



# Manual de Usuario

## F22

Dispositivo de Control de Acceso con Wi-Fi

Versión: 1.0

## Acerca de este manual

- Este manual presenta las operaciones de las interfaces de usuario y funciones del menú del dispositivo de control de acceso con Wifi y pantalla TFT de 2.4 pulgadas.
- Las imágenes usadas en este manual pueden no ser completamente consistentes con las del producto adquirido. Prevalecerán las imágenes del producto real.
- Las funciones marcadas con ★ no están disponibles en todos los dispositivos.

## CONTENIDO

<b>1. Notas de Guía.....</b>	<b>1</b>
1.1 Método para colocar la huella digital.....	1
1.2 Métodos de Verificación.....	2
1.2.1 Verificación de Huellas Digitales 1:N.....	2
1.2.2 Verificación de Huellas Digitales 1:1.....	2
1.2.3 Verificación con contraseña.....	3
1.2.4 Verificación con Tarjeta ★.....	4
1.3 Interfaz Inicial.....	4
<b>2. Menú Principal.....</b>	<b>5</b>
<b>3. Fecha/Hora .....</b>	<b>6</b>
3.1 Horario de Verano.....	6
<b>4. Usuarios.....</b>	<b>8</b>
4.1 Agregar Usuario.....	8
4.2 Configuración de Control de Acceso.....	9
4.3 Buscar Usuario.....	10
4.4 Editar Usuario.....	11
4.5 Eliminar Usuario.....	11
4.6 Estilo de Pantalla.....	12
<b>5. Privilegios de Usuarios.....</b>	<b>12</b>
5.1 Habilitar Privilegios de Usuario.....	13
5.2 Asignación de Permisos.....	13
<b>6. Ajustes de Comunicación.....</b>	<b>14</b>
6.1 Configuración de Ethernet.....	14
6.2 Ajustes de Comunicación Serial.....	14
6.3 Conexión a PC.....	16
6.4 Configuración de Red Inalámbrica.....	17
6.5 ADMS★.....	19
6.6 Ajustes Wiegand.....	20
6.6.1 Entrada Wiegand.....	20
6.6.2. Salida Wiegand.....	22
<b>7. Control de Acceso.....</b>	<b>23</b>
7.1 Opciones de Control de Acceso .....	24
7.2 Ajustes de Horarios.....	25
7.3 Ajustes de Días Festivos.....	27
7.4 Ajustes de Grupos de Acceso.....	27
7.4.1 Configurar Día Festivo para un grupo de acceso.....	28
7.5. Ajustes de Verificación Multi-Usuario.....	29
7.6 Ajustes Anti-Passback.....	31
7.7 Ajustes de Opciones de Coacción.....	33
7.7.1 Configuración de la tecla de Coacción.....	34

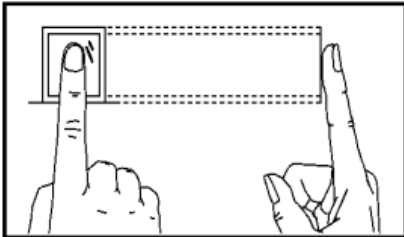
<b>8. Configuraciones de Sistema .....</b>	<b>35</b>
8.1 Ajustes de Asistencias.....	35
8.2 Ajustes de Huella Digital.....	35
8.3 Restablecer Valores de Fábrica.....	36
8.4. Actualización por USB.....	38
<b>9. Configuraciones de Personalización .....</b>	<b>38</b>
9.1 Ajustes de Interfaz de Usuario.....	38
9.2 Ajustes de Voz. ....	39
9.3 Ajustes de Timbre.....	40
9.4 Ajustes de Estados de Asistencia.....	40
9.5 Asignación de Teclas de Atajo.....	41
<b>10. Gestión de Datos .....</b>	<b>42</b>
10.1. Borrar Datos .....	42
10.2 Respaldo de Datos.....	43
10.3 Restauración de Datos.....	43
<b>11. Gestión USB.....</b>	<b>44</b>
11.1 Descargar en USB.....	44
11.2 Cargar desde USB.....	44
11.3 Ajustes de Opciones de Descarga.....	45
<b>12. Búsqueda de Registros.....</b>	<b>45</b>
<b>13. Ajustes de Impresión★.....</b>	<b>46</b>
13.1 Ajustes de Impresión de Campos de Datos.....	46
13.2 Ajustes de Opciones de Impresión.....	47
<b>14. Pruebas.....</b>	<b>47</b>
<b>15. Información del Sistema.....</b>	<b>48</b>
<b>16. Resolución de Problemas.....</b>	<b>49</b>
<b>17. Anexos.....</b>	<b>50</b>
17.1 Especificaciones.....	50
17.2 Introducción a Wiegand.....	50
17.3 Procedimiento para Cargar Imágenes.....	51
17.4 Función de Impresión★.....	52
17.5 Declaración de Derechos Humanos y de Privacidad.....	53
17.6 Descripción de Uso amigable con el Medio Ambiente.....	54

# 1. Notas de Guía

## 1.1 Método para colocar la huella digital.

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

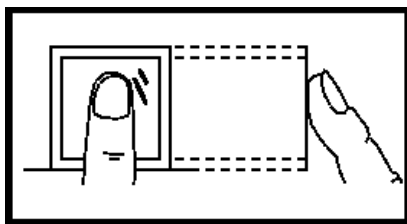
### 1. Forma correcta de colocar la huella digital:



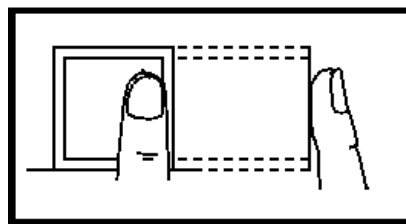
Presione el dedo horizontalmente en el sensor de huellas digitales; el centro de la huella digital se debe colocar en el centro del sensor.

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

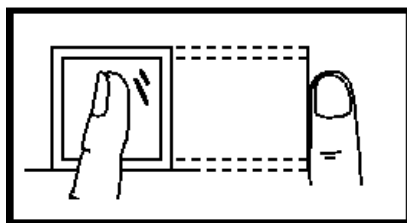
Vertical



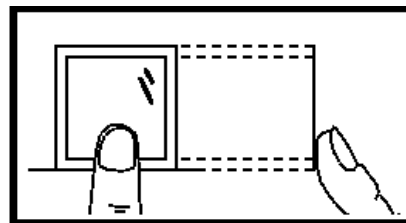
A los lados



Inclinado



Demasiado abajo



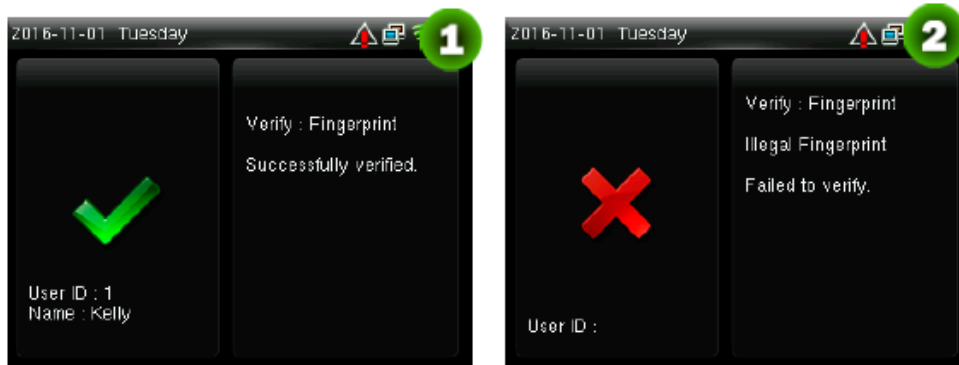
**Nota:** Utilice el método correcto para colocar las huellas digitales para el registro y la verificación. Nuestra empresa no asume la responsabilidad por el mal desempeño de la verificación causado por la operación incorrecta del usuario. Los derechos a la interpretación final y modificación están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

## 1.2 Modos de Verificación

### 1.2.1 Verificación de Huellas Digitales 1:N

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

**Nota:** Utilice la forma correcta de colocar la huella digital en el sensor (para obtener instrucciones detalladas, consulte [1.1 Método para colocar la huella digital](#)).



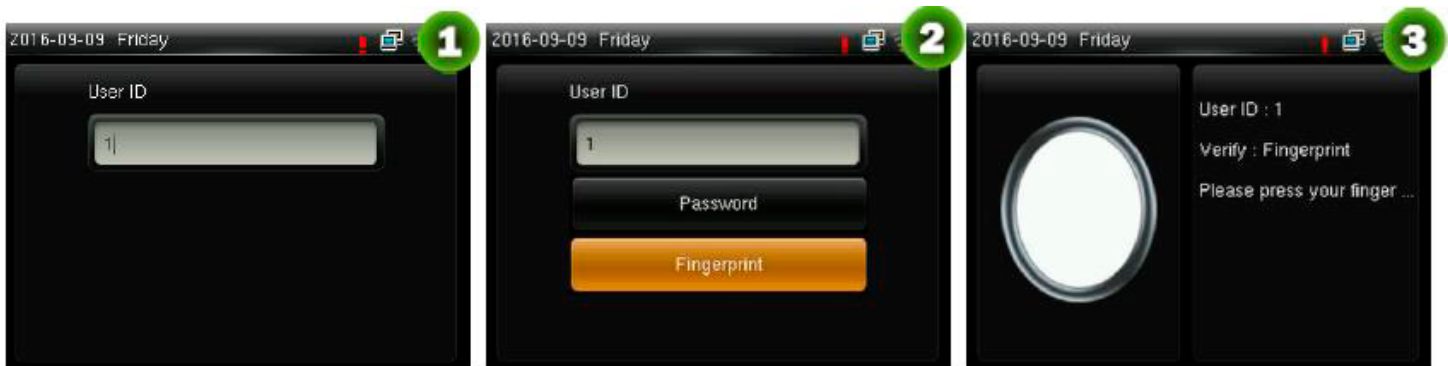
Verificación Exitosa

Verificación Fallida

**Observaciones:** Cuando el dispositivo muestra “por favor coloque el dedo de nuevo”, coloque de nuevo su dedo en el sensor de huellas digitales.

### 1.2.2 Verificación de Huellas Digitales 1:1

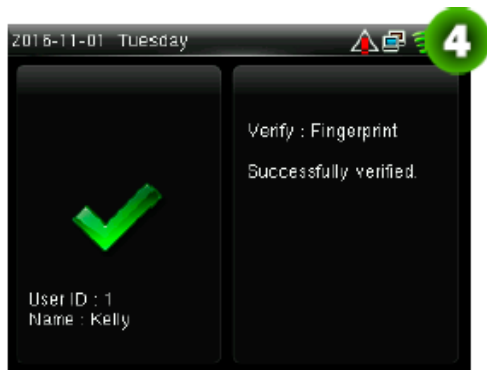
En el método de verificación de huellas digitales 1:1, la huella digital es obtenida por el sensor y se verifica con la huella digital correspondiente al ID de usuario introducido previamente. Favor de usar este método de verificación cuando sea difícil reconocer la huella en el método 1:N.



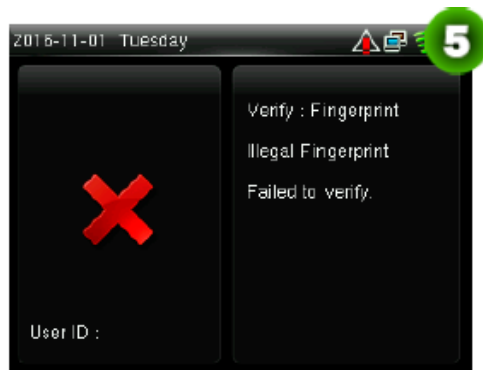
Introduzca el ID del usuario y presione **[M/OK]**

Presione ▼ para elegir “Huella” y pulse **[M/OK]**

Después coloque el dedo sobre el sensor



Verificación Exitosa



Verificación Fallida

### Observaciones:

1. Introduzca el ID de Usuario y presione **[M/OK]**. Si se muestra el mensaje “¡ID de Usuario Incorrecto!” esto significa que el ID de usuario no existe.

2. Cuando el dispositivo muestra “por favor coloque el dedo de nuevo”, coloque de nuevo su dedo en el sensor de huellas digitales. Si la verificación falla aún después de 3 intentos, saldrá a la interfaz inicial.

### 1.2.3 Verificación con contraseña

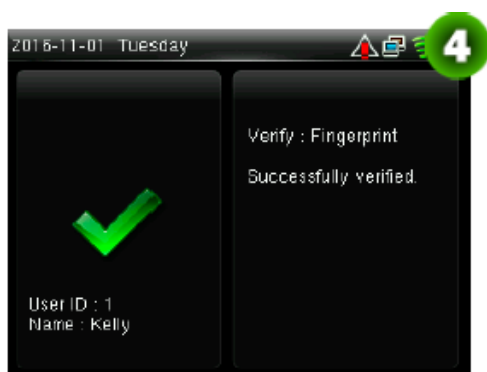
En este método de verificación, la contraseña introducida se verifica con la contraseña del ID de usuario.



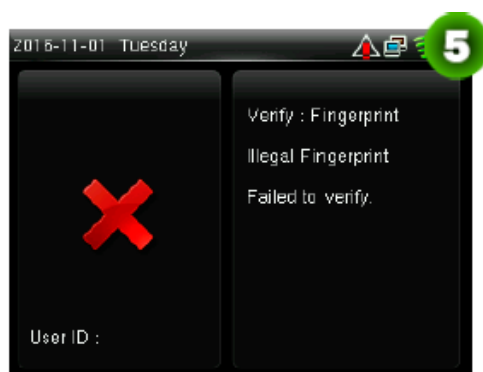
Introduzca el ID del usuario y presione **[M/OK]**

Selecciones “Contraseña” y presione **[M/OK]**

Introduzca la contraseña



Verificación Exitosa



Verificación Fallida

## Observaciones:

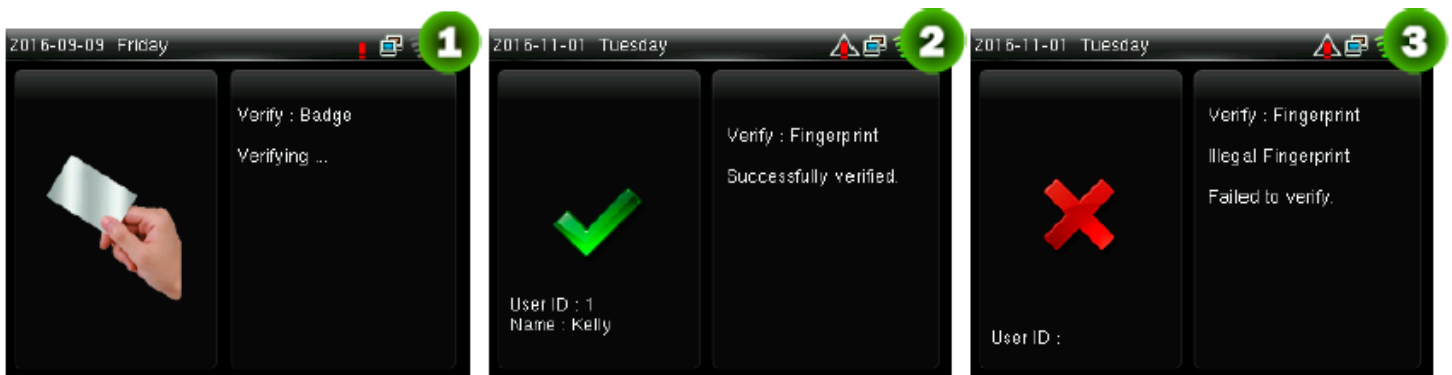
Si se muestra el mensaje "Contraseña Incorrecta", por favor introduzca la contraseña de nuevo. Si la verificación falla aún después de 3 intentos, saldrá a la interfaz inicial.

### 1.2.4 Verificación con Tarjeta ★

## Observaciones:

La función de tarjeta es opcional, sólo los productos con un módulo de tarjetas integrado están equipados con la función de verificación con tarjeta. Por favor, póngase en contacto con nuestro soporte técnico según sea necesario.

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



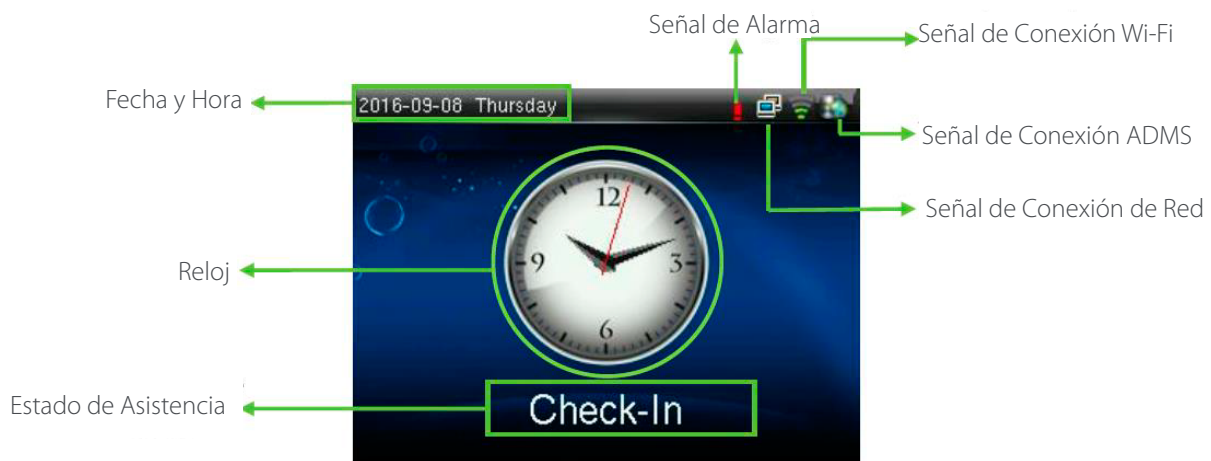
Deslice la tarjeta por encima del lector de tarjetas (la tarjeta ya debe de estar registrada)

Verificación Exitosa

Verificación Fallida

### 1.3 Interfaz Inicial

Cuando el dispositivo está encendido, la interfaz inicial se muestra como a continuación:





## 2. Menú principal

Cuando el dispositivo está en modo de espera, presione [M/OK] para entrar al menú principal.



**Gest. De Usuarios:** Usted puede administrar la información de los usuarios registrados incluyendo ID de usuario, nombre, privilegios, huella digital, tarjeta ★ (las tarjetas ID y MiFare son opcionales), contraseña y privilegios de control de acceso.

**Privilegios:** Aquí puede asignar los privilegios de cada usuario de acceder a los menús y cambiar configuraciones.

**Comunicación:** Establecer los parámetros relacionados con la comunicación entre el dispositivo y la PC, incluyendo parámetros de Ethernet como la dirección IP, comunicación Serial, conexión a PC, red inalámbrica, así como ajustes ADMS ★ y Wiegand.

**Sistema:** Para ajustar los parámetros relacionados del sistema y actualizar el firmware, incluyendo ajuste de fecha y hora, los parámetros de huellas digitales y restablecimiento a la configuración de fábrica.

**Personalizar:** Esto incluye la visualización de la interfaz, el sonido, timbre, modo de estado de asistencia y configuración de las teclas de atajo.

**Gestor de Datos:** Borra los registros de acceso, borrar todos los datos, borrar privilegio de administrador, elimine los protectores de pantalla, etc.

**Control de Acceso:** Para ajustar los parámetros de la cerradura.

**Gestión USB:** Para transferir datos tales como datos de usuario y los registros de acceso desde la unidad USB al software de apoyo u otros dispositivos.

**Búsqueda de Asistencia:** Para buscar los registros almacenados en el dispositivo después de las verificaciones exitosas.

**Imprimir★:** Para establecer las funciones e información de impresión (si la impresora está conectada al dispositivo).

**Pruebas:** Para probar de forma automática funciones diferentes módulos, incluyendo la pantalla LCD, voz, teclado, sensor de huellas digitales, la cámara y el reloj de tiempo real.

**Información del Sistema:** Para comprobar la capacidad, información y firmware actual del dispositivo.

### 3. Fecha/Hora



En la interfaz inicial, pulse **[M/OK]** > Sistema> Fecha y Hora para entrar en la Interfaz de configuración de la fecha / hora. Se incluye el establecimiento de la fecha, hora, reloj de 24 horas, formato de fecha y el horario de verano.

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

#### Observaciones:

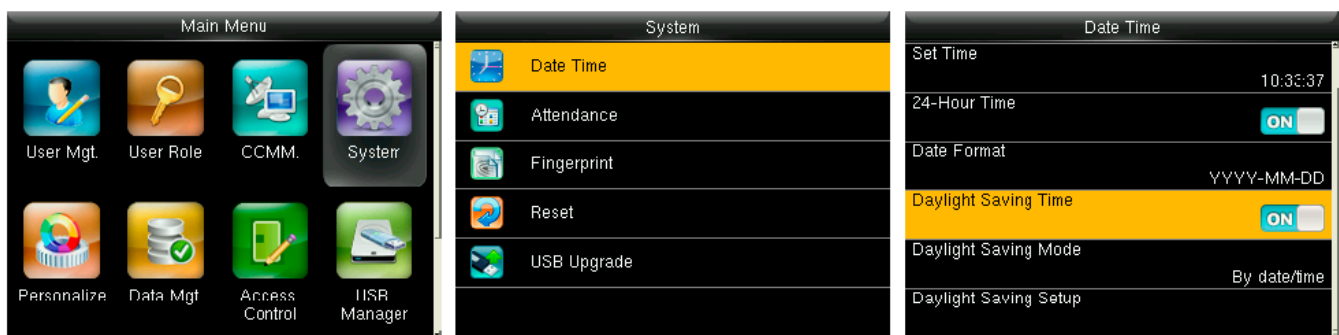
Al restablecer la configuración de fábrica, no se restaurará la fecha / hora del dispositivo (si la fecha / hora se ajusta a 18:30 el 1 de enero de 2020, después de restablecer los ajustes, la fecha / hora se mantendrá en 18:30 de 1 de enero, 2020).

#### 3.1 Horario de Verano

El Horario de Verano, que también llamado DST, es un sistema de ajuste de la hora local con el fin de ahorrar energía.

El tiempo que se adopta durante las fechas establecidas se llama "Horario de Verano". Por lo general, se adelanta una hora en el verano. Esto permite a los usuarios dormir o levantarse más temprano, y también reduce la iluminación del dispositivo para ahorrar energía. En otoño, el tiempo se reanuda el tiempo estándar. Las regulaciones son diferentes en distintos países. En la actualidad, cerca de 110 países adoptan el horario de verano.

Para satisfacer la demanda del horario de verano, una opción especial puede personalizarse. Adelante el tiempo una hora a las XX (hora) XX (día) XX (mes), y retroceda el tiempo una hora a XX (hora) XX (día) XX (mes).



