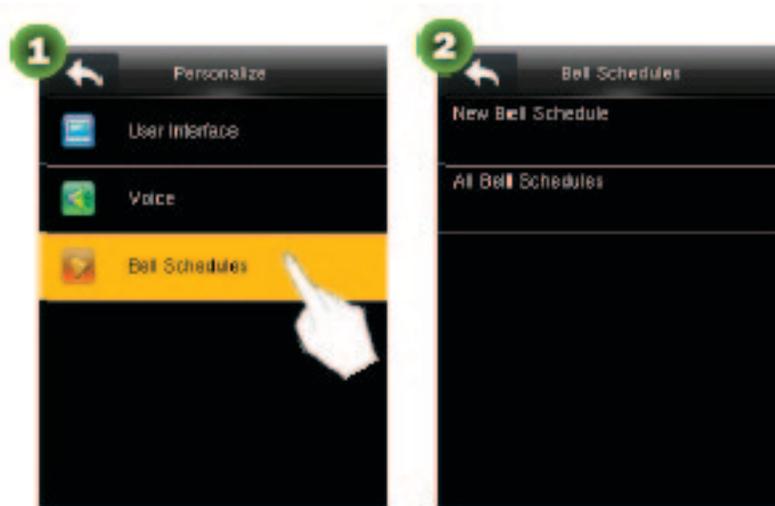
**Consola de Teclado:** Seleccione si desea activar la voz de teclado mientras presiona el teclado. El valor por defecto es **ON**, indica que la consola de voz está habilitada. Usted puede dar clic para deslizar entre **ON** y **OFF**. El ícono **OFF** indica que el mensaje de voz está deshabilitado.

**Volumen:** Establezca el volumen del dispositivo. El valor por defecto es 70. Haga clic en **Volumen** para entrar a la interfaz. De clic en **</>** para subir/bajar el volumen, después de clic en **Confirmar (OK)** (ver **Imagen 4**) para guardar los cambios y regrese a la interfaz de Voz.

### 7.3 Configuración de Sirena

Algunas empresas prefieren usar los timbres para simbolizar en servicio y fuera de servicio. Al llegar a la hora programada para el timbre, el dispositivo sonará con el tono seleccionado automáticamente hasta que la duración de éste pase.

De clic en **Tiempos de Sirena** para entrar a la interfaz.



#### 7.3.1 Nuevo Tiempo de Sirena

1. De clic en **Nuevo Tiempo de Sirena** para entrar en la interfaz (ver **Imagen 4**).



2. Usted puede establecer los parámetros que necesita. El detalle de la operación es como sigue:

- **Estado de Sirena**

Por defecto el valor es , indica que la sirena está deshabilitada. De clic para deslizar entre  y . El icono  indica que la sirena está habilitada.

**Nota:** El horario es efectivo solo si el estado de la sirena se establece en .

- **Tiempo de la Sirena**

Establezca la hora de inicio para la sirena.

De clic en Tiempo de Sirena para entrar a la interfaz.

③ Establezca el tiempo de la sirena dando clic en  para incrementar y  disminuir números y de clic en Confirmar (OK) (ver **Imagen 6**) para salvar y regrese a la interfaz **Nuevo Horario de Sirena**.

- **Repetir**

Por defecto el valor es **Nunca**, la cual se usa para que suene una sola vez.

Para repetir el horario de sirena, dar clic en **Repetir** para entrar a la interfaz. Marque una o varias fechas según lo requiera y de clic en  (ver **Imagen 6**) para guardar la configuración y regrese a la interfaz **Nueva Sirena**.

Interfaz de **Horario**: Cuando seleccione las fechas y el tiempo de sirena, se transmiten señales, se activan y se muestra el conjunto de sirena. Cuando la duración de la sirena se prolonga el timbre se detiene automáticamente.

- **Tono de Timbre**

Establezca el tono de timbre para el horario de la sirena.

De clic en **Tono de Timbre** para entrar a la interfaz.

③ En la lista de tonos de timbre, hacer clic a un tono para seleccionarlo y de clic en  (ver **Imagen 8**) para salvar la configuración y regresar a la interfaz **Nuevo Horario de Sirena**.

- **Retardo de Sirena Interna**

Establezca el retraso de la sirena. El valor por defecto es de 5 segundos. Usted puede establecer el valor que va de 1 a 999.



3. Después de configurar, de clic en  en la interfaz Nuevo Horario de Sirena (Imagen 9) para salvar y regresar a la interfaz previa.

### 7.3.2 Todos los Tiempos de Sirena

En la interfaz **Horario de Sirena**, haga clic en **Todos los tiempos de Sirena** y entrar a la interfaz como se muestra en la **Imagen 10**. Usted puede editar/borrar los horarios según sea necesario.

**Nota:** El método de editar/borrar horarios de sirena es lo mismo con la de edición/eliminación de usuarios. Para más detalles, ver 3.2.2 Editar/Borrar un Usuario.

## 8. Gestión de Datos

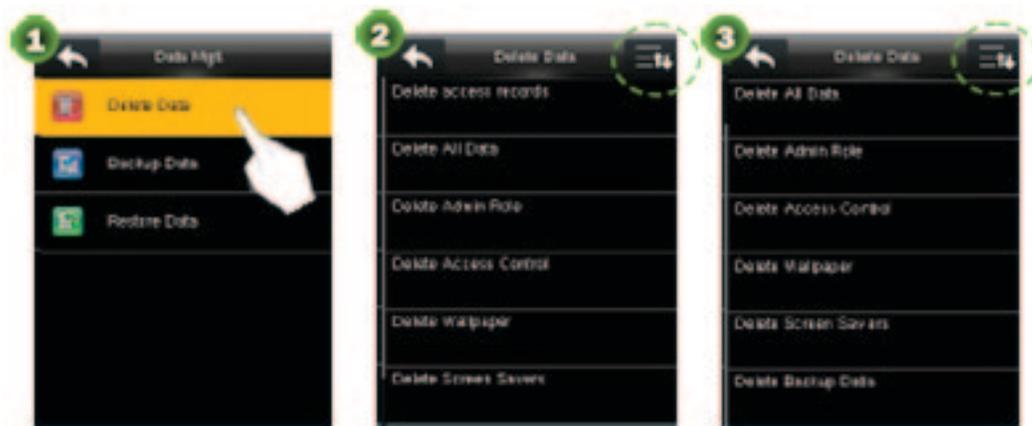
En la interfaz menú principal, de clic en **Gestión de Datos** para entrar a la interfaz.



## 8.1 Borrar Datos

Administrar datos en el dispositivo, que incluye la eliminación de los datos de asistencia, eliminación de todos los datos, eliminación de roles administrativos y eliminación de protectores de pantalla, etc.

Dar clic en **Borrar Datos** para entrar a la interfaz y de clic en  para desplazarse hacia abajo de la pantalla para ver el contenido. (Nota: Puede dar clic en  de nuevo para deslizarse hacia arriba.)

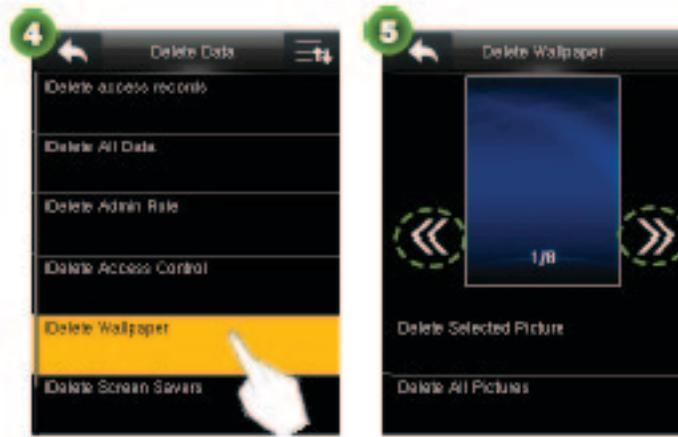


- **Borrar Registros de Acceso★**: Borrar todos los registros de acceso.
- **Borrar Todos los Datos**: Borrar toda la información del usuario, información del registro con vena y registros de asistencia, etc.
- **Borrar Rol de Administración**: Hacer a todos los administradores Usuarios Normales.
- **Borrar Control de Acceso**: Restaurar la configuración de control de acceso así como días festivos, permisos a usuarios, reglas de tiempo, grupos de usuarios, configuración de valores de fábrica. Los registros de acceso no serán borrados.
- **Borrar Fondos de Escritorio**

Borrar fondos de escritorio. La operación específica es como sigue.

1. De clic en **Borrar Fondo de Escritorio**

2. De clic en  para deslizarse y seleccionar un fondo de escritorio y después de clic en **Borrar Imagen Seleccionada** para borrar la imagen seleccionada o de clic en **Borrar Todas la Imágenes** para borrar todas las imágenes.

