Manual de Usuario

Modelo aplicable(s): M2 LR

Fecha: Enero 2025
Versión: 1.0

Gracias por elegir nuestro producto. Por favor, lea atentamente las instrucciones antes de utilizarlo. Siga estas instrucciones para asegurarse de que el producto funciona correctamente. Las imágenes mostradas en este manual son sólo para fines ilustrativos. Para más información, visite el sitio www.zkteco.com

Copyright 2020 ZKTECO CO, LTD. Todos los derechos reservados.

Marca Registrada

ZKTeco es una marca registrada de ZKTeco. Las marcas registradas involucradas en este manual son propiedad de sus respectivos dueños.

Aviso Legal

Este manual contiene información sobre el funcionamiento y el mantenimiento del equipo ZKTeco. El copyright de todos los documentos, dibujos, etc. relacionados con el equipo suministrado por ZKTeco es propiedad de ZKTeco. Su contenido no debe ser utilizado ni compartido por el receptor con terceros sin la autorización expresa y por escrito de ZKTeco.

El contenido de este manual debe leerse en su totalidad antes de iniciar el funcionamiento y mantenimiento del equipo suministrado. Si alguno de los contenidos del manual parece poco claro o incompleto, póngase en contacto con ZKTeco antes de iniciar el funcionamiento y mantenimiento de dicho equipo.

Un requisito previo esencial para el funcionamiento y mantenimiento satisfactorios es que el personal de funcionamiento y mantenimiento esté plenamente familiarizado con el diseño y que dicho personal haya recibido una formación completa sobre el funcionamiento y mantenimiento de la máquina/unidad/equipo. Además, es esencial para el funcionamiento seguro de la máquina/unidad/equipo que el personal haya leído, comprendido y seguido las instrucciones de seguridad contenidas en el manual.

En caso de conflicto entre los términos y condiciones de este manual y las especificaciones del contrato, planos, hojas de instrucciones o cualquier otro documento relacionado con el contrato, prevalecerán las condiciones/documentos del contrato. Se aplicarán prioritariamente las condiciones/documentos específicos del contrato.

ZKTeco no ofrece ninguna garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones introducidas en el mismo. ZKTeco no extiende la garantía de ningún tipo, incluyendo, sin limitación, cualquier garantía de diseño, comerciabilidad o idoneidad para un propósito particular.

ZKTeco no asume responsabilidad alguna por errores u omisiones en la información o documentos a los que se hace referencia o que están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos de la utilización de la información.

ZKTeco no será responsable en ningún caso ante el usuario ni ante terceros de ningún daño incidental, consecuente, indirecto, especial o ejemplar, incluyendo, sin limitación, la pérdida de negocio, la pérdida de beneficios, la interrupción de negocio, la pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o en relación con el uso de la información contenida en o referenciada por este manual, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños. etc.

Este manual y la información que contiene pueden incluir imprecisiones técnicas o de otro tipo, o errores tipográficos. ZKTeco modifica periódicamente la información aquí contenida, que se incorporará en nuevas adiciones/enmiendas al manual. ZKTeco se reserva el derecho de añadir, eliminar, enmendar o modificar la información contenida en el manual de vez en cuando en forma de circulares, cartas, notas, etc. para un mejor funcionamiento y seguridad de la máquina/unidad/equipo. Dichas adiciones o modificaciones tienen por objeto mejorar/mejorar el funcionamiento de la máquina/unidad/equipo y tales modificaciones no darán derecho a reclamar ninguna indemnización o daños y perjuicios bajo ninguna circunstancia.

ZKTeco no será en ningún caso responsable (i) en caso de mal funcionamiento de la máquina/unidad/equipo debido a cualquier incumplimiento de las instrucciones contenidas en este manual (ii) en caso de funcionamiento de la máquina/unidad/equipo más allá de los límites de tarifa (iii) en caso de funcionamiento de la máquina y equipo en condiciones diferentes a las prescritas en el manual.

El producto se actualizará periódicamente sin previo aviso. Los procedimientos de funcionamiento más recientes y los documentos pertinentes están disponibles en http://www.zkteco.com.

Si tiene algún problema con el producto, póngase en contacto con nosotros.

Sede de ZKTeco

Dirección ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tang Xia Town, Dong guan, China.

Teléfono +86 769 – 82109991

Fax +86 755 - 89602394

Para consultas relacionadas con la empresa, escríbanos a: **sales@zkteco.com.**
Para saber más sobre nuestras sucursales en todo el mundo, visite **www.zkteco.com**

Acerca de la empresa

ZKTeco es uno de los mayores fabricantes del mundo de lectores RFID y biométricos (huella dactilar, facial y reconocimiento de vena). Su oferta de productos incluye lectores y paneles de control de acceso, cámaras de reconocimiento facial de corto alcance. Cámaras de reconocimiento facial de largo alcance, controladores de acceso de elevadores, torniquetes, controladores de puertas con reconocimiento de placas vehiculares (LPR) y productos de consumo, como cerraduras de puertas con lector facial y de huellas dactilares que funcionan con pilas. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas. En las modernas instalaciones de fabricación de ZKTeco, de 700.000 pies cuadrados y con certificación 1509001, controlamos la fabricación, el diseño de productos, el montaje de componentes y la logística y el envío, todo bajo un mismo techo.

Los fundadores de ZKTeco se han empeñado en la investigación y el desarrollo independientes de procedimientos de verificación biométrica y en la producción del SDK de verificación biométrica, que inicialmente se aplicó ampliamente en los campos de la seguridad de PC y la autenticación de identidad. Con la mejora continua del desarrollo y un montón de aplicaciones de mercado, el equipo ha construido gradualmente una identidad y un ecosistema de seguridad inteligente basados en técnicas de verificación biométrica. Con años de experiencia en la industrialización de verificaciones biométricas, ZKTeco se estableció oficialmente en 2007 y ahora ha sido una de las empresas líderes a nivel mundial en la industria de verificación biométrica que posee varias patentes y ha sido seleccionada como Empresa Nacional de Alta Tecnología durante 6 años consecutivos. Los productos están protegidos por derechos de propiedad intelectual.

Acerca de este manual

Este manual presenta el funcionamiento de M2-LR/M2F PRO-LR.

Todas las figuras mostradas son solo ilustrativas. Las figuras de este manual pueden no coincidir exactamente con los productos reales.

Las funciones y parámetros con ★ no están disponibles en todos los dispositivos.

Convenciones del Documento

A continuación, se enumeran las convenciones utilizadas en este manual:

Convenciones GUI

Para el software	
Convención	**Descripción**
Negritas	Usado para identificar interfaz del software como: **OK, Confirmar, Cancelar**
>	Los menús de varios niveles están separados por estos corchetes. Por ejemplo, Archivo > Crear > Carpeta.
Para el dispositivo	
Convención	**Descripción**
<>	Nombres de botones o teclas para dispositivos. Por ejemplo, pulse <OK>.
[ ]	Los nombres de ventanas, opciones de menú, tablas de datos y campos aparecen entre corchetes. Por ejemplo, abra la ventana [Nuevo usuario].
/	Los menús de varios niveles se separan mediante barras inclinadas. Por ejemplo, [Archivo / Crear / Carpeta].

Símbolos

Convención	Descripción
	Esto implica sobre el aviso o presta atención en el manual.
	Información general que ayuda a realizar las operaciones más rápidamente.
	Información a considerar.
	Para evitar peligros o errores.
	Declaración o acontecimiento de advertencia de algo o que sirve de ejemplo.

Índice

Declaración de seguridad de datos

ZKTeco, como proveedor de productos inteligentes, puede necesitar recopilar y conocer cierta información personal suya para brindarle un mejor soporte en el uso de los productos y servicios de ZKTeco. Nos comprometemos a tratar su privacidad con cuidado mediante el desarrollo de una Política de Privacidad.
Le solicitamos leer y comprender completamente todas las regulaciones y puntos clave de la política de protección de privacidad que se presentan en el dispositivo antes de utilizar los productos de ZKTeco.

Como usuario de nuestros productos, debe cumplir con las leyes y normativas aplicables relacionadas con la protección de datos personales al recopilar, almacenar y utilizar estos datos. Esto incluye, pero no se limita a, implementar medidas de protección para los datos personales, como realizar una gestión adecuada de derechos sobre los dispositivos, fortalecer la seguridad física en los escenarios de aplicación de los dispositivos, entre otras acciones.

Medidas de seguridad

Las siguientes precauciones están destinadas a garantizar la seguridad del usuario y prevenir cualquier daño. Por favor, léalas detenidamente antes de la instalación.

1. Leer, seguir y conservar las instrucciones: Todas las instrucciones de seguridad y operación deben ser leídas y seguidas correctamente antes de poner el dispositivo en funcionamiento.

2. No ignorar las advertencias: Cumpla con todas las advertencias indicadas en la unidad y en las instrucciones de operación.

3. Accesorios: Utilice únicamente accesorios recomendados por el fabricante o vendidos con el producto. No use componentes distintos a los sugeridos por el fabricante.

4. Precauciones para la instalación: No coloque este dispositivo en un soporte o marco inestable. Podría caerse, causar lesiones graves y dañar el dispositivo.

5. Servicio técnico: No intente reparar este dispositivo por su cuenta. Abrir o retirar las cubiertas puede exponerlo a voltajes peligrosos u otros riesgos.

6. Daños que requieren servicio técnico: Desconecte el sistema de la fuente principal de energía (CA o CC) y contacte al personal de servicio en las siguientes condiciones:

- Cuando el cable o la conexión de control presenten problemas.
- Si se derrama líquido o cae un objeto dentro del sistema.
- Si el sistema está expuesto a agua o condiciones climáticas adversas (lluvia, nieve, etc.).
- Si el sistema no funciona normalmente siguiendo las instrucciones operativas.
- Si se realizan ajustes diferentes a los definidos en las instrucciones operativas. Ajustes incorrectos pueden causar daños y requerir un técnico calificado para restaurar el funcionamiento normal del dispositivo.

7. Repuestos: Cuando se necesiten piezas de repuesto, los técnicos de servicio deben utilizar únicamente piezas proporcionadas por el proveedor. Sustituciones no autorizadas pueden implicar riesgos de quemaduras, descargas eléctricas u otros peligros.

8. Revisión de seguridad: Una vez completado el servicio o la reparación del dispositivo, solicite al técnico que realice verificaciones de seguridad para garantizar el correcto funcionamiento del equipo.

9. Fuentes de alimentación: Operar el sistema solo con la fuente de energía indicada en la etiqueta del dispositivo. Si no está seguro del tipo de fuente de energía que debe usar, consulte a su distribuidor.

10. Protección contra rayos: Considere instalar conductores externos contra rayos para proteger el sistema de tormentas eléctricas, evitando daños al equipo.

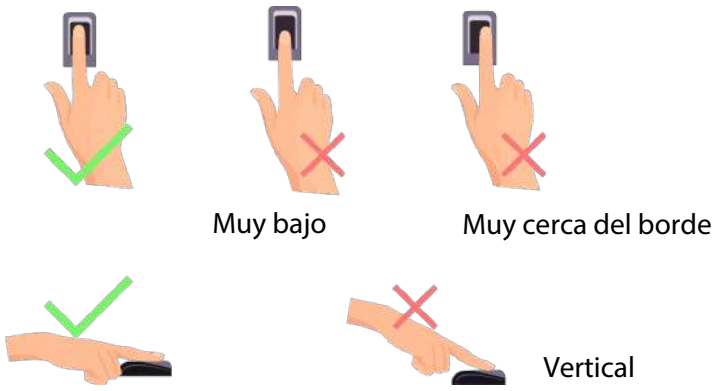
11. Instalación en áreas restringidas: Los dispositivos deben instalarse en áreas de acceso limitado.

1 Instrucciones de uso

Antes de explorar las características y funciones del dispositivo, se recomienda familiarizarse con los conceptos fundamentales que se describen a continuación.

1.1 Posición de los dedos

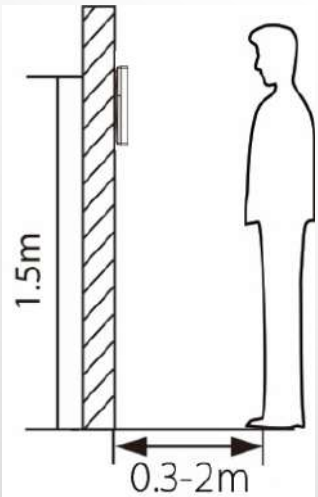
Dedos recomendados: Se recomienda utilizar los dedos índice, corazón o anular, y evitar el pulgar o el meñique, ya que son difíciles de colocar correctamente en el lector de huellas dactilares.



Nota: Utilice el método correcto al presionar los dedos sobre el lector de huellas dactilares para el registro y la identificación. Nuestra empresa no asumirá ninguna responsabilidad por los problemas de reconocimiento que puedan derivarse de un uso incorrecto del producto. Nos reservamos el derecho de interpretación y modificación final en relación con este punto.

1.2 Posición de pie, postura y expresión facial ★

➢ **Distancia recomendada:**



Se recomienda que la distancia entre el dispositivo y un usuario cuya estatura esté comprendida entre 1,55 m y 1,85 m sea de 0,3 m a 2 m. Los usuarios pueden moverse ligeramente hacia delante o hacia atrás para mejorar la calidad de las imágenes faciales captadas.

➢ **Postura de pie y expresión facial recomendadas:**

Postura de pie

Expresión facial

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

1.3 Registro de plantillas faciales

Asegúrese de que la plantilla facial está en el centro de la pantalla durante el registro. Mire hacia la cámara y permanezca quieto durante el registro de la plantilla facial. La pantalla debe parecerse a la imagen siguiente:

Método de registro y autenticación de la cara correcta

- **Recomendación para registrar una plantilla facial**

ˇ Al registrar una plantilla facial, mantenga una distancia de 40 cm a 80 cm de espacio entre el dispositivo y la plantilla facial
ˇ Tenga cuidado de no cambiar la expresión facial. (Plantilla de cara sonriente, con gesto, guiño, etc.)
ˇ Si no sigue las instrucciones de la pantalla, el registro de la plantilla facial puede tardar más o fallar.

◊ Al registrar una plantilla facial, mantenga una distancia de 40 cm a 80 cm de espacio entre el dispositivo y la plantilla facial

◊ Tenga cuidado de no cambiar la expresión facial. (Plantilla de cara sonriente, con gesto, guiño, etc.) ˜ Si no sigue las instrucciones de la pantalla, el registro de la plantilla facial puede tardar más o fallar.

- **Recomendación para autenticar una plantilla facial**

◊ Asegúrese de que la plantilla facial aparece dentro de la directriz que aparece en la pantalla del dispositivo.