Presione **[M/OK]** > Sistema> Fecha y Hora> Horario de Verano, a continuación, pulse **[M/OK]** para activar el Horario de Verano

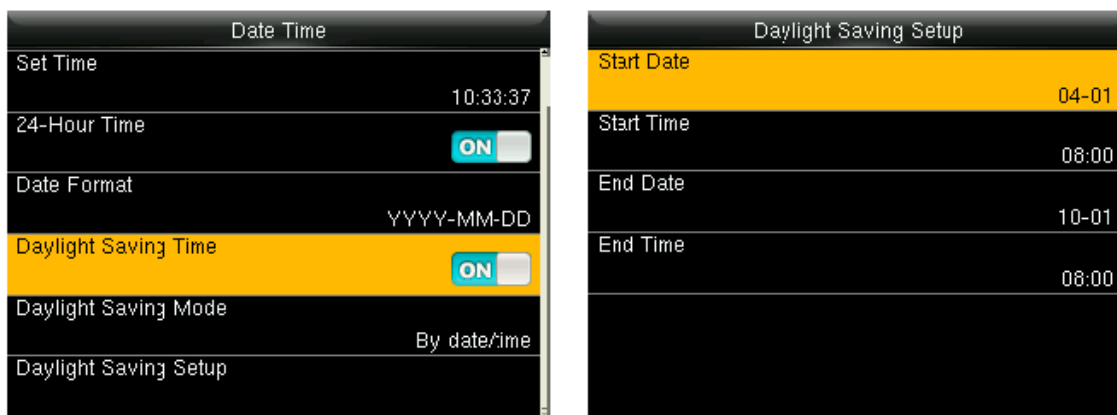
**Modo de Horario de Verano:** Elija el modo del horario de verano. Puede elegir entre el modo por fecha/hora o el modo por semana/día.

**Configuración del Horario de Verano:** Ajuste la fecha/hora o la semana/día del horario de verano de acuerdo al modo seleccionado.

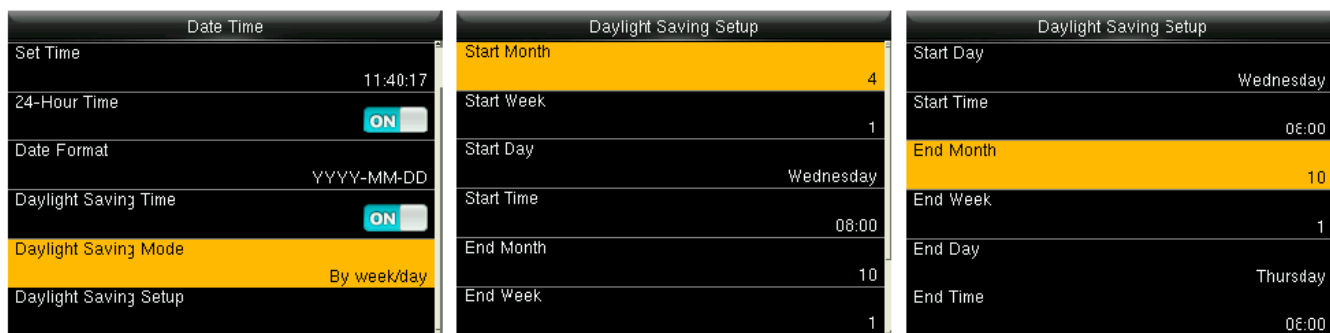
### ¿Cómo establecer el horario de verano?

Por ejemplo, adelantar el reloj una hora a las 08:00 el 1 de abril y retrasar una hora a las 08:00 el 1 de octubre (el sistema vuelve a la hora original).

- Por el modo de fecha / hora:



- Por el modo de semana / día:



### Observaciones:

1. Si el mes en que se inicia el horario de verano es posterior al mes en que termina, el horario de verano se extiende por dos años diferentes. Por ejemplo, la hora de inicio del horario de verano es 2014-9-1 las 4:00 y la hora de finalización es 2015-4-1 a las 4:00.

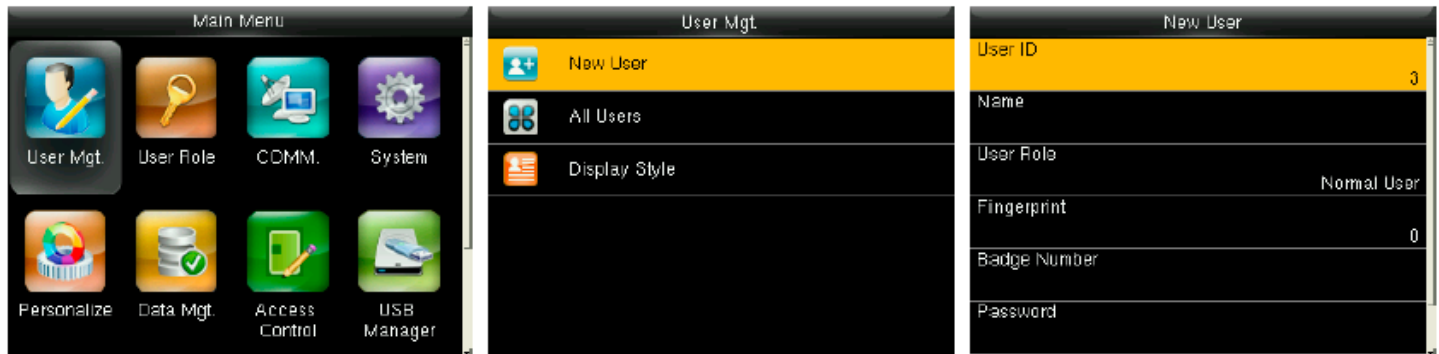
2. Supongamos que el modo de semana/día fue seleccionado en **[Modo de Horario de Verano]** y el horario de verano comienza desde el domingo de la sexta semana de septiembre de 2013. De acuerdo con el calendario, septiembre de 2014 no tiene seis semanas sino 5. En este caso, en 2014, el horario de verano comienza en el punto de tiempo correspondiente del último domingo de septiembre.

3. Supongamos que el horario de verano se inicia desde el lunes de la primera semana de septiembre de 2014. De acuerdo con el calendario, la primera semana de septiembre de 2015 no tiene lunes. En este caso, el horario de verano se inicia desde el primer lunes de septiembre de 2015.

## 4. Gestión de Usuarios

### 4.1 Agregar Usuario

Aquí puede registrar un usuario nuevo incluyendo a un administrador o a un usuario normal.

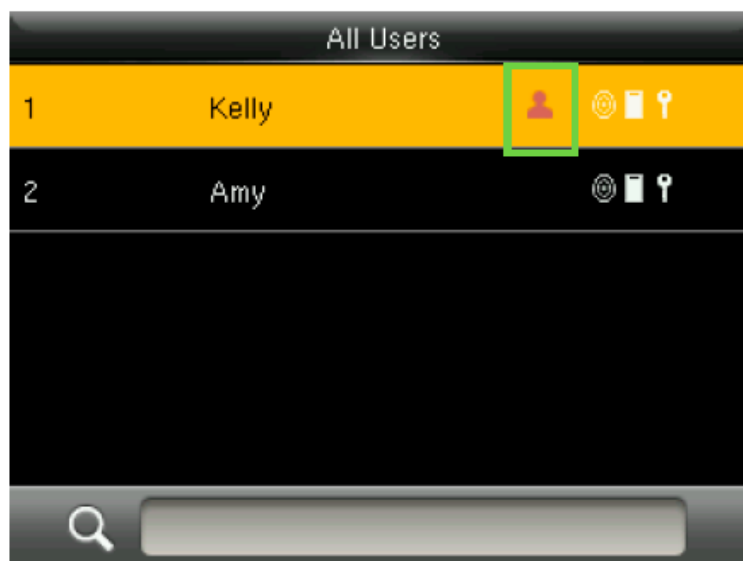


En la interfaz inicial, pulse **[M/OK]** > Gest. De usuarios > Nuevo Usuario.

Los ajustes incluyen establecer el ID de usuario, nombre, elegir los privilegios de usuario, registro de huellas digitales y número de tarjeta ★(Tarjetas ID y Mifare son opcionales), el establecimiento de contraseña y de privilegios de control de acceso.

Añadir Administrador: Elija "Administrador" en [Privilegios de usuario], quién está autorizado para operar todas las funciones en el menú.

Como se muestra a continuación, el usuario con el ID de usuario 1 es un administrador.



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

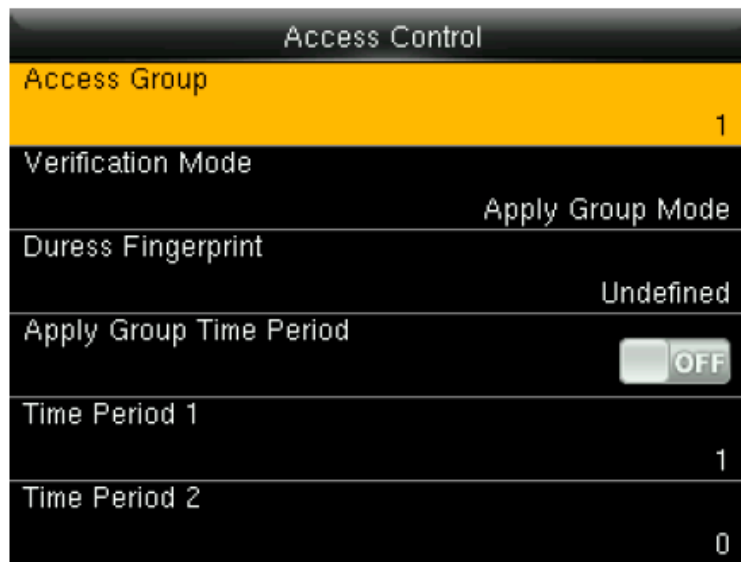
**Contraseña:** Se aceptan contraseñas de 1 a 8 dígitos.

**Observaciones:**

1. El dispositivo asigna automáticamente los ID de usuario en secuencia, pero el usuario puede configurarlo manualmente.
2. El dispositivo es compatible con IDs de usuarios de 1 a 9 dígitos.

## 4.2 Configuración de Control de Acceso

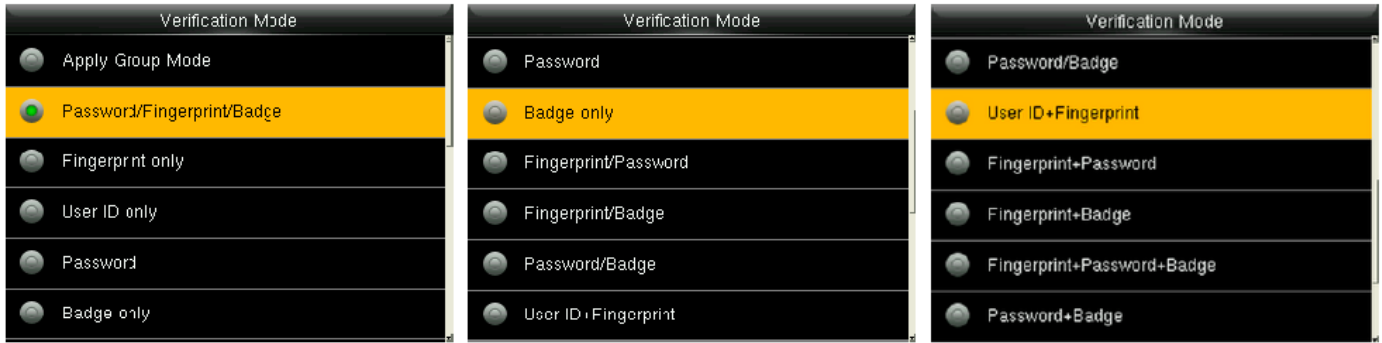
La opción de Control de Acceso de los usuarios se usa para configurar el acceso a la puerta, dirigido a todos, incluyendo ajustes de grupos de acceso, método de verificación, horarios válidos para acceder y la configuración de las huellas digitales de coacción.



**Grupo de acceso:** Para asignar los usuarios a diferentes grupos de control de acceso para su gestión. Los nuevos usuarios pertenecen a Grupo 1 en la configuración por defecto, que pueden ser reasignados a otros grupos.

**Modo de Verificación:** El usuario puede elegir entre el modo de verificación del grupo o individual. Si la verificación individual es escogida, los métodos de verificación utilizado por otros miembros del grupo no se verán afectados.

**Tipo de Verificación Individual:** Se incluye contraseña / huella digital / tarjeta, sólo huella digital, sólo ID de usuario, contraseña, sólo tarjeta, huella digital / contraseña / tarjeta, tarjeta / contraseña, ID de usuario y huella dactilar, huella digital y contraseña, huella digital y tarjeta, huella digital y contraseña & tarjeta, contraseña & tarjeta, ID de usuario y contraseña y huella digital, huella digital y (tarjeta / ID de usuario).



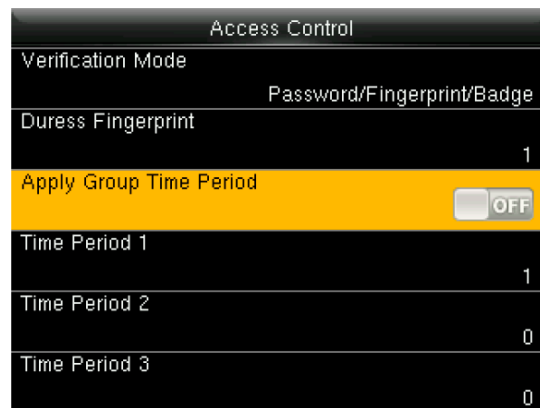
**Observaciones:** El modo de verificación individual tiene prioridad sobre el modo de verificación grupal.

**Huellas digitales de coacción:** El usuario puede elegir una o más huellas digitales registradas como huellas de coacción. Cuando se verifica con esa huella digital, se activará la alarma de coacción.

**Ejemplo:** Entre las huellas digitales registradas (6, 7, 8), elija la 8ª como la huella digital de coacción.

### Usar horario de grupo:

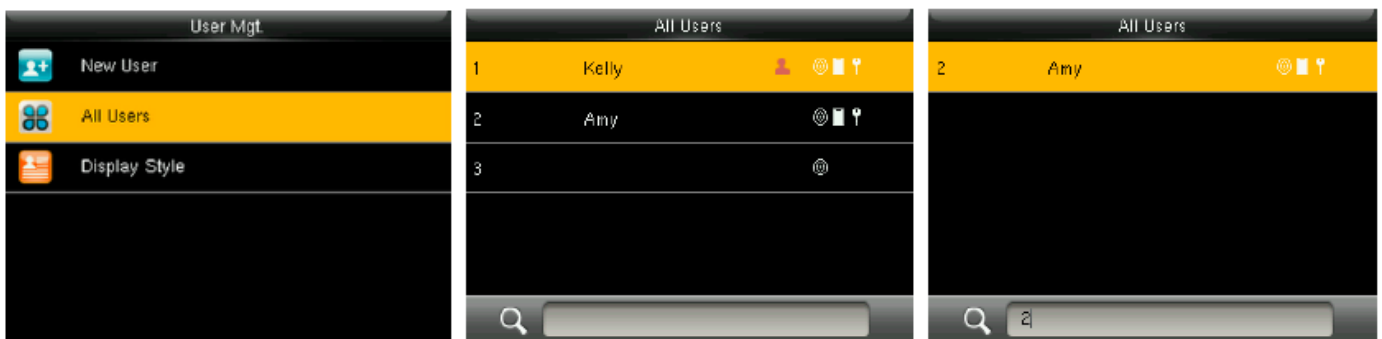
1. Cuando esta función está activada, el usuario utiliza el horario establecido en su grupo.
2. Cuando esta función está desactivada, el usuario necesita establecer un horario personal (no se usa el horario de grupo). Esto no afectará el horario de acceso de los otros miembros del grupo.



**Observaciones:** Cada usuario puede establecer hasta un máximo de 3 horarios.

## 4.3 Buscar Usuario

Introduzca la ID de usuario en la Lista de Usuarios para buscar un usuario.



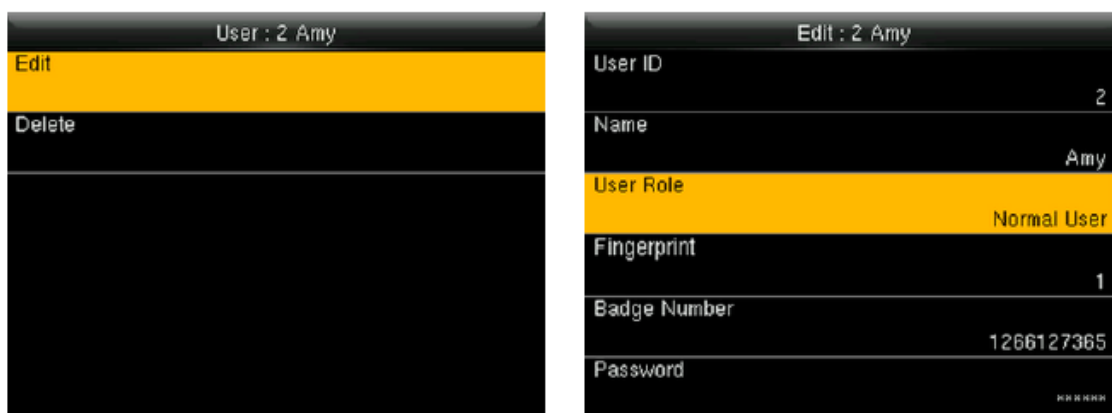
En la Interfaz, presione **[M/OK]** > Gest. De usuarios > Todos los Usuarios para entrar en la Interfaz de Todos los Usuario. Introduzca el ID de usuario en y aparecerá el usuario correspondiente, Como se muestra en la figura anterior, busque al usuario con el ID de usuario "2".

#### 4.4 Editar Usuario

Después de elegir un usuario a través de [4.3 Buscar Usuarios](#), presione **[M/OK]** y seleccione [Editar] para entrar en la interfaz de edición de usuario.

O desde la interfaz inicial presione **[M/OK]** > Gest. De usuarios > Todos los usuarios > Buscar un usuario > Presione **[M/OK]** > Editar para entrar en la interfaz de edición de usuario.

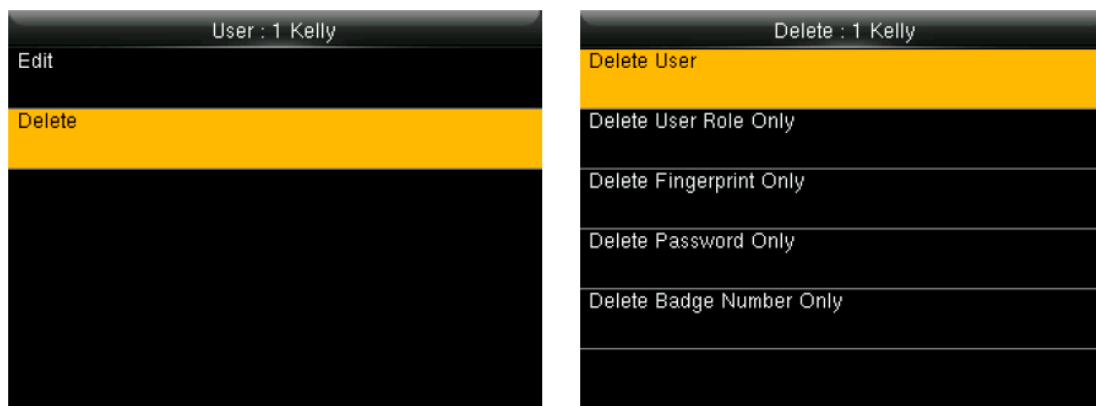
Los pasos para editar un usuario son los mismos que para agregar un usuario, pero el ID de usuario no se puede editar.



#### 4.5 Eliminar Usuario

Después de elegir un usuario a través de [4.3 Buscar Usuarios](#), presione **[M/OK]** y seleccione [Borrar] para entrar en la interfaz de eliminación de usuario.

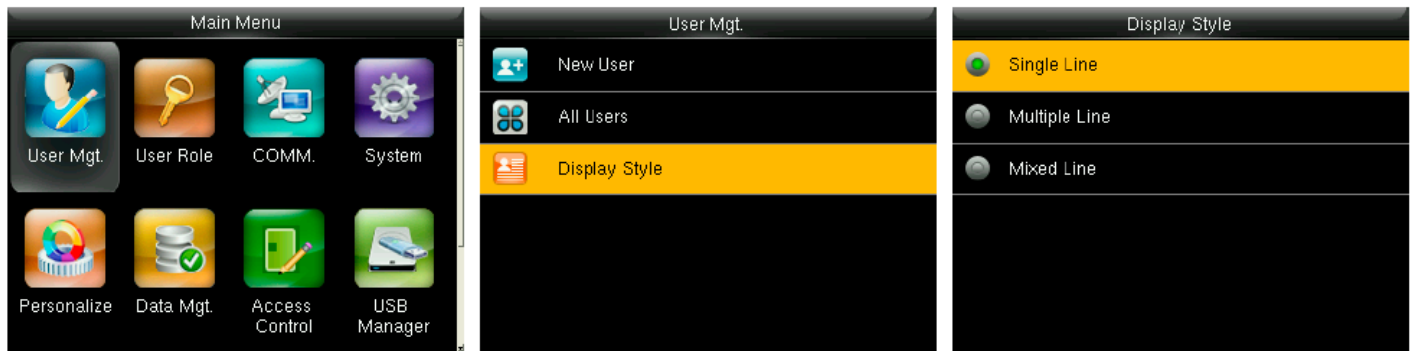
O desde la interfaz inicial presione **[M/OK]** > Gest. De usuarios > Todos los usuarios > Buscar un usuario > Borrar para entrar en la interfaz de eliminación de usuario.



#### Nota:

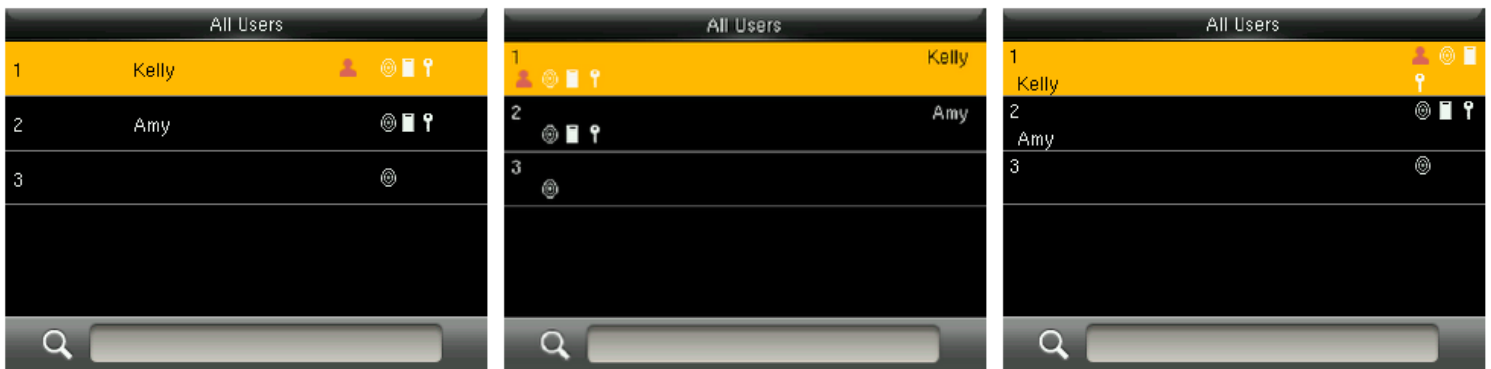
1. Sólo cuando el usuario haya registrado huella digital, contraseña o tarjeta ★, se mostrará elemento en la lista para su eliminación.
2. La función de tarjeta es opcional.