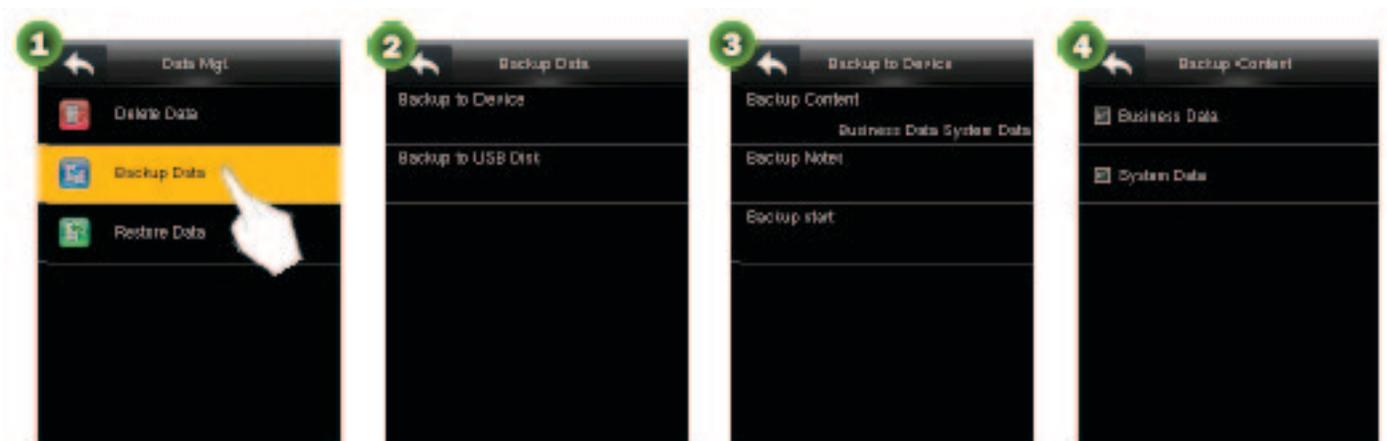


- **Borrar Protectores de Pantalla**

El método para borrar protectores de pantalla es el mismo como la eliminación de fondos de pantalla. (Para detalles acerca de cómo subir protectores de pantalla, ver 10.2 Descargar USB.)

- **Borrar Copia de Seguridad:** Borrar todas las copias de seguridad.

## 8.2 Datos de Copia de Seguridad



- **Copia de Seguridad para Dispositivo**

Usted puede hacer una copia de seguridad de los datos de la empresa o configurar los datos en el dispositivo para la PC local.

1. De clic en **Copia de Seguridad para Dispositivo** para entrar a la interfaz.
2. Usted puede establecer los parámetros que necesite. El detalle de operación es como sigue.

**Contenido de Copia de Seguridad:** De clic en Contenido de Copia de Seguridad para entrar a la interfaz. Seleccione el contenido que quiere respaldar. (Nota: El ícono  indica un elemento elegido.)

**Notas de Copia de Seguridad:** Entrar al contenido de la copia de seguridad. Los detalles del método son como siguen:

De clic en **Notas de Copia de Seguridad** para entrar en la interfaz (ver **Imagen 5**).

① De clic en la pantalla. Aparecerá un teclado. Ingrese la nota usando el método de entrada T9 y después de clic en **OK** (ver **Imagen 6**) para confirmar y regresar a la interfaz **Notas de Copia de Seguridad**.

② De clic en Confirmar (**OK**) (ver **Imagen 7**) para salvar la configuración y regresar a la interfaz **Copia de Seguridad para Dispositivo**.



3. Después de configurar, dar clic en **Inicio de Copia de Seguridad** para empezar a hacer la copia de seguridad del contenido en el dispositivo.

- **Copia de Seguridad para USB**

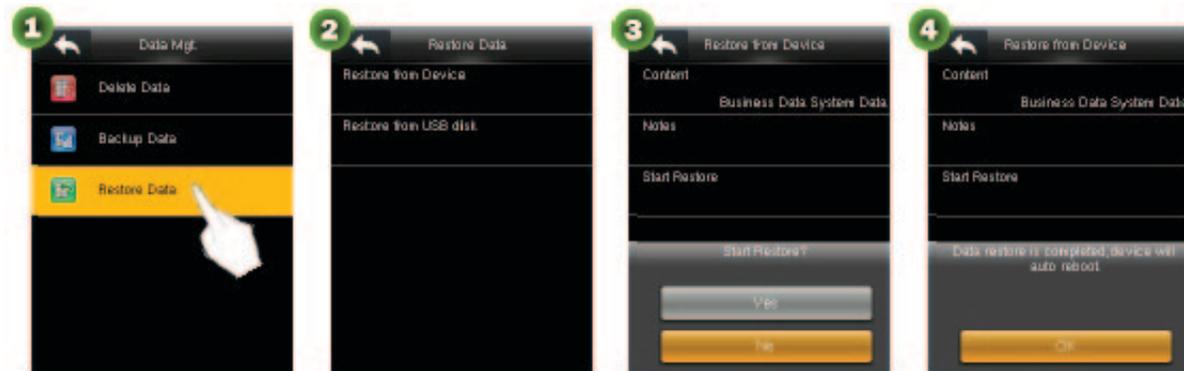
Copia de seguridad de los datos de la empresa o configuración de datos del dispositivo al USB. El método es el mismo que el utilizado en **Copia de Seguridad para Dispositivo**.

**Notas:**

- ① Antes del realizar copias de seguridad al USB, por favor insertar una memoria USB en el puerto USB del dispositivo.
- ② Antes de realizar copias de seguridad a la PC local, el sistema reemplaza la copia de seguridad vieja con una más actualizada.

## 8.3 Restaurar Datos

En la interfaz **Gestión de Datos**, haga clic en **Restaurar Datos** para entrar a la interfaz



- **Restaurar desde el dispositivo**

Restaurar los datos en el dispositivo desde la PC local.

1. Haga clic en Restaurar desde el dispositivo para entrar a la interfaz.
2. Haga clic en Inicio de Copia de Seguridad y aparecerá un cuadro de diálogo (ver Imagen 3). Dar clic en SI para empezar.

**Nota:** Después de la restauración, haga clic en OK para restaurar el dispositivo.

- **Restaurar desde USB**

Restaurar los datos del dispositivo desde una memoria USB. Los detalles de operación son iguales a los de Restaurar desde el dispositivo.

**Nota:** Antes de la restauración de datos desde la memoria USB, inserte el USB que lleva los datos de copia de seguridad en el puerto USB del dispositivo.

## 9. Control de Acceso

La configuración de la función control de acceso es para los períodos de acceso de los usuarios y los parámetros del bloqueo de acceso y el dispositivo relacionado.



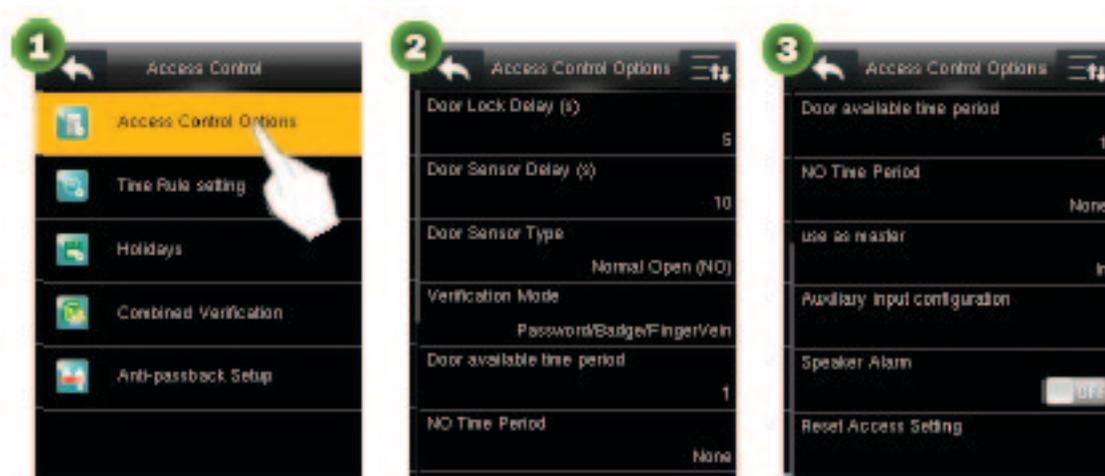
Para poder acceder, el usuario registrado deberá cumplir las siguientes condiciones:

1. El horario de acceso de los usuarios se configura con la zona horaria del personal o zona horaria del grupo.
2. El grupo de usuario debe estar en el combo de acceso (cuando hay otros grupos en el mismo combo de acceso, también se requieren verificaciones de los miembros de esos grupos para abrir la puerta.)

En la configuración predeterminada, los nuevos usuarios se asignan en el primer grupo con la zona horaria del grupo predeterminado y el grupo de acceso como 1, establecer el desbloqueo de estado.

### 9.1 Configuración de las Opciones de Control de Acceso

En la interfaz de **Control de Acceso**, hacer clic en **Configuración de las Opciones de Control de Acceso** para entrar a la interfaz y hacer clic en  para deslizarse hacia abajo de la pantalla para ver el contenido. (Nota: Puede dar clic  de nuevo para deslizarse hacia arriba.)