◊ Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado la plantilla facial sin gafas, siga autenticando la plantilla facial sin gafas. Si se ha registrado la plantilla facial con gafas, autentique la plantilla facial con las gafas usadas anteriormente.

◊ Si una parte de la plantilla facial está cubierta con un sombrero, una máscara, un parche en el ojo o gafas de sol, la autenticación puede fallar. No cubra la plantilla facial, permita que el dispositivo reconozca tanto las cejas como la plantilla facial.

1.4 Interfaz de espera

El dispositivo utiliza una pantalla en color de 2,8 pulgadas, y todas las operaciones se realizan a través del teclado. Tras conectar la fuente de alimentación, se muestra la siguiente interfaz de espera:

- Introduzca cualquier número para acceder a la interfaz de entrada de ID de usuario.

- Si no hay ningún superadministrador configurado en el dispositivo, pulse **M/OK** para ir al menú

- Después de añadir un superadministrador en el dispositivo, se requiere la verificación del superadministrador antes de abrir las funciones del menú.

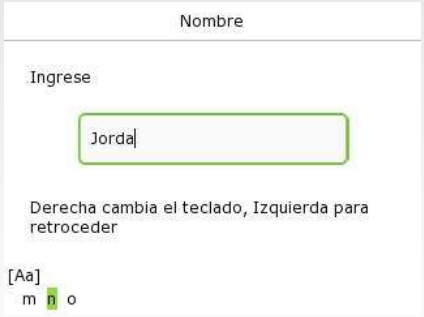
Nota: *Por la seguridad del dispositivo, se recomienda registrarse como superadministrador la primera vez que lo utilice.*

- En la interfaz de espera, las opciones de estado de perforación también pueden mostrarse y utilizarse directamente. Las asignaciones de teclas de acceso directo se mostrarán en la pantalla si pulsa la tecla de acceso directo correspondiente en el teclado, como se muestra enla imagen siguiente. Para conocer el método de funcionamiento específico, consulte "Asignaciones de teclas de acceso directo".

1.5 Modo T9

El modo T9 le permite introducir mayúsculas, minúsculas y caracteres especiales en los campos de entrada de texto. Puede introducir los caracteres alfabéticos y especiales pulsando una tecla por letra. Pulse la tecla < ▶> en el cuadro de texto para activar el modo T9.

1. Desplácese hasta el campo de texto deseado y pulse **<M/OK>**.



2. Cada tecla del teclado tiene unas letras impresas encima. Por ejemplo, pulsando 3 puedesintroducir D, E y F. Para introducir "F", pulsa 3 tres veces. Esto se consigue comparando el númerode pulsaciones con el diccionario sintáctico interno para determinar la letra.

3. Pulse < ▶> para cambiar entre mayúsculas, minúsculas y caracteres especiales.

4. Para añadir el carácter especial, pulse una vez la tecla correspondiente. Por ejemplo, para introducir"@" pulse 2 una vez.

5. Una vez completada la entrada, pulse la tecla <M/OK> dos veces para guardar.

1.6 Modo de verificación

1.6.1 Verificación de huellas digitales

- **1: N Modo de verificación de huellas digitales**

  El dispositivo compara la huella dactilar actual con los datos de huellas dactilares disponibles almacenados en su base de datos.

  El modo de autenticación por huella dactilar se activa cuando el usuario coloca el dedo sobre el escáner de huellas dactilares.

  Por favor, siga la forma recomendada para colocar el dedo en el sensor. Para más detalles, consulte la sección ***Colocación del dedo***

Verificación correcta:

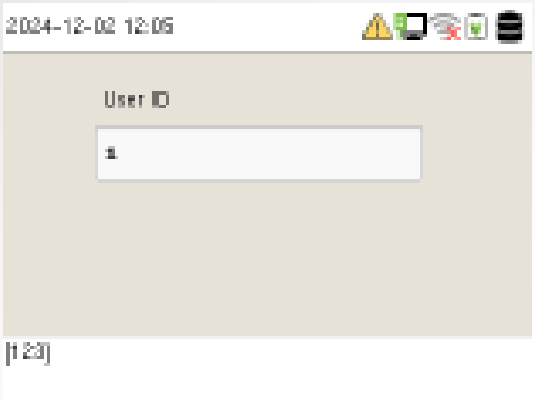
Verificación fallida:

- **1:1 Modo de verificación de huellas digitales**

  El dispositivo compara la huella dactilar actual con las huellas dactilares vinculadas a la ID de usuario introducida a través del teclado.

  En caso de que los usuarios no puedan acceder utilizando el método de autenticación 1:N, pueden intentar verificar su identidad utilizando el modo de verificación 1:1.

Introduzca el ID de usuario y pulse **M/OK** para acceder al modo de verificación de huella dactilar 1:1.Si el usuario ha registrado tarjeta, cara y contraseña además de la huella dactilar, y el método de verificación está configurado en Contraseña/Huella dactilar/Tarjeta/Cara ★ , aparecerá la siguiente pantalla. Seleccione Huella dactilar para acceder al modo de verificación por **huella dactilar.**



Pulse la huella para verificar.

Verificación correcta:

Verificación fallida:

1.6.2 Verificación de tarjetas

- **1: N Modo de verificación de tarjetas**

El modo de verificación de tarjeta 1:N compara el número de tarjeta en el área de inducción detarjeta con todos los datos de número de tarjeta registrados en el dispositivo; La siguientepantalla se muestra en la verificación de tarjeta:

- **1:1 Modo de verificación de tarjetas**

El modo de verificación de tarjetas 1:1 compara el número de tarjeta en el área de inducción detarjetas con el número asociado al ID de usuario del empleado registrado en el dispositivo.

Introduzca el ID de usuario y pulse M/OK para entrar en el modo de verificación de tarjeta 1:1.

Si el usuario ha registrado la huella dactilar, la cara y la contraseña además de la tarjeta, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Cara★, aparecerá la siguientepantalla. Seleccione Tarjeta para acceder al modo de verificación con tarjeta. Una vez realizada la verificación, aparecerá el mensaje **"Verificado correctamente"**, como se muestra a continuación

1.6.3 Verificación facial

- **1: N Modo de verificación facial**

El dispositivo compara las imágenes faciales adquiridas en ese momento con todos los datos de plantillas faciales registradas almacenados en su base de datos. A continuación se muestra el cuadro de diálogo emergente con el resultado de la comparación.

- **1:1 Modo de verificación facial**

En este modo de verificación, el dispositivo compara la cara captada por la cámara con laplantilla facial relacionada con el ID de usuario introducido. Introduzca el ID de usuario y pulse **M/OK** para acceder al modo de verificación facial 1:1.

Si el usuario ha registrado la huella dactilar, la tarjeta y la contraseña además de la cara, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Cara, aparecerá la siguiente pantalla. Seleccione Rostro para acceder al modo de verificación facial

Una vez realizada la verificación, aparecerá el mensaje "**Verificado correctamente**", como se muestra a continuación:

1.6.4 Verificación de contraseñas

El dispositivo compara la contraseña introducida con la contraseña registrada y el ID de usuario.

Introduzca el ID de usuario y pulse **M/OK** para entrar en el modo de verificación de contraseña 1:1. A continuación, introduzca el ID de usuario y pulse **M/OK**.

Si el usuario ha registrado la huella dactilar, la tarjeta y la cara además de la contraseña, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Cara★, aparecerá la siguiente pantalla. Seleccione Contraseña para acceder al modo de verificación de contraseña.

Después de introducir una contraseña correcta y una contraseña incorrecta, respectivamente, aparece la siguiente pantalla.

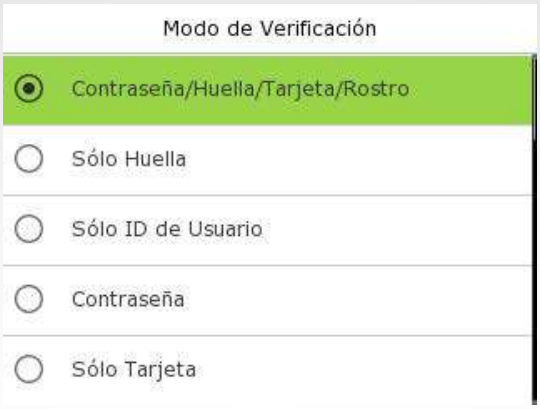
Verificación correcta:

Verificación fallida:

1.6.5 Verificación combinada

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación. Se puede utilizar un total de 21 combinaciones de verificación diferentes, como se muestra a continuación:

Símbolo	Definición	Explicación
/	o	Este método compara la verificación introducida de una persona con la plantilla de verificación relacionada almacenada previamente para ese ID de personal en el dispositivo.
+	y	Este método compara la verificación introducida de una persona con todas las plantillas de verificación almacenadas previamente para ese ID de personal en el dispositivo.



- **Procedimiento para configurar el modo de verificación combinada**

  ◊ La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar correctamente el proceso de verificación combinada.

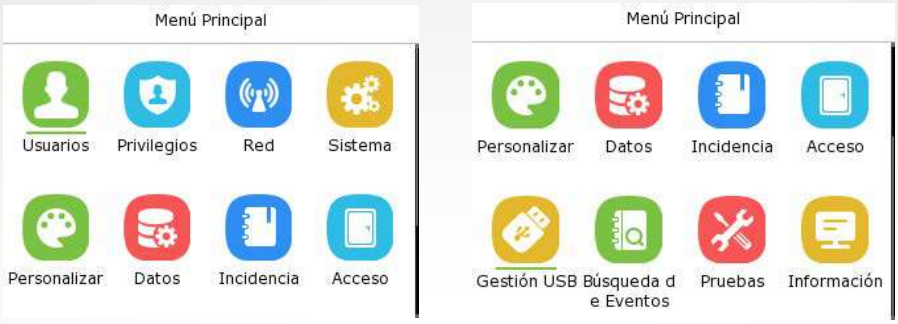
  ◊ Por ejemplo, cuando un empleado ha registrado sólo los datos, pero el modo de verificación del dispositivo está configurado como "Cara + Contraseña", el empleado no podrá completar el proceso de verificación con éxito.

  ◊ Esto se debe a que el Dispositivo compara la plantilla facial escaneada de la persona con la plantilla de verificación registrada (tanto la plantilla facial como la contraseña) almacenada previamente para ese ID de personal en el Dispositivo.

  ◊ Pero como el empleado sólo ha registrado la plantilla facial pero no la contraseña, la verificación no se completará y el dispositivo mostrará "Verificación fallida".

2 Menú principal

Pulse **M/OK** para entrar en el **Menú Principal,** se mostrará la siguiente pantalla:



Menú	Descripción
Gestión de Usuarios	Para añadir, editar, ver y eliminar información básica de un Usuario.
Función del Usuario	Para establecer el ámbito de permiso del rol personalizado para los usuarios, es usuario decir, los derechos para operar el sistema
COMM	Para configurar los parámetros relevantes de red, conexión PC, red inalámbrica, servidor cloud y diagnóstico de red
Sistema	Para configurar los parámetros relacionados con el sistema, incluyendo fecha hora, asistencia, los parámetros de plantilla facial y huella dactilar, la configuración de seguridad, la actualización del firmware en línea, la actualización USB y el restablecimiento a los valores de fábrica
Personalice	Esto incluye la configuración de la interfaz de usuario, la voz, los horarios de timbre, las Personalice opciones de estado de perforación y las asignaciones de teclas de acceso directo
Gestión de Datos	Para borrar todos los datos relevantes del dispositivo.
Código de Trabajo	Establecer diferentes tipos de trabajo
Código de Acceso	Para configurar los parámetros de la cerradura y del dispositivo de control de acceso correspondiente
Gestor USB	Para cargar o descargar los datos específicos mediante una unidad USB
Búsqueda de Asistentes	Para consultar los registros de eventos especificados, comprueba las fotos de asistencia y bloquea las fotos de asistencia.
Autotest	Para comprobar automáticamente si cada módulo funciona correctamente, incluidos la pantalla LCD, el audio, el teclado, la cámara, el sensor de huellas dactilares y el reloj en tiempo real.
Información del Sistema	Para ver la capacidad de datos, la información sobre el dispositivo y el firmware y la política de privacidad del dispositivo.

Nota: *Cuando los usuarios utilicen el producto por primera vez, deberán hacerlo después de configurar los privilegios de administrador. Pulse* ***Gestión de usuarios*** *para añadir un administrador o editar los permisos de usuario como superadministrador. Si el producto no tiene una configuración de administrador, el sistema mostrará una solicitud de comando de configuración de administrador cada vez que acceda al menú del dispositivo.*

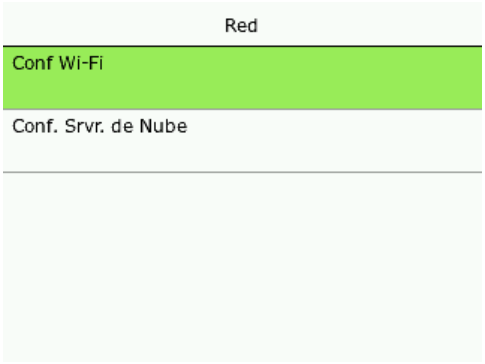
3 Gestión de usuarios

3.1 Registro de usuarios

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en **Gestión de usuario. > Nuevo usuario**.

3.1.1 ID y nombre de usuario

Introduzca el ID de usuario y el nombre.



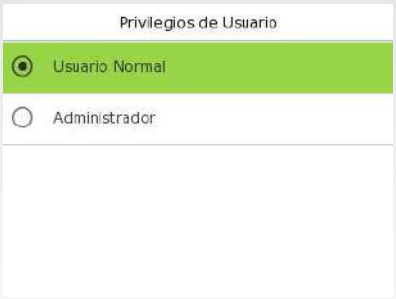
Nota:

- ◊ *Un nombre de usuario puede contener un máximo de 34 caracteres.*
- ◊ *El ID de usuario puede contener de 1 a 14 dígitos por defecto, admitiendo tanto números como caracteres alfabéticos.*
- ◊ *Durante el registro inicial, puede modificar su ID, que no podrá modificarse después del registro.*
- ◊ *Si aparece el mensaje "¡Duplicado!", debe elegir otro ID, ya que el ID de usuario introducido ya existe.*

3.1.2 Función del usuario

En la interfaz **Nuevo usuario,** seleccione **Rol de usuario** para establecer el rol del usuario como **Usuario normal** o **Superadministrador.**

- **Super Admin:** El Super Administrador posee todos los privilegios de gestión en el Dispositivo.
- **Usuario normal:** Si el Super Admin ya está registrado en el Dispositivo, los Usuarios Normalesno tendrán privilegios para gestionar el sistema y sólo podrán acceder a las verificaciones deautenticación.
- **Funciones definidas por el usuario:** El Usuario Normal también puede ser configurado conun **Rol Definido por el Usuario** que son los roles personalizados que pueden serconfigurados para el Usuario Normal.