## 4.6 Estilo de Pantalla



En la interfaz inicial, presione [M/OK] > Gestión de usuarios > Estilo de pantalla para entrar en la interfaz de configuración de Estilo de Pantalla.

A continuación, se muestran los diferentes estilos de pantalla.



Línea Simple

Línea Múltiple

Línea Mixta

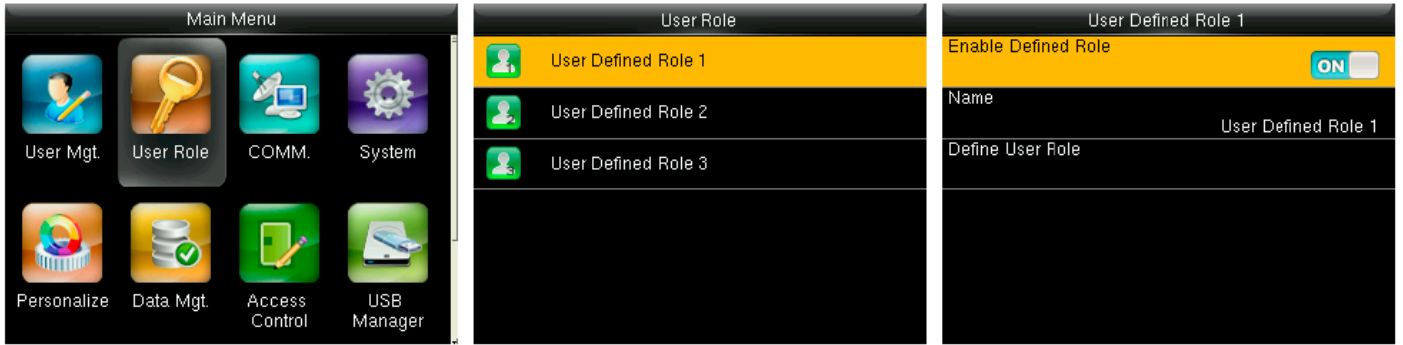
## 5. Privilegios de Usuario

Se configuran los permisos de operación del menú que puede tener un usuario (se pueden configurar un máximo de 3 perfiles de privilegios). Cuando los Privilegios de Usuarios están habilitados, en [Usuarios] > [Nuevo Usuario] > [Privilegios], puede asignar los privilegios adecuados a cada usuario.

**Privilegios:** El Administrador tiene que asignar diferentes permisos a los nuevos usuarios. Para evitar tener que establecer permisos para cada usuario uno por uno, usted puede establecer perfiles de privilegios para categorizar diferentes niveles de permisos durante la gestión de usuarios.



## 5.1 Habilitar Función de Usuario



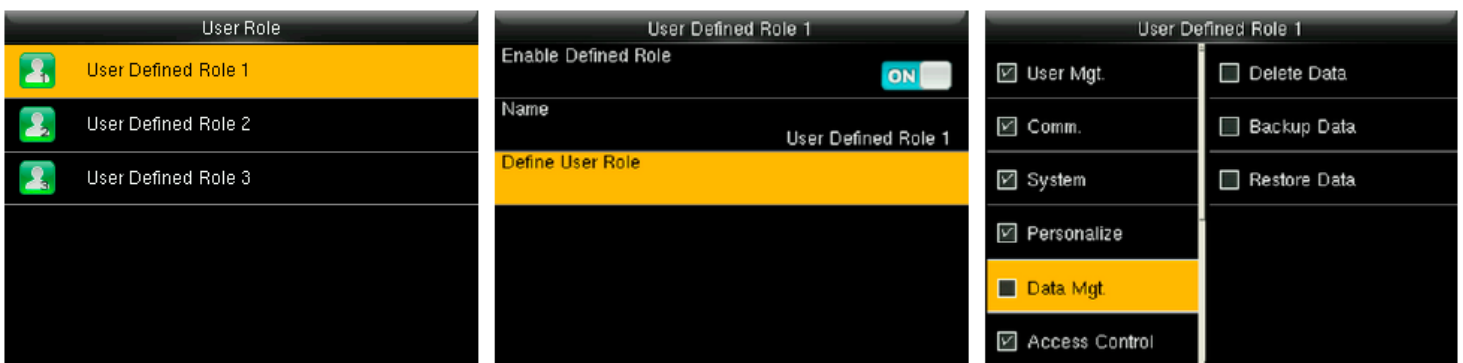
En la interfaz inicial, pulse [M/OK] > Privilegios > Privilegio de Usuario 1 (2/3)> Activar Privilegio, presione [M/OK] para activar el privilegio.

Después de activar privilegios, puede asignar estos privilegios en [Usuarios]> [Nuevo usuario]> [Privilegios de Usuario].

### Observaciones

Se requiere de al menos un administrador registrado para activar los privilegios de usuario.

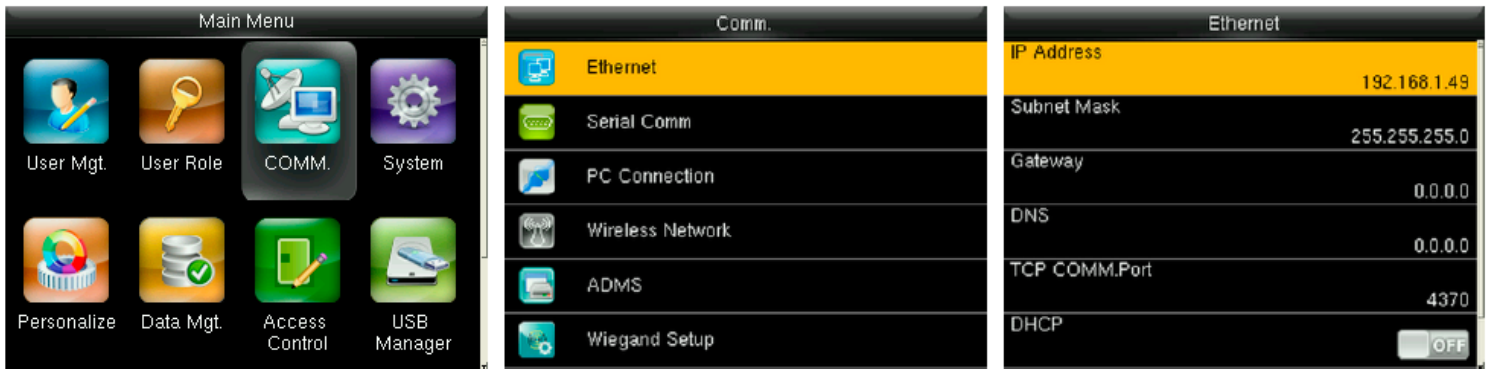
## 5.2 Asignación de Permisos



En la interfaz inicial, presione [M/OK] > Privilegios > Privilegio de Usuario1 (2/3)> Definir Privilegios para entrar en la interfaz de asignación de Privilegio de Usuario 1 (2/3). Presione [M/OK] para seleccionar o cancelar el privilegio de acceder a cada menú para Privilegio de Usuario 1 (2/3).

## 6. Ajustes de Comunicación

### 6.1 Ajustes de la Red Ethernet



En la interfaz inicial, presione [M/OK] > Comunicación > Ethernet para entrar en la interfaz de Configuración de Ethernet.

Los parámetros siguientes son los valores predeterminados de fábrica, por favor, ajuste de acuerdo a la situación real de la red.

**Dirección IP:** 192.168.1.201

**Máscara de Subred:** 255.255.255.0

**Puerta de enlace:** 0.0.0.0

**DNS:** 0.0.0.0

**Puerto de comunicación TCP:** 4370

**DHCP:** Protocolo de Configuración Dinámica de Host (por sus siglas en inglés). Es utilizado para asignar direcciones IP dinámicas a clientes en una red a través de un servidor. Si el DHCP está activado, la dirección IP no puede ajustarse manualmente.

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

### 6.2 Ajustes de Comunicación Serial

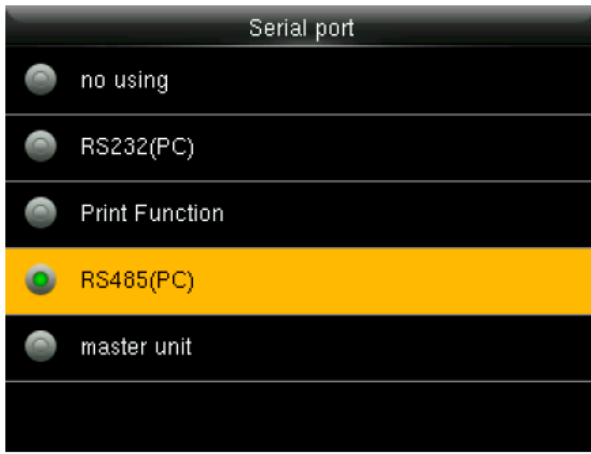
#### - Encendido/Apagado de la función RS485



Presione [M/OK] para entrar al Menú Principal y seleccione **Comunicación**

Presiona la tecla ▼ para seleccionar **Comunicación Serial** y presione [M/OK].

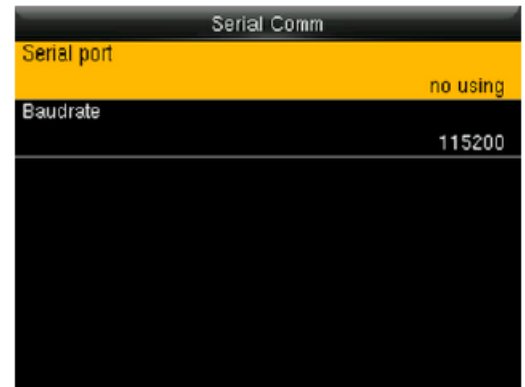
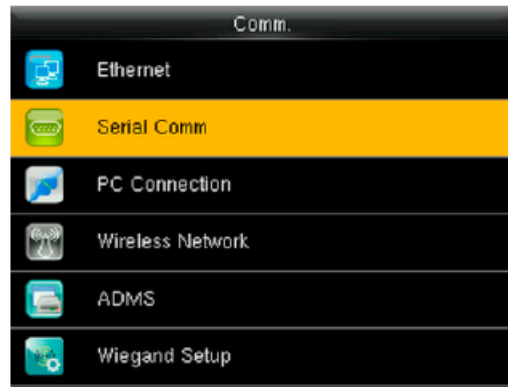
Presione [M/OK] para acceder a puerto serial.



Presione ▼ para seleccionar RS485(PC).

Finalizar

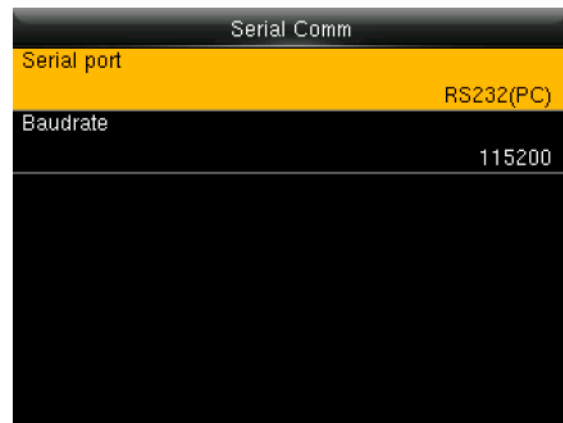
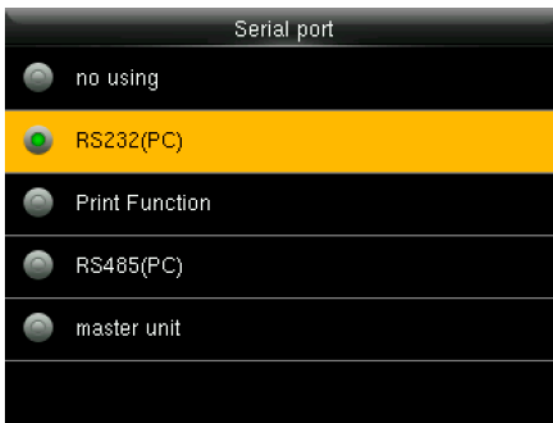
*- Encendido / Apagado de la función RS232*



Presione [M/OK] para entrar al Menú Principal y seleccione Comunicación

Presiona la tecla ▼ para seleccionar Comunicación Serial y presione [M/OK].

Presione [M/OK] para acceder a puerto serial.



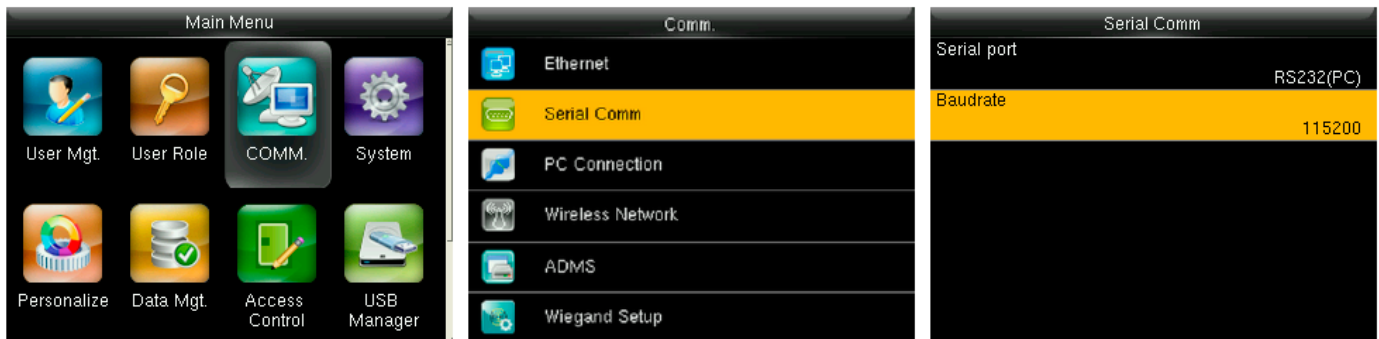
Presione ▼ para seleccionar RS232(PC).

Finalizar

## Observaciones:

1. Las funciones de comunicación RS485 y RS232 no pueden usarse al mismo tiempo.
2. Cuando se elige la "Función de Impresión★" y el dispositivo se reinicia, es posible configurar parámetros de impresión en el submenú "Imprimir". Para más detalles de la función de impresión, consulte la sección [17.4 Función de Impresión★](#)

### - Ajustes de Velocidad de Baudios



En la interfaz inicial, presione [M/OK] > Comunicación > Comunicación Serial > Velocidad de Baudios para entrar en la interfaz de Velocidad de Baudios.

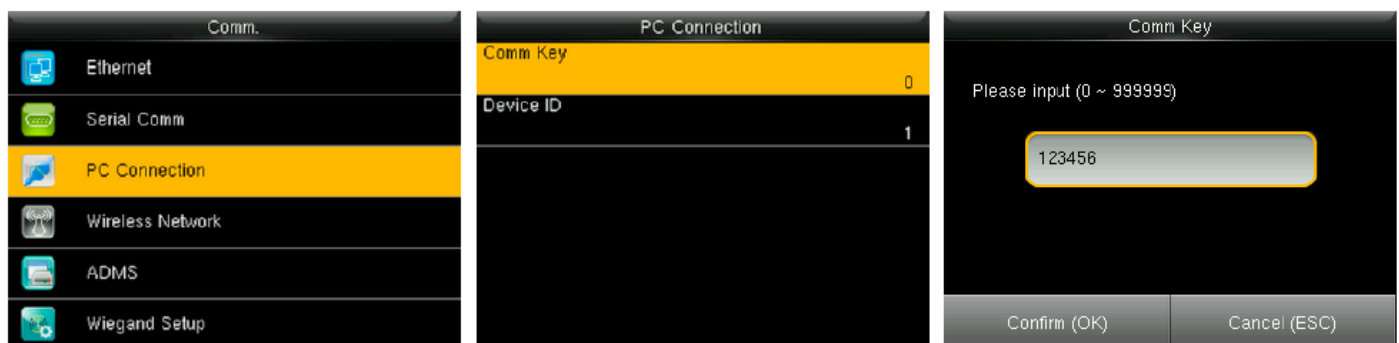
Velocidad de Baudios: La velocidad de comunicación con la PC; hay 4 velocidades: 115200 (por defecto), 57600, 38400 y 19200. Entre más alta la velocidad de baudios, es más rápida la comunicación, pero también es menos estable. En general, una velocidad alta puede usarse cuando la distancia de comunicación es corta; cuando la distancia es muy larga, elegir una velocidad más baja da más estabilidad.

## 6.3 Conexión a PC

### - Configuración de Clave de Comunicación

Para mejorar la seguridad de los datos, una Clave de Comunicación entre el dispositivo y el PC necesita ser establecida.

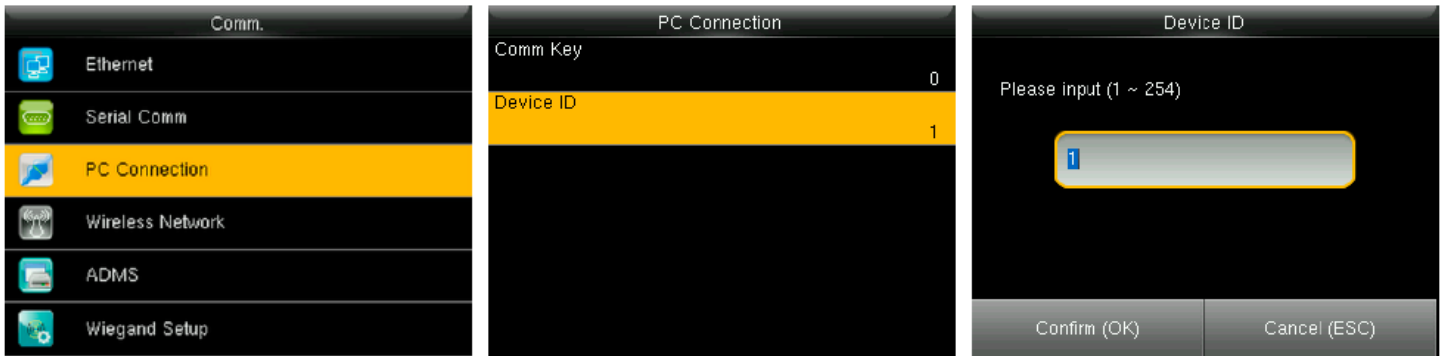
Si una Clave de Comunicación se establece en el dispositivo, la contraseña de conexión se debe introducir cuando el dispositivo se conecte al software de PC, de forma que el dispositivo y el software puedan comunicarse.



En la Interfaz inicial, presione [M/OK] > Comunicación > Conexión a PC > Clave de Comunicación.  
 Clave de Comunicación: La contraseña por defecto es 0 (no hay clave). La Clave de Comunicación puede tener de 1 a 6 dígitos y oscilar entre 0 ~ 999999.

**- Configuración del ID del Dispositivo.**

Si el método de comunicación es RS232 / RS485, se requiere introducir el ID del Dispositivo en la interfaz de comunicación con el software.



En la interfaz inicial, presione [M/OK] > Comunicación > Conexión a PC > ID del Dispositivo.

**ID del Dispositivo:** Número de identificación del dispositivo, que oscila entre 1 ~ 254.

**6.4 Configuración de Red Inalámbrica**

La red inalámbrica también puede ser llamada WIFI. El módulo WIFI viene integrado dentro del dispositivo y provee un entorno de red inalámbrica para lograr la transmisión de datos de forma inalámbrica.

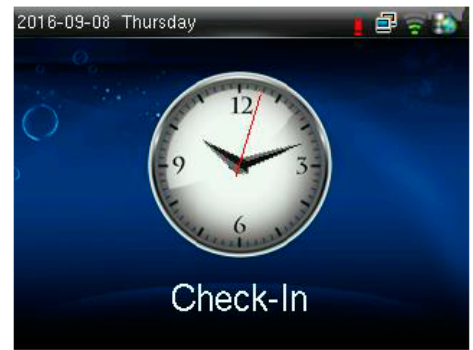
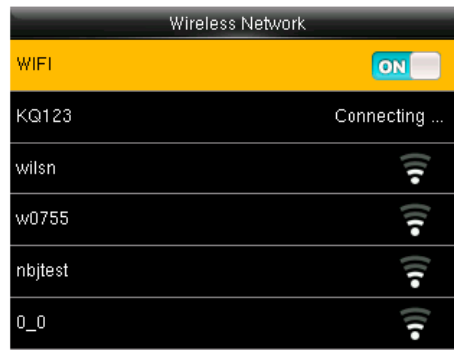
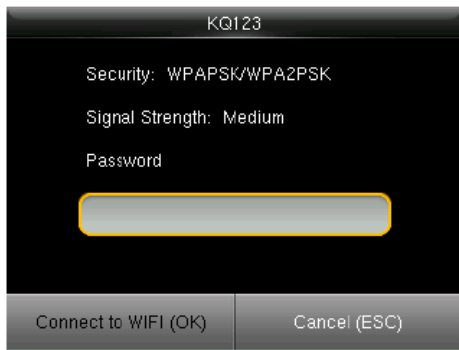
**- Conexión WIFI**



Presione [M/OK] para entrar al Menú Principal y seleccione Comunicación

Presiona la tecla ▼ para seleccionar Red Inalámbrica y presione [M/OK].

Presione [M/OK] para activar el Wi-Fi, el dispositivo busca una red automáticamente



Seleccione una red Wi-Fi disponible, presione **[M/OK]** para entrar a la interfaz de introducir contraseña.

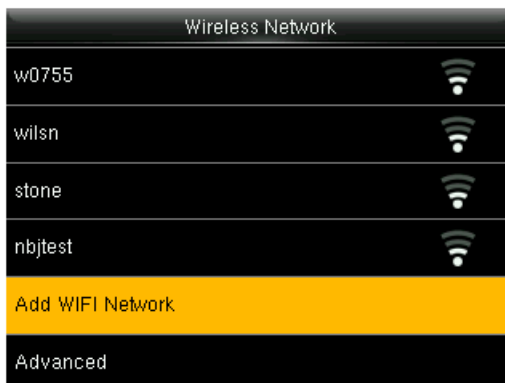
Conectando...

Finalizar

**Cuando el dispositivo se haya conectado exitosamente a la red WIFI, la interfaz inicial mostrará el logo **

### - Agregar Red WIFI

Usted puede agregar manualmente la red wifi cuando la red wifi a la que desea conectarse no aparece en la lista.