Establecer los parámetros del control de bloqueo y dispositivos relacionados.

**Retrasos en el Control de Puerta:** El periodo de tiempo de desbloqueo (desde la apertura de la puerta al cerrado automático) después del bloqueo electrónico recibe una señal abierta enviada desde el dispositivo (el rango de valores son desde 0 a 10 segundos).

**Retraso del Sensor de Puerta:** Cuando la puerta es abierta, el sensor de puerta se comprobará después de un periodo de tiempo; si el estado del sensor de puerta es inconsistente con la del modo de sensor de puerta, se activará la alarma. El periodo de tiempo es el Retraso del Sensor de Puerta (el rango de valores son desde 0 a 255 segundos.)

**Tipo de Sensor de Puerta:** Incluye No, Apertura Normal y Cerrado Normal. No significa que el sensor de la puerta no está en uso; Apertura Normal significa que la puerta se abre cuando está conectada a la electricidad; Cerrado Normal significa que la puerta se cierra cuando está conectada a la electricidad.

**Modo de Verificación:** Usted puede seleccionar **Contraseña/Registro de Vena, Solo Tarjeta, Contraseña, Registro de Vena, Contraseña y Registro de Vena, Tarjeta/Huella Digital★ Solo Huella Digital★, Solo Tarjeta★, Huella Digital y Contraseña★, Tarjeta y Contraseña★, Tarjeta y Huella Digital★ o Tarjeta y Huella Digital y Contraseña★** según sea necesario.

**Período de Tiempo de Puerta Disponible:** Establezca los periodos para abrir la puerta para usuarios.

**Utilizar como maestro:** Mientras configura los dispositivos maestros y esclavo, usted puede establecer el estado del maestro como Salida o Entrada.

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

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

**Configuración de Entrada Auxiliar:** Establezca la **Salida Auxiliar/bloquear tiempo abierto** y **Tipo de Salida Auxiliar** para el dispositivo con el conector auxiliar. **Tipo de Salida Auxiliar** incluye **Ninguna, apuntador de puerta abierta, apuntador de alarma y apuntador de puerta abierta y alarma.**

**Altavoz de Alarma:** Cuando el **[Altavoz de Alarma]** está habilitado, el altavoz elevará una alarma cuando el dispositivo esté siendo desmantelado.

**Restablecer Configuración de Acceso:** Restablecer parámetros del retraso de bloqueo de la puerta, retraso de sensor de puerta, tipo de sensor de puerta, retraso de alarma de puerta, repetir alarma, periodo de tiempo NO, configuración de entrada auxiliar, excluyendo los datos de acceso que desea eliminar en **Gestión de Datos.**

Parámetros de Acceso	Predeterminado de Fábrica
Retraso de bloqueo de puerta	10s
Retraso de sensor de puerta	10s
Modo de sensor de puerta	No
Retraso de alarma de puerta	30s
Horario NO	No
Tiempo de acceso para salida auxiliar★	255s

**Observaciones:** Después de configurar **Periodo de Tiempo NC**, por favor bloquear así la puerta, de otra manera la alarma podría ser activada durante el **Periodo de Tiempo NC.**

## 9.2 Configuración de Hora

La configuración del tiempo es la unidad mínima del control de acceso; se pueden establecer máximo 50 horarios para el sistema. Cada configuración de tiempo consiste en 7 secciones de tiempo (una semana) y cada tiempo es el tiempo válido dentro de 24hrs.

Usted puede establecer máximo 3 periodos para cada regla de tiempo. La relación entre este periodo es "o". Cuando la verificación del tiempo cae en cualquiera de éstos periodos, la verificación es válida. El formato del periodo es HH:MM:-HH:MM en sistema de 24hrs. con precisión para segundos.

En la interfaz **Control de Acceso**, dar clic en **Configuración de Reglas de Tiempo** para entrar a la interfaz y dar clic en  para desplazarse hacia debajo de la pantalla para ver el contenido. (**Nota:** Usted puede dar clic en  nuevamente para desplazarse hacia arriba)



## ● Editar Reglas de Horario

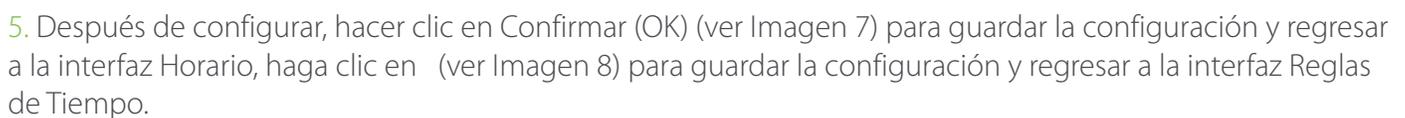
Un super Administrador puede editar las reglas de horario que sean necesarias. Los detalles de operación son como siguen:

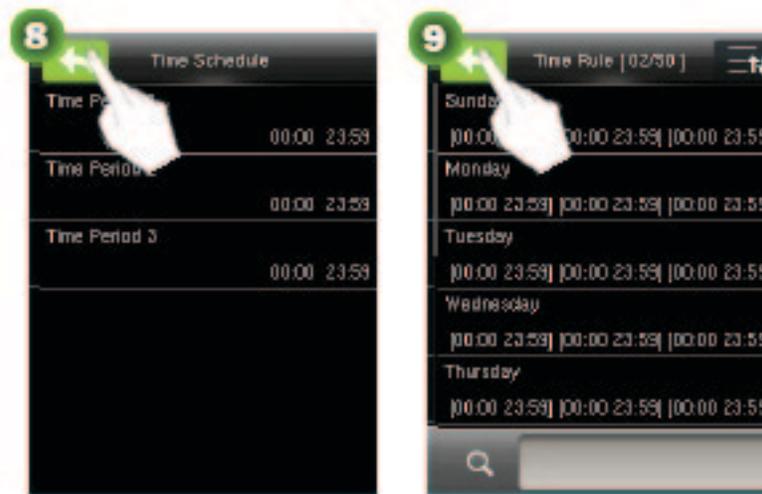
1. Haga clic en el recuadro de búsqueda (ver **Imagen 2**) para entrar a la interfaz.
2. Ingrese un número de regla de horario, de clic en **OK** (ver **Imagen 3**) para entrar a la interfaz (ver Imagen 4).
3. En la lista de periodo de tiempo, hacer clic en un periodo para editarlo (ver **Imagen 5**) para entrar a la interfaz (ver **Imagen 6**).



4. En la lista de horarios, haga clic en Periodo de tiempo 1/2/3 para entrar a la interfaz. Usted puede establecer la hora de inicio y la hora de finalización de un periodo como sea necesario.

**Tips:** De clic en el ícono  para aumentar/disminuir números mientras configura la hora.

5. Después de configurar, hacer clic en Confirmar (OK) (ver Imagen 7) para guardar la configuración y regresar a la interfaz Horario, haga clic en  (ver Imagen 8) para guardar la configuración y regresar a la interfaz Reglas de Tiempo.



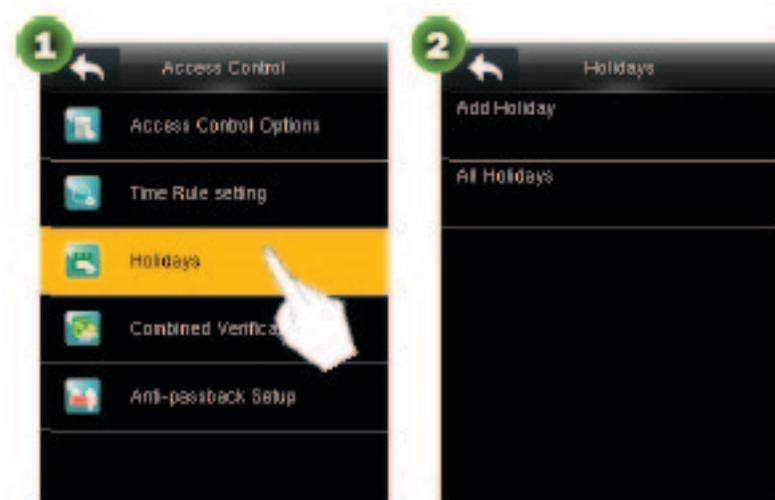
6. Establezca otros periodos de reglas de tiempo. Haga clic en  (ver **Imagen 9**) en la interfaz **Reglas de Tiempo** para guardar la configuración y regresar al nivel superior.

#### Notas:

- ① Cuando la hora de finalización es más temprana que la hora de inicio (por ejemplo, 23:57-23:56), esto significa que todos los días estará cerrado. Cuando la hora de finalización es mas tarde que la hora de inicio (por ejemplo, 00:00-23:59), esto significa que éste intervalo es válido.
- ② **Horario Válido:** 00:00-23:59 (Todo el día valido) o cuando la hora de finalización es mayor que la hora de inicio.
- ③ Por defecto, la regla de tiempo numerada 1 indica abierto día completo.