Nota: *Si el rol de usuario seleccionado es el de Super Admin, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en el método o métodos de autenticación que el superadministrador haya registrado. Consulte* ***Modo de verificación****.*

3.1.3 Modo de verificación

Seleccione el modo de verificación para el usuario, se pueden utilizar un total de 21 combinaciones de verificación diferentes. ***Consulte 1.6.5 verificación*** combinada para obtener más detalles

3.1.4 Registrar huella dactilar

Seleccione Huella dactilar en la interfaz Nuevo usuario para acceder a la página de registro de huellas dactilares.

- Seleccione el dedo que desea registrar
- Presione tres veces el mismo dedo en el lector de huellas dactilares
- El color verde indica que la huella se ha registrado correctamente

3.1.5 Registro plantilla facial ★

Seleccione rostro en la interfaz de nuevo usuario para acceder a la página de registro de rostros.

- Mire hacia la cámara, coloque la plantilla facial dentro del recuadro blanco de guía y permanezca quieto durante el registro de la plantilla facial.

- Aparecerá una barra de progreso mientras se registra la plantilla facial y se mostrará "Registrado correctamente" cuando se complete la barra de progreso.

- Si la plantilla facial ya está registrada, aparecerá el mensaje "Rostro duplicado". La interfaz de registro es la siguiente:

3.1.6 Tarjeta

Seleccione **Tarjeta** en la interfaz **Nuevo usuario** para acceder a la página de registro de tarjetas.

- En la interfaz Tarjeta, pase la tarjeta por debajo de la zona de lectura de tarjetas. El registro dela tarjeta se realizará correctamente.

- Si la tarjeta ya está registrada, aparecerá el mensaje "**Tarjeta duplicada**". La interfaz de registro es la siguiente:

3.1.7 Contraseña

Seleccione **Contraseña** en la interfaz **Nuevo usuario** para acceder a la página de registro de la contraseña.

- En la interfaz Contraseña, introduzca la contraseña necesaria y vuelva a introducirla para confirmarla y pulse **M/OK**.

- Si la contraseña que se vuelve a introducir es diferente de la que se introdujo inicialmente, el dispositivo muestra el mensaje "**¡No coincide la contraseña!**", en el que el usuario debe volver a confirmar la contraseña.

- La contraseña puede contener de 6 a 8 dígitos por defecto.

3.1.8 Foto de perfil

Seleccione **Foto de perfil** en la interfaz de **Nuevo Usuario** para ir a la página de registro de Foto de perfil.

- Cuando un usuario registrado con una foto supera la autenticación, se mostrará la foto registrada (entre en [**Sistema**] > [**Asistencia**] para activar **Mostrar foto de usuario**).

- Pulse **Foto de perfil,** se abrirá la cámara del dispositivo y pulse **M/OK** para hacer una foto. La foto capturada se muestra en la esquina superior izquierda de la pantalla y la cámara se abre de nuevo para tomar una nueva foto, después de tomar la foto inicial.

Nota: *Al registrar una plantilla facial, el sistema captura automáticamente una foto como foto de perfil del usuario. Si no registra una foto de perfil, el sistema establece automáticamente la foto capturada durante el registro como foto predeterminada*

3.2 Búsqueda de usuarios

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en **Gestión de usuario.** > T**odos los usuarios**.

- En la interfaz **Todos los usuarios,** seleccione la barra de búsqueda de la lista de usuarios para introducir la palabra clave de recuperación necesaria (donde la palabra clave puede ser el ID de usuario, los apellidos o el nombre completo) y el sistema buscará la información de usuario relacionada.

3.3 Editar usuario

En la interfaz **Todos los usuarios**, seleccione el usuario deseado de la lista, pulse **M/OK** y seleccione

Editar para editar la información del usuario.

Nota: *El proceso de edición de un usuario es el mismo que el de añadir un usuario, salvo que el ID de usuario no puede modificarse al editar los detalles de un usuario. El proceso en detalle se refiere a la "**Gestión de usuarios**".*

3.4 Borrar usuario

En la interfaz **Todos los usuarios**, seleccione el usuario deseado de la lista, pulse **M/OK** y seleccione **Eliminar** para borrar el usuario o la información de un usuario específico del dispositivo. En la interfaz **Eliminar**, seleccione la operación deseada y pulse **M/OK** para confirmar la eliminación

- **Procedimiento de eliminación**

Borrar Usuario: Se borrará toda la información del usuario (borra el Usuario seleccionado en su totalidad) del Dispositivo.

Borrar sólo huella dactilar: Elimina la información de la huella dactilar del usuario seleccionado.

Borrar sólo el rostro ★: Elimina la información de la plantilla facial del usuario seleccionado.

Borrar sólo contraseña: Borra la información de la contraseña del usuario seleccionado.

Borrar sólo número de tarjeta: Borra la información de la tarjeta del usuario seleccionado.

Borrar sólo foto de perfil★: Elimina la foto de perfil del usuario seleccionado.

3.5 Estilo de visualización

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en **Gestión de usuario**. > **Estilo de pantalla**.

A continuación se muestran diferentes estilos de visualización:

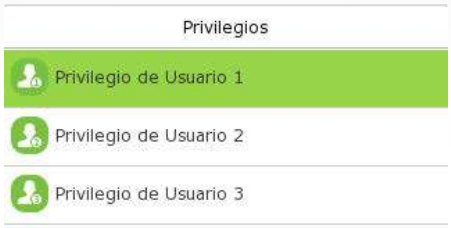
Línea múltiple:

Línea mixta::

4 Función del usuario

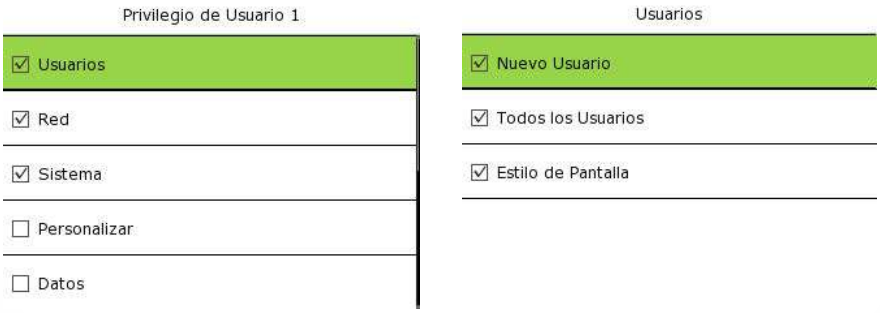
El **rol de usuario** facilita la asignación de permisos específicos a usuarios concretos, en función de las necesidades.

- Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en R**ol de usuario > Rol definido por el usuario** para establecer los permisos definidos por el usuario.
- El ámbito de permiso del rol personalizado puede configurarse en 3 roles, es decir, el ámbito operativo personalizado de las funciones de menú del usuario.



- A continuación, seleccionando en Definir rol de usuario, seleccione los privilegios necesarios para el nuevo rol y pulse la tecla **M/OK**.

- En primer lugar, seleccione el nombre de la función del **menú principal** que desee y, a continuación, pulse **M/OK** y seleccione los submenús que desee de la lista.



Nota: *Si el Rol de Usuario está habilitado para el Dispositivo, pulse* ***Gestión de Usuarios > Nuevo Usuario > Rol de Usuario*** *para asignar los roles creados a los usuarios requeridos. Sin embargo, si no hay ningún superadministrador registrado en el equipo, éste le preguntará "Por favor, inscriba primero al superadministrador" al activar la función Rol de usuario.*

5 Ajustes de comunicación

Los Ajustes de Comunicación se utilizan para configurar los parámetros de la Red, Conexión PC, Wi-Fi★, Servidor Cloud y Diagnóstico de Red.

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione **COMM**.

5.1 Ajustes de red

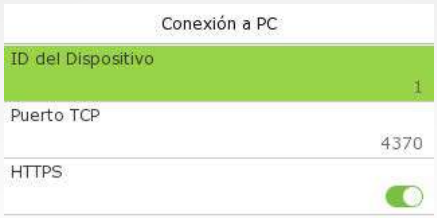
Cuando el dispositivo necesita comunicarse con un PC a través de Ethernet, es necesario configurar los ajustes de red y asegurarse de que el dispositivo y el PC se conectan al mismo segmento de red.

Selecciona **Ethernet** en la interfaz **COMM** para configurar los ajustes.

Nombre de la función	Descripción
Visualización en la barra de estado	Seleccione si desea mostrar el icono de red en la barra de estado.
Dirección IP	La dirección IP por defecto es 192.168.1.201. Puede modificarse en función de la disponibilidad de la red.
Máscara de subred	La máscara de subred por defecto es 255.255.255.0. Puede modificarse en función de la disponibilidad de la red.
Gateway	La dirección de puerta de enlace por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
DNS	La dirección DNS por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
DHCP	El protocolo de configuración dinámica de host sirve para asignar DHCP dinámicamente direcciones IP a los clientes a través del servidor.

5.2 Conexión a PC

Seleccione **Conexión PC** en el menú **COMM**. Ajustes para configurar los ajustes de comunicación.



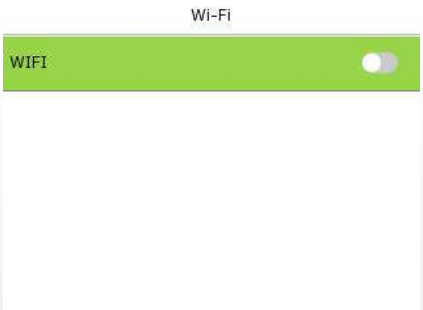
Nombre de la función	Descripción
ID del dispositivo	El número de identidad del dispositivo, que oscila entre 1 y 254
Puerto TCP COMM	El valor por defecto del puerto TCP COMM es 4370. Puede modificarse en función de la disponibilidad de la red.
HTTPS	Para aumentar la seguridad del acceso al software, los usuarios pueden activar el protocolo HTTPS para crear una transmisión de red segura y cifrada y garantizar la seguridad de los datos enviados mediante la autenticación de la identidad y la comunicación cifrada. Esta función está activada por defecto. Esta función puede activarse o desactivarse a través de la interfaz de menú, y al cambiar el estado HTTPS, el dispositivo mostrará un mensaje de seguridad y se reiniciará tras la confirmación.

5.3 Red inalámbrica★

El dispositivo proporciona un módulo Wi-Fi, que puede estar integrado en el molde del dispositivo o puede conectarse externamente.

El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (Wireless Fidelity) y establece un entorno de red inalámbrica. El Wi-Fi está activado por defecto en el dispositivo. Si no necesita utilizar la red Wi-Fi, puede desactivar el botón Wi-Fi.

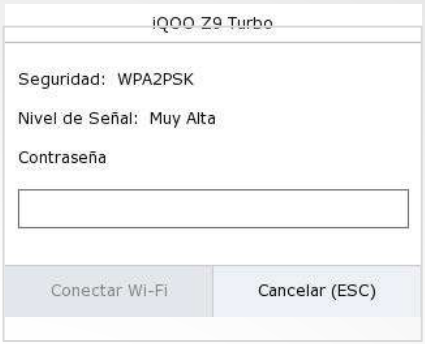
Seleccione **Ajustes de Wi-Fi** en la **COMM**. Ajustes para configurar los ajustes Wi-Fi.



- **Buscar en la red Wi-Fi**
  - WIFI está activado en el dispositivo por defecto. Pulse el botón para activar o desactivar
  - Una vez encendido el Wi-Fi, el dispositivo buscará el WIFI disponible dentro del alcance dela red.

- Elija el nombre de Wi-Fi adecuado de la lista disponible, introduzca la contraseña correcta en la interfaz de contraseña y pulse **M/OK**.

WIFI habilitado:
Pulse en la red deseada de la lista de redes buscadas.



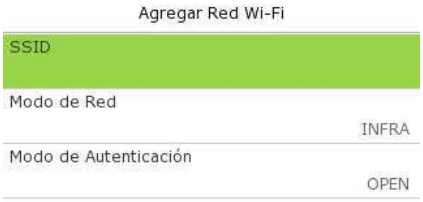
Pulse en el campo de contraseña para introducir la contraseña y, a continuación, pulse en **M/OK.**

- Cuando la conexión WIFI se haya realizado correctamente, la interfaz inicial mostrará el logotipo de Wi-Fi.

- **Añadir red Wi-Fi manualmente**

El Wi-Fi también se puede añadir manualmente si el Wi-Fi requerido no aparece enla lista

Pulse en **Añadir Red WIFI** para añadir la WIFI manualmente.

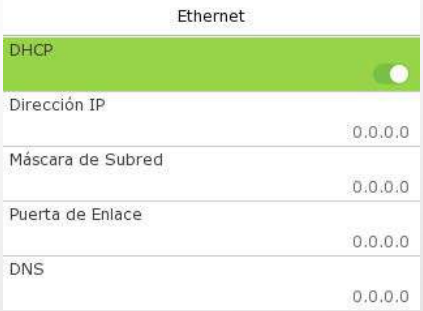


En esta plantilla de interfaz, introduzca los parámetros de la red WIFI. (La red añadida debe existir).

Nota: *Después de añadir con éxito el WIFI manualmente, siga el mismo proceso para buscar el nombre del WIFI añadido.*

- **Configuración avanzada**

En la interfaz de la **red inalámbrica**, pulse en **Avanzado** para configurar los parámetrospertinentes según sea necesario.



Nombre de la función	Descripción
DHCP	El Protocolo de Configuración Dinámica de Host (DHCP) asigna dinámicamente direcciones IP a los clientes de la red. Si el DHCP está activado, la IP no se puede configurar manualmente.
Dirección IP	Dirección IP para la red WIFI, por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
Máscara de subred	La máscara de subred por defecto de la red WIFI es 255.255.255.0. Puede modificarse en función de la disponibilidad de la red.
Gateway	La dirección de puerta de enlace predeterminada es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red
DNS	La dirección DNS por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.

5.4 Configuración del servidor en la nube

Pulse **Cloud Server Setting** en el menú **COMM** para conectar con el servidor ADMS.