Presiona la tecla ▼ para seleccionar Agregar Red Wi-Fi y presione **[M/OK]**.

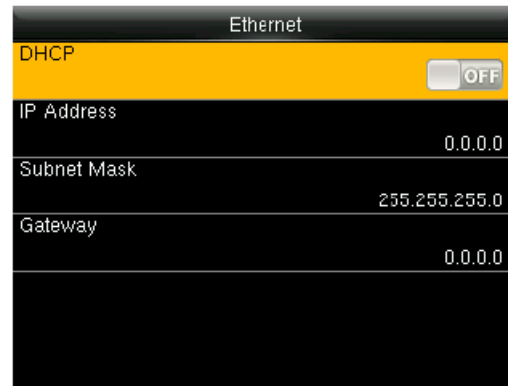
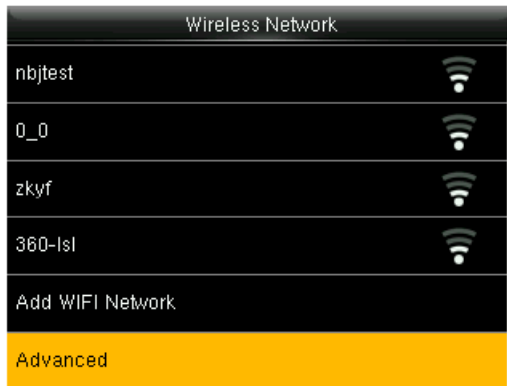


Introduzca los parámetros relevantes (la red agregada debe existir).

### Observaciones:

Después de agregar una red WIFI manualmente, para encontrar los elementos agregados a la lista WIFI, para el método de conexión, favor de consultar [Conexión Wi-Fi](#).

## - Avanzado



Presiona la tecla ▼ para seleccionar Avanzado y presione [M/OK].

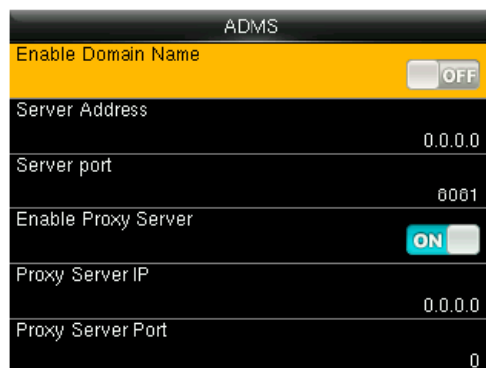
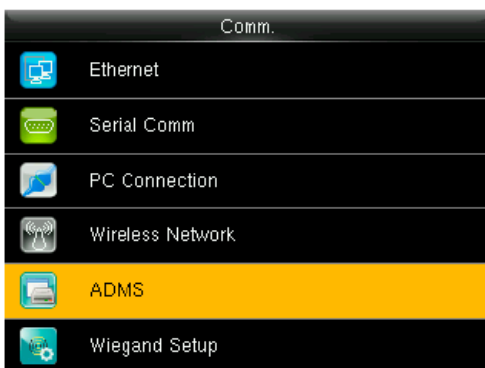
Introduzca los parámetros relevantes.

DHCP: Protocolo de Configuración Dinámica de Host (por sus siglas en inglés). Es utilizado para asignar direcciones IP dinámicas a clientes en una red a través de un servidor. Si el DHCP está activado, la dirección IP no puede ajustarse manualmente. Dirección IP: 0.0.0.0 Máscara de Subred: 255.255.255.0 Puerta de enlace: 0.0.0.0

### 6.5 Configuración ADMS ★

**Observaciones:** No todos los equipos cuentan con la función ADMS.

Ajustes utilizados para la conexión con el servidor ADMS, como la dirección IP, configuración del puerto, y si se debe habilitar el servidor proxy, etc.



En la Interfaz inicial, presione [M/OK] > Comunicación > ADMS para entrar a la interfaz de configuración del servidor ADMS.

Cuando el servidor web está conectado correctamente, la interfaz principal mostrará el logo 🍷

**Habilitar nombre de Dominio:** Cuando se activa esta función, el nombre de dominio en forma "http://..." se usará, por ejemplo http://www.XXX.com. Donde XXX denota el nombre del dominio cuando esta función esta activada; cuando esta desactivada, introduzca la dirección IP en XXX.

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

**Puerto del Servidor:** Introduzca el número de puerto utilizado por el servidor ADMS.

**Habilitar Servidor Proxy:** Método para activar proxy. Para habilitar el Proxy, configure la dirección IP y número de puerto del servidor proxy. La forma de introducir la IP del Proxy y la dirección del servidor es la misma.

## 6.6 Ajustes Wiegand



En la interfaz inicial, presione **[M/OK]** > Comunicación > Ajustes Wiegand

### 6.6.1 Entrada Wiegand

La conexión de entrada Wiegand es compatible con lectores de tarjetas, o conecta el dispositivo como un dispositivo maestro a otro dispositivo (dispositivo esclavo), formando un sistema maestro / esclavo.

Wiegand Setup	Wiegand Options	Wiegand Options
Wiegand Input	Wiegand Format	26Bits Wiegand26
Wiegand Output	Wiegand Bits	34Bits no using
Card format detect automatically	Pulse Width(us)	36Bits no using
	Pulse Interval(us)	37Bits no using
	ID Type Badge Number	50Bits Wiegand50

**Formato Wiegand:** Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a y Wiegand 50.

**Bits Wiegand:** Número de bits de los datos wiegand. Después de elegir los [Bits de Entrada Wiegand], el dispositivo usará este valor para encontrar el formato wiegand más adecuado en [Formato Wiegand].

**Amplitud de Pulso (us):** La amplitud del pulso enviado por Wiegand. El valor predeterminado es 100



microsegundos, pero puede ajustarse entre 20 a 400 microsegundos.

**Intervalo de Pulso (us):** El valor predeterminado es 1000 microsegundos, pero puede ajustarse entre 200 a 20000 microsegundos.

**Tipo de ID:** El contenido de entrada incluido en la señal de entrada Wiegand. Se puede elegir entre ID de Usuario o Número de Tarjeta.

**Definiciones de los formatos Wiegand:**

<b>Formatos Wiegand</b>	<b>Definición</b>
Wiegand 26	ECCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El bit 1 es el bit de paridad par del 2 al 13 de 26 bits, mientras que el bit es el bit de paridad impar del 14 al 25. La segunda a 25 bits son el número de la tarjeta.
Wiegand 26a	ESSSSSSSSCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El bit 1 es el bit de paridad par del 2 al 13 de 26 bits, mientras que el bit es el bit de paridad impar del 14 al 25. Del 2º al 9 bits son el código del sitio, mientras que los días 10 a 25 bits son el número de la tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El bit 1 es el bit de paridad par del 2 al 17 bits, mientras que la 34bit es el bit de paridad impar de la 18 a 33 bits. La segunda a 25 bits son el número de la tarjeta.
Wiegand 34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCO Se compone de 34 bits de código binario. El bit 1 es el bit de paridad par del 2 al 17 bits, mientras que la 34bit es el bit de paridad impar de la 18a 33bits. Del 2º al 9 bits son el código del sitio, mientras que los días 10 a 25 bits son el número de la tarjeta.
Wiegand 36	OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El bit 1 es el bit de paridad impar de la 2ª a 18 bits, mientras que la 36bit es el bit de paridad par de la 19ª a 35bits. Del 2 al 17 bits son el código del dispositivo, la 18ª a 33 bits son el número de la tarjeta, y la 34ª a 35 bits son el código de fabricante.



**Formato Wiegand:** Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a and Wiegand 50. Aunque se soportan varios formatos, el formato real está determinado por los Bits de Salida Wiegand.

Por ejemplo, si se selecciona el formato Wiegand26, Wiegand34a, Wiegand36, Wiegand37a o Wiegand50 en Formato Wiegand, pero se eligió 36 en los Bits de Salida Wiegand, el formato que se usará será Wiegand36 de 36 bits.

**Bits de Salida Wiegand:** Número de bits de los datos wiegand. Después de elegir los Bits de Salida Wiegand, el dispositivo usará este valor para encontrar el formato wiegand más adecuado en Formato Wiegand

**ID Fallida:** Se define como el valor de salida de una verificación de usuario fallida. El formato de salida depende del Formato Wiegand seleccionado. El valor predeterminado oscila de 0 a 65535.

**Código de Área:** Es similar al ID del dispositivo excepto que este puede establecerse manualmente y puede repetirse en diferentes dispositivos. El valor predeterminado oscila de 0 a 256.

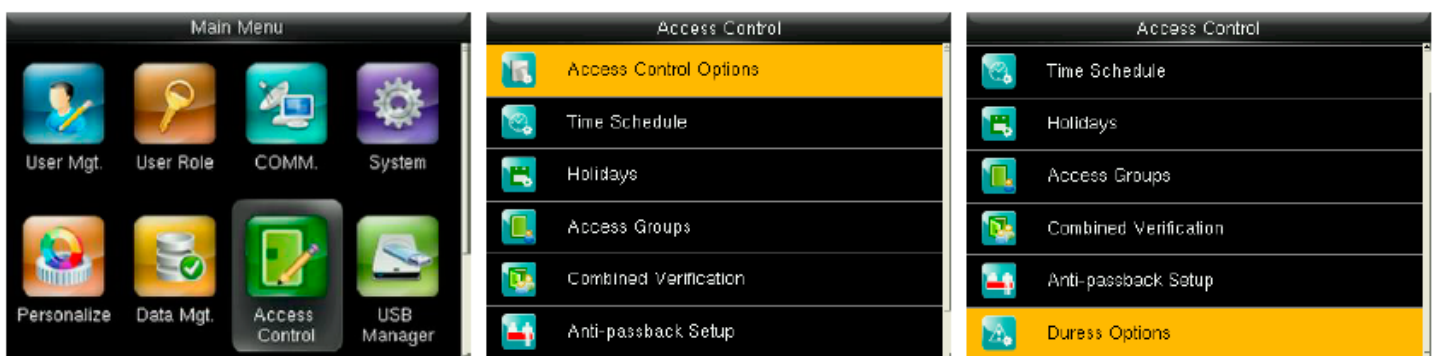
**Amplitud de Pulso (us):** La amplitud del pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, pero puede ajustarse entre 20 a 400 microsegundos.

**Intervalo de Pulso (us):** El valor predeterminado es 1000 microsegundos, pero puede ajustarse entre 200 a 20000 microsegundos.

**Tipo de ID:** El contenido de salida después de una verificación exitosa. Se puede elegir entre ID de usuario o número de tarjeta.

## 7. Control de Acceso

La opción Control de Acceso se usa para establecer horarios, días festivos, grupos de acceso, verificaciones multi-usuario, etc., así como todos los parámetros relacionados al control de la cerradura y otros dispositivos.



En la interfaz inicial, presione [M/OK] > Control de Acceso.

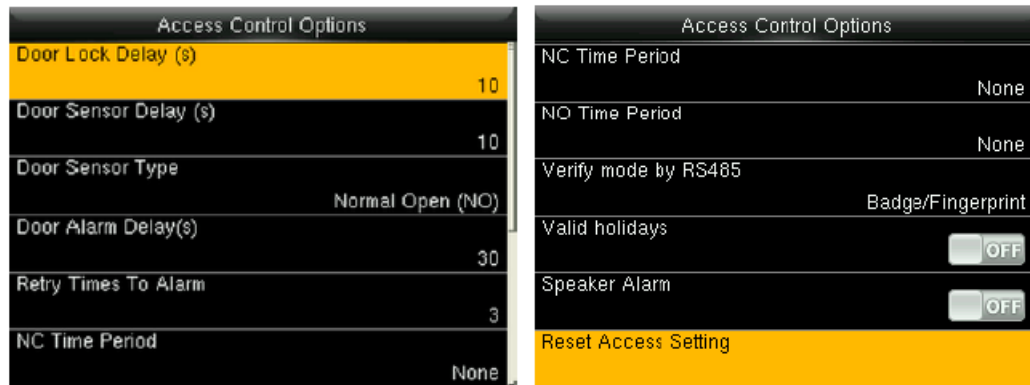
Para poder acceder, el usuario registrado debe cumplir las siguientes condiciones:

1. La hora de acceso del usuario debe estar dentro del horario personal del usuario o en el horario de su grupo.

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

En las configuraciones predeterminadas, los usuarios nuevos son asignados en el primer grupo de acceso con el horario de grupo predeterminado [1] y combinación de acceso "1", además quedan en estado desbloqueado.

## 7.1 Opciones de Control de Acceso



En la interfaz inicial, presione [M/OK] > Control de Acceso > Opciones de Control de Acceso

- **Retardo de la cerradura (s):** Tiempo en que la cerradura electrónica permanece abierta después de recibir la señal de apertura y hasta que se cierra automáticamente (el valor oscila entre 0 a 10 segundos).

- **Retardo de sensor de puerta (s):** Cuando la puerta se abre, el sensor de la puerta se activará luego de un periodo de tiempo; si el Estado del Sensor de la puerta no coincide con el Tipo de Sensor de la Puerta, se activará una alarma. Este periodo de tiempo es el Retardo de Sensor de Puerta (el valor oscila entre 1 a 255 segundos).

- **Tipo de Sensor de la Puerta:** Incluye **Normalmente Abierto (NO)**, **Normalmente Cerrado (NC)** y **Ninguno**. Ninguno significa que no está en uso el sensor de puerta; Normalmente Abierto significa que la puerta está abierta cuando tiene corriente eléctrica; Normalmente Cerrado significa que la puerta está cerrada cuando tiene corriente eléctrica.

- **Retardo de Alarma de Puerta(s):** Cuando el estado del sensor de puerta no coincide con el tipo de sensor de puerta, se activará la alarma luego de este periodo de tiempo (el rango varía de 1 a 999 segundos)

- **Reintentos para Activar Alarma:** Cuando el número de verificaciones fallidas llega al valor establecido (el rango varía de 0 a 9 intentos), la alarma se activará. Si el valor es 0, la alarma no se activará después de verificaciones fallidas.

- **Periodo de Tiempo NO:** Establece el periodo de tiempo para el modo Normalmente Abierto, de forma que la puerta siempre esté abierta durante este periodo.

- **Periodo de Tiempo NC:** Establece el periodo de tiempo para el modo Normalmente Cerrado, de forma que nadie pueda acceder durante este periodo.

- **Verificar Modo con RS485:** Para activar la función de lector RS485; es el método de verificación usado por el dispositivo cuando es el dispositivo maestro/esclavo.

- **Válido en Días Festivos:** Establecer si el Periodo de Tiempo NC o el Periodo de Tiempo NO son válidos durante los horarios de días festivos.

- **Alarma de Altavoz:** Cuando el altavoz de alarma está habilitado, el altavoz sonará una alarma cuando el dispositivo esté siendo desmantelado.

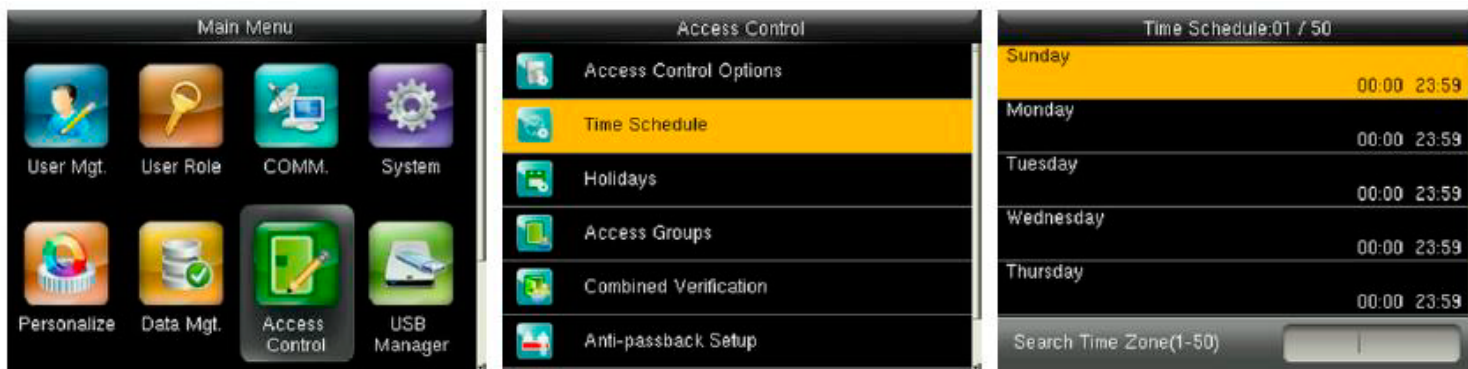
- **Reiniciar configuraciones de acceso:** Para reiniciar los parámetros de Retardo de la Cerradura, Retardo del Sensor de Puerta, Tipo de Sensor de Puerta, Reintentos para Activar Alarma, Periodo de Tiempo NO, Periodo de Tiempo NC, Normalmente Abierto/Cerrado en Días Festivos, Alarma de Altavoz, Dirección de Anti-Passback, Estado del Dispositivo, Función de Coacción, Alarma en Verificación 1:1, Alarma en Verificación 1:N, Alarma en Verificación con Contraseña y Retardo de Alarma. Sin embargo, el contenido de Borrar Datos de Acceso en [Gestión de Datos] no se verá afectado.

Parámetros de Acceso	Valor de Fábrica
Retardo de la cerradura	10 s
Retardo de sensor de puerta	10 s
Tipo de Sensor de la Puerta	Ninguno
Retardo de Alarma de Puerta	30 s
Intentos para Alarma	3 intentos
Periodo de Tiempo NC	Ninguno
Periodo de Tiempo NO	Ninguno
Validez de NO/NC en Días Festivos	Desactivado
Alarma de Altavoz	Apagado
Dirección de Anti-Passback	Sin Anti-passback
Estado del Dispositivo	Fuera
Tecla de Ayuda	Desactivada
Alarma de Verificación 1:1	Desactivada
Alarma de Verificación 1:N	Desactivada
Alarma en Verificación con Contraseña	Desactivada
Retardo de Alarma de Coacción	10 s

**Observaciones:** Después de Establecer el Periodo de Tiempo Normalmente Cerrado, favor de cerrar bien la puerta, de lo contrario la alarma podría activarse.

## 7.2 Ajustes de Horarios

El horario es la unidad de tiempo mínima de los ajustes de control de acceso; se pueden establecer un máximo de 50 horarios en el sistema. Cada Horario consiste de 7 secciones de tiempo (una semana) y cada sección de tiempo es el tiempo válido dentro de 24 horas.

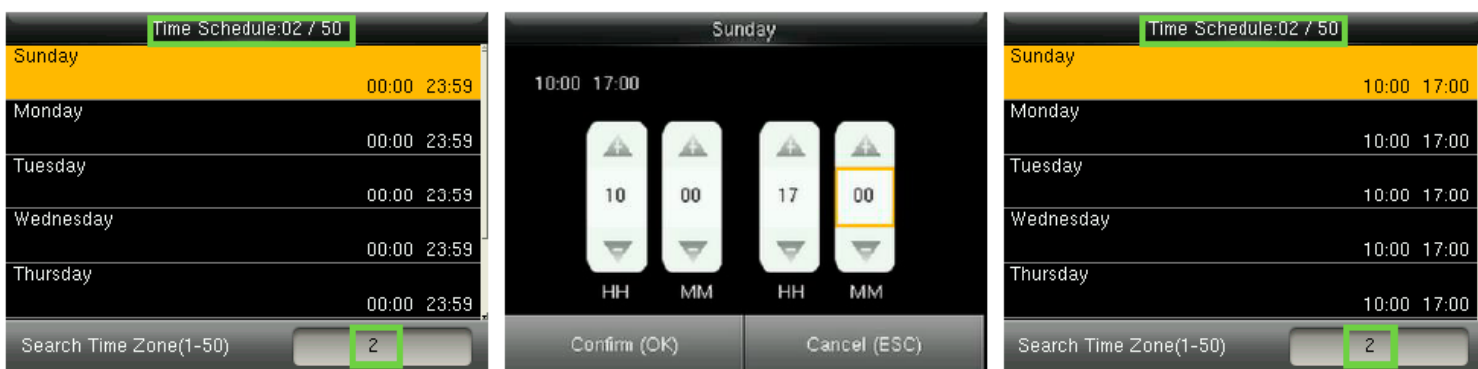


En la interfaz inicial, presione [M/OK] > Control de Acceso > Ajustes de Horarios para entrar en la interfaz de **Ajustes de Horarios**. El número predeterminado de Horario es 1 (válido todo el día), y se puede editar.

**Horario Válido:** 00:00 – 23:59 (Válido todo el día) o cuando la hora final sea después de la hora inicial.

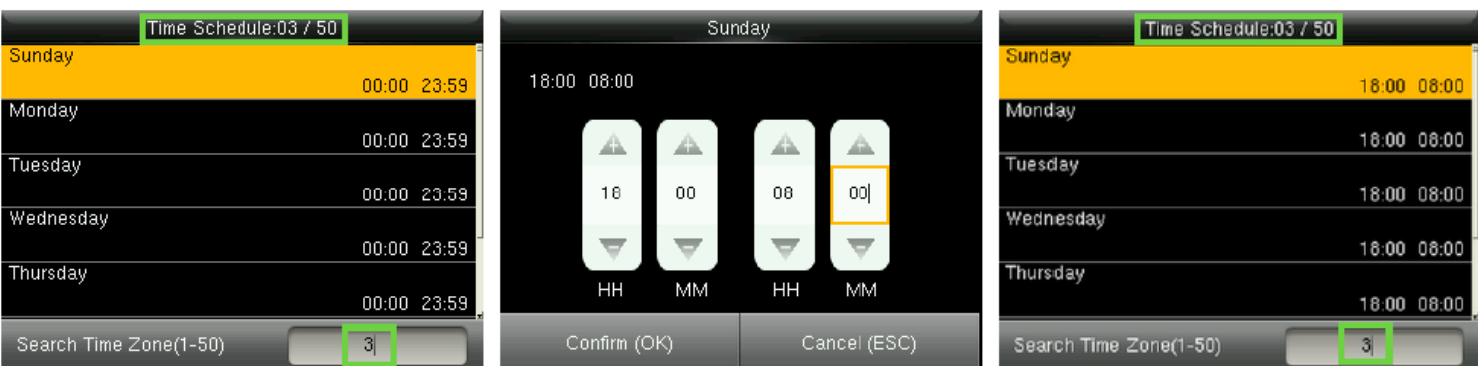
**Horario Inválido:** Cuando la hora inicial es después de la hora final.

### Ejemplo 1: Establecer Horario 02 (Valido)



Se establece el horario de 10:00 a 17:00 de domingo a sábado, pues la hora final es después de la hora inicial, por lo tanto, el horario 02 es válido.