### 9.3 Configuración de Días Festivos

Añadir por el dispositivo, en control de acceso días festivos y establecer los periodos de tiempo en días festivos según sea necesario. El dispositivo controla el acceso en días festivos de acuerdo a la configuración de estos mismos.



### 9.3.1 Añadir Día Festivo

1. Haga clic en **Añadir Día Festivo** para entrar en la interfaz (ver **Imagen 4**).



2. Establecer parámetros para el día festivo según sea necesario. Los parámetros los puede establecer como sigue:

- **No.**

El dispositivo automáticamente asigna un número al día festivo. De clic en **No.** Para entrar en la interfaz. Ingrese el **No.** del día festivo según sea necesario y de clic en **OK** (ver **Imagen 5**) para guardar la configuración y regresar a la interfaz **Días Festivos**.

- **Fecha**

Establezca la fecha del día festivo.

(1) De clic en **Fecha** para entrar a la interfaz.

(2) Haga clic en ▲ para aumentar un número o ▼ para disminuir un número para establecer la fecha. Después, haga clic en **Confirmar (OK)** (ver **Imagen 6**) para guardar la configuración y regresar a la interfaz **Días Festivos**.

- **Tipo de Día Festivo**

Establecer el tipo del día festivo.

① Haga clic en **Tipo de Día Festivo** para entrar en la interfaz.

② Seleccione el tipo del día festivo y haga clic en + (ver **Imagen 8**) para guardar la configuración y regresar a la interfaz **Días Festivos**.



- **Repetitivo o No**

El valor por defecto es  ON. Usted puede hacer clic en **Repetitivo o No** y elegir entre  ON y  OFF.

Para que los días festivos sean fijos cada año, por ejemplo, Año Nuevo es 1° de Enero, en **Repetitivo o No** puede establecer  ON para estos casos. Para que estos días no sean fijos cada año, por ejemplo, el Día de las Madres es el segundo domingo de Mayo, la fecha específica es incierta y en **Repetitivo o No** puede establecer  OFF para estos casos.

Por ejemplo, cuando la fecha del día festivo se establece el 1° de Enero de 2010 y el tipo de día festivo 1, el control de acceso el 1° de Enero se realizó de acuerdo a la configuración del periodo de tiempo del **día festivo tipo 1** en lugar de la configuración del periodo de tiempo del viernes.

Después de configurar, haga clic en  en la interfaz **Días Festivos** (ver **Imagen 9**) para guardar las configuraciones y regresar a la interfaz superior.

### 9.3.2 Incluir Día Festivo

En la interfaz **Días Festivos** se muestra en la **Imagen 3**, dar clic en **Todos los Días Festivos** para entrar en la interfaz (ver **Imagen 10**). Usted puede editar o eliminar días festivos según sea necesario.

## 9.4 Configuración de Verificación Combinada

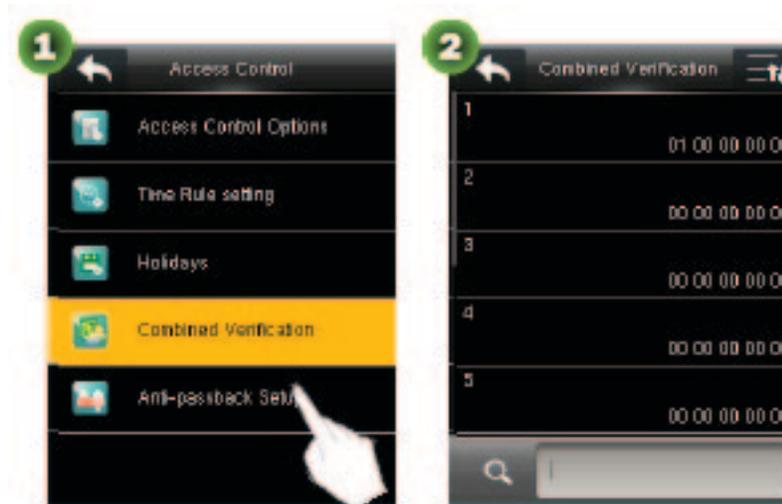
### Notas:

- ① El software Access3.5 no es necesario si el dispositivo es usado por primera vez. Usted puede establecer una verificación combinada directamente en el dispositivo.
- ② Después de que la verificación combinada se encuentra en el software Access3.5 y los ajustes se entregan al dispositivo, el dispositivo solo soporta la configuración de verificación combinada del software Access3.5 y ésta no puede ser establecida en el dispositivo.

Combina dos o más miembros para lograr multi-verificación y mejorar la seguridad.

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

En la interfaz **Control de Acceso**, de clic en **Verificación Combinada** para entrar a la interfaz.

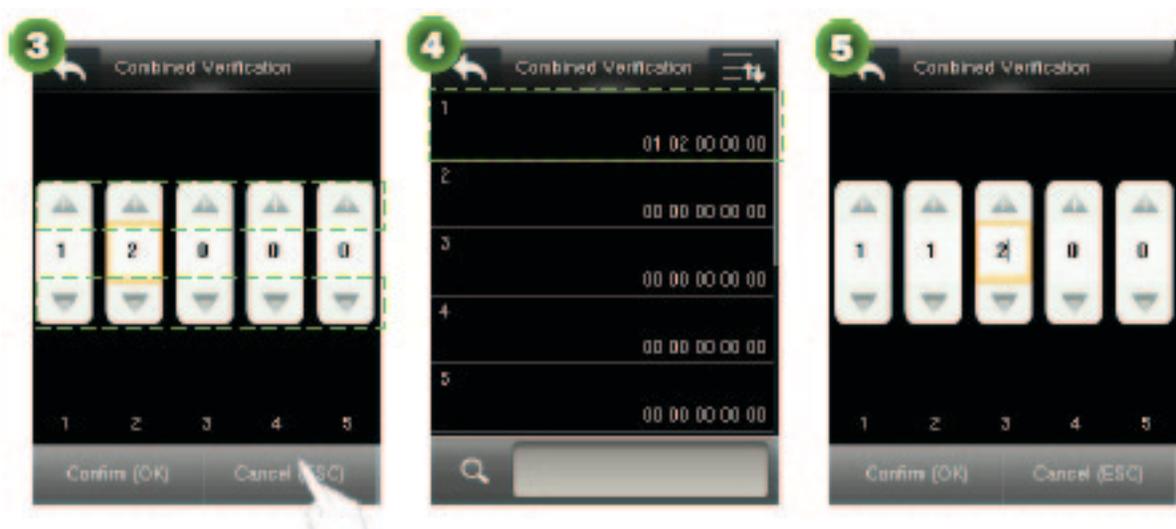


Por defecto, el dispositivo soporta diez combinaciones de desbloqueo. Los usuarios pueden modificar la configuración de la verificación combinada según sea necesario. La operación se especifica a continuación:

Por ejemplo, agregue una combinación de desbloqueo que requiere la verificación simultánea del grupo de usuarios 1 y grupo de usuarios 2.

1. En la interfaz **Verificación Combinada**, haga clic en una combinación que se desea modificar para entrar a la interfaz como se muestra en la **Imagen 3**.

2. Haga clic en ▲ para aumentar un número o haga clic en ▼ para disminuir un número para establecer la ID de un grupo de usuario. Después, haga clic en **Confirmar (OK)** para guardar la configuración y regresar a la interfaz **Verificación Combinada**.



Después de que la configuración es exitosa, una puerta puede abrirse solo después de un usuario en grupo de usuario 1 y un usuario en grupo de usuario 2 pase la verificación.

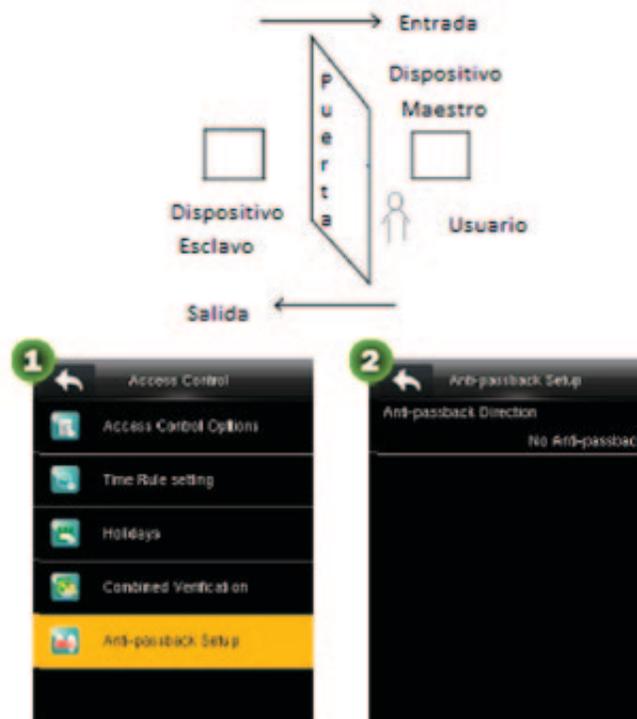
#### Notas:

- ① Una combinación desbloqueo soporta un máximo de cinco grupos de usuarios. Esto es, en una combinación de desbloqueo, una puerta puede abrirse solo después de que un máximo de 5 usuarios pasen la verificación.
- ② Después de que se establece una combinación de desbloqueo como se muestra en la **Imagen 5**, una puerta puede ser abierta solo después de que un usuario en grupo de usuarios 2 y dos usuarios del grupo de usuarios 1 pase la verificación.
- ③ Una combinación de desbloqueo se borra cuando los IDs de los grupos de usuarios en la combinación de desbloqueo se configuran en 0.

