

Manual de Usuario

Modelo aplicable(s): M1

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.

Sin el consentimiento previo por escrito de ZKTeco, ninguna parte de este manual puede ser copiada o reenviada de ninguna manera o forma. Todas las partes de este manual pertenecen a ZKTeco y sus filiales (