### Ejemplo 2: Establecer Horario 03 (Inválido)

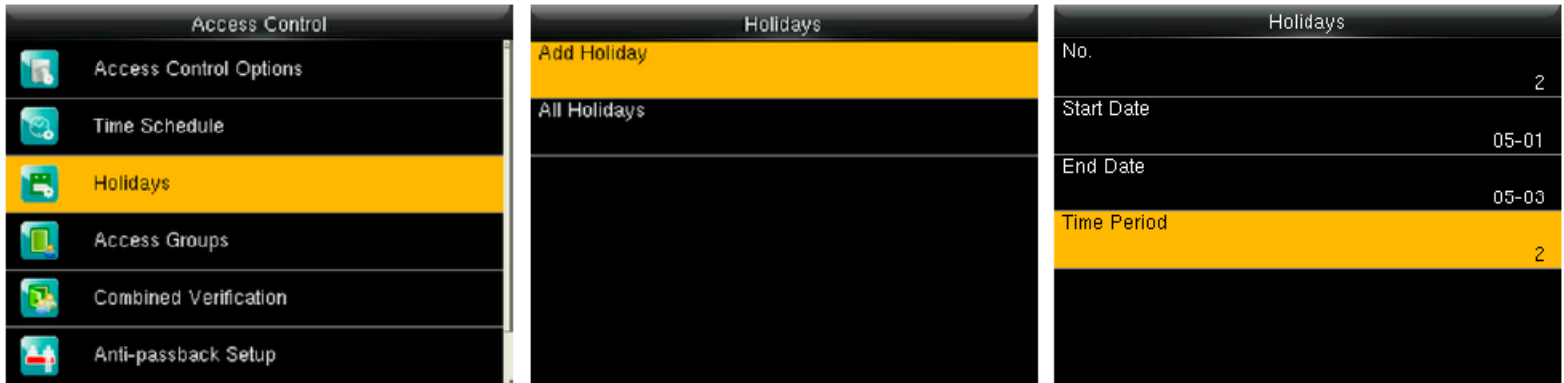


En el horario 03, la hora final de todos los días es antes de la hora inicial, por lo que es inválido.

**Observaciones:** El horario no puede establecerse entre 2 días, por eso la hora final debe ser mas tarde que la hora inicial.

### 7.3 Ajustes de Días Festivos

Se pueden establecer horarios de control de acceso para días festivos, que aplican para todos los usuarios durante los días festivos.



En la interfaz inicial, presione [M/OK] > Control de Acceso > Días Festivos.

Las configuraciones incluyen número, fecha de inicial, fecha final y horario.

**Observaciones:** La fecha inicial/final sólo requiere introducir el mes (M/M) y día (DD), lo cual aplica a todo el año. Como se muestra en la figura anterior: El día festivo 2 empieza el 1 de mayo y termina el 3 de mayo de cada año, adoptando el horario 2 (10:00 a 17:00 de domingo a sábado).

#### Para activar la función de día festivo:

En la interfaz inicial, presione [M/OK] > Control de Acceso > Grupos de Acceso > Todos los Grupos > Seleccionar un grupo de control de acceso > Editar > Incluir Días Festivos, presione [M/OK] para activar (ON) el día festivo.

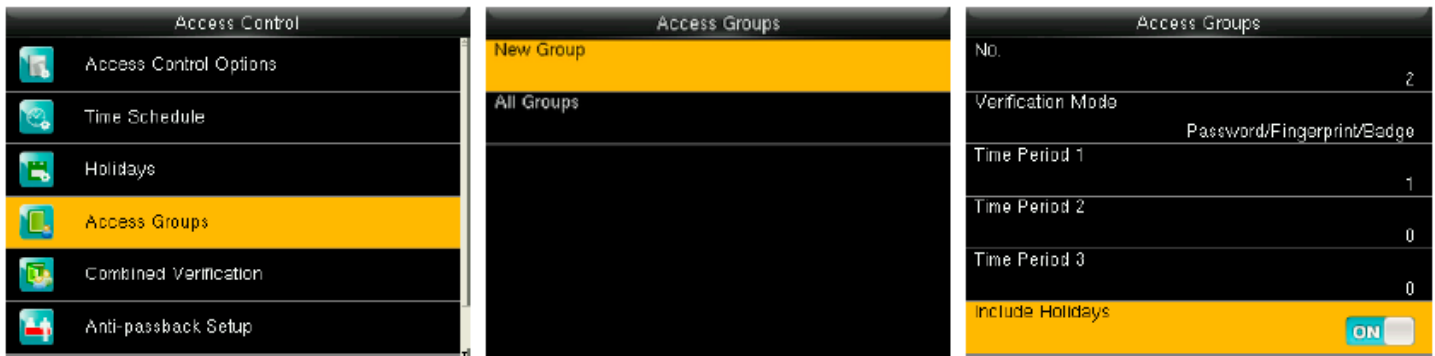
Activar o desactivar la función de días festivos se aplica para todos los miembros de un mismo grupo de acceso.

### 7.4 Ajustes de Grupos de Acceso

Los grupos son para administrar usuarios en grupos.

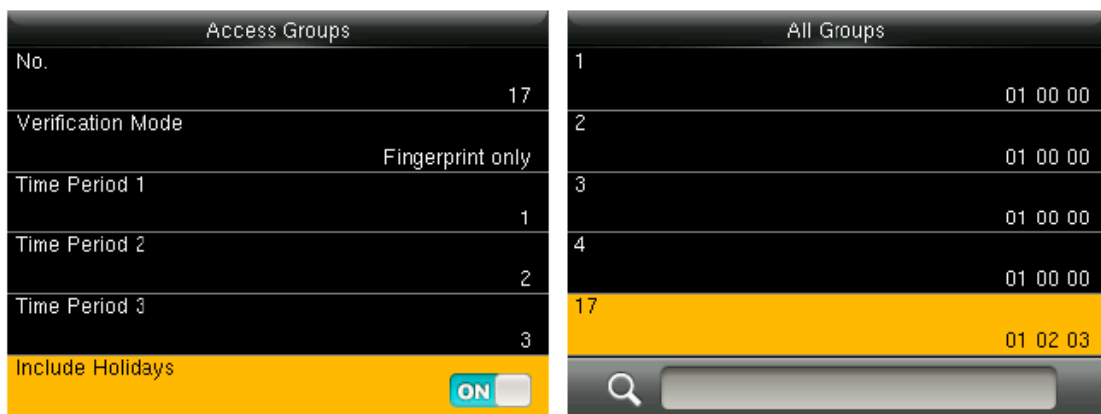
El horario de un grupo aplica para todos los miembros del grupo, pero los usuarios pueden establecer su propio horario personal. Cada grupo puede definir 3 horarios como máximo, siempre que uno de ellos sea válido, el grupo puede ser verificado correctamente.

Por defecto, los usuarios nuevos pertenecen al Grupo de Acceso 1, pero pueden ser asignados a otro grupo de acceso.



En la interfaz inicial, presione [M/OK] > Control de Acceso > Grupos de Acceso > Nuevo Grupo para entrar a la interna de Nuevo Grupo.

Tome las siguientes figuras como ejemplo:



Como se ve, el Método de Verificación del Grupo de Acceso 17 es solo huella digital, los Horarios 1, 2 y 3 se han establecido y la función de Días Festivos esta activada.

#### 7.4.1 Configurar Día Festivo para un grupo de acceso.

Para activar la función de día festivo:

Establezca **Horarios** (incluyendo Horario de Acceso y Horario de día Festivo) > configure Días Festivos > asigne usuarios a un grupo de acceso > active la opción [**Incluir Días Festivos**] en el grupo de acceso.

**Observaciones:**

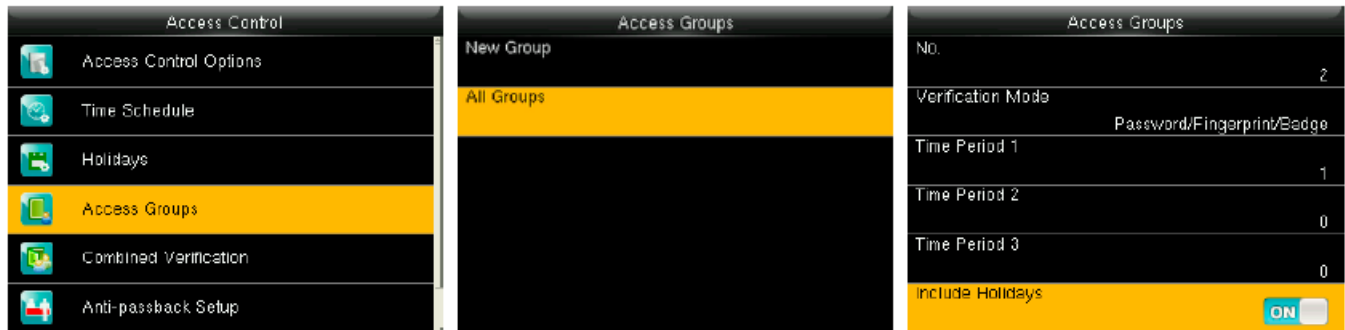
1. Cuando la función de Días Festivos está activada, sólo cuando los horarios del grupo de acceso y de los días festivos se superponen los miembros pueden tener acceso.
2. Cuando la función de Días Festivos está desactivada, los horarios de acceso de los usuarios de un grupo de acceso no se verán afectados.

Por ejemplo: Si el Grupo de Acceso 2 requiere para utilizar el Horario de Día Festivo 2 en el Día Internacional del Trabajador, lo que significa se debe permitir a los usuarios acceder durante las 10:00 ~ 17:00 (Horario 2) del 1 al 3 de mayo.



## Método de Operación:

1. Establezca Horario 2 a 10:00 ~ 17:00, de domingo a sábado. Para el método de configuración, consulte el ejemplo de la configuración de la Horario 2 en [7.2 Ajustes de Horario](#).
2. Use el Horario 2 para pasar los días festivos. Para el método de establecer de días festivos, consulte [7.3 Ajustes de días festivos](#).
3. Configure un Grupo de acceso, consulte [7.4 Ajustes de grupos de acceso](#) para ver las instrucciones.
4. Habilitar la función de Días Festivos. En el interfaz inicial, pulse [M/OK] > Control de Acceso > Grupos de Acceso > Todos los grupos > 2 > Presione [M/OK] >



5. Los usuarios en el grupo de acceso 2 pueden verificar para acceder durante el día festivo.

Observaciones: Si un día festivo debe ser válido para todos los usuarios, asigne a todos los usuarios al mismo grupo o active [Incluir Días Festivos] para todos los grupos de acceso.

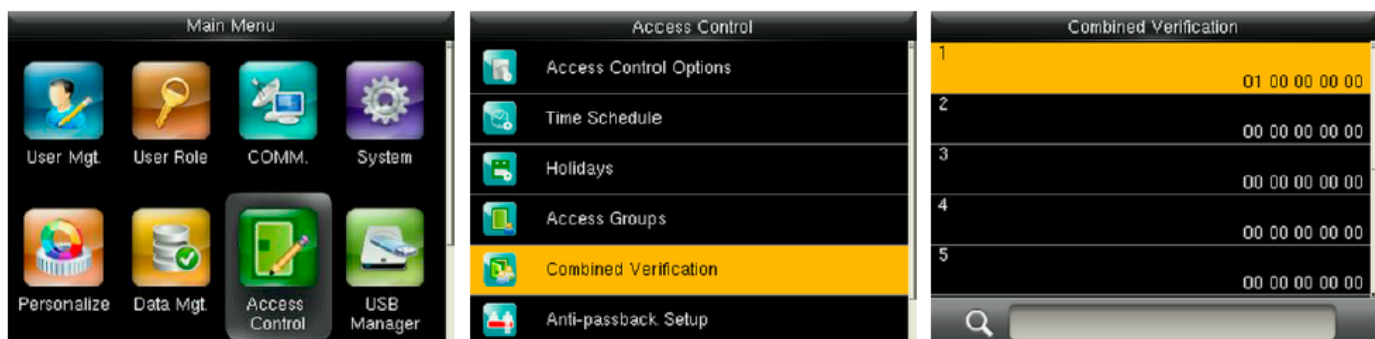
## 7.5 Ajustes de Verificación Multi-Usuario.

Combine 2 o más grupos de acceso para lograr una multi-verificación y así aumentar la seguridad.

En la verificación Multi-Usuario, se pueden combinar hasta 5 usuarios; todos los usuarios pueden pertenecer a un mismo grupo de acceso o a hasta 5 grupos diferentes.

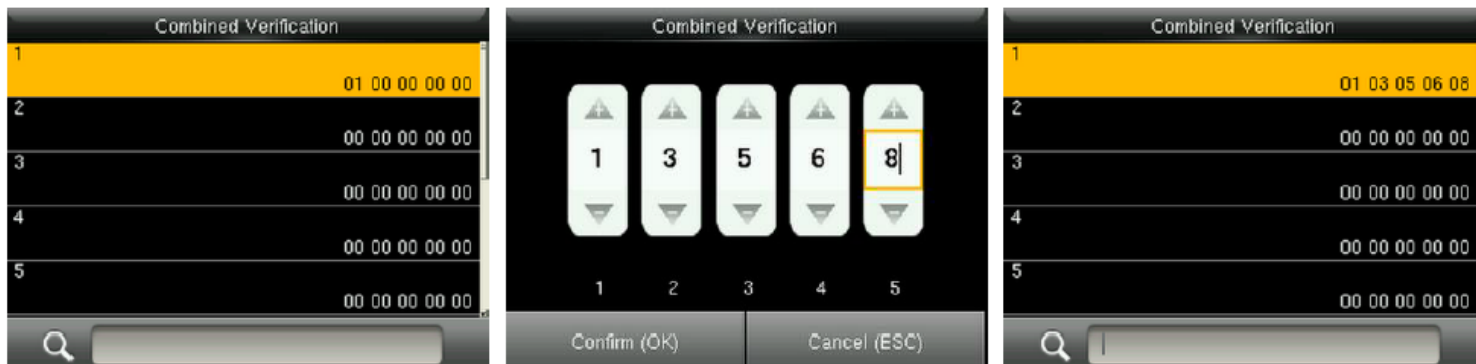
**Observaciones:** Solo los grupos de acceso creados en la interfaz Grupos de Acceso pueden seleccionarse para establecer una Verificación Multi-Usuario.

## Ajustes de Verificación.

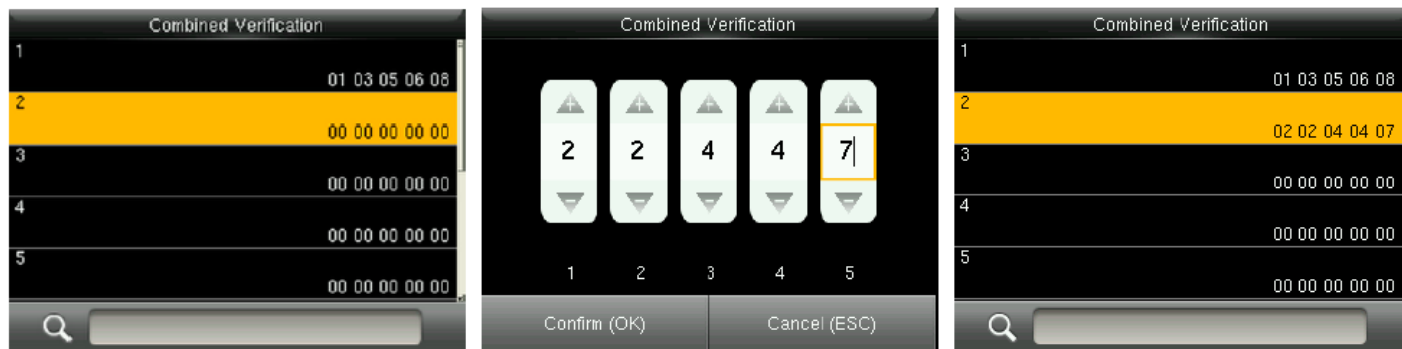


En la interfaz inicial, presione [M/OK] > Control de Acceso > Verificación Multi-Usuario > 1 para entrar a la interfaz de configuración de la primer Verificación Multi-Usuario.

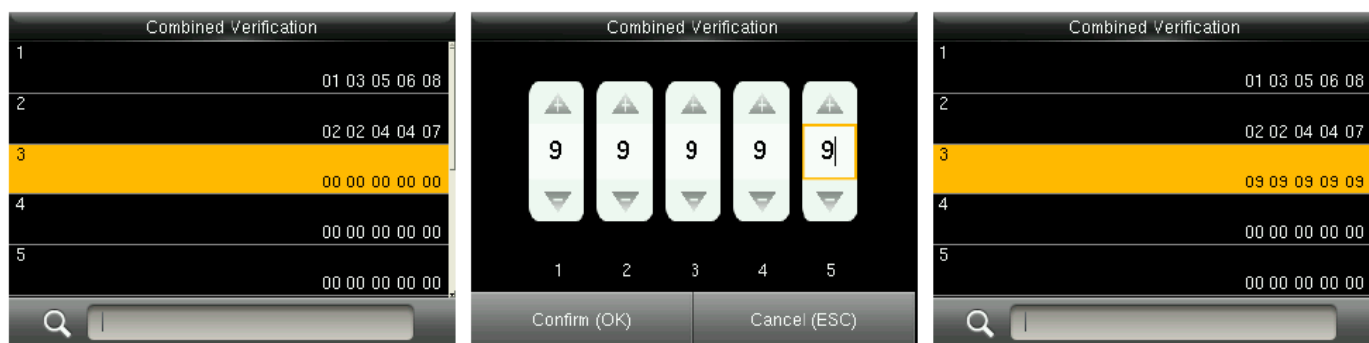
Por ejemplo (los siguientes grupos de acceso ya se han configurado en la interfaz Grupos de Acceso):



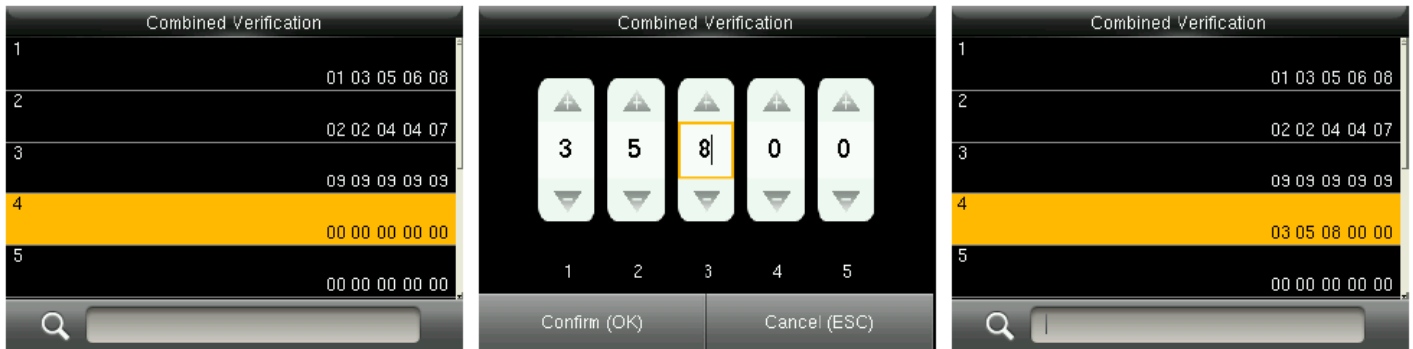
En la figura anterior, la Verificación Multi-Usuario 1 está compuesta de cinco miembros de cinco grupos de acceso diferentes --- Grupo de acceso 1, 3, 5, 6, 8 respectivamente.



En la figura anterior, la Verificación Multi-Usuario 2 está compuesta de cinco miembros de tres grupos de acceso diferentes: dos miembros del grupo de acceso 2, dos miembros del grupo de acceso 4 y un miembro del grupo de acceso 7.



En la figura anterior, la Verificación Multi-Usuario 3 está compuesta de cinco miembros, todos ellos del grupo de acceso 9.

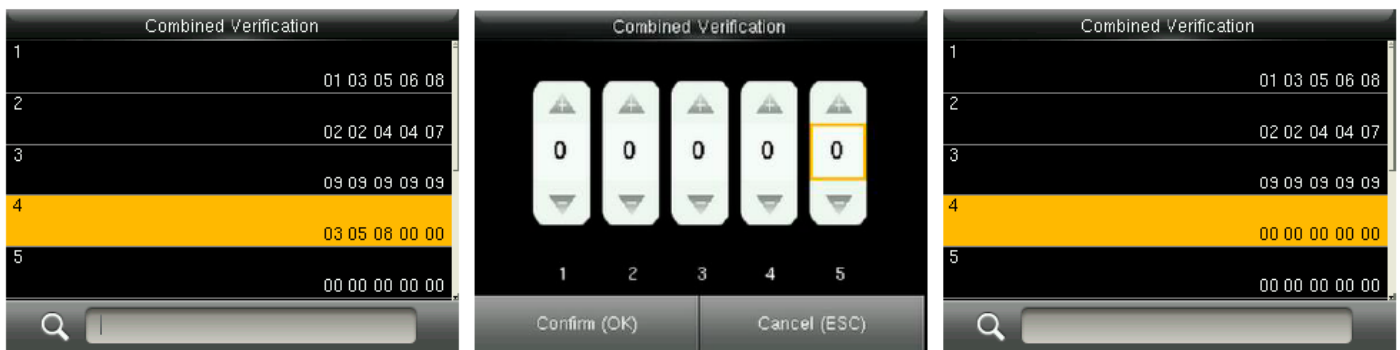


En la figura anterior, la Verificación Multi-Usuario 4 está compuesta de tres miembros de tres grupos de acceso diferentes --- Grupos de acceso 3, 5, 8 respectivamente.

### Eliminar una Verificación Multi-Usuario

Para eliminar una Verificación Multi-Usuario, establece todos los números de grupos de acceso a 0.