### 9.5 Configuración Anti-passback

Para evitar que algunas personas sigan entrando sin verificación, lo que resulta un problema de seguridad, los usuarios pueden configurar la función anti-passback. El registro de entrada debe coincidir con el registro de salida de manera que la puerta se abra.

Esta función requiere dos dispositivos para trabajar juntos: uno se instala por dentro de la puerta (dispositivo maestro) y el otro se instala por fuera de la puerta (dispositivo esclavo). Los dos dispositivos se comunican con señal Wiegand. El formato Wiegand y el tipo de salida (ID de Usuario/Tarjeta) adoptado por el dispositivo maestro y dispositivo esclavo debe ser consistente.



## Dirección Anti-Passback

**No Anti-passback:** La función anti-passback es deshabilitada, esto significa que la verificación pasa ya sea con el dispositivo maestro o con el esclavo esta puede desbloquear la puerta. El estado de la asistencia no es reservada.

**Salida Anti-passback:** Después de que el usuario registra su salida, solamente si el registro pasado es un registro de entrada puede el usuario registrar su salida nuevamente; de otra manera, la alarma se activará. Sin embargo, el usuario podrá entrar libremente.

**Entrada Anti-passback:** Después de que el usuario registra su entrada, solamente si el registro anterior fue un registro de salida puede registrar su entrada nuevamente; de otra manera, la alarma se activará. Sin embargo, el usuario podrá salir libremente.

**Entrada/Salida Anti-passback:** Después de que el usuario registra su entra/sale, solamente si el registro pasado es un registro de salida el usuario puede registrar su entrada nuevamente, o si es un registro de entrada puede registrar su salida nuevamente; de otra manera, la alarma se activará.

## 10. Gestión USB

La información del usuario, plantillas de vena, plantillas de huella digital, datos de verificación y otros datos pueden ser exportados del software mediante una memoria USB y la información del usuario, plantillas de vena y otros datos pueden ser importados del dispositivo usando una memoria USB.

**Observaciones:** Después de subir/descargar los datos del/a la memoria USB, inserte la memoria USB en el puerto USB.



## 10.1 Descargar USB

Descargar los registros de control de acceso★ y datos de usuario del dispositivo a una memoria USB.

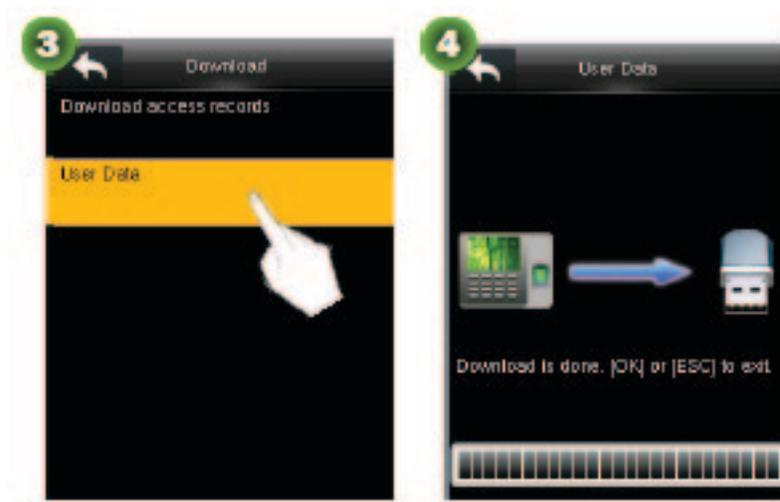
**Descargar registros de acceso★:** Almacene los registros de control de acceso en un rango de fecha específica del dispositivo a una memoria USB.

**Datos de Usuario:** Descargar la información de todos los usuarios y la información del registro de vena del dispositivo a una memoria USB.

Los siguientes pasos muestran la operación de la descarga de los datos de usuario a la memoria USB.

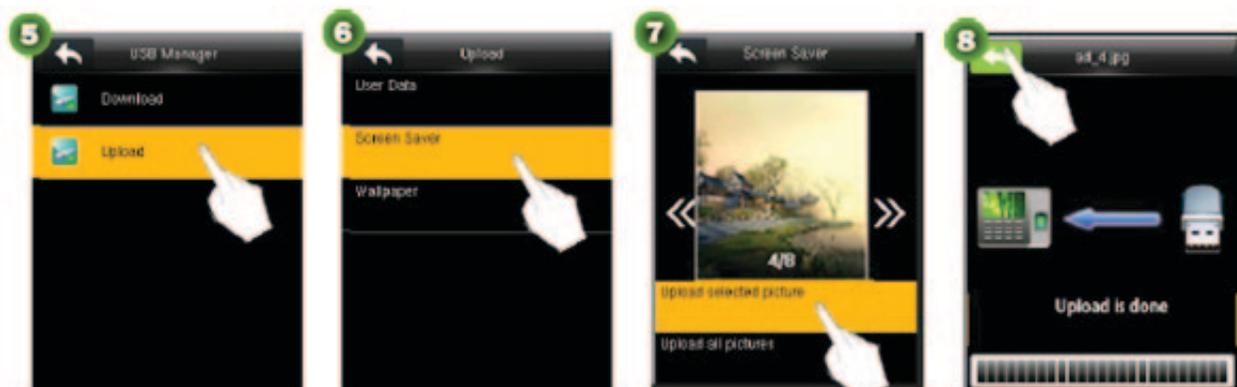
1. Escoja **Descarga>Datos de Usuario** para empezar la descarga de los datos de usuario a la memoria USB. Después de que la descarga es exitosa, aparecerá un cuadro de texto en la pantalla que dirá "Descarga Exitosa" (ver Imagen 4).

2. Remueva la memoria USB y de clic en  para regresar a la interfaz **Descarga**.



## 10.2 Cargar de la USB

Cargar los datos de usuario, protector de pantalla y fondo de pantalla de la memoria USB al dispositivo. Haga clic en **Cargar** para entrar a la interfaz.



- **Datos de Usuario: Cargar toda la información de los usuarios de la memoria USB al dispositivo.**
- **Protector de Pantalla**

Cargar el protector de pantalla de la memoria USB al dispositivo. Después de que el dispositivo entra en modo de espera, la descarga del protector de pantalla aparecerá. La operación se especifica a continuación:

1. Haga clic en **Protector de Pantalla** (ver **Imagen 6**) para entrar a la interfaz.
2. De clic en  para desplazarse y seleccionar un protector de pantalla y de clic en **Cargar Imagen Seleccionada** para cargar la imagen seleccionada al dispositivo o de clic en **Cargar Todas las Imágenes** para cargar todas las imágenes que cumplan con los requisitos de la memoria USB al dispositivo.
3. Después de que la carga es exitosa, aparecerá un cuadro de texto en la pantalla que dirá "Carga Exitosa". Después dar clic en  para regresar a la interfaz superior.

- **Fondo de Pantalla**

Cargar todos los fondos de pantalla de la memoria USB al dispositivo. La operación de este método es la misma al método para cargar los protectores de pantalla por lo que no se describen aquí.

#### Notas:

- ① Después de cargar los protectores de pantalla, puede poner las imágenes cargadas en el folder de publicidad en la memoria USB.
- ② Después de cargar el fondo de pantalla, puede poner las imágenes cargadas en el folder de fondos de pantalla en la memoria USB.
- ③ Las imágenes de protector de pantalla y fondos de pantalla deben estar en formato PNG, JPG o BMP, con un tamaño no más grande que 30KB.
- ④ Los nombres de los protectores de pantalla y fondos de pantalla deben contener no más de 20 caracteres.

## 11. Búsqueda de Asistencia

El dispositivo automáticamente almacena los registros de verificación de los usuarios. Con la función de búsqueda de asistencia, los usuarios pueden consultar todos los registros.

1. De clic en **Búsqueda de Asistencia** en el menú principal para entrar a la interfaz **ID de Usuario** (ver **Imagen 2**).



2. Ingrese el ID de usuario y de clic en **OK** para entrar a la interfaz **Rango de Tiempo** (ver Imagen 3).

3. Haga clic en el rango de tiempo que quiera ver según lo necesite o de clic en **Definir Usuario** para especificar la hora de inicio y la hora final y ver los registros relevantes.

**Notas:** Si usted da clic en **OK** sin ingresar un ID de usuario, se mostrarán los registros de verificación de todos los usuarios en el rango de tiempo seleccionado.