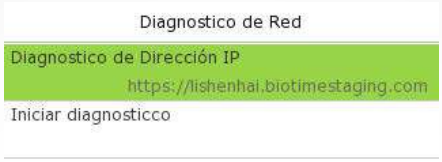
Nombre de la función		Descripción
Habilitar nombre de dominio	**Dirección del servidor**	Una vez activada esta función, se utilizará el modo de nombre de dominio "https://...", como https://www.XYZ.com, mientras que "XYZ" indica el nombre del dominio (cuando este modo está activado).
Desactivar nombre de dominio	**Dirección del servidor**	Dirección IP del servidor ADMS.
	Puerto del servidor	Puerto utilizado por el servidos ADMS.
Activar servidor proxy		Cuando decida activar el proxy, deberá establecer la dirección IP y el número de puerto del servidor proxy.

Nota:*Al emparejar el dispositivo con el software* ***BioTime Cloud,*** *debe activar* ***Nombre de dominio*** *e introducir la dirección correcta del servidor.*

5.5 Diagnóstico de red

Ayuda a configurar los parámetros de diagnóstico de la red.

Seleccione **Diagnóstico de red** en la interfaz **COMM**. Configuración. Introduzca la dirección IP que debe diagnosticarse y pulse **Iniciar la prueba de diagnóstico** para comprobar si la red puede conectarse al dispositivo.



6 Configuración del sistema

Configure los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione **Sistema.**

6.1 Fecha y hora

Seleccione **Fecha Hora** en la interfaz **Sistema** para ajustar la fecha y la hora.

- Pulse **Servidor NTP** para activar la sincronización horaria automática basada en la dirección de servicio que introduzca.
- Pulse **Fecha y hora manual** para ajustar manualmente la fecha y la hora y, a continuación,pulse **M/OK** y guarde.
- Pulse **Seleccionar zona horaria** para seleccionar manualmente la zona horaria en la que se encuentra el dispositivo.
- Active o desactive este formato seleccionando Hora 24 horas. Si está activado, pulse **Formato de fecha** para ajustar la fecha.
- Pulse **Horario de verano** para activar o desactivar la función. Si está activada, pulse **Modo de ahorro de luz diurna** para seleccionar un modo de ahorro de luz diurna y, a continuación,pulse C**onfiguración de ahorro de luz diurna** para ajustar la hora del interruptor.

Modo semana **Modo día**

- Al restaurar los ajustes de fábrica, se puede restaurar la hora (24 horas) y el formato de fecha (AAAA-MM-DD), pero no se puede restaurar la fecha y la hora del dispositivo.

Nota: *Por ejemplo, el usuario ajusta la hora del dispositivo (18:35 del 15 de marzo de 2019) a las 18:30 del 1 de enero de 2020. Tras restablecer los ajustes de fábrica, la hora del equipo seguirá siendo las 18:30 del 1 de enero de 2020*

6.2 Asistencia

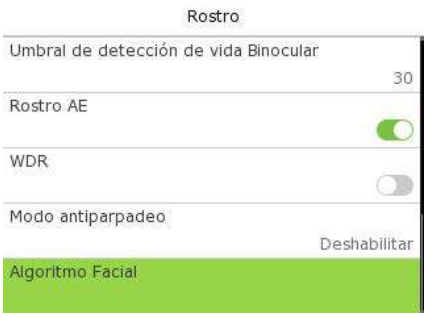
Seleccione **Asistencia** en la interfaz Sistema.

Nombre de la función	Descripción
Periodo de Marcaje Duplicado (M)	Dentro de un periodo de tiempo establecido (unidad: minutos), el registro de asistencia duplicado no se reservará (el valor oscila entre 1 y 999999 minutos).
Modo Cámara	Esta función está desactivada por defecto. Si está activada, aparecerá un aviso de seguridad y el sonido del obturador de la cámara se activará obligatoriamente. Hay 5 modos: **Sin foto:** No se toma ninguna foto durante la verificación del usuario. Tomar foto, no guardar: Se toma una foto pero no se guarda durante la verificación. **Tomar foto y guardar:** Se guardan todas las fotos tomadas durante la verificación. **Guardar en verificación correcta:** Se toma una foto y se guarda para cada verificación correcta. **Guardar en verificación fallida:** La foto se toma y se guarda sólo para cada verificación fallida.
Mostrar foto de usuario	Esta función está desactivada por defecto. Si está activada, aparecerá un mensaje de seguridad.
ID de usuario alfanumérico	Activar/desactivar el alfanumérico como ID de usuario.
Alerta de registro de asistencia	Cuando el espacio de registro de la asistencia alcanza el valor umbral máximo, el aparato muestra automáticamente el aviso de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Reporte de datos T&A	Cuando los registros de asistencia alcanzan su capacidad máxima de almacenamiento, el dispositivo borra automáticamente un conjunto de registros de asistencia antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
Reporte periodico de foto de T&A	Cuando las fotos de asistencia alcanzan su capacidad máxima de almacenamiento, el dispositivo elimina automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.

Actualización periódica de la foto en lista negra	Cuando las fotos de la lista de bloqueadas alcanzan su capacidad máxima de almacenamiento, el dispositivo elimina automáticamente un conjunto de fotos antiguas de la lista de bloqueadas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Tiempo de espera de autenticación	Tiempo que tarda en aparecer un mensaje de verificación correcta. Valor válido: 1~9 segundos.
Intervalo de reconocimiento	Después de pulsar (seleccionar) el intervalo de identificación, por ejemplo, si el intervalo de comparación se establece en 5 segundos, el reconocimiento facial verificará la cara cada 5 segundos. Valor válido: de 0 a 9 segundos. 0 significa identificación continua, 1 a 9 significa identificación a intervalos.

6.3 Parámetros de la plantilla facial

Seleccione **Rostro** en la interfaz del sistema para ir a la configuración de los parámetros de la plantilla de cara.



Nombre de la función	Descripción
Umbral 1:N	En el modo de verificación 1:N, la verificación sólo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será el porcentaje de errores de apreciación y mayor el porcentaje de rechazos, y viceversa. Se recomienda fijar el valor por defecto en 40.
Umbral 1:1	En el modo de verificación 1:1, la verificación sólo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea superior al valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de error de apreciación y mayor la tasa de rechazo, y viceversa. Se recomienda fijar el valor por defecto en 30.

Umbral de inscripción de rostros	Durante el registro de la plantilla facial, se utiliza la comparación 1:N para determinar si el usuario ya se ha registrado anteriormente. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este umbral, indica que la plantilla facial ya ha sido registrada.
Calidad de imagen	Calidad de imagen para el registro y la comparación facial. Cuanto mayor sea el valor, más clara será la imagen requerida.
Distancia de reconocimiento facial	Cuanto más alejado esté el individuo, más pequeño será el rostro y menor el número de píxeles del rostro obtenidos por el algoritmo. Por lo tanto, el ajuste de este parámetro puede ajustar la distancia de comparación más lejana de los rostros.
Valor de activación de la luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, la luz LED se encenderá o apagará con más frecuencia.
Detección en vivo	Detecta el intento de suplantación utilizando imágenes de luz visible para determinar si la muestra de origen biométrico proporcionada es de una persona real (un ser humano vivo) o una representación falsa.
Umbral de detección en vivo	Facilita juzgar si la imagen visible capturada es una persona real (un ser humano vivo). Cuanto mayor sea el valor, mejores serán las prestaciones anti-spoofing mediante luz visible.
Anti-spoofing mediante NIR	Utilización de imágenes espectrales en el infrarrojo cercano para identificar y prevenir ataques con fotos y videos falsos.
Umbral de detección binocular en vivo	Es conveniente juzgar si las imágenes espectrales del infrarrojo cercano son fotos y vídeos falsos. Cuanto mayor sea el valor, mejor será la eficacia antifalsificación de las imágenes espectrales en el infrarrojo cercano.
Rostro AE	Cuando la cara está delante de la cámara en el modo Face AE, el brillo de la zona de la cara aumenta, mientras que las otras zonas se oscurecen.
WDR	El amplio rango dinámico (WDR) equilibra la luz y amplía la visibilidad de la imagen para vídeos de vigilancia en escenas con iluminación de alto contraste y mejora la identificación de objetos en entornos claros y oscuros.
Modo antiparpadeo	Se utiliza cuando el WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea con la misma frecuencia que la luz.
Algoritmo facial	Información relacionada con el algoritmo facial y actualización de la plantilla facial en pausa.

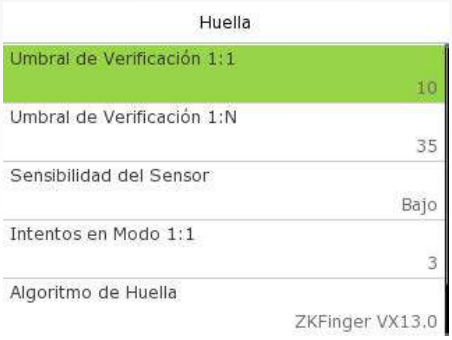
Nota: *Un ajuste incorrecto de los parámetros de exposición y calidad puede afectar gravemente al rendimiento del aparato. Ajuste el parámetro de exposición únicamente bajo la orientación del personal del servicio posventa de nuestra empresa.*

- **Proceso para modificar la precisión del reconocimiento facial**
  - En la interfaz del sistema, pulse en Cara y, a continuación, active Anti-Spoofing mediante NIR para configurar el anti-spoofing.
  - A continuación, en el menú principal, pulse Autotest > Test Face y realice el test facial.
  - Pulse tres veces para las puntuaciones en la esquina superior derecha de la pantalla y aparecerá el cuadro rectangular rojo para empezar a ajustar el modo.

- Mantenga un brazo de distancia entre el dispositivo y la cara. Se recomienda no mover la cara en un amplio rango.

6.4 Parámetros de huellas dactilares

Seleccione **Huella digital** en la interfaz **Sistema** para ir a la configuración de los parámetros de Huella digital.



Nombre de la función	Descripción
Umbral 1:1	En el método de verificación 1:1, la verificación sólo tendrá éxito cuando la similitud entre los datos de la huella dactilar adquirida y la plantilla de huella dactilar asociada a la ID de usuario introducida y registrada en el dispositivo se superior al valor establecido.
Umbral 1:N	En el método de verificación 1:1, la verificación sólo tendrá éxito cuando la similitud entre los datos de la huella dactilar adquirida y la plantilla de huella dactilar asociada a la ID de usuario introducida y registrada en el dispositivo se superior al valor establecido.
Sensibilidad del sensor FP	Para ajustar la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel por defecto "**Medio**". Cuando el entorno es seco, lo que provoca una detección lenta de la huella dactilar, puede ajustar el nivel a "**Alto**" para aumentar la sensibilidad; cuando el entorno es húmedo, lo que dificulta la identificación de la huella dactilar, puede ajustar el nivel a "**Bajo**".
1:1 Intentos de reintento	En la verificación 1:1, los usuarios pueden olvidar la huella registrada o presionar el dedo de forma incorrecta. Para reducir el proceso de reintroducción del ID de usuario, se permite el reintento.
Algoritmo Huella dactilar	Versión del algoritmo de huellas dactilares. Soporte por defecto ZKFinger VX13.0, puede cambiar a ZKFinger VX10.0.
Imagen de huella dactilar	Esta función está desactivada por defecto. Tras desactivarla, la imagen de la huella dactilar no se mostrará al registrar y verificar las huellas dactilares. La interfaz del menú permite activar o desactivar esta función, y hay avisos de seguridad al cambiar. Hay cuatro opciones disponibles: **Mostrar para registro:** para mostrar la imagen de la huella dactilar en la pantalla sólo durante el registro. **Mostrar para coincidencia:** para mostrar la imagen de la huella dactilar en la pantalla sólo durante la verificación. **Mostrar siempre:** para mostrar la imagen de la huella dactilar en pantalla durante la inscripción y la verificación. **Ninguna:** para no mostrar la imagen de la huella dactilar.

6.5 Ajustes de seguridad

Seleccione **Configuración de seguridad** en la interfaz del **sistema** para ir a la configuración de seguridad.

Nombre de la función	Descripción
Comunicación autónoma	Por defecto, esta función está desactivada. Esta función puede activarse o desactivarse a través de la interfaz de menú. Cuando está activada, aparece una pregunta de seguridad y el dispositivo se reiniciará después de que usted lo confirme.
SSH	El dispositivo no admite la función Telnet, por lo que normalmente se utiliza SSH para la depuración remota. Por defecto, SSH está activado. La interfaz de menú permite activar y desactivar SSH. Cuando esté habilitado, aparecerá un mensaje de seguridad, pero no será necesario reiniciar el dispositivo tras la confirmación
Enmascaramiento de ID de usuario	Una vez activada, la ID de usuario se mostrará parcialmente tras el resultado de la verificación de personal (sólo la ID de usuario con más de 2 dígitos admite la visualización enmascarada), y está activada por defecto.
Mostrar nombre de verificación	Una vez activado, el nombre del usuario se mostrará tras el resultado de la verificación del personal. El resultado de la verificación no mostrará el nombre después de desactivarlo.
Modo de verificación de la pantalla	Una vez activada, el resultado de la verificación del personal mostrará el modo de verificación del usuario. El resultado de la verificación no mostrará el modo de verificación después de desactivarlo.
Guardar foto como plantilla	Después de desactivar esta función, es necesario volver a registrar la plantilla facial tras una actualización del algoritmo.

6.6 Actualización USB

Seleccione **Actualización USB** en la interfaz del sistema.

El programa de firmware del dispositivo se puede actualizar con el archivo de actualización en una unidad USB. Antes de realizar esta operación, asegúrese de que la unidad USB contiene el archivo de actualización correcto y de que está correctamente insertada en el dispositivo.

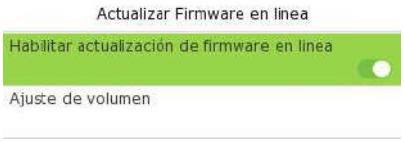
Si no hay ningún disco USB insertado, el sistema mostrará el siguiente mensaje después de pulsar **Actualización USB** en la interfaz del sistema.

Nota: *Si necesita un archivo de actualización, póngase en contacto con nuestro servicio de asistencia técnica. No se recomienda actualizar el firmware en circunstancias normales.*

6.7 Actualizar el firmware en línea

Pulse **Actualizar Firmware Online** en la interfaz del Sistema.

Pulse **Activar la función de Actualización de Firmware Online**, el dispositivo le indicará que la actualización puede conllevar algunos riesgos de seguridad de los datos, lo que requiere la confirmación manual por parte del usuario.