Por ejemplo, para eliminar la Verificación Multi-Usuario 4, por favor observe las siguientes figuras:

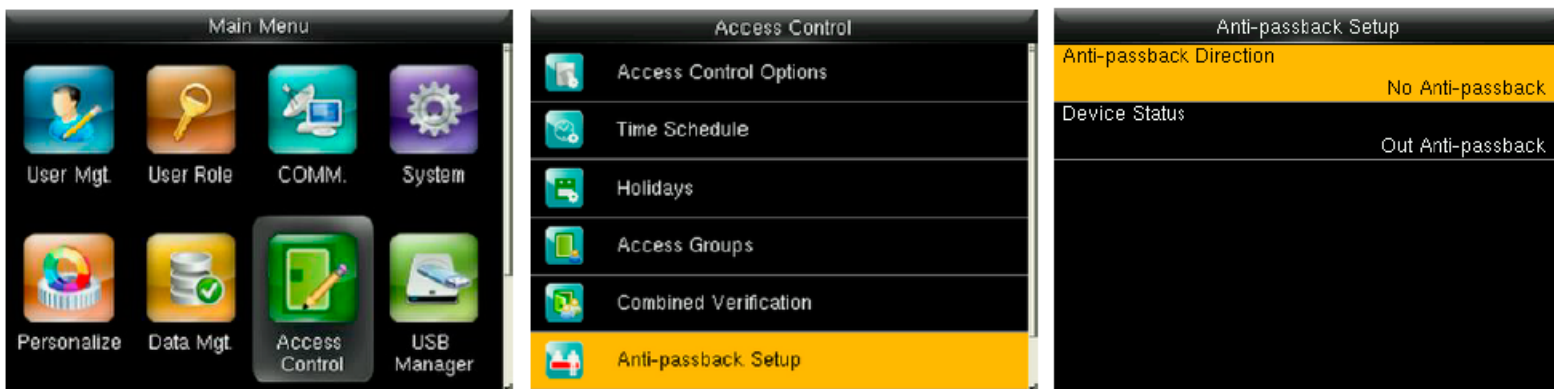
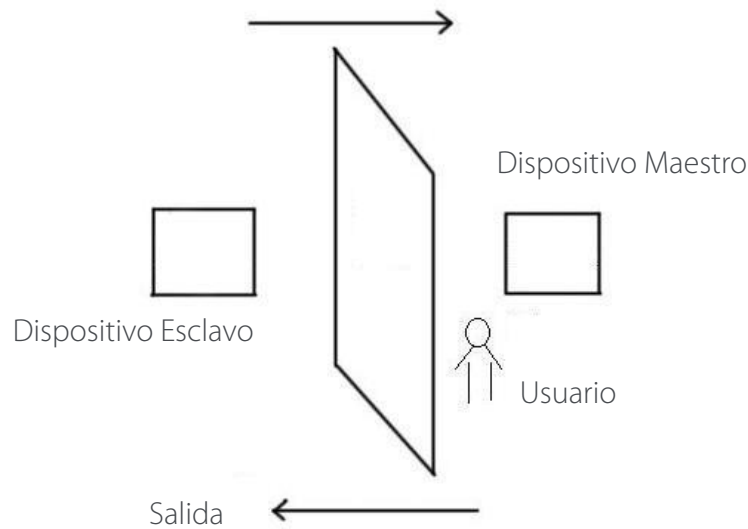


Si todos los números de grupos de acceso de la Verificación Multi-Usuario 4 se establecen a 0, la verificación queda eliminada.

### 7.6 Ajustes Anti-Passback

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

Esta función requiere de 2 dispositivos trabajando juntos: Uno instalado dentro de la puerta (dispositivo maestro) y otro instalado fuera de la puerta (dispositivo esclavo). Ambos dispositivos se comunican a través de una señal Wiegand. El formato Wiegand y el tipo de salida (ID de Usuario/Número de Tarjeta) de ambos dispositivos debe ser consistente.



En la interfaz inicial, presione [M/OK] > Control de Acceso > Ajustes Anti-Passback

- Dirección de Anti-Passback

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

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

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

**Entrada/Salida Anti-Passback:** Después de que el usuario registre una entrada/salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida, y sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada; de lo contrario, se activará la alarma.

**Desactivar y Guardar:** La función Anti-Passback está desactivada, pero el estado de asistencia se guarda.

- Estado del Dispositivo

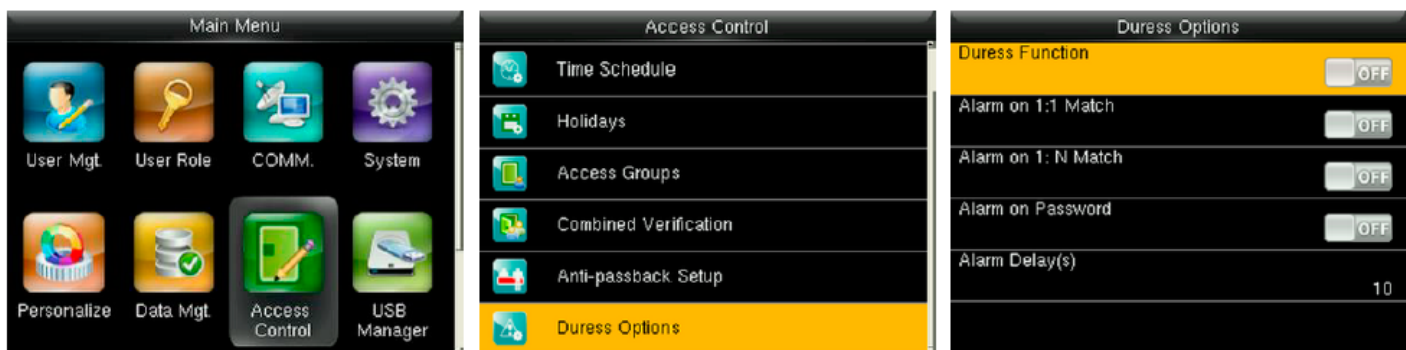
**Ninguno:** Para desactivar la función Anti-Passback.

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

**Entrada:** Todos los registros en el dispositivo son registros de entrada

## 7.7. Ajustes de Opciones de Coacción

Cuando los usuarios se encuentran en una situación de coacción, el dispositivo se encargará de abrir la puerta como de costumbre y enviará la señal de alarma discreta.



En la interfaz inicial pulse [M/OK] > Control de Acceso > Opciones de Coacción para entrar en la interfaz de configuración de opciones de coacción.

**Observaciones:** Los cuatro tipos de métodos de activación de alarma de coacción (Función de coacción, Alarma en Verificación 1:1, Alarma en 1:N y Alarma en contraseña) están desactivados de forma predeterminada.

**Función de Coacción:** Si está activado, presione "Clave de coacción" y, a continuación, presione cualquier huella registrada (en 10 segundos), la alarma de coacción será enviada al verificar con la huella de coacción. Si la función está desactivada, presionar "Clave de coacción" no activará la alarma.

**Alarma en 1:1:** Si está activada, cuando un usuario utilice el método de verificación 1:1 para verificar cualquier huella registrada, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

**Alarma en 1:N:** Si está activada, cuando un usuario utilice el método de verificación 1:N para verificar cualquier huella registrada, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

**Alarma con Contraseña:** Si está activada, cuando un usuario utilice el método de verificación con contraseña para verificar cualquier huella registrada, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

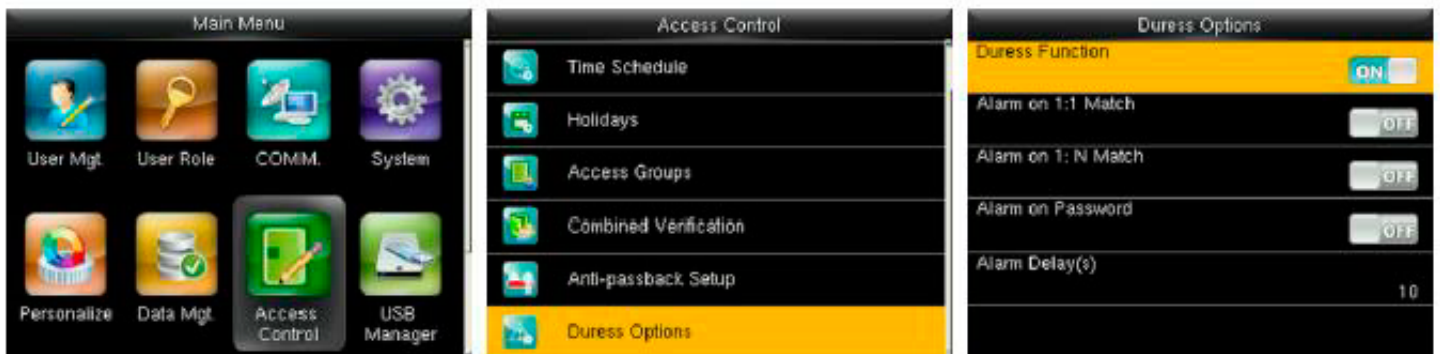
**Retardo de alarma (s):** Cuando se activa la alarma de coacción, el dispositivo enviará una señal de alarma después de 10 segundos (por defecto); el tiempo de retardo de la alarma puede modificarse (el valor varía de 0 a 999 segundos).

## 7.7.1 Configuración de la Tecla de Coacción

**Función de Coacción:** Si está activado, presione “Tecla de coacción” y, a continuación, presione cualquier huella registrada (en 10 segundos), la alarma de coacción será enviada al verificar con la huella de coacción. Si la función está desactivada, presionar “Tecla de coacción” no activará la alarma.

- Para establecer [M/OK] como tecla de coacción.

1. Activar la función de coacción: En la interfaz inicial, pulse [M/OK] > Control de Acceso> Opciones de Coacción> Función de coacción, pulse [M/OK] para activar la función de coacción [ON].



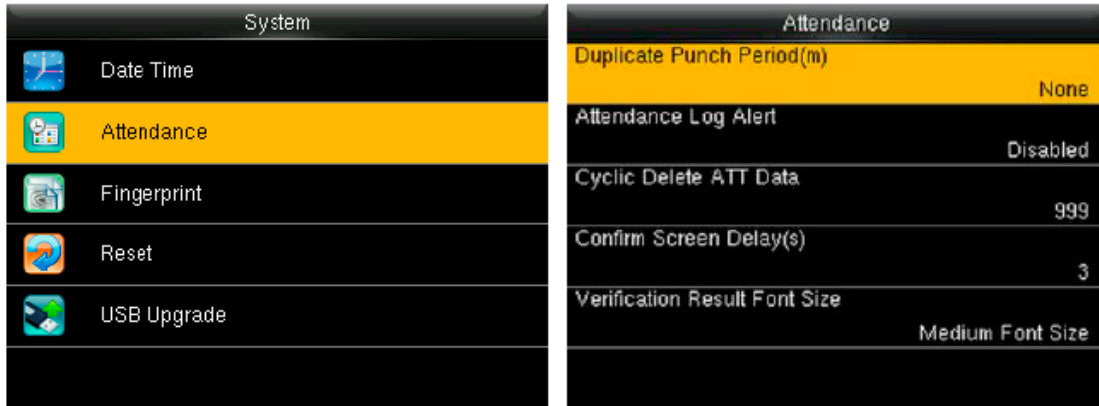
2. Configuración de tecla de coacción: En la interfaz inicial, pulse [M/OK] > Personalizar > Asignación de teclas de atajo > seleccione [M/OK] > pulse [M/OK] > Función > Seleccione la opción “Tecla de coacción”. (El menú de tecla de coacción se mostrará después de que la Función de coacción este activada).



**Observaciones:** Las teclas de dirección y la tecla ESC también pueden configurarse como teclas de coacción.

## 8. Configuraciones de Sistema

### 8.1 Ajustes de Asistencias



En la interfaz inicial, presione [M/OK] > Sistema > Ajustes de Asistencia

**Tiempo de asistencia duplicada (m):** Durante un tiempo definido (Unidad: minutos), los registros de asistencia duplicados no se guardarán (el valor varía de 1 a 999999 minutos).

**Alerta por Memoria Baja:** Cuando la memoria de almacenamiento restante es menor al valor establecido, el dispositivo alertará automáticamente a los usuarios sobre la cantidad de almacenamiento restante. La función puede desactivarse o establecerse a un valor de entre 1 a 9999.

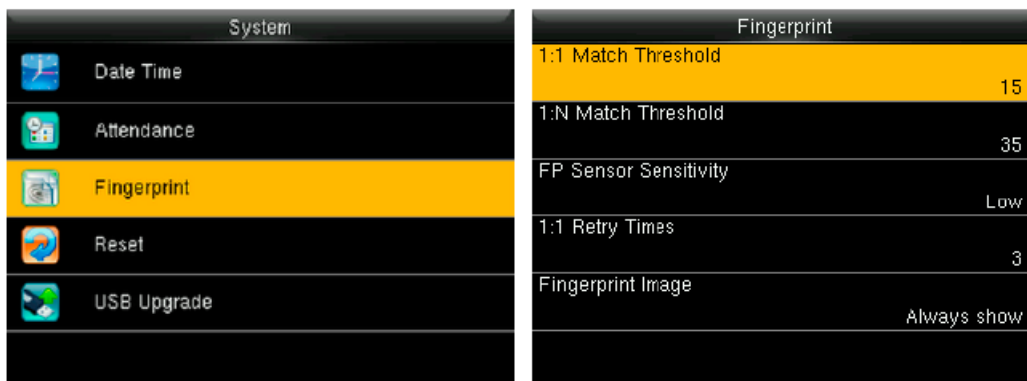
**Limpieza periódica de Eventos:** La cantidad de registros de asistencia que serán eliminados cada vez que se llega a la máxima capacidad de almacenamiento. La función puede desactivarse o establecerse a un valor de entre 1 a 999.

**Duración de Pantalla de Confirmación (s):** El tiempo que se muestra en la pantalla el resultado de las verificaciones. El valor oscila de 1 a 9 segundos.

Por ejemplo, si la Duración de Pantalla de Confirmación se establece en 5s, después de una verificación exitosa, la interfaz de información de verificación se cerrará después de 5 segundos.

**Tamaño de letra del Resultado de Verificación:** Después de la Verificación, se muestra el resultado de la misma. Hay 3 tamaños de letra: Mediano, Grande y Extra-Grande.

### 8.2 Ajustes de Huella Digital





En la interfaz inicial, presione [M/OK] > Sistema > Huella Digital.

**Umbral de Verificación 1:1:** Bajo el método de verificación 1:1, la verificación sólo será exitosa cuando la similitud entre la huella digital a verificar y la huella registrada del usuario sea mayor al valor establecido.

**Umbral de Verificación 1:N:** Bajo el método de verificación 1:N, la verificación sólo será exitosa cuando la similitud entre la huella digital a verificar y las huellas registradas sea mayor al valor establecido.

**Umbral de Verificación Recomendado:**

		Umbral de Verificación	
FRR	FAR	1:N	1:1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

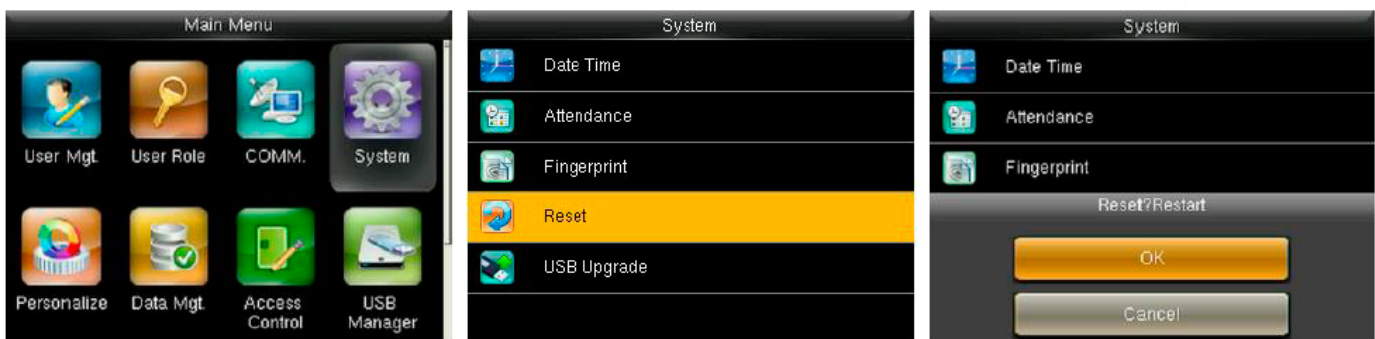
**Sensibilidad del Sensor de Huellas:** Se recomienda dejar el valor predeterminado "Medio". Cuando el ambiente sea seco y la detección de huellas sea lenta, puede establecer el nivel a "Alto" para aumentar la sensibilidad. Cuando el ambiente sea húmedo, haciendo difícil la detección de huellas, puede establecer el nivel a "Bajo".

**Reintentos 1:1:** Este parámetro es utilizado para establecer el número de reintentos en el caso de que ocurran errores en la verificación 1:1 o en la verificación con contraseña debido a que el dedo se presiona incorrectamente o a que el usuario olvidó su contraseña. Para evitar tener que volver a escribir el ID del usuario, se permiten los reintentos. El número de reintentos puede oscilar entre 1 a 9.

**Imagen de la Huella Digital:** Esta función determina si desea mostrar la imagen de la huella digital durante el registro o verificación de estas. Hay 4 opciones disponibles: Mostrar en registro, Mostrar en Verificación, Siempre mostrar, No mostrar.

### 8.3 Restablecer Valores de Fábrica.

Restablece información tal como Ajustes de Comunicación o de Sistema a los ajustes de fábrica.



En la interfaz inicial, presione [M/OK] > Sistema > Restablecer > OK para restablecer los valores de fábrica. Los ajustes que se restablecen incluyen las opciones de Control de Acceso, configuraciones de Coacción, configuraciones Anti-passback, configuraciones de Red (esto es, las configuraciones ethernet, comunicación serial, Conexión a PC, WIFI, ADMS ★ y configuraciones Wiegand), Configuraciones de Personalización (como Voz, Sonido del Teclado, Volumen y Tiempo de Espera para Reposo), cerrar estado de asistencia, etc.



Parámetros	Por defecto
Opciones de Control de Acceso	Retardo de puerta: 10 seg
	Retardo del sensor de puerta: 10 seg
	Tipo de sensor de puerta: Ninguno
	Retardo de alarma de puerta: 30 seg
	Tiempos de reintento de alarma: 3 veces
	Periodo de Tiempo NC: Ninguno
	Periodo de Tiempo NO: Ninguno
	Normalmente abierto/cerrado en días festivos: Desactivado
Opciones de Amago	Función de Amago: Desactivada
	Alarma en verificación 1:1: Apagada
	Alarma en verificación 1:N: Apagada
	Alarma en verificación con contraseña: Apagada
	Retraso de Alarma: 10 segundos
	Alarma de Contraseña: Apagado
	Retardo de Alarma: 10 seg
Anti-Passback	No Anti-passback
Ethernet	Dirección IP: 192.168.1.201
	Máscara de Subred: 255.255.255.0
	Puerta de Enlace: 0.0.0.0
Conexión a PC	Clave de Comunicación: 0 (ninguno)
	ID de Dispositivo: 1
Wi-Fi	DHCP: Desactivado
	Dirección IP: 0.0.0.0
	Máscara de Subred: 255.255.255.0
	Puerta de enlace: 0.0.0.0
ADMS ★	Activar Nombre de Dominio: Desactivado
	Dirección de Servidor: 0.0.0.0
	Puerto de Servidor: 8081
	Activar Servidor Proxy: Activado
	Dirección IP de servidor Proxy: 0.0.0.0
	Puerto de Servidor Proxy: 0
Configuración Wiegand	Tipo de ID de Entrada/Salida Wiegand: ID de Usuario
	Amplitud de Pulso: 100 us
	Intervalo de Pulso: 1000 us
Tiempo de Espera para Diapositivas	30 segundos
Tiempo de Espera para Reposo	30 Segundos
Tiempo de Espera del Menú	60 Segundos
Sonido del Teclado	Activado
Sonido de Voz	Activado
Volumen	70

**Observaciones:** Al restablecer a los valores de fábrica, la hora y fecha no se verán afectadas. Por ejemplo, si la fecha y hora del dispositivo es 18:30 del 1 de enero de 2020, la fecha y hora se mantendrá igual después de restablecer los valores de fábrica.

## 8.4 Actualización por USB

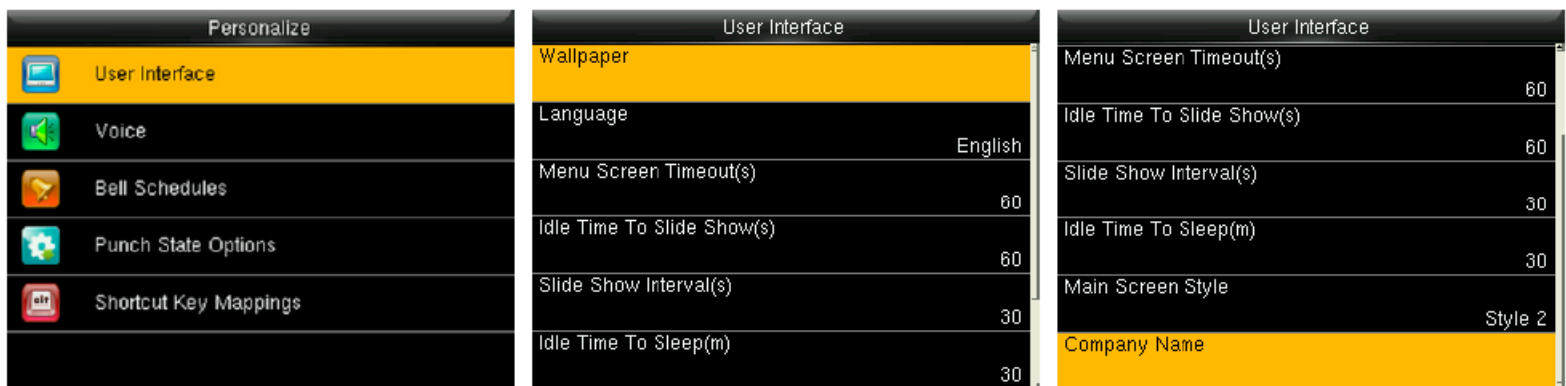


Inserte la Unidad USB con el archivo de actualización en el puerto USB del dispositivo, y en la interfaz inicial presione [M/OK] > Sistema > Actualización por USB para completar la operación de actualización de firmware.

**Nota:** Si necesita un archivo de actualización, póngase en contacto con nuestro soporte técnico. La actualización de Firmware no se recomienda bajo circunstancias normales

## 9. Configuraciones de Personalización

### 9.1 Ajustes de Interfaz de Usuario



En la interfaz inicial, presione [M/OK] > Personalizar > Interfaz de Usuario.

**Fondo de Pantalla:** Seleccione la imagen a utilizar como fondo de pantalla, puedes encontrar varios estilos dentro del dispositivo.

**Idioma:** Seleccione el idioma del dispositivo.

**Tiempo de Espera del Menú (s):** El dispositivo vuelve automáticamente a la interfaz inicial si no se hace ninguna operación después del periodo de tiempo seleccionado (el rango es de 60 a 99999 segundos). Esta función puede ser desactivada.

**Observaciones:** Si se desactiva esta opción, el sistema no regresará a la interfaz inicial cuando no haya ninguna operación. No se recomienda desactivar esta función debido al alto consumo de energía y a que representaría un problema de seguridad.

**Tiempo de Espera para Diapositivas (s):** Cuando no se haga ninguna operación en la interfaz inicial después del periodo de tiempo seleccionado, iniciará una presentación de diapositivas. Esta opción puede desactivarse (elija "Ninguno") o establecerse entre 3 a 999 segundos.

**Intervalo de tiempo para Dispositivos (s):** Se refiere al intervalo de tiempo entre dispositivos diferentes. Puede desactivarse o establecerse entre 3 a 999 segundos.

**Tiempo de espera para Reposo (m):** Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Presione cualquier tecla para sacar al dispositivo del estado de reposo. El rango de espera es de 1 a 999 minutos. Esta función se puede desactivar.