## 12. Autoprueba

El dispositivo automáticamente hará una prueba si todos los módulos funcionan correctamente, que incluyen el LCD, voz, sensor de huella digital, sensor de vena y reloj (RTC).



**Prueba de Todo:** Prueba el LCD, voz, sensor de huella digital★ y RTC. Durante la prueba, haga clic en la pantalla para continuar con la siguiente prueba o haga clic en  para salir de la prueba.

**Prueba LCD:** Prueba el efecto de la exhibición de la pantalla LCD de todo el color, blanco puro y negro puro para comprobar si la pantalla muestra los colores correctamente. Durante la prueba, haga clic en la pantalla para continuar con la siguiente prueba o dar clic en  para salir de la prueba.

**Prueba de Voz:** Comprueba si los archivos de voz guardados en el dispositivo están completos y la calidad de voz es buena. Durante la prueba haga clic en la pantalla para continuar con la siguiente prueba o haga clic en  para salir de la prueba.

**Prueba de Sensor de Huella Digital★:** Comprueba si el sensor de huellas funciona correctamente. Durante la prueba necesitará ver si el sensor de la huella está limpio. Cuando una huella sea presionada en el sensor, aparecerá en la pantalla la imagen de la huella digital en tiempo real. Haga clic en  para salir de la prueba.

**Prueba del Reloj (RTC):** El dispositivo hará una prueba para comprobar que el reloj trabaje correctamente y con precisión marcando el cronómetro. Haga clic en  para salir de la prueba.

## 13. Información del Sistema

La función de información de sistema permite a los usuarios ver la condición del almacenamiento y la versión del dispositivo.

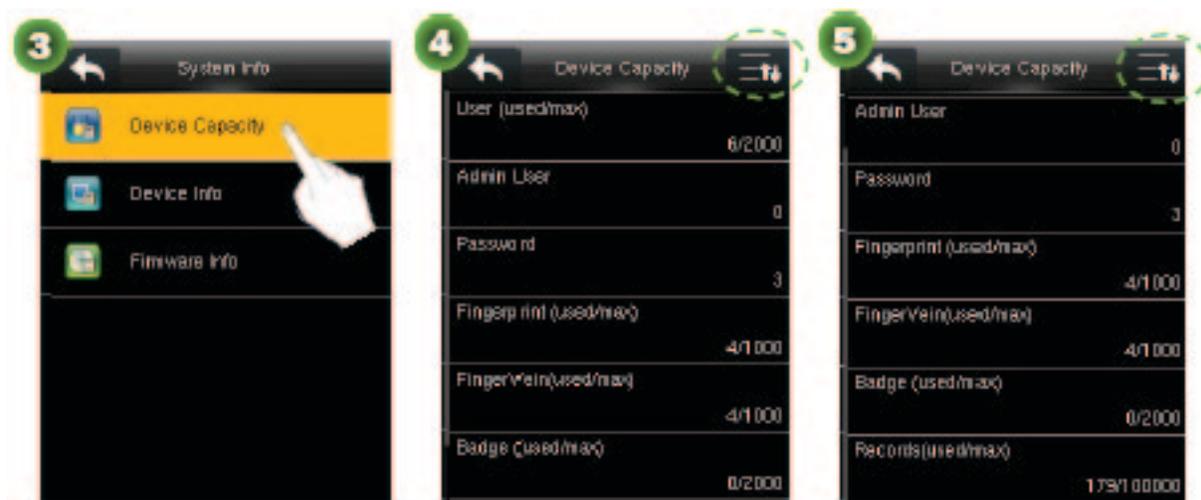
Hacer clic en **Información del Sistema** en el menú principal para entrar a la interfaz (ver **Imagen 2**).



- **Capacidad del Dispositivo**

El dispositivo muestra el número de usuarios registrados, números de administradores, contraseñas, huellas digitales, registros de vena, números de tarjetas registradas★ y registros de control de acceso en el dispositivo.

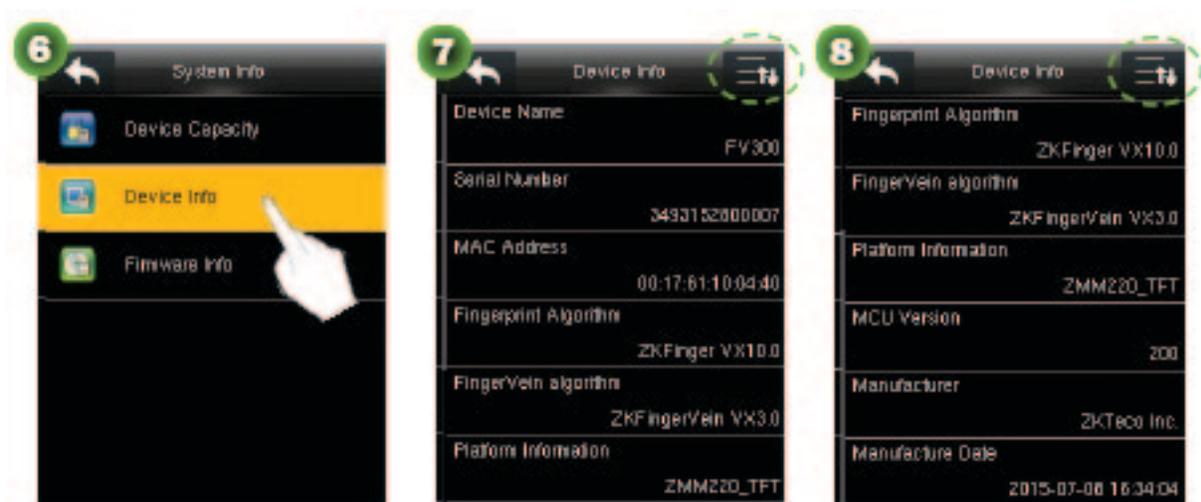
Haga clic en Capacidad del Dispositivo para entrar a la interfaz. Haga clic en  para desplazarse hacia abajo de la pantalla para ver el contenido. (Nota: Usted puede hacer clic en  nuevamente para deslizarse hacia arriba de la pantalla).



- **Información del Dispositivo**

**Información del Dispositivo:** Muestra el nombre del dispositivo, número de serie, dirección MAC, algoritmo del registro de vena★, plataforma de información, versión MCU★, fabricante y día de fabricación.

Haga clic en **Información del Dispositivo** para entrar a la interfaz. De clic en  para desplazarse hacia abajo de la pantalla para ver el contenido. (Nota: Usted puede hacer clic en  nuevamente para deslizarse hacia arriba de la pantalla).



- **Información del Firmware**

Muestra la versión del Firmware, servicio biométrico, servicio push, servicio pull y servicio Dev.

Haga clic en **Información del Firmware** para entrar a la interfaz.



## Apéndices

### Apéndice 1 Instrucción de la Operación de Entrada de Texto

El dispositivo es compatible con idioma Chino e inglés, números y símbolos. De clic en el lugar en el que el texto necesita ser ingresado para entrar en la interfaz de entrada correspondiente. Por ejemplo, de clic en **Nombre** para entrar a la interfaz.



El siguiente paso 1 utiliza la entrada de caracteres Chinos por ejemplo.

1. Haga clic en el teclado de la pantalla para entrar al chino pinyin zhong. El dispositivo muestra el pinyin chino de acuerdo a las letras introducidas en el área de visualización pinyin chino (ver **Imagen 1**).

2. Haga clic y seleccione el pinyin chino correspondiente con el carácter chino para ser ingresado. El dispositivo muestra el carácter chino correspondiente con el texto que se muestra en el área de acuerdo al pinyin seleccionado (ver **Imagen 2**).

**Nota:** Usted puede dar clic en  o  para mover hacia adelante o hacia atrás para mostrar más texto.



3. De clic y seleccione el carácter chino requerido en el texto que se muestra en el área (ver **Imagen 4**). El carácter seleccionado se muestra en el **Nombre** (ver **Imagen 5**).



4. Ingrese otro texto, repita los pasos 1-3. Después ingrese la información requerida, haga clic en **OK** para salvar la configuración y regrese a la interfaz superior.

## Apéndice 2 USB

El dispositivo sirve como un host USB, el cual puede ser conectado a una memoria USB para intercambiar datos.

El tradicional dispositivo de vena soporta la transmisión de datos a través de RS485 o Ethernet. Cuando la cantidad de datos es grande, se necesita gran tiempo para transmitir datos debido a las limitaciones físicas. La transmisión de datos vía USB es muy rápida tanto como el modo de transmisión tradicional. Al descargar los datos se usa una memoria USB, inserta la memoria USB en el dispositivo para descargar y después insértela en una PC para importar los datos a la PC.

## Apéndice 3 Introducción Wiegand

Protocolo Wiegand26 es el protocolo estándar en el control de acceso desarrollado por el Subcomité de Control de Acceso Estándar afiliado a la Asociación es un protocolo utilizado para la tarjeta sin contacto IC puerto y salida de lector.