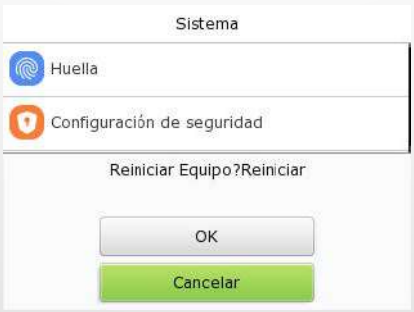
Pulse **Buscar actualizaciones** puede tener los siguientes 3 escenarios:

- Si la consulta falla, la interfaz mostrará el mensaje "**Consulta fallida**".
- Si la versión de firmware del dispositivo es la última, aparecerá el mensaje "**Ya es la última versión**".
- Si la versión de firmware del dispositivo no es la última, se mostrará el número de versión y el registro de cambios de la última versión. Los usuarios pueden elegir si desean actualizar a la última versión del firmware.

6.8 Restablecimiento de fábrica

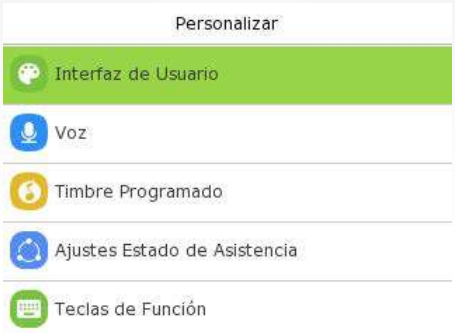
La función Restablecimiento de fábrica restaura los ajustes del dispositivo, como los ajustes de comunicación y los ajustes del sistema, a los ajustes predeterminados de fábrica (Esta función no borra los datos de usuario registrados).

Seleccione **Reiniciar** en la interfaz **Sistema** y pulse **M/OK** para restablecer la configuración de fábrica por defecto.



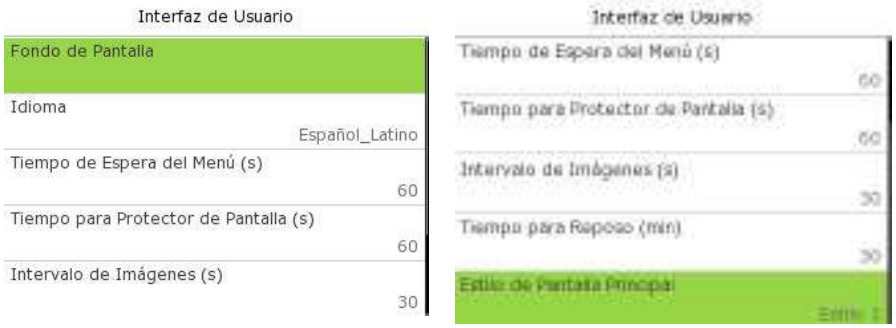
7 Personalizar la configuración

Cuando el dispositivo se encuentre en la interfaz inicial, pulse **M/OK** y seleccione **Personalizar** para personalizar la configuración de la interfaz, las opciones de voz, timbre, estado de perforación y las asignaciones de teclas de acceso directo.



7.1 Configuración de la interfaz de usuario

Seleccione Interfaz de usuario en el menú **Personalizar** para personalizar el estilo de visualización de la interfaz principal.



Nombre de la función	Descripción
Fondo de pantalla	El fondo de pantalla principal puede seleccionarse según las preferencias del usuario.
Idioma	Selecciona el idioma del dispositivo.
Tiempo de espera del menú (s)	Cuando no hay ninguna operación, y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. La función puede desactivarse o ajustar el valor deseado entre 60 y 99999 segundos.
Tiempo de inactividad hasta la presentación de diapositivas (s)	Cuando no hay ninguna operación, y el tiempo excede el valor establecido, se reproducirá una presentación de diapositivas. La función puede desactivarse o puede ajustar el valor entre 3 y 999 segundos.
Intervalo de proyección de diapositivas (s)	Es el intervalo de tiempo en pasar de una foto a otra. La función puede desactivarse, o puede ajustar el intervalo entre 3 y 999 segundos.
Tiempo de reposo (m)	Si se activa el modo de reposo, y cuando no hay ninguna operación en el dispositivo, entonces el dispositivo entrará en modo de espera. Esta función se puede desactivar o establecer un valor entre 1-999 minutos.
Estilo de la pantalla principal	El estilo de la pantalla principal puede seleccionarse según las preferencias del usuario.

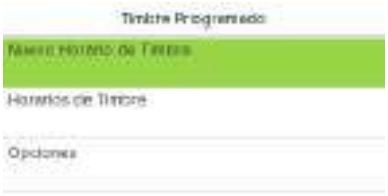
7.2 Ajustes de voz

Selecciona **Voz** en la interfaz **Personalizar** para configurar los ajustes de voz

Nombre de la función	Descripción
Mensaje de voz	Permite activar o desactivar las indicaciones de voz durante las operaciones de las funciones.
Indicación táctil	Activa o desactiva los sonidos del teclado.
Volumen	Ajusta el volumen del dispositivo, que puede oscilar entre 0 y 100.

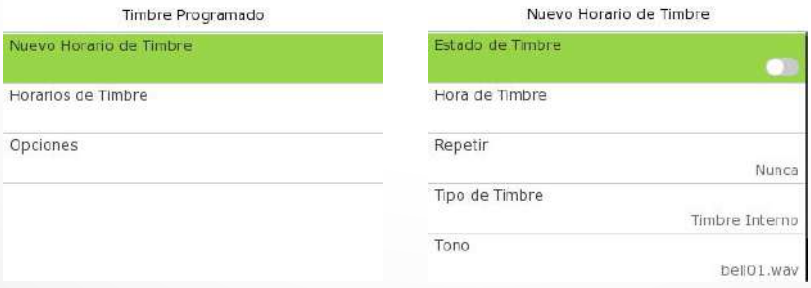
7.3 Horarios de timbres

Seleccione **Horarios de timbres** en la interfaz **Personalizar** para configurar los ajustes de timbre.



- **Nuevo horario de timbres**

.Seleccione **Nuevo horario de timbre** en la interfaz **Horario de timbre** para añadir uno nuevo.



Nombre de la función	Descripción
Estado de timbre	Permite activar o desactivar el estado del timbre.
Hora de Timbre	Una vez ajustado el tiempo deseado, el dispositivo se activará automáticamente para hacer sonar el timbre durante ese tiempo.
Repetir	Establezca el número de cuentas necesario para repetir el timbre programado.

Tipo de timbre	Seleccione el tipo de timbre: Timbre interno, Timbre externo o Timbre interno y externo.
Tono de llamada	Selecciona un tono de llamada.
Retardo de timbre interno	Ajuste el tiempo de reproducción de la campana interna. Los valores válidos van de 1 a 999 segundos.

- **Todos los horarios de los timbres:**

  Una vez programado el timbre, en la interfaz de **Horarios de timbres** pulse Todos los **Horarios de timbre** para ver el timbre recién programado.

- **Editar timbre programado:**

  En la interfaz **Todos los horarios de timbre**, seleccione el horario de timbre deseado y seleccione **Editar** para editar el horario de timbre seleccionado. El método de edición es el mismo que para añadir un nuevo horario de timbre.

- **Borrar una timbre:**

  En la interfaz **Todos los horarios de timbre**, seleccione el horario de timbre deseado, seleccione **Borrar** y, a continuación, pulse **M/OK** para borrar el timbre seleccionado.

- **Opciones:**

  Seleccione **Opciones** en la interfaz **Programa de timbre** para configurar el terminal de salida de timbre externo **NC1/NO1**, que está desactivado por defecto.

Nota: *El timbre exterior y la cerradura son opciones mutuamente excluyentes. Cuando esté activada la función de timbre externo, tenga cuidado de no conectar el cable equivocado.*

7.4 Opciones de estados de registro

Seleccione **Opciones de estado de registro** en la interfaz **Personalizar** para configurar los ajustes de estado de registro.

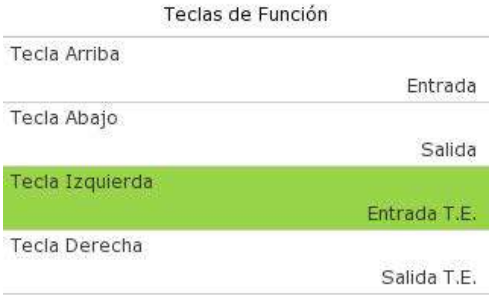
Nombre de la función	Descripción
Modo de Estado de Marcación	**Desactivado:** Desactiva la función de estado de marcación. Por lo tanto, la tecla de estado de marcación establecida en el menú de asignaciones de teclas de acceso directo no será válida. **Modo Manual:** Cambie la tecla de estado de marcación manualmente, y la tecla de estado de marcación desaparecerá después del tiempo de espera del estado de marcación. **Modo automático:** La tecla de estado de marcación cambiará automáticamente a un estado de marcación específico de acuerdo con el horario predefinido que puede establecerse en las asignaciones de teclas de acceso directo.

	Modo manual y automático: La interfaz principal mostrará la tecla de estado de fichaje automático. Sin embargo, los usuarios todavía podrán seleccionar la alternativa que es el estado de asistencia manual. Una vez transcurrido el tiempo de espera, la tecla de estado de marcación de conmutación manual se convertirá en tecla de estado de marcación de conmutación automática. **Modo Manual Fijo:** Una vez que la tecla de estado de fichaje se ajusta manualmente a un estado de marcación determinado, la función permanecerá sin cambios hasta que se vuelva a cambiar manualmente. **Modo fijo:** Sólo se mostrará la tecla de estado de marcación fijada manualmente. Los usuarios no pueden cambiar el estado pulsando ninguna otra tecla.
Tiempo de espera del estado de marcación	Es el tiempo durante el cual se muestra el estado de marcación. El valor oscila entre 5 y 999 segundos.
Estado de marcación requerido	Seleccione si es necesario seleccionar un estado de asistencia tras la verificación. **ENCENDIDO:** El estado de asistencia debe seleccionarse después de la verificación. **APAGADO:** No es necesario seleccionar el estado de asistencia tras la verificación

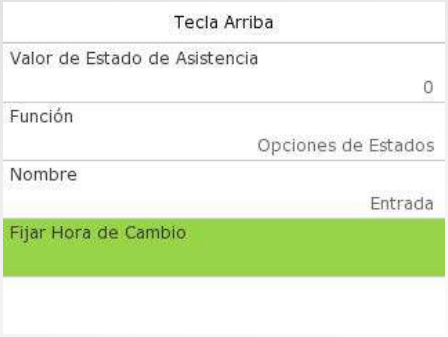
7.5 Asignación de teclas de acceso directo

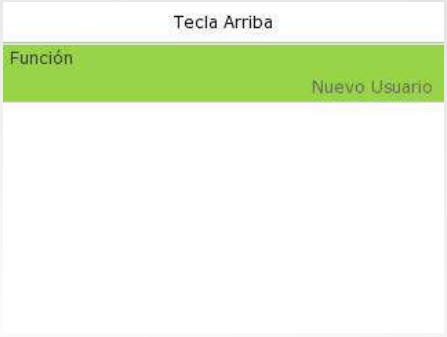
Los usuarios pueden definir teclas de acceso directo para el estado de asistencia y para las teclas funcionales que se definirán en la interfaz principal. Así, en la interfaz principal, cuando se pulsen las teclas de acceso directo, se mostrará directamente el estado de asistencia correspondiente o la interfaz de funciones.

Seleccione **Asignaciones de teclas de acceso directo** en la interfaz **Personalizar** para configurar las teclas de acceso directo necesarias.



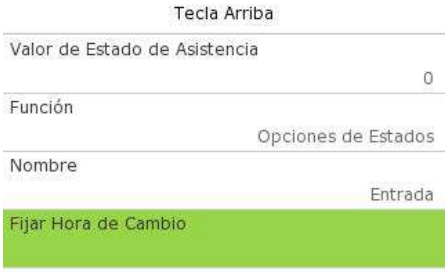
- En la interfaz de **asignaciones de teclas de acceso directo**, seleccione la tecla de **acceso directo** necesaria para configurar los ajustes de la tecla de acceso directo.
- En la interfaz **Tecla de acceso directo,** pulse **Función** para establecer el proceso funcional dela tecla de acceso directo como tecla de estado de perforación o tecla de función.
- Si la tecla de acceso directo se define como una tecla de función (como Nuevo usuario, Todoslos usuarios, etc.), la configuración se completa como se muestra en la imagen siguiente.

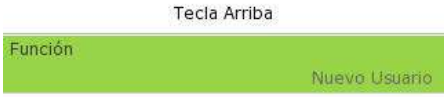




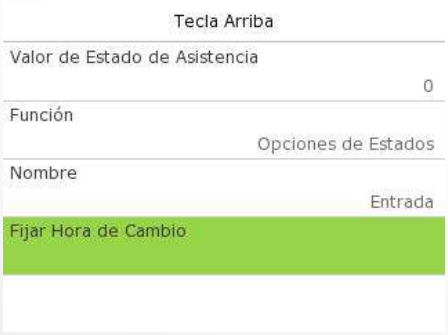
- Si la tecla de acceso directo está configurada como tecla de estado de perforación (como registro de entrada, registro de salida, etc.), es necesario configurar el valor de estado deperforación (valor válido 0~250), nombre.

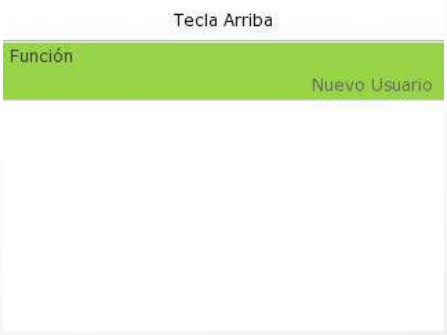
- **Ajustar la hora de conmutación**
  - El tiempo de conmutación se ajusta de acuerdo con las opciones del estado de perforación.
  - Cuando el Modo de Estado de Perforación se establece en Modo Automático, se debeestablecer el tiempo de conmutación.
  - En la interfaz de teclas de acceso rápido, pulse Ajustar hora de conmutación para ajustar la hora de conmutación.
  - En la interfaz Ciclo de conmutación, seleccione el ciclo de conmutación (lunes, martes, etc.) como se muestra en la imagen siguiente.





  - Una vez seleccionado el Ciclo de conmutación, ajuste la hora de conmutación para cada díay pulse **M/OK** para confirmar, como se muestra en la imagen siguiente

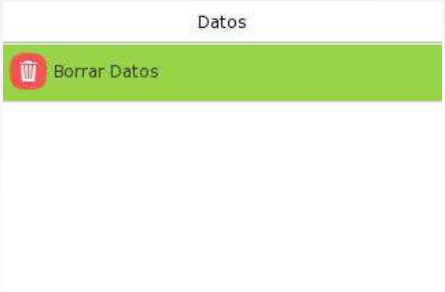




Nota: *Cuando la función está configurada en Indefinido, el dispositivo no habilitará la tecla de estado de marcación*

8 Gestión de datos

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione **Gestión de datos** para gestionar los datos relevantes del dispositivo.