**Observaciones:** No se recomienda desactivar esta función debido al alto consumo de energía.

**Estilo de la Pantalla Principal:** Seleccione la posición y forma del reloj y teclas de estado de la pantalla inicial.

**Nombre de la empresa:** Introduzca el nombre de la empresa.

**Estilo de la Pantalla Principal:** Seleccione la posición y forma del reloj y teclas de estado de la pantalla inicial.

**Nombre de la empresa:** Introduzca el nombre de la empresa.

## 9.2 Ajustes de Voz



En la interfaz inicial, presione [M/OK] > Personalizar > Voz

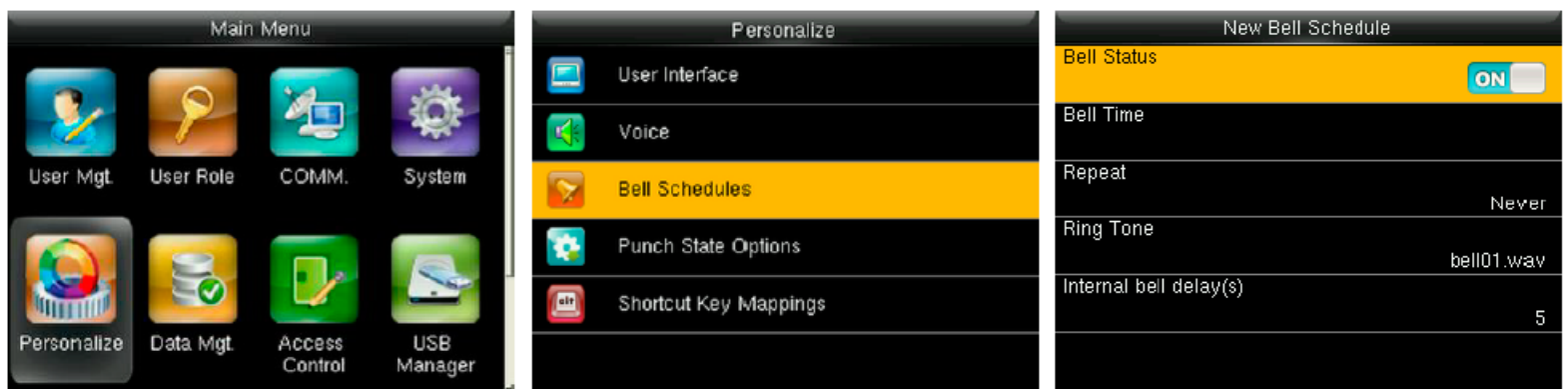
**Sonido de Voz:** Seleccione si desea activar los mensajes de voz durante la operación del dispositivo. Presione [M/OK] para activarlo.

**Sonido de Teclado:** Seleccione si desea activar el sonido al tocar el teclado. Presione [M/OK] para activarlo.

**Volumen.** - Ajuste el volumen del dispositivo. Presione > para incrementar el volumen, presione < para disminuirlo.

### 9.3 Ajustes de Timbre

Muchas empresas eligen utilizar un timbre para dar aviso del inicio/fin de la jornada laboral. Cuando llegue la hora programada de un timbre, el dispositivo hará sonar automáticamente el tono seleccionado durante el tiempo establecido por el usuario.



En la interfaz inicial, presione [M/OK] > Personalizar > Timbres Programados > Nuevo Horario de Timbre.

**Estado del Timbre:** ON es para activar el timbre, OFF es para desactivarlo.

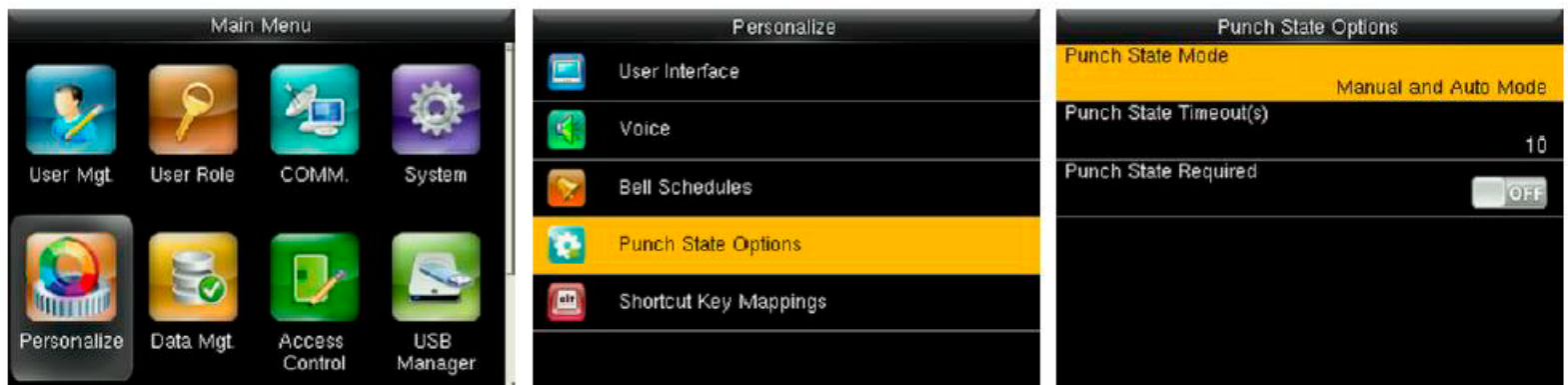
**Hora de Timbre:** El timbre suena automáticamente cuando se llega a la hora especificada.

**Repetir:** Establecer si el timbre se repite de lunes a domingo.

**Tono de Timbre:** El tono que suena como timbre.

**Duración del Timbre:** Para establecer la duración del timbre. El valor oscila entre 1 a 999 segundos.

### 9.4 Ajustes de Estados de Asistencia



En la interfaz inicial, presione [M/OK] > Personalizar > Opciones de Estados de Asistencia

**Modo de Estado de Asistencia:** Esta opción es para seleccionar el Estado de Asistencia. Las siguientes opciones están disponibles:

1. **Apagado:** El Estado de Asistencia no es utilizado. El Estado de Asistencia definido en Asignación de Teclas de Atajo queda inhabilitado.

2. **Modo Manual:** Los Estados de Asistencia son cambiados manualmente y el Estado de Asistencia actual desaparecerá cuando transcurra el Tiempo de Espera del Estado de Asistencia.

3. **Modo Automático:** Cuando se elige este modo, establezca la hora de cambio de estado en Asignación de Teclas de Atajo. Cuando llegue la hora establecida, el Estado de Asistencia cambiará automáticamente.

4. **Modo Manual & Automático:** La interfaz principal muestra los Estados de Asistencia que cambian automáticamente y además usted tiene la opción de cambiar el Estado de Asistencia manualmente. Un Estado de Asistencia que usted seleccione manualmente cambiará automáticamente cuando pase el tiempo de espera configurado.

5. **Modo Fijo Manual:** Cuando el Estado de Asistencia sea cambiado manualmente, se mantendrá fijo hasta que sea cambiado manualmente de nuevo.

6. **Modo Fijo:** Un Estado de Asistencia es siempre mostrado y no puede ser cambiado.

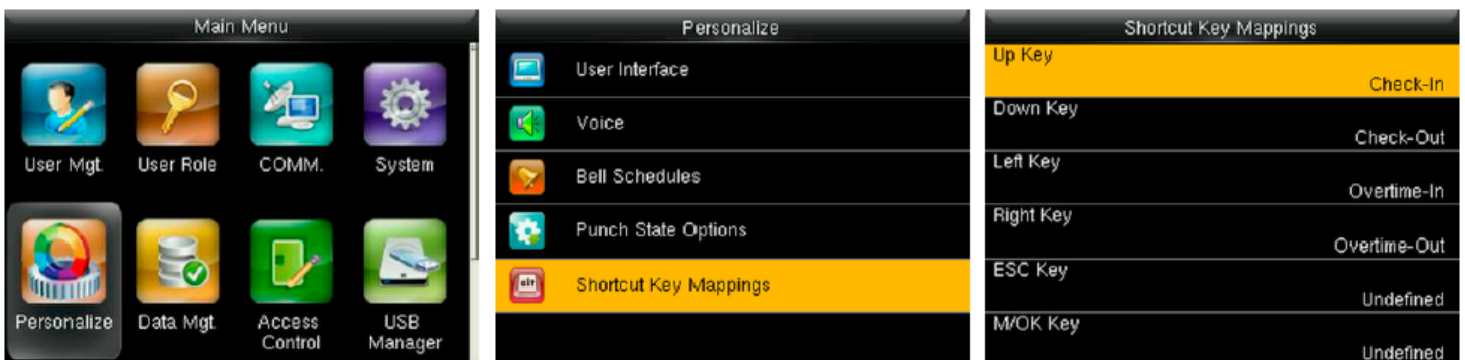
**Tiempo de Espera del Estado de Asistencia (s):** Especificar el tiempo que se muestra el Estado de Asistencia seleccionado. El valor varía de 5 a 999 segundos.

**Estado de Asistencia Requerido:** Especificar si el Estado de Asistencia debe ser seleccionado durante la verificación.

**Observaciones:** Hay 4 Estados de Asistencia: Entrada, Salida, Entrada a Tiempo Extra y Salida de Tiempo Extra.

## 9.5 Asignación de Teclas de Atajo

Usted puede definir Teclas de que sirvan de atajo hacia un Estado de Asistencia o hacia funciones del menú. Cuando el dispositivo se encuentre en la interfaz principal, oprima la Tecla de Atajo correspondiente para mostrar un Estado de Asistencia o para acceder a la interfaz de un menú de operaciones.



En la interfaz inicial, presione [M/OK] > Personalizar > Asignación de Teclas de Atajo.

Para establecer la hora de cambio automático de Estado.

Elija cualquier tecla de atajo, seleccione **[Opciones de Estado de Asistencia]** en **[Funciones]**, de forma que se pueda establecer la hora para el cambio automático de Estado de Asistencia.

**Cambio Automático:** Cuando llegue la hora establecida, el dispositivo cambiará el Estado de Asistencia automáticamente.

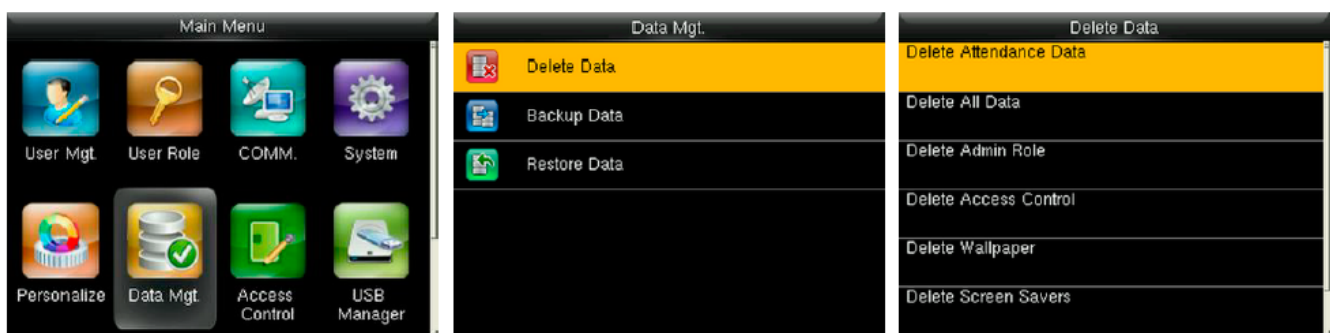


Cuando una tecla de atajo tenga asignada un Estado de Asistencia, pero el **[Modo de Estado de Asistencia]** está establecido en desactivado **[OFF]** (Personalizar > Opciones de Estado de Asistencia > Modo de Estado de Asistencia > Seleccionar OFF), la tecla de atajo no estará activada.

## 10. Gestión de Datos

### 10.1. Borrar Datos

Aquí puede gestionar los datos en el dispositivo, que incluye borrar registros de eventos, borrar todos los datos, borrar privilegios de administrador, borrar protectores de pantalla, etc.



En la interfaz inicial, presione **[M/OK]** > Gestión de Datos > Borrar Datos.

**Borrar Registros de Acceso:** Eliminar todos los registros de acceso guardados en el dispositivo o borrar registros de acceso de un rango de tiempo específico.

**Borrar Todo:** Eliminar toda la información de los usuarios, huellas digitales, registros de acceso, etc.

**Borrar Privilegios de Administrador:** Convertir a todos los administradores en usuarios normales.

**Borrar Control de Acceso:** Borrar todos los datos de acceso.

**Borrar Fondo de Pantalla:** Eliminar todos los fondos de pantalla en el dispositivo.

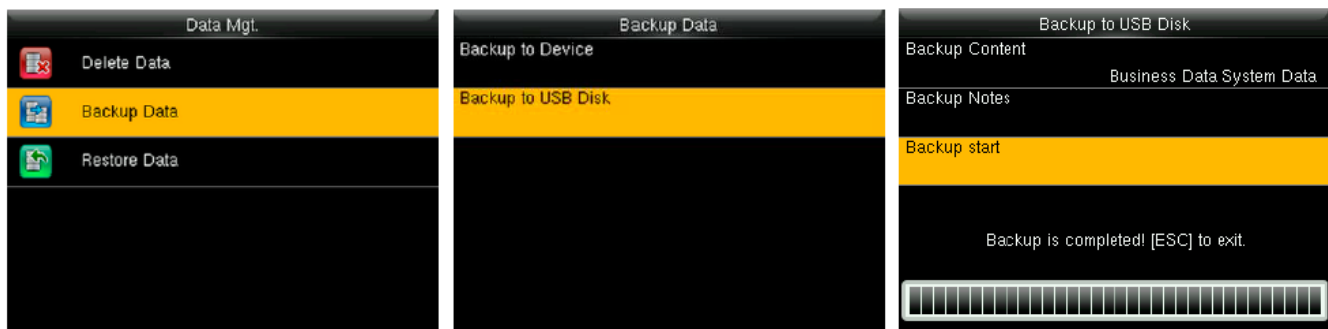
**Borrar Protectores de Pantalla:** Eliminar protectores de pantalla seleccionados o todos los protectores de pantalla en el dispositivo. (Para más detalles sobre cargar protectores de pantalla, favor de consultar 17.3 Procedimiento para Cargar Imágenes)

**Borrar Datos de Respaldo:** Eliminar los datos pertenecientes a la copia de seguridad.

## 10.2 Respaldo de Datos

Usted puede respaldar los datos de la empresa o datos de configuración en el dispositivo o unidad USB.

### Respaldo en Unidad USB



Inserte la unidad USB. En la interfaz inicial, presione [M/OK] > Gestión de Datos > Respaldo Datos > Respaldo en Unidad USB > Respaldo Contenido > Elija el contenido que quiere respaldar (Datos de la empresa / Datos del Sistema) > Iniciar respaldo para iniciar el respaldo. No es necesario reiniciar el dispositivo después de concluir el respaldo.

**Observaciones:** Los pasos para Respaldo en el Dispositivo son los mismos que para Respaldo en Unidad USB.

## 10.3 Restauración de Datos

Sirve para restaurar datos almacenados en el dispositivo o en una unidad USB hacia el dispositivo.

### Restaurar desde Unidad USB





Inserte la unidad USB. En la interfaz inicial, presione [M/OK] > Gestión de Datos > Restaurar Datos > Restaurar desde Unidad USB > Contenido > Elija el contenido que quiere restaurar (Datos de la empresa / Datos del Sistema) > Iniciar Restauración > Seleccione SI para iniciar la restauración. Cuando la restauración finalice, pulse [OK] para reiniciar el dispositivo.

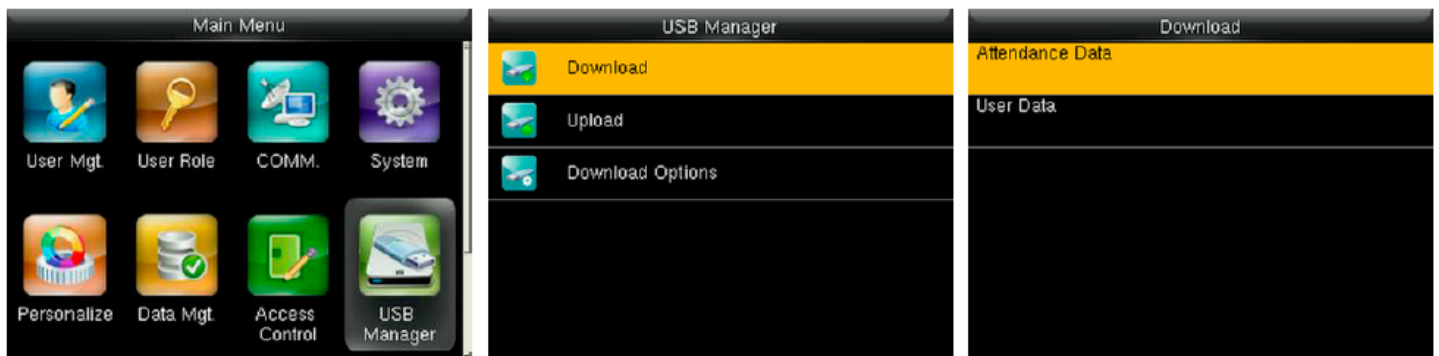
Observaciones: Los pasos para Restaurar Datos desde Dispositivo son los mismos que para Restaurar Datos desde Unidad USB.

## 11. Gestión USB

Usted puede exportar información desde el dispositivo a un software relevante para su procesamiento, o importar datos de usuarios hacia el dispositivo por medio de una unidad USB.

Antes de cargar/descargar datos desde/en una unidad USB, inserte la unidad en el puerto USB del dispositivo.

### 11.1 Descargar en USB



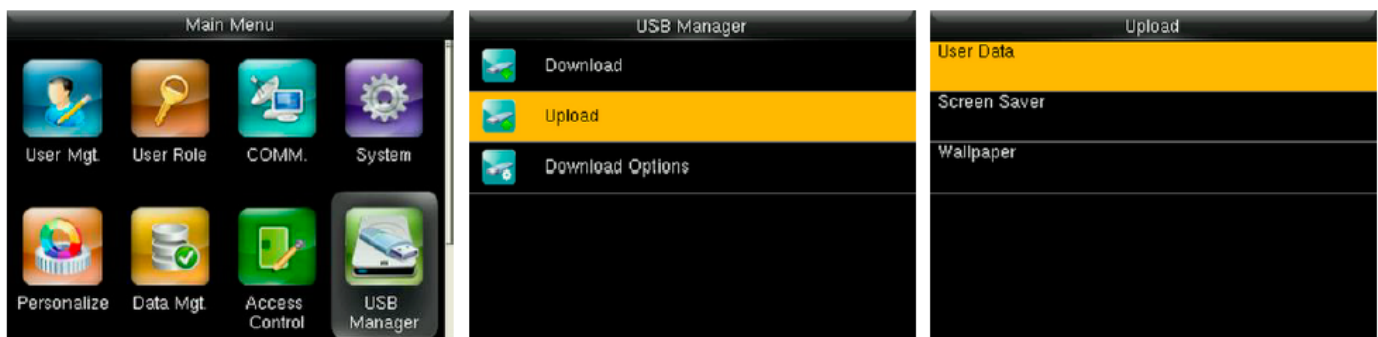
En la interfaz inicial, presione [M/OK] > Gestión USB > Descargar.

El horario solo está disponible para elegirse al descargar registros de asistencia.

**Descargar registros de asistencia.** - Descargar registros de acceso de un periodo de tiempo específico en la unidad USB.

**Datos de Usuario.** - Descargar toda la información de usuarios y huellas digitales del dispositivo en la unidad USB.

### 11.2 Cargar desde USB





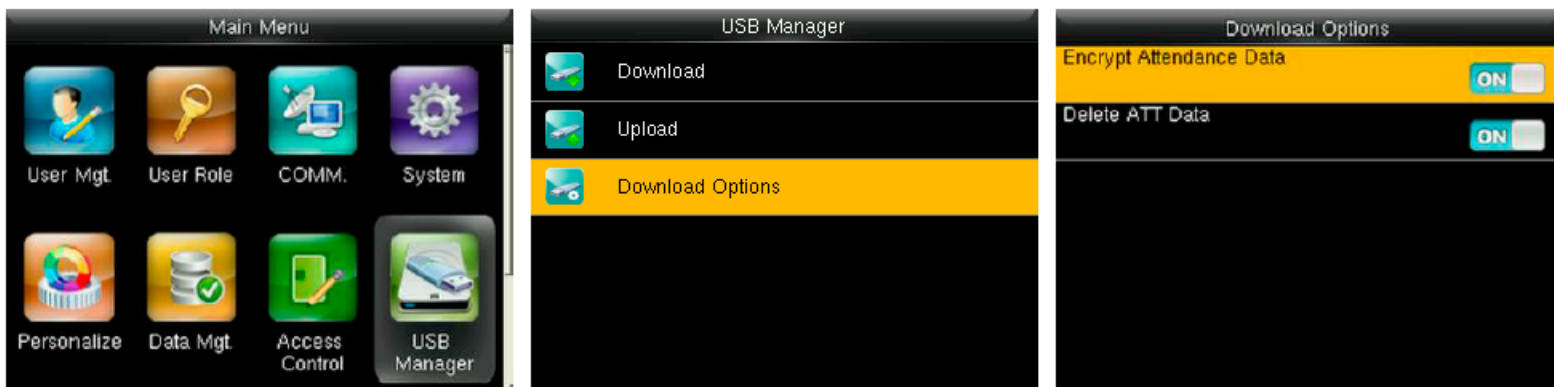
En la interfaz inicial, presione [M/OK] > Gestión USB > Cargar.

**Datos de Usuario.** - Cargar toda la información de usuario y huellas digitales desde la unidad USB al dispositivo. Protector de Pantalla. - Para cargar protectores de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. Las imágenes se mostrarán en la interfaz de espera del dispositivo después de la carga. Para las especificaciones de protectores de pantalla, consulte la sección [17.3 Procedimiento para Cargar Imágenes](#).

**Fondo de Pantalla.** - Para cargar fondos de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. Las imágenes se mostrarán en la pantalla principal después de la carga. Para las especificaciones de fondos de pantalla, consulte la sección [17.3 Procedimiento para Cargar Imágenes](#).

### 11.3 Ajustes de Opciones de Descarga

Para encriptar los datos de asistencia en la unidad USB o borrar los datos de asistencia.



En la interfaz inicial, presione [M/OK] > Gestión USB > Opciones de Descarga para entrar a la interfaz de Opciones de Descarga.

Presione [M/OK] para activar o desactivar las opciones [Encriptar Datos de Asistencia] o [Eliminar datos de Asistencia].

**Observaciones:** Los datos de asistencia encriptados solo pueden importarse en el software ZKAccess3.5.

## 12. Búsqueda de Registros

Cuando los usuarios verifican exitosamente, se guarda un registro en el sistema. Esta función permite a los usuarios ver registros de acceso/asistencia.