EL protocolo define el puerto entre el lector de tarjeta y el controlador que son ampliamente usados en control de acceso, seguridad y otra industria relacionada. Esto ha estandarizado el trabajo de los diseñadores del lector de tarjeta y controladores de fábrica. El dispositivo de control de acceso producido por nuestra compañía también aplica éste protocolo.

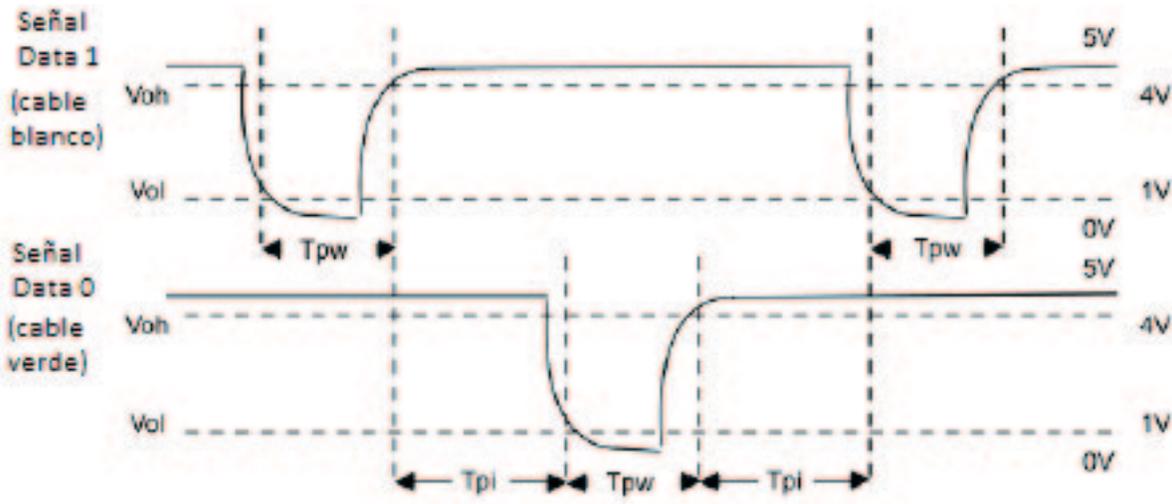
### Señal Digital

La Imagen 1 muestra la secuencia del diagrama del lector de tarjeta que envía la señal digital en bits al controlador de acceso. El protocolo Wiegand en este diagrama sigue el control de acceso estándar de SIA, los objetivos en el lector de tarjetas Wiegand 26 bits (con un pulso de tiempo de entre 20us a 100us y un tiempo de salto de impulsos de 200us y 20ms.) Data1 y Data0 son señales de alto nivel (mejor que Voh) hasta que el lector de tarjetas está listo para enviar un flujo de datos. El lector de tarjeta manda impulsos no simultáneos a bajo nivel (menos que vol), la transmisión de flujo de datos a través del cable Data1 o Data0 para acceder a la caja de control (como el diente de sierra en la imagen 1). Data1 y Data0 no coinciden o sincronizan. En la imagen 1 se muestra el tiempo máximo y ancho mínimo del pulso y el salto de impulsos permitido por las terminales de control de acceso de la serie f.

**Tabla 1: Tiempo de Pulso**

Signo	Definición	Valor Típico del Lector de Tarjeta
Tpw	Ancho de pulso	100µs
Tpi	Intervalo de pulso	1µs

Figura 1: Diagrama de Secuencia



### Apéndice 3.1 Introducción Wiegand 26

El sistema prohíbe incrustar el formato Wiegand 26-bit.

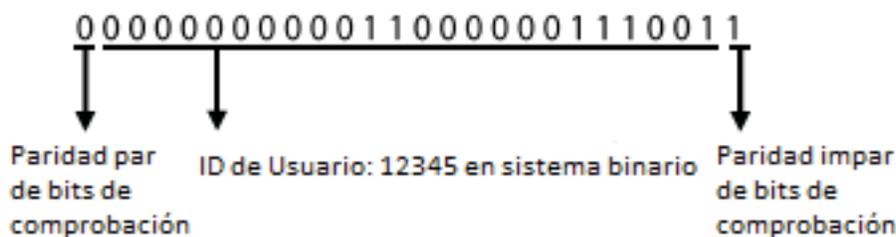
La composición del formato Wiegand 26-bit: 2 bits de verificación de paridad y el contenido de salida de 24 bits (ID de usuario o número de tarjeta). El código binario 24-bit puede indicar 16 777 216 (0- 16 777 215) valores diferentes.

	1 2	25 26
Paridad par de bits de comprobación	ID de Usuario/Número de tarjeta	Paridad impar de bits de comprobación

La tabla que sigue describe los campos.

Campo	Descripción
Paridad par de bits de comprobación	La paridad par de bits de comprobación es determinada por los bits 2-13. Si hay un número par de 1, el de bit de comprobación de paridad par es 0. Si hay un número impar de 1, el bit de comprobación de paridad par es 1.
ID de Usuario/Tarjeta numérica (bit 2 mediante bit 25)	El ID de usuario/Número de Tarjeta (código de tarjeta, 0-16777215) y el bit 2 indica el bit más significativo (MSB).
Paridad impar de bits de comprobación	La paridad impar de bits de comprobación es determinada por los bits 14-25. Si hay un número par de 1, el bit de comprobación de paridad impar es 1. Si hay un número de impar de 1, el bit de comprobación de paridad impar es 0.

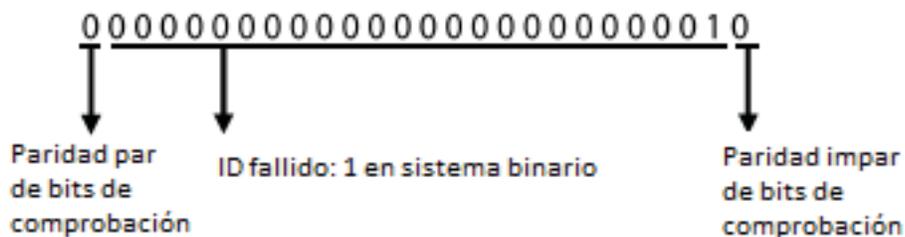
1. Cuando el contenido de salida se establece en ID de usuario, la salida Wiegand del sistema es la siguiente vez que el usuario pasa la verificación.



2. Cuando el contenido de salida se establece en el número de tarjeta, la salida Wiegand del sistema es la siguiente vez que el usuario pasa la verificación.



3. Cuando la verificación es fallida, la salida Wiegand del sistema es como sigue:



**Nota:** Cuando el contenido de salida está fuera del rango preestablecido del formato Wiegand, los bits de orden inferior son reservados y los bits de orden superior son descartados. Por ejemplo, si el ID de usuario es 888 888 888, el cual en sistema binario es 110 100 111 110 110 101 111 000 111 000, los últimos 24 bits, esto es, 111 110 110 101 111 000 111 000 se generan y los primeros 6 bits 110 100 serán descartados porque el formato Wiegand26 soporta 24 bits de contenido de salida.

## Apéndice 3.2 Introducción Wiegand 34

El sistema prohíbe la incrustación del formato Wiegand 34-bit.

La composición del formato Wiegand 34-bit: 2-bit de verificación de paridad y 32-bit de contenido de salida (ID de Usuario o Número de Tarjeta). EL código binario 32-bit puede indicar 4 294 967 296 (o-4 294 967 295) valores diferentes.

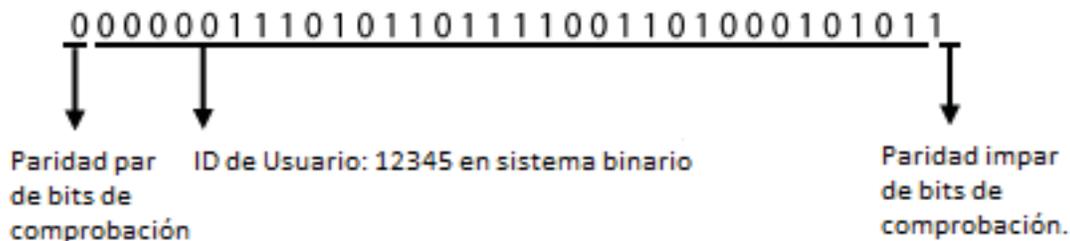
	1 2	25 26
Paridad par de bits de comprobación	ID de Usuario/Número de tarjeta	Paridad impar de bits de comprobación

La tabla que sigue describe los campos.

Campo	Descripción
Paridad par de bits de comprobación	La paridad par de bits de comprobación es determinada por los bits 2-17. Si hay un número par de 1, el de bit de comprobación de paridad par es 0. Si hay un número impar de 1, el bit de comprobación de paridad par es 1.
ID de Usuario/Tarjeta numérica (bit 2 mediante bit 25)	El ID de usuario/Número de Tarjeta (código de tarjeta, 0-4 294 967 295) y el bit 2 indica el MSB.
Paridad impar de bits de comprobación	La paridad impar de bits de comprobación es determinada por los bits 18-33. Si hay un número par de 1, el bit de comprobación de paridad impar es 1. Si hay un número de impar de 1, el bit de comprobación de paridad impar es 0.