Seleccione **Borrar Datos** en la interfaz de **Gestión de Datos** para borrar los datos necesarios.

Nombre de la función	Descripción
Eliminar datos de asistencia	Para borrar datos de asistencia condicionalmente.
Eliminar foto de asistencia	Para borrar las fotos de presencia del personal designado.
Eliminar foto de la lista negra	Para borrar las fotos tomadas durante las verificaciones fallidas.
Eliminar todos los datos	Para borrar la información y los registros de asistencia de todos los usuarios registrados.
Eliminar función de administrador	Para eliminar todos los privilegios de administrador.
Eliminar plantillas de fotos de usuario	Para borrar plantillas de fotos de usuario en el dispositivo. Al eliminar fotos de plantilla, hay un recordatorio de riesgo: "**Es necesario volver a registrar la cara después de una actualización del algoritmo**".

El usuario puede seleccionar **Borrar todo** o **Borrar por intervalo de tiempo** al borrar los datos de asistencia, las fotos de asistencia o las fotos de la lista de bloqueados. Al seleccionar **Borrar porintervalo de tiempo**, debe establecer un intervalo de tiempo específico para borrar todos los datos dentro de un periodo concreto.

Seleccione **Borrar por intervalo de tiempo**.

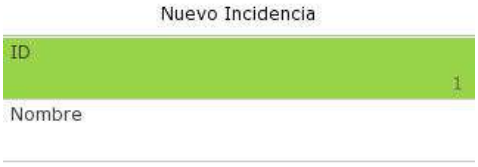
Ajuste el intervalo de tiempo y pulse **M/OK.**

9 Código de trabajo

Los salarios de los empleados están sujetos a sus registros de asistencia. Un empleado puede realizar más de un tipo de trabajo, que puede variar con el tiempo. Dado que el salario varía en función de los tipos de trabajo, el terminal FFR proporciona un parámetro para indicar el tipo de trabajo correspondiente para cada registro de asistencia, con el fin de facilitar una rápida comprensión de las distintas situaciones de asistencia durante el tratamiento de los datos de asistencia.

Seleccione **Código de trabajo** en la interfaz del menú principal.

9.1 Añadir un código de trabajo



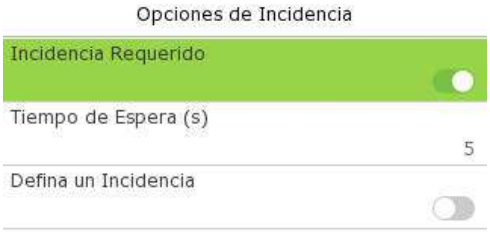
Menú	Descripción
ID	Es el código digital del código de trabajo. Los usuarios pueden establecer un valor válido entre 1 y 99999999.
Nombre	Es la denominación del código de trabajo.

9.2 Todos los códigos de trabajo

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

9.3 Opciones de código de trabajo

Para establecer si es obligatorio introducir el código de trabajo y si el código de trabajo introducido debe existir durante la autenticación.



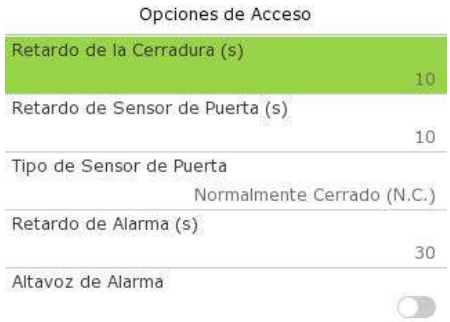
En la verificación **1:N** o **1:1**, el sistema mostrará automáticamente la siguiente ventana. Seleccione manualmente el código de palabra correspondiente para realizar la verificación correctamente.

10 Control de acceso

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione **Control de acceso** para establecer el control de bloqueos y configurar otros ajustes de parámetros relacionados con el control de acceso.

10.1 Opciones de control de acceso

Seleccione **Opciones de control de acceso** en la interfaz **Control de acceso** para configurar los parámetros del bloqueo de control del terminal y los equipos relacionados.



Nombre de la función	Descripción
Retraso del bloqueo de la(s) puerta(s)	El tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1~10 segundos; 0 segundos representa la desactivación de la función.
Retraso del sensor de puerta(s)	Si la puerta no está bloqueada y se deja abierta durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido de Retardo del sensor de puerta oscila entre 1 y 255 segundos.
Tipo de sensor de puerta(s)	Existen tres tipos de sensores: **Ninguno, Normal Abierto(NO), y Normal Cerrado(NC).** **Ninguno:** Significa que el sensor de la puerta no está en uso. **Normalmente abierto (NO)**: Significa que la puerta siempre se deja abierta cuando hay corriente eléctrica. **Normalmente cerrado (NC):** Significa que la puerta siempre se deja cerrada cuando la energía eléctrica está conectada.
Retraso de la alarma de la puerta(s)	Cuando el estado del sensor de puerta es incoherente con el del tipo de sensor de puerta, la alarma se activará tras un periodo de tiempo; este periodo de tiempo es el Retardo de Alarma de Puerta (el valor oscila entre 0 y 999 segundos).
Sonido de la alarma	Transmite una alarma sonora o de desmontaje desde el local. Cuando la puerta se cierra o la verificación se realiza correctamente, el sistema cancela la alarma desde el local.

11 Gestor USB

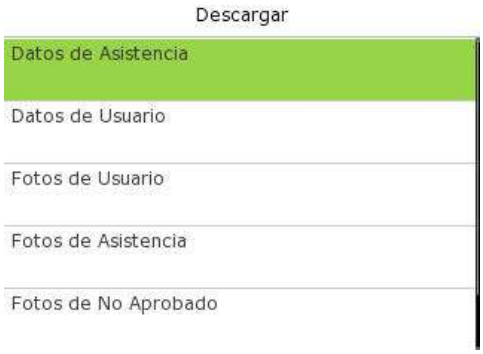
Puede importar la información del usuario y los datos de asistencia de la máquina al software de asistencia correspondiente para procesarlos mediante un disco USB, o importar la información del usuario a otros dispositivos para realizar copias de seguridad. Antes de cargar/descargar datos desde/al disco USB, inserte primero el disco USB en la ranura USB.

Seleccione **Gestor USB** en la interfaz del menú principal.

Nota: *Sólo se admite el formato FAT32 cuando se descargan datos mediante un disco USB.*

11.1 Descarga USB

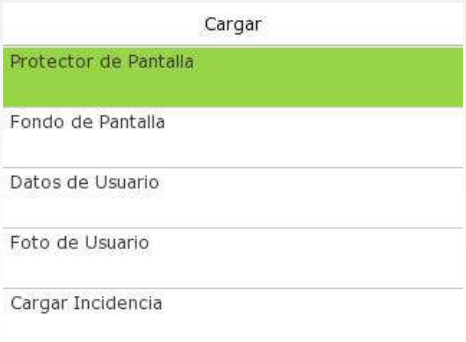
En la interfaz del **Administrador USB**, pulse **Descargar**.



Nombre de la función	Descripción
Datos de asistencia	Para descargar todos los datos de asistencia en el período de tiempo especificado en el disco USB.
Datos del usuario	Para descargar toda la información del usuario del dispositivo en un disco USB.
Retrato de usuario	Para descargar todos los retratos de usuario del dispositivo en un disco USB.
Foto de asistencia	Para descargar todas las fotos de asistencia del dispositivo en un disco USB.
Lista bloqueo de fotos	Para descargar todas las fotos bloqueadas (fotos tomadas después de verificaciones fallidas) del dispositivo al disco USB.
Código de trabajo	Para descargar todo el código de trabajo del dispositivo en el disco USB.

11.2 Carga USB

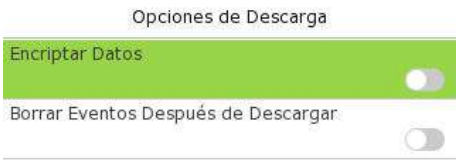
En la interfaz del **Administrador USB**, pulse **Descargar**



Nombre de la función	Descripción
Protector de pantalla	Para cargar todos los protectores de pantalla del disco USB en el dispositivo. Puede elegir Cargar la foto seleccionada o cargar todas las fotos. Las imágenes se mostrarán en la interfaz principal del dispositivo después de la carga.
Fondo de pantalla	Para cargar todos los fondos de pantalla del disco USB en el dispositivo. Puede elegir Cargar la foto seleccionada o cargar todas las fotos. Las imágenes se mostrarán en la pantalla después de la carga.
Datos del usuario	Para cargar toda la información del usuario desde el disco USB al dispositivo.
Retrato de usuario	Para cargar todos los retratos de usuario desde el disco USB al dispositivo.
Cargar código de trabajo	Para cargar todo el código de trabajo del disco USB en el dispositivo.

11.3 Descargar opciones

En la interfaz del **Administrador USB**, pulse **Opciones de descarga**.

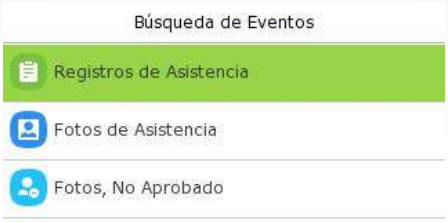


Nombre de la función	Descripción
Cifrar fecha de asistencia	Los datos de asistencia se encriptan durante la carga y descarga.
Borrar datos de T&A	Tras la descarga, los datos de asistencia del dispositivo se eliminan.

12 Búsqueda de asistentes

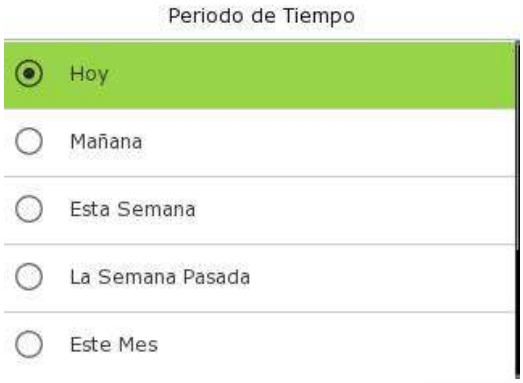
Una vez verificada la identidad de un usuario, los registros de eventos se guardarán en el dispositivo. Esta función permite a los usuarios comprobar sus registros de asistencia.

Cuando el dispositivo se encuentre en la interfaz inicial, pulse **M/OK** y seleccione Búsqueda de asistencia para buscar el registro de asistencia requerido.

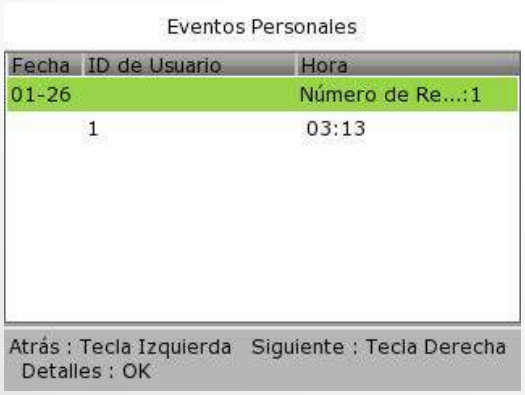


El proceso de búsqueda de fotos de asistencias y listas de bloqueo es similar al de búsqueda de registros de sucesos. A continuación se muestra un ejemplo de **búsqueda de registro de asistencia.** En la interfaz de búsqueda de asistencia, pulse **Registro de asistencia** para buscar el registro deseado

1. Introduzca el ID de usuario que desea buscar y pulse **M/OK**. Si desea buscar registros de todos los usuarios, pulse **M/OK** sin introducir ningún ID de usuario.



2. Seleccione el intervalo de tiempo en el que deben buscarse los registros.



3. Una vez finalizada la búsqueda de registros. Pulse el registro resaltado en verde para ver sus detalles.

4. La figura muestra los detalles del registro seleccionado.

13 Autotest

Cuando el dispositivo está en la interfaz inicial, pulse **M/OK** y seleccione **Autotest**, permite al sistema comprobar automáticamente si las funciones de varios módulos funcionan con normalidad, incluida la pantalla LCD, voz, Teclado, Huella Dactilar, Cámara y Reloj en Tiempo Real (RTC).

Nombre de la función	Descripción
Prueba LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mediante la visualización a todo color, blanco puro y negro puro para comprobar si la pantalla muestra los colores con normalidad.
Prueba de voz	Para comprobar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de la voz es buena.
Prueba de tablero	El terminal comprueba si todas las teclas del teclado funcionan con normalidad. Pulse cualquier tecla de la interfaz Teclado de prueba para comprobar si la tecla pulsada coincide con la tecla mostrada en la pantalla. Las teclas se muestran en gris oscuro antes y se vuelven verdes después de pulsarlas. Pulse ESC para salir de la prueba.
Prueba de sensor de huella dactilar	Para probar el sensor de huellas dactilares, presione con un dedo sobre el escáner para comprobar si la imagen de la huella dactilar adquirida es nítida. Cuando presione con un dedo sobre el escáner, la imagen de la huella dactilar aparecerá en la pantalla.
Prueba de cámara	Para comprobar si la cámara funciona correctamente, comprueba las fotos tomadas para ver si son lo suficientemente claras. (Igual que "Rostro de prueba").
Reloj de prueba RTC	Para probar el RTC. El dispositivo comprueba si el reloj funciona con normalidad y precisión con un cronómetro. Pulse M/OK para iniciar el conteo y púlselo de nuevo para detenerlo.

14 Información del sistema

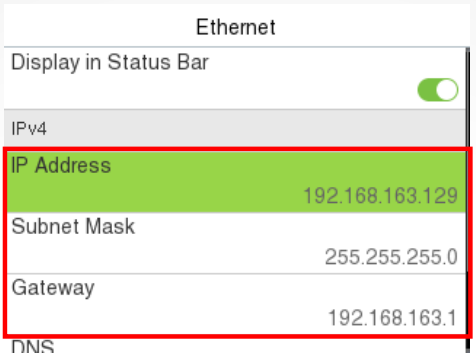
Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione **Información del sistema** para ver el estado de almacenamiento, la información de la versión del dispositivo, la información del firmware y la política de privacidad.

Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuario del dispositivo actual, la contraseña, la plantilla facial, la huella dactilar y almacenamiento de tarjetas, registros T&A, fotos de asistencia y lista de bloqueo y fotos de perfil.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC y el algoritmo de huella digital, algoritmo de plantilla facial, información de plataforma, versión de MCU, BAT MCU y fabricante.
Info firmware	Muestra la versión del firmware y otra información sobre la versión del dispositivo.
Política de privacidad	El control de la política de privacidad aparecerá cuando el gadget se encienda por primera vez. Tras hacer clic en "La he leído", el cliente puede utilizar el producto con regularidad. Haga clic en **Información del sistema** > **Política de privacidad** para ver el contenido de la política de privacidad. El contenido de la política de privacidad no permite la exportación de discos U. ***Nota:*** *El texto de la política de privacidad actual solo está disponible en chino simplificado/inglés. Sin embargo, la traducción de otros contenidos en varios idiomas está en progreso, con más iteraciones.*

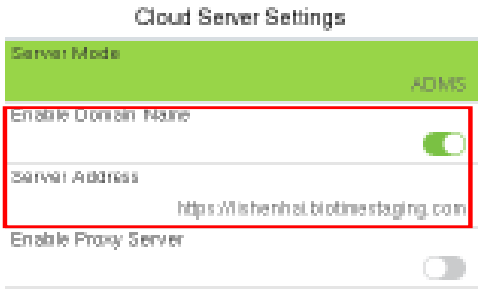
15 Conectar con el software BioTime Cloud

15.1 Añadir dispositivo al software

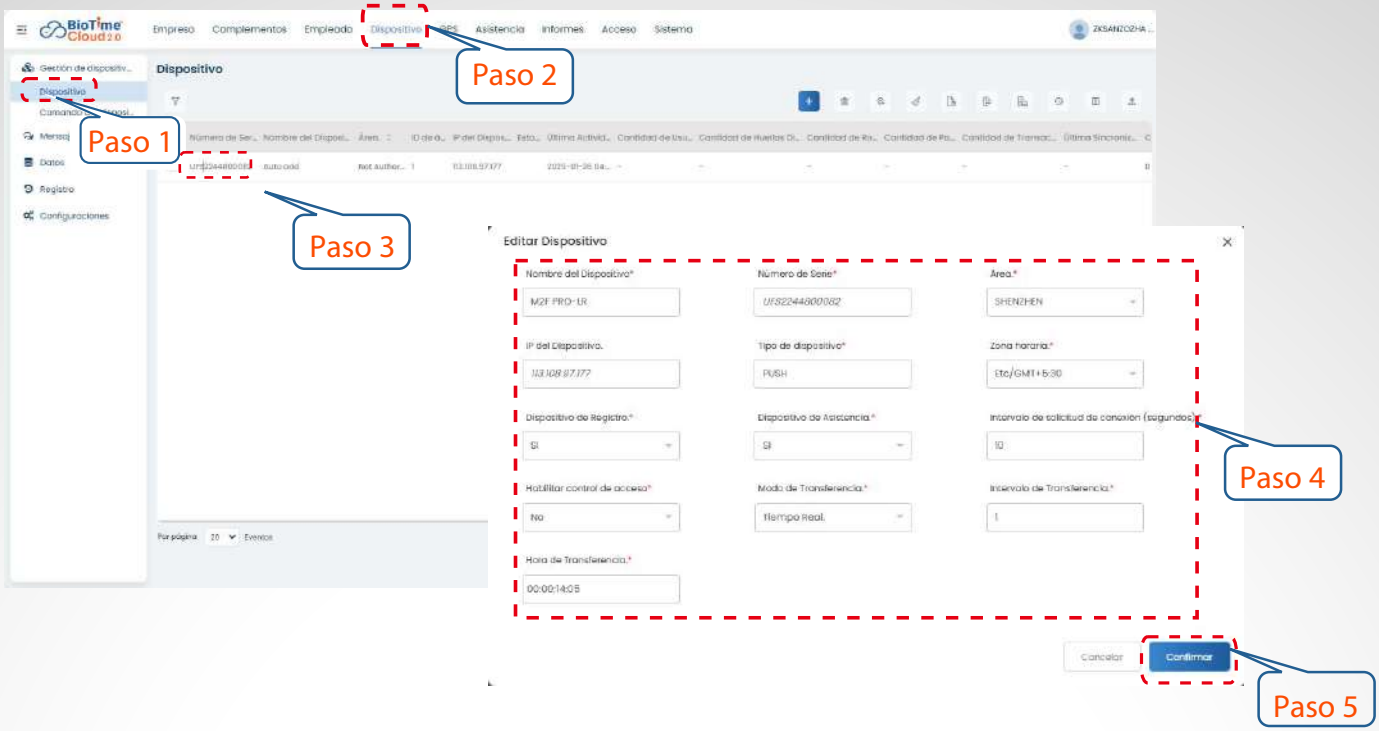
1. Pulse **COMM**. > **Ethernet** en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.



2. En el menú principal, pulse **COMM**> **Configuración del servidor en nube** para activar Nombre de dominio e introducir el nombre de dominio correcto..

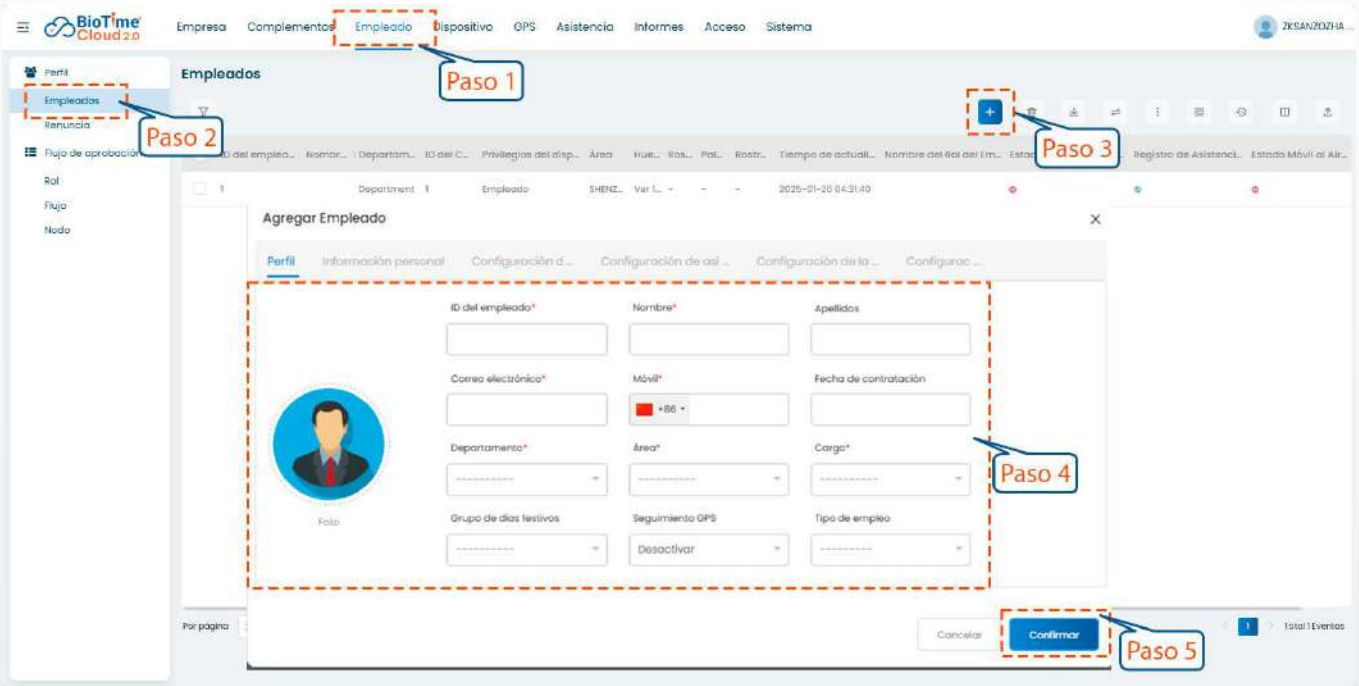


3. Después de configurar el dispositivo, éste se añadirá automáticamente al software. Abrir BioTime Cloud, haga clic en **Dispositivo** > **Gestión de dispositivos** > **Dispositivo**, seleccione el dispositivo en la lista, cambie el Nombre del dispositivo y el Área, y podrá comunicarse con el software.



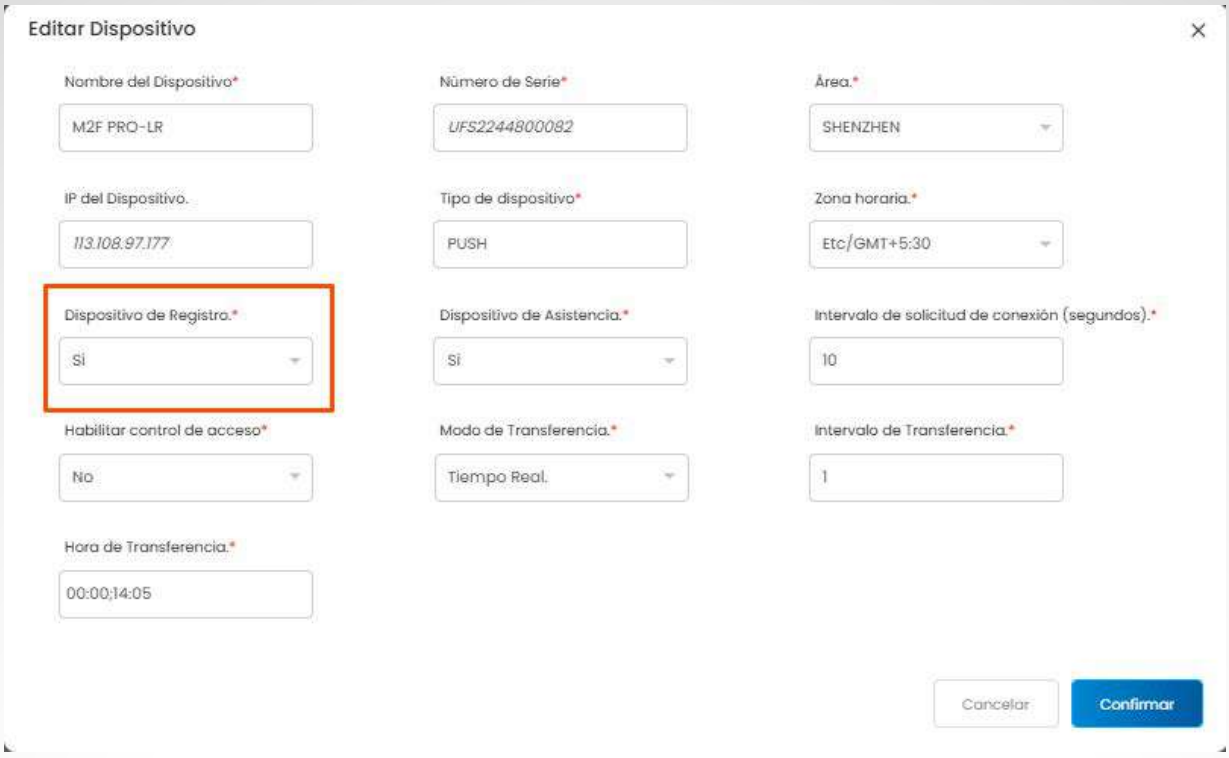
15.2 Añadir personal en el software y registro de huellas dactilares en línea

1. Haga clic en Empleado > Perfil > Empleados > + icono

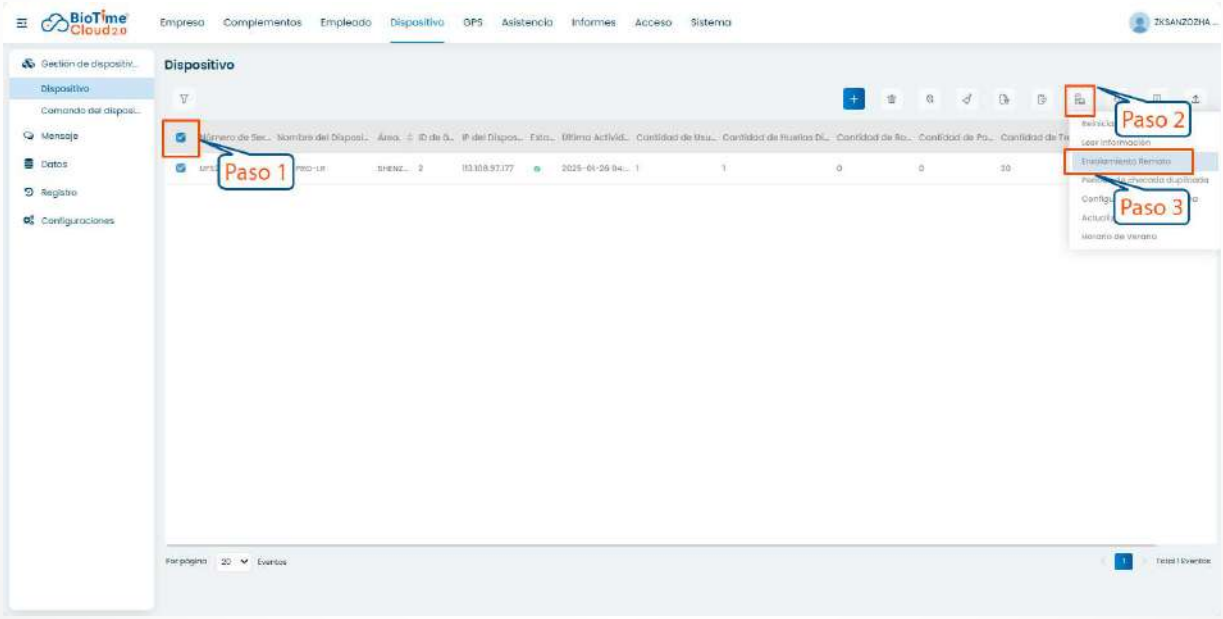


2. Rellene todos los campos obligatorios y haga clic en Confirmar para registrar un nuevo usuario.

3. Haga clic en **Dispositivo** > **Gestión de Dispositivos** > **Dispositivo**, seleccione el dispositivo en la lista, haga clic en el icono para entrar en la interfaz Editar Dispositivo, establezca el Dispositivode Registro como Sí y haga clic en Confirmar.