Personel Kart Yönetimi		
Tarih	Kull. ID	Devamlılık
11-01		Kayıt sayısı:11
	1	11:42 11:12 10:20 10:19 10:18 10:17 10:17 10:15 10:10 10:09 10:06
10-31		Kayıt sayısı:14
	1	15:48 15:48 15:11 15:10 14:21 11:09 11:08 09:14 09:12 09:11 09:11 09:08 09:08 09:08

Önceki : Sol Tuşu Sonraki : Sağ Tuşu Detaylar : O K

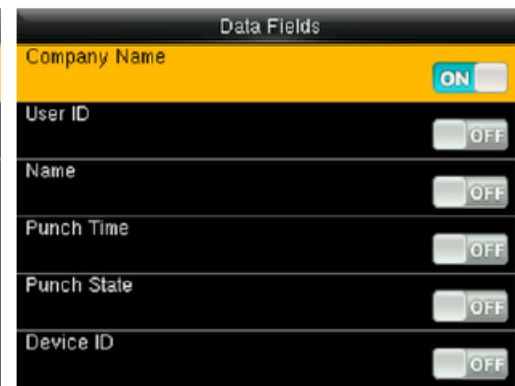
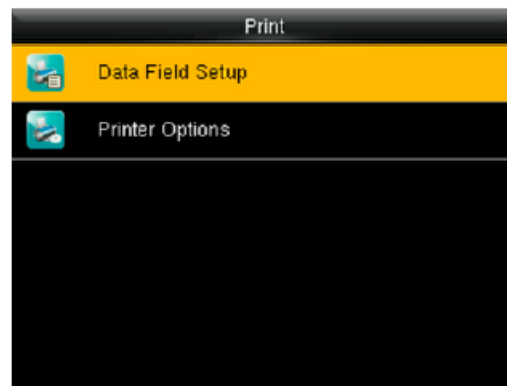
En la interfaz inicial, presione [M/OK] > Búsqueda de Asistencia > Introduzca un ID de Usuario (Si no se introduce un ID, se buscan todos los registros) > Seleccione un Rango de Tiempo > presione [M/OK], los registros de asistencia correspondientes se mostrarán.

**Observaciones:** Los datos de asistencia encriptados solo pueden importarse en el software ZKAccess3.5.

## 13 Ajustes de Impresión ★

Los dispositivos con la función de Impresión pueden imprimir registros de asistencia cuando se les conecta una impresora (esta función es opcional y solo puede ser agregada en algunos productos).

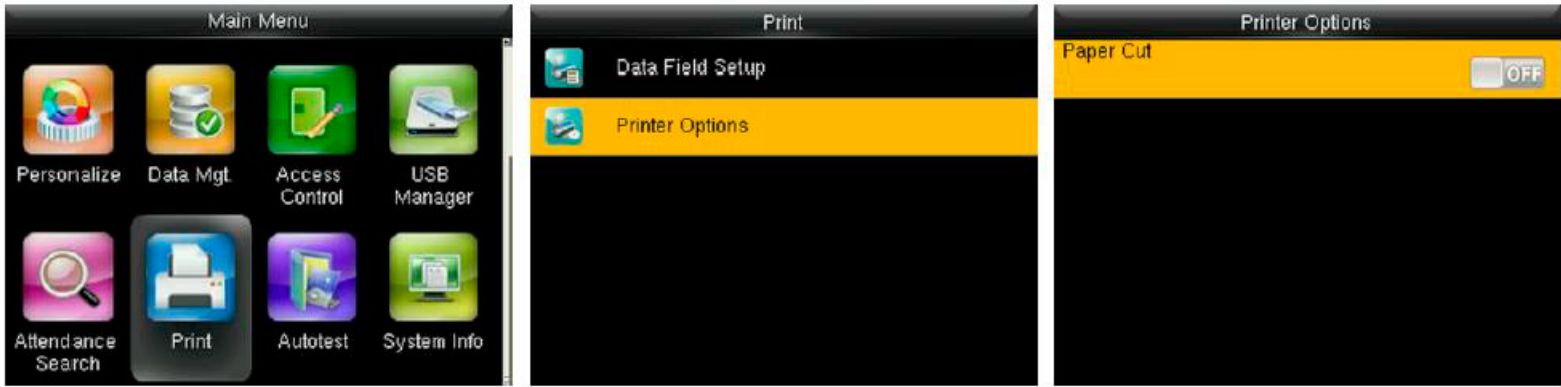
### 13.1 Ajustes de Impresión de Campos de Datos



En la interfaz inicial, presione [M/OK] > Imprimir > Configurar Campos de Datos > Presione [M/OK] para activar o desactivar los campos que necesite imprimir.

**Observaciones:** Al imprimir, la posición de la información de los campos puede ajustarse por las teclas izquierda/derecha: Presione la tecla izquierda para moverse al elemento anterior y presione la tecla derecha para moverse al siguiente elemento.

## 13.2 Ajustes de Opciones de Impresión

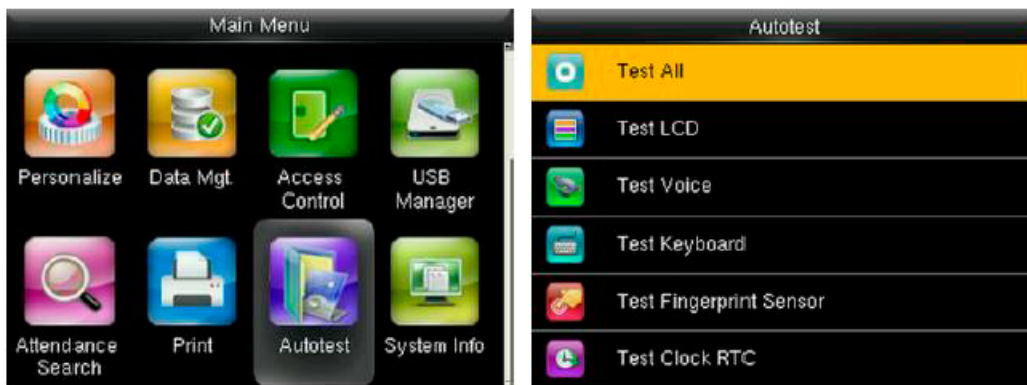


En la interfaz inicial, presione [M/OK] > Imprimir > Opciones de Impresión > Presione [M/OK] para activar o desactivar la función Corte de Papel.

**Observaciones:** Para activar la función Corte de Papel, es necesario conectar el dispositivo a una impresora con esa función, de forma que la impresora pueda cortar el papel de acuerdo a la información seleccionada.

## 14. Pruebas

Las pruebas automáticas permiten al dispositivo comprobar el correcto funcionamiento de sus módulos, incluyendo la pantalla LCD, sonido, sensor de huellas, teclado, cámara★ y reloj de tiempo real.



En la interfaz inicial, presione [M/OK] > Pruebas.

**Probar Todo:** Probar pantalla LCD, sonido, teclado, sensor de huellas, cámara y reloj. Durante la prueba, presione [M/OK] para continuar a la siguiente prueba, o presione [ESC] para salir de la prueba.

**Probar LCD:** Probar los efectos de color de la pantalla LCD mostrando imágenes en colores vivos, blanco y negro para comprobar si la pantalla está funcionando adecuadamente. Durante la prueba, presione [M/OK] para continuar a la siguiente prueba, o presione [ESC] para salir de la prueba.

**Probar Sonido:** La terminal probará automáticamente si los archivos de voz están completos y que la calidad del sonido sea la adecuada reproduciendo los archivos de sonido almacenados dentro de la misma. Durante la prueba, presione [M/OK] para continuar a la siguiente prueba, o presione [ESC] para salir de la prueba.

**Probar Teclado:** Probar si todas las teclas funcionan correctamente. Presione cualquier tecla en la interfaz de pruebas de Teclado; si la tecla presionada coincide con el símbolo que se muestra en pantalla, la tecla funciona correctamente. Presione [M/OK] o [ESC] para salir de la prueba.

**Probar Sensor de Huellas:** Probar si el sensor de huellas digitales encuentra funcionando con normalidad y si la calidad de las imágenes de las huellas es apta. Cuando el usuario presione el dedo en el sensor, la imagen de la huella será mostrada en pantalla. Presione [M/OK] o [ESC] para salir de la prueba.

**Probar Reloj RTC:** Probar el Reloj en Tiempo Real. La terminal revisará el rendimiento del reloj examinando el cronómetro. Presione [M/OK] para iniciar el conteo, presione [M/OK] de nuevo para detenerlo y ver si el cronómetro toma el tiempo de forma precisa. Presione [ESC] para salir de la prueba.

## 15. Información del Sistema

Con este parámetro usted puede ver la capacidad de almacenamiento de datos, información del dispositivo y del firmware.



En la interfaz inicial, presione [M/OK] > Información de Sistema.

Device Capacity	
User (used/max)	3/5000
Admin User	0
Password	2
Fingerprint (used/max)	9/1000
Badge (used/max)	2/5000
ATT Record (used/max)	6/30000

Capacidad del Dispositivo

Device Info	
Device Name	
Serial Number	3985163200003
MAC Address	00:17:61:12:2e:48
Fingerprint Algorithm	
Platform Information	
Manufacturer	

Información del Dispositivo

Firmware Info	
Firmware Version	Ver 8.0.4.1-20160620
Bio Service	Ver 2.1.12-20160812
Push Service	Ver 2.0.22-20160810
Standalone Service	Ver 2.1.0-20160819
Dev Service	Ver 2.0.1-20160820
System Version	Ver 16.8.8-20160712

Firmware del Dispositivo


**Capacidad del Dispositivo:** Muestra la cantidad de usuarios registrados, administradores, contraseñas, huellas digitales, tarjetas, registros, también muestra la capacidad total de almacenamiento de usuarios, huellas, tarjetas y registros.

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

**Información de Firmware:** Muestra la versión de firmware, Servicio Bio, Servicio Push, y Servicio Dev.

**Observaciones:** La forma en que se muestra la capacidad del dispositivo, información del dispositivo y de firmware en la interfaz de información de sistema de diferentes productos puede variar; prevalecerá el producto real.

## 16. Resolución de Problemas

- **El sensor de huellas no puede leer y verificar una huella de forma efectiva.**
  - Revise si el dedo está mojado o si el sensor de huella está mojado o polvoriento.
  - Limpie el dedo y sensor de huellas e intente de nuevo.
  - Si el dedo está muy seco, soplelo e intente de nuevo.
  
- **Se muestra el mensaje “Horario Inválido” después de una verificación.**
  - Contacte al administrador para verificar si el usuario tiene privilegio de acceder dentro de ese horario.
  
- **La verificación se realiza con éxito, pero el usuario no puede abrir la puerta.**
  - Revise si el privilegio del usuario está establecido correctamente.
  - Revise si el cableado de la cerradura es correcto.
  
- **Suena la alarma Anti-Sabotaje**
  - Revise si el dispositivo y la placa posterior están unidas; si no, el botón de alarma de sabotaje en la parte trasera del dispositivo se activará y lanzará una alarma, el icono  aparecerá en la esquina superior derecha de la interfaz. Sólo cuando la función [Alarma de Altavoz] (Control de Acceso > Opciones de Control de Acceso > Alarma de Altavoz) esté activada, el altavoz lanzará una alarma.

## 17. Anexos

### 17.1 Especificaciones

Capacidad de Huellas	1.000
Capacidad de Tarjetas	5.000
Capacidad de Eventos	30.000
Pantalla	LCD TFT a Color de 2.4 Pulgadas
Indicador LED	Rojo/Verde
Comunicación	Ethernet (10/1000M), RS232, RS485, USB-Host, Wi-Fi
Señal Wiegand	Entrada/Salida Wiegand
Velocidad de Reconocimiento	≤ 2 seg
FAR	≤ 0.0001%
FRR	≤ 1%
Temperatura de Operación	0 – 45°C
Fuente de Alimentación	12V/3A
Voltaje	12V
Corriente	3A
Puertos de Control de Acceso	Cerradura, Alarma, Botón de Salida, Lector y Sensor de Puerta

### 17.2 Introducción a Wiegand

El protocolo Wiegand26 es un protocolo estándar de control de acceso desarrollado por el Subcomité de Estándar de Control de Acceso afiliado a la Asociación de la Seguridad Industrial (SIA por sus siglas en inglés). Es un protocolo usado para puertos y salidas de lectores de tarjetas IC sin contacto.

El protocolo define la conexión entre el lector de tarjetas y el controlador los cuales son ampliamente usados en la industria del control de acceso, seguridad, entre otras. Esto ha estandarizado el trabajo de los diseñadores de lectores de tarjetas y fabricantes de controladores. Los dispositivos de control de acceso producidos por nuestra empresa también aplican este protocolo.

#### Señal Digital

La figura 1 muestra el diagrama secuencial del lector de tarjetas que envía señales digitales en bits hacia el controlador de acceso.

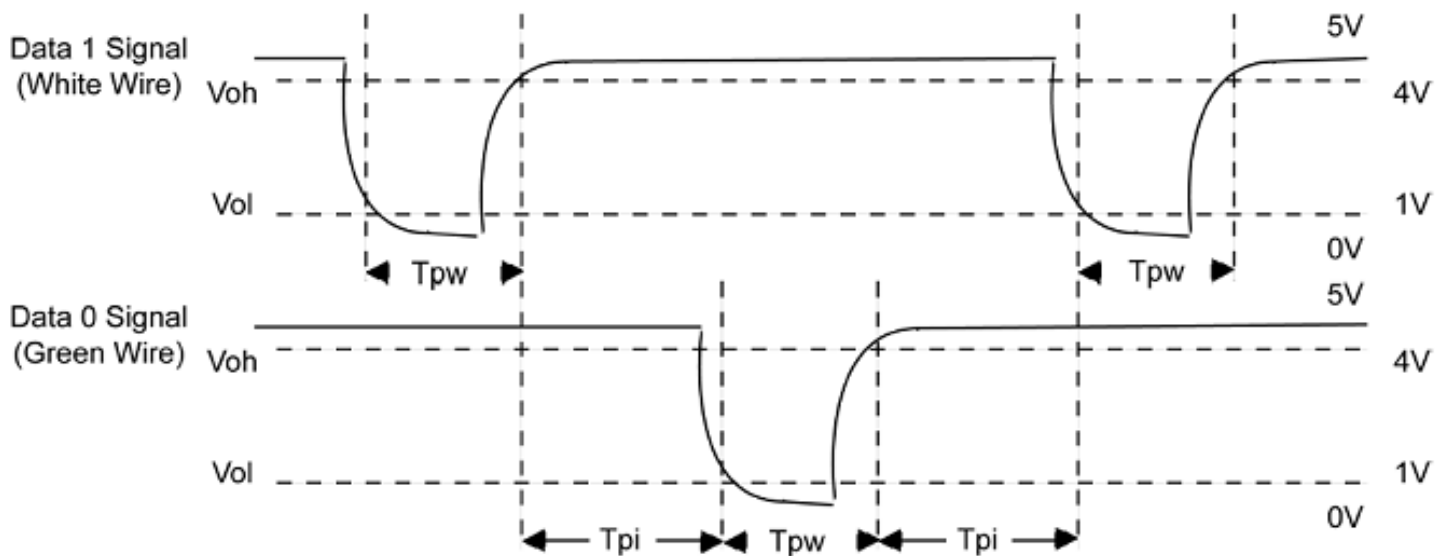
El Wiegand en este diagrama sigue el protocolo estándar de control de acceso de la SIA, que tiene como objetivo lectores de tarjetas Wiegand de 26 bits (con un tiempo de pulso de entre 20us hasta 100us y un tiempo de salto de pulso de entre 200us hasta 20ms). Las señales Data0 y Data1 son de alto nivel (más que Voh) hasta que el lector de tarjetas está listo para enviar un flujo de datos. El lector de tarjetas envía un pulso asíncrono de bajo nivel (menor que vol), transmitiendo un flujo de datos a través de los cables Data1 y Data0 para acceder a la caja de control (como se ve en el diente de sierra de la figura 1). Los pulsos Data0 y Data1 no se traslapan

ni sincronizan. La figura 1 muestra la máxima y mínima amplitud de pulso (pulsos sucesivos) y el tiempo de salto de pulso (el tiempo entre 2 pulsos) permitido por las terminales de control de acceso de huellas digitales de la serie F.

Tabla 1: Tiempo de Pulso

Señal	Definición	Valor Típico del Lector de Tarjeta
Tpw	Ancho de pulso	100 $\mu$ s
Tpi	Intervalo de pulso	1 ms

Figura 1: Diagrama Secuencial



### 17.3 Procedimiento para Cargar Imágenes

**1. Foto de Usuario ★:** Se necesita crear una carpeta llamada "photo" en la unidad USB y agregar las fotos de usuario dentro de esa carpeta. La capacidad es de 8000 imágenes (considerando la capacidad real del dispositivo, se sugiere no cargar más de 5000 imágenes), que no excedan los 15Kb cada una. El nombre de la imagen es x.jpg (x siendo el número de ID del usuario, máximo 9 dígitos). El formato de la foto debe ser JPG.

**2. Protector de Pantalla:** Se necesita crear una carpeta llamada "advertise" en la unidad USB y agregar las fotos a usar como protectores de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes, que no excedan los 30Kb cada una. El nombre y formato de la imagen no está restringido.

**3. Fondo de Pantalla:** Se necesita crear una carpeta llamada "wallpaper" en la unidad USB y agregar las fotos a usar como fondos de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes, que no excedan los 30Kb cada una. El nombre y formato de la imagen no está restringido.

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

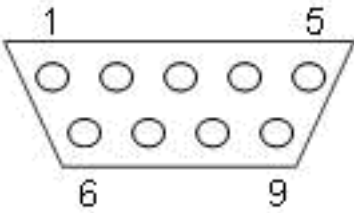


## 17.4 Función de Impresión ★

**Observaciones:** Sólo algunos modelos son compatibles con la función de impresión.

### Instrucciones de Función

Esta función sólo soporta el puerto de comunicación serial, pero no soporta impresión por puertos paralelos. El contenido a imprimir es enviado a través del formato RS232; cada vez se enviará información de verificación al puerto serial. La impresión está disponible si se conecta una impresora, pero también puede usarse una hyper terminal para leer el contenido de salida.

La conexión entre el dispositivo y la impresora	Dispositivo Impresora 2 TXD < ----- > 3 RXD 3 RXD < ----- > 2 TXD 5 GND < ----- > 7 FG
PIN para línea RS232	

### Diagrama de Conexión



### Operación

1. En la interfaz principal, presione **(M/OK)** > Comunicación > Comunicación Serial > Velocidad de Baudios y elija 19200.
2. En la interfaz inicial, presione **(M/OK)** > Imprimir para establecer el formato y parámetros de impresión. Favor de consultar 13 Ajustes de Impresión.

**Nota:** 1.- La velocidad de baudios del dispositivo e impresora debe ser consistente. 2.- Si el formato de impresión predeterminado no es satisfactorio, usted puede contactar a nuestra empresa para configurar otros formatos.



## 17.5 Declaración de Derechos Humanos y Privacidad

### **Estimado consumidor:**

Gracias por elegir el híbrido productos biométricos diseñados y fabricados por nosotros. Como un proveedor de renombre mundial de tecnologías y servicios biométricos, prestamos mucha atención al cumplimiento de las leyes relativas a los derechos humanos y privacidad en cada país mientras que constantemente realiza actividades de investigación y desarrollo.

### **Por esta razón consignamos en este documento la siguiente información:**

1. Todos nuestros dispositivos de reconocimiento de huellas dactilares para uso civil solamente se recogen los puntos característicos de las huellas dactilares en lugar de las imágenes de la huella dactilar y, por lo tanto, no intervienen cuestiones de privacidad.
2. Los puntos característicos de las huellas dactilares recogidas por nuestros productos no se pueden utilizar para restaurar las imágenes de la huella original y, por lo tanto, no intervienen cuestiones de privacidad.
3. Nosotros, como el proveedor del equipo, no será jurídicamente responsables, directa o indirectamente, de las consecuencias que se derivan de la utilización de nuestros productos.
4. Para cualquier controversia relacionada con los derechos humanos o la privacidad al usar nuestros productos, póngase en contacto con su empleador directamente.

Nuestros productos de huellas dactilares para uso policial, o herramientas de desarrollo apoyar la recopilación de las imágenes de la huella original. En cuanto a si este tipo de recogida de huellas dactilares constituye una violación de su privacidad, por favor póngase en contacto con el gobierno o el proveedor de equipamiento final. Nosotros, como fabricante de equipos originales, no deberán ser considerados jurídicamente responsables de toda infracción resultante de la misma.

### **La ley de la República Popular de China tiene las siguientes normas relativas a la libertad personal:**

1. La detención ilegal, la detención o la búsqueda de los ciudadanos de la República Popular de China está prohibida; la violación de la privacidad individual está prohibida.
2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.
3. La casa de los ciudadanos de la República Popular de China es inviolable.
4. La libertad y la privacidad de la correspondencia de los ciudadanos de la República Popular de China están protegidos por la ley.

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

## 17.6 Descripción de Uso Favorable para el Medio Ambiente

- El periodo de uso respetuoso con el medio ambiente (EFUP) marcado en este producto se refiere a la seguridad periodo de tiempo en el que el producto sea utilizado bajo las condiciones especificadas en las instrucciones del producto sin escapes de sustancias nocivas y sustancias nocivas.
- El EFUP de este producto no cubre las piezas consumibles que necesitan ser reemplazadas regularmente como baterías y así sucesivamente. El EFUP de las baterías es de 5 años.

### Nombre y concentración de sustancias o elementos tóxicos y peligrosos

Nombre de la Pieza	Sustancias o Elementos Tóxicos y Peligrosos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip Resistencia	x	o	o	o	o	o
Chip Capacitor	x	o	o	o	o	o
Chip de Inductor	x	o	o	o	o	o
Chip de Diodo	x	o	o	o	o	o
Componentes ESD	x	o	o	o	o	o
Altavoz	x	o				
Adaptador	x	o	o	o	o	o
Tornillos	x	o	o	x	o	o

o: indica que esta sustancia tóxica o peligrosa contenida en todos los materiales homogéneos utilizados para esta parte está por debajo de los LÃ mites establecidos en SJ/T11363-2006.

x: indica que esta sustancia tóxica o peligrosa incluida en al menos uno de los materiales homogéneos utilizados para esta parte está por encima de los LÃ mites establecidos en SJ/T11363-2006.

**Nota:** el 80% de las piezas de este producto son fabricados con los no peligrosos materiales respetuosos con el medio ambiente. Las sustancias peligrosas o elementos contenidos no se pueden reemplazar con materiales respetuosos con el medio ambiente en la actualidad debido a 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)

Derechos de Autor © 2017, ZKTeco Co., Ltd Todos los derechos reservados.  
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.  
El logo ZKTeco y la marca son propiedad de ZKTeco Co., Ltd.