**Ejemplo:** Un usuario con el ID de usuario 123456789 tiene el número de tarjeta 0013378512 y el ID de fallo se establece en 1.

1. Cuando el contenido de salida se establece en ID de usuario, la salida Wiegand del sistema es la siguiente vez que el usuario pasa la verificación.





## [Trabajo Principal]

El dispositivo maestro soporta la función de entrada Wiegand y el dispositivo esclavo soporta la función de salida Wiegand. Después el puerto de salida Wiegand del dispositivo esclavo es conectado al puerto de entrada Wiegand del dispositivo maestro, la señal Wiegand enviada por el dispositivo esclavo no puede contener el ID del dispositivo y los números enviados del dispositivo esclavo al dispositivo maestro deben existir en el dispositivo maestro. Esto es, la información en el dispositivo esclavo soporta la función anti-passback que debe asignar para la información del usuario en el dispositivo maestro soporta la función anti-passback.

## [Función descriptiva]

El dispositivo detecta el anti-passback basado en el último registro de evento de entrada/ evento de salida de los usuarios. El registro de evento de entrada debe coincidir con el registro de evento de salida. El dispositivo soporta la salida anti-passback, entrada anti-passback y entrada/salida anti-passback.

Cuando la **Salida Anti-passback** es establecida para un usuario en el dispositivo maestro, el último registro del usuario debe ser un registro de checado de entrada si el usuario necesita checar libremente entrada/salida. De otra manera, el usuario no podrá registrar salida y el registro de salida solicitado por el usuario será rechazado por el anti-passback. Por ejemplo, si el primer registro reciente del usuario es evento de entrada, el segundo registro del usuario deberá ser ya sea evento de entrada o evento de salida pero el tercer registro debe basarse en el segundo registro, asegurando que el registro de evento de entrada coincide con el registro del evento de salida. Nota: Si un usuario no tiene registro, el usuario puede solamente registrar entrada.

Cuando la **Entrada Anti-passback** es establecida para un usuario en el dispositivo maestro, el último registro de usuario deberá ser un registro de evento de salida si el usuario necesita checar libremente entrada/salida. De otra manera, el usuario no podrá registrar entrada y el registro de entrada solicitado por el usuario será rechazado por el anti-passback. Nota: Si un usuario no tiene registro, el usuario puede solamente registrar salida.

Cuando la **Entrada/Salida Anti-passback** es establecida para un usuario en el dispositivo maestro, si el último registro del usuario es un evento de salida o evento de entrada, el siguiente evento deberá ser un evento de entrada o un evento de salida por el usuario para registrar libremente entrada/salida. Esto es, el registro de evento de entrada debe coincidir con el registro de evento de salida.

## [Descripción de la Operación]

### ① Selección de modelo

Dispositivo maestro: los dispositivos soportan la función de entrada Wiegand, excepto el lector F10.

Dispositivo esclavo: los dispositivos soportan la función de salida Wiegand.

### ② Configuración de Menú

## ► Estado del Dispositivo

La opción de Estado del Dispositivo incluye Ninguno, Salida y Entrada.

**Ninguno:** para inhabilitar la función Anti-passback.

**Salida:** todos los registros en el dispositivo son registros de eventos de salida.

**Entrada:** todos los registros en el dispositivo son registros de eventos de entrada.

### ③ Modificación del formato de salida Wiegand para el dispositivo

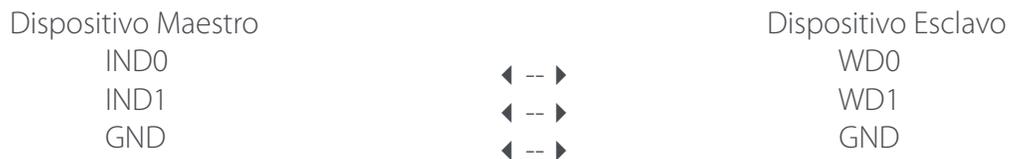
Cuando dos dispositivos se comunican entre sí, solamente la señal Wiegand que no contiene el ID del dispositivo es aceptable. Usted lo puede cambiar **Comn.>Configuración Wiegand** y establecer **Formato Definido** para **Wiegand26-bits** o **Wiegand26 sin ID del dispositivo**.

### ④ Registro de Usuario

Los IDs de usuario deben existir en ambos dispositivos maestro y esclavo y el ID de usuario debe ser consistente. Por lo tanto, los usuarios necesitan ser registrados en ambos dispositivos.

### ⑤ Descripción del cableado

El dispositivo maestro y esclavo se comunican entre sí a través de Wiegand y el cableado es como sigue:



## Apéndice 5 Declaración Sobre los Derechos de Privacidad

Estimados Clientes:

Gracias por elegir los productos híbridos diseñados y fabricados por nosotros. Como un proveedor de renombre mundial de tecnología y servicios biométricos, prestamos mucha atención para seguir las leyes relacionadas con los derechos de privacidad en cada país, mientras realizamos una investigación y desarrollo constante.

### Por la presente, hacemos las siguientes declaraciones:

1. Todos nuestros dispositivos de reconocimiento de huellas dactilares para uso civil sólo almacenan los puntos característicos de la huella dactilar en lugar de las imágenes de huellas dactilares y por lo tanto no hay problemas de privacidad que estén involucrados.
2. Los puntos característicos de la huella dactilar almacenados por nuestros productos no puede ser usados para restaurar las imágenes originales de la huella dactilar y por lo tanto no hay problemas de privacidad que estén involucrados.

3. Nosotros, como proveedor de equipos, no podremos ser legalmente responsables, directa o indirectamente, de las consecuencias derivadas por el uso de nuestros productos.
4. Si se ve envuelto en alguna disputa y se ven afectados los derechos humanos o la privacidad cuando utilice nuestros productos, por favor contacte a su distribuidor directo.

Nuestros productos de huellas digitales puede servir de apoyo a la policía o de desarrollo de herramientas de apoyo a la recopilación de las imágenes de huellas dactilares originales. En cuanto a si un tipo de huellas dactilares almacenadas constituya en una violación de su privacidad, por favor contacte al gobierno o al proveedor final. Nosotros, como el fabricante original de equipo, no podremos ser legalmente responsables por ninguna violación que surja de los mismos.

### La ley de la República Popular de China tiene las siguientes regulaciones con respecto a la libertad personal:

1. Detención ilegal, el encarcelamiento o la búsqueda de los ciudadanos de la República Popular de China está prohibido; violación de la privacidad individual está prohibido.
2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.
3. El hogar de los ciudadanos de la República Popular de China es inviolable.
4. La libertad y privacidad que corresponde a los ciudadanos de la República Popular de China está protegida por la ley.

Por fin, hacemos hincapié una vez más que la biometría, como una tecnología de reconocimiento avanzado, debe ser aplicada en gran cantidad de sectores incluyendo comercio, banca, seguros y asuntos legales. Cada año gente alrededor del mundo sufre de gran pérdida debido a la inseguridad de las contraseñas. Los productos biométricos actuales proveen una protección adecuada para su identidad bajo un alto ambiente de seguridad.

## Apéndice 6 Descripción del Uso Amigable al Medio Ambiente

El periodo de uso amigable al medio ambiente (EFUP) marcado en este producto se refiere al período de tiempo de seguridad en el cual el producto es usado bajo las condiciones especificadas en las instrucciones del producto sin fuga de sustancias nocivas.

El EFUP de este producto no cubre las piezas consumibles que necesiten ser reemplazadas sobre una base regular tales como baterías y así sucesivamente. El EFUP de las baterías es de 5 años.

### Nombres y Concentraciones de Tóxicos y Sustancias o Elementos Peligrosos

Nombre de Piezas	Tóxicos y Sustancias o Elementos Peligrosos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	o	o	o	o	o	o
Chip capacitor	x	o	o	o	o	o
Chip inductor	x	o	o	o	o	o
Chip diodo	x	o	o	o	o	o
Componentes ESD	x	o	o	o	o	o
Bocina	x	o	o	o	o	o
Adaptador	x	o	o	o	o	o
Tornillos	o	o	o	x	o	o

**o:** Indica que este tóxico o sustancia peligrosa contiene en su totalidad materiales homogéneos para esta parte está por debajo del límite del requerimiento en SJ/T11363-2006.

**x:** Indica que este tóxico o sustancia peligrosa contiene al menos un material homogéneo para esta parte está por arriba del límite del requerimiento en SJ/T11363-2006.

**Nota:** El 80% de las partes de éste producto son fabricadas con materiales favorables al medio ambiente no-peligrosos. Las sustancias peligrosas o elementos contenidos no pueden ser reemplazados con materiales favorables al medio ambiente en la actualidad, debido a las limitaciones técnicas o económicas.



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

© Copyright 2014. ZKTeco Inc. ZKTeco Logo is a registered trademark of ZKTeco or a related company. All other product and company names mentioned are used for identification purposes only and may be the trademarks of their respective owners. All specifications are subject to change without notice. All rights reserved.