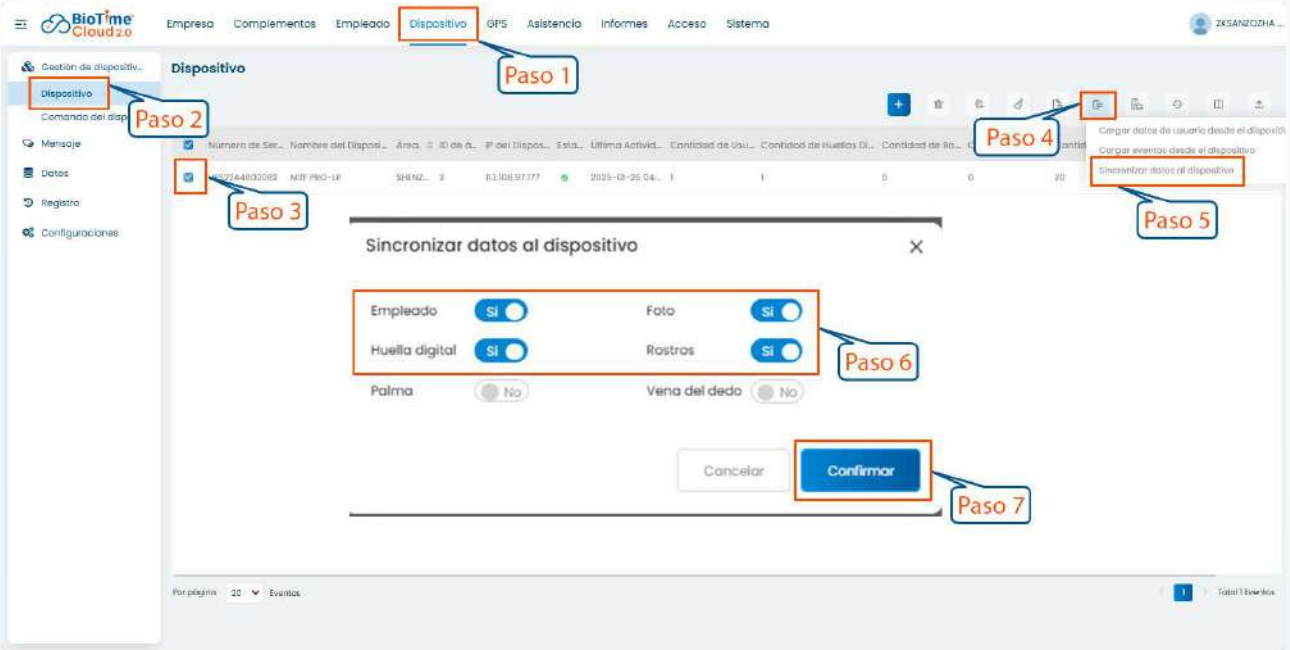


4. Seleccione el dispositivo en la lista, haga clic en **icono** > **Inscribirse a distancia**.



5. Introduzca el ID de empleado y seleccione el dedo que desea registrar y pulse con el dedo en el sensor de huellas dactilares del dispositivo tres veces. Si la huella se registra correctamente, el dispositivo mostrará "Registrado correctamente".

6. Seleccione el dispositivo en la lista, haga clic en el icono >**Sincronizar datos** con el dispositivo para sincronizar todos los datos en el dispositivo, incluidos los nuevos usuarios.



Anexo 1

Requisitos de la recogida y registro en vivo de plantillas faciales de luz visible

1. Se recomienda realizar el registro en un ambiente interior con una fuente de luz adecuada sin subexposición ni sobreexposición.

2. No coloque el dispositivo hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz intensa.

3. Para el registro se recomienda ropa de color oscuro, diferente del color de fondo.

4. Por favor, exponga la plantilla de la cara y la frente correctamente y no cubra la plantilla de la cara y las cejas con el pelo.

5. Se recomienda mostrar una expresión facial sencilla. (Una sonrisa es aceptable, pero no cierre los ojos, ni incline la cabeza hacia ninguna orientación).

6. Se requieren dos plantillas para una persona con gafas, una plantilla con gafas y la otra sin lasgafas.

7. No lleve accesorios como pañuelo o mascarilla que puedan taparle la boca o la barbilla.

8. Por favor, mire la plantilla hacia la derecha en dirección al dispositivo de captura, y sitúe la plantilla de su cara en el área de captura de la plantilla como se muestra en la siguiente plantilla.

9. No incluya más de una plantilla facial en el área de captura.

10. Se recomienda una distancia de 50 cm a 80 cm para capturar la plantilla. (La distancia puede ajustarse en función de la altura del cuerpo).

Anexo 2

Política de privacidad

Noticia

Para ayudarle a utilizar mejor los productos y servicios de ZKTeco (en lo sucesivo, "nosotros", "nuestro" o "nos"), un proveedor de servicios inteligentes, recopilamos sistemáticamente su información personal. Puesto que entendemos la importancia de su información personal, tomamos su privacidad sinceramente y hemos formulado esta política de privacidad para proteger su información personal. Hemos enumerado las políticas de privacidad a continuación para entender con precisión las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes.

Antes de utilizar nuestros productos y servicios, lea atentamente y comprenda todas las normas y disposiciones de la presente Política de Privacidad. Si no está de acuerdo con el acuerdo correspondiente o con alguna de sus cláusulas, deberá dejar de utilizar nuestros productos y servicios.

- **Recolección de la información**

Para garantizar el funcionamiento normal del producto y contribuir a la mejora del servicio,recopilaremos la información que nos facilite voluntariamente o que nos autorice durante el registro y el uso o que se genere como resultado de su uso de los servicios.

1. Información de registro del usuario: En su primer registro, la plantilla de características(plantilla de huella dactilar/plantilla de rostro/plantilla de palma) se guardará en el dispositivo según el tipo de dispositivo que haya seleccionado para verificar la similitud única entre usted y el ID de usuario que ha registrado. Opcionalmente puede introducir su Nombre y Código. La información anterior es necesaria para que pueda utilizar nuestros productos. Si no facilita dicha información, no podrá utilizar regularmente algunas funciones del producto.

2. Información sobre el producto: De acuerdo con el modelo de producto y su permiso concedido cuando instala y utiliza nuestros servicios, la información relacionada del producto en el que se utilizan nuestros servicios se recopilará cuando el producto se conecte al software, incluido el Modelo de producto, el Número de versión del firmware, el Número de serie del producto y la Información de capacidad del producto. Cuando conecte su producto al software, lea atentamente la política de privacidad del software específico.

- **Seguridad y gestión de los productos**

1. Cuando utilice nuestros productos por primera vez, deberá establecer el privilegio de administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que debe establecer el privilegio de administrador cuando acceda a la interfaz del menú principal. Si sigue sin establecer el privilegio de administrador después de recibir el aviso del sistema, debe ser consciente del posible riesgo para la seguridad(por ejemplo, los datos pueden modificarse manualmente).

2. Todas las funciones de visualización de la información biométrica están desactivadas en nuestros productos por predeterminada. Puede elegir Menú > Configuración del sistema para establecer si desea mostrar la información biométrica. Si habilita estas funciones, asumimos que es consciente de los riesgos de seguridad de la privacidad personal especificados en la política de privacidad.

3. Por defecto, sólo se muestra su ID de usuario. Puede configurar si desea mostrar otra información de verificación de usuario (como Nombre, Departamento, Foto, etc.) bajo el privilegio de Administrador. Si decide mostrar dicha información, asumimos que es consciente de los posibles riesgos de seguridad (por ejemplo, su foto se mostrará en la interfaz del dispositivo).

4. La función de cámara está desactivada por defecto en nuestros productos. Si desea habilitar esta función para tomar fotos de sí mismo para el registro de asistencia o tomar fotos de extraños para el control de acceso, el producto habilitará el tono de aviso de la cámara. Una vez que habilite esta función, asumimos que es consciente de los posibles riesgos de seguridad.

5. Todos los datos recogidos por nuestros productos se cifran mediante el algoritmo AES256.Todos los datos cargados por el Administrador en nuestros productos se cifran automáticamente utilizando el algoritmo AES 256 y se almacenan de forma segura. Si el Administrador descarga datos de nuestros productos, asumimos que usted necesita procesar los datos y que conoce el riesgo potencial de seguridad. En tal caso, usted asumirá la responsabilidad de almacenar los datos. Debe saber que algunos datos no pueden descargarse por motivos de seguridad.

6. Toda la información personal de nuestros productos puede ser consultada, modificada o eliminada. Si ya no utiliza nuestros productos, borre sus datos personales.

- **Cómo tratamos la información personal de los menores**

Nuestros productos, sitio web y servicios están diseñados principalmente para adultos. Sin el consentimiento de los padres o tutores, los menores no podrán crear su propia cuenta. Si es usted menor de edad, le recomendamos que pida a sus padres o tutores que lean atentamente esta Política, y que sólo utilice nuestros servicios o la información que le proporcionamos con el consentimiento de sus padres o tutores.

Sólo utilizaremos o divulgaremos información personal de menores recopilada con el consentimiento de sus padres o tutores si y en la medida en que dicho uso o divulgación esté permitido por la ley o hayamos obtenido el consentimiento explícito de sus padres o tutores, y dicho uso o divulgación tenga por objeto proteger a los menores.

Cuando nos demos cuenta de que hemos recopilado información personal de menores sin el consentimiento previo de los padres verificable, eliminaremos dicha información lo antes posible.

- **Otros**

Puede visitar https://www.zkteco.com/cn/index/Index/privacy_protection.html para obtener más información sobre cómo recopilamos, utilizamos y almacenamos de forma segura su información personal. Para seguir el ritmo del rápido desarrollo de la tecnología, el ajuste de las operaciones comerciales y hacer frente a las necesidades de los clientes, deliberaremos y optimizaremos constantemente nuestras medidas y políticas de protección de la privacidad. Le invitamos a visitar nuestro sitio web oficial en cualquier momento para conocer nuestra política de privacidad más reciente.

Operación ecológica

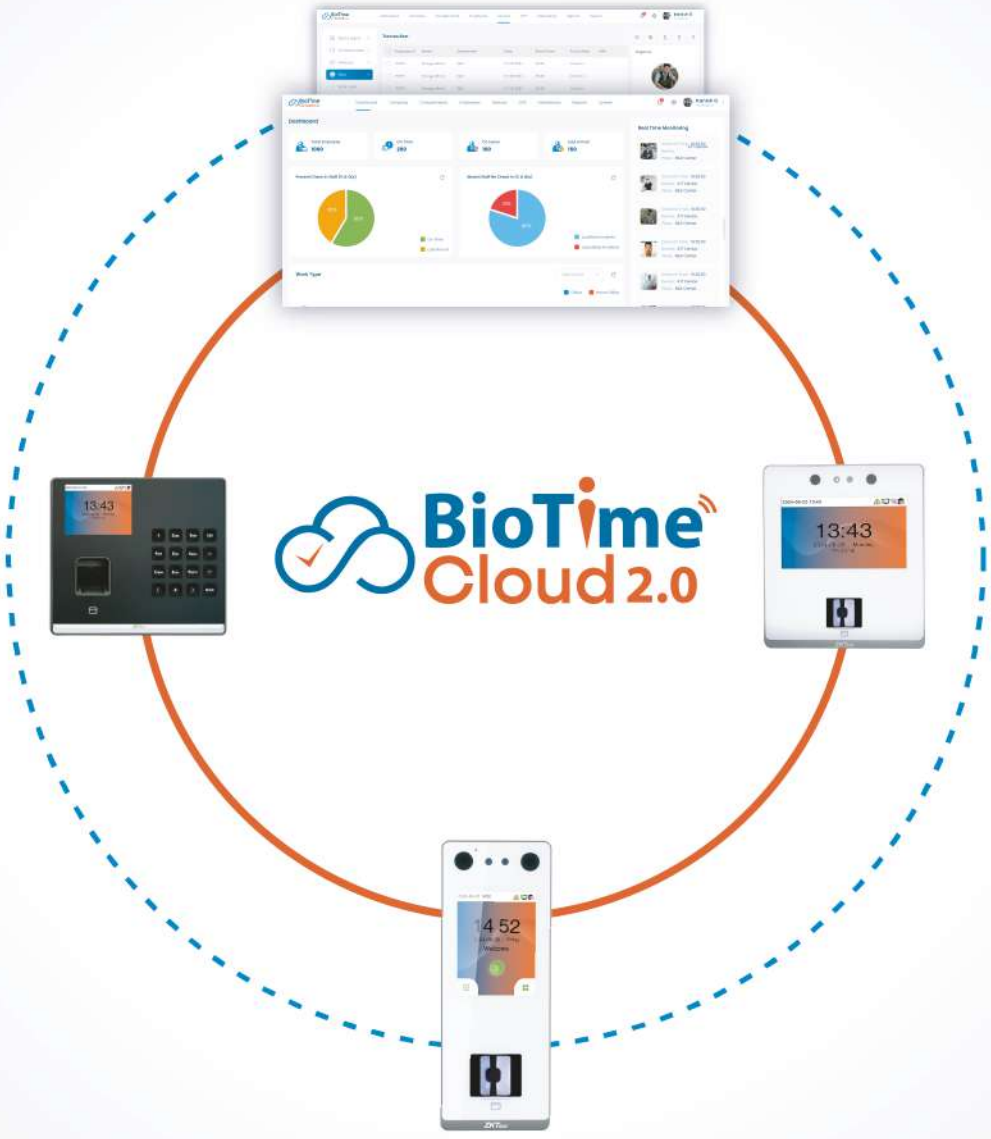
El "periodo de operación ecológica" del producto se refiere al tiempo durante el cual este producto no liberará sustancias tóxicas o peligrosas cuando se utilice de acuerdo con los requisitos establecidos en este manual.
El periodo de operación ecológica especificado para este producto no incluye baterías u otros componentes que se desgasten fácilmente y deban ser reemplazados periódicamente. El periodo de operación ecológica de la batería es de 5 años.

Sustancias Peligrosas o Tóxicas y sus Cantidades

Hazardous/Toxic Substance/Element

Nombre del Componente	Plomo (Pb)	Mercurio (Hg)	Cadmio (Cd)	Cromo Hexavalente (Cr6+))	Bifenilos Polibromados (PBB)	Éteres de Difénil Polibromado (PBDE)
Resistor de chip	x	o	o	o	o	o
Capacitor de Chip	x	o	o	o	o	o
Introductor de Chip	x	o	o	o	o	o
Diodo	x	o	o	o	o	o
Componente ESD	x	o	o	o	o	o
Bocina	x	o	o	o	o	o
Adaptador	x	o	o	o	o	o
Tornillos	o	o	o	x	o	o

o indica que la cantidad total de contenido tóxico en todos los materiales homogéneos está por debajo del límite especificado en SJ/T 11363—2006.
× indica que la cantidad total de contenido tóxico en todos los materiales homogéneos excede el límite especificado en SJ/T 11363—2006.
Nota: El 80% de los componentes de este producto están fabricados utilizando materiales no tóxicos y ecológicos. Los componentes que contienen toxinas o elementos dañinos se incluyen debido a limitaciones económicas o técnicas actuales que impiden su reemplazo por materiales o elementos no tóxicos.



www.zkteco.com

www.zkteco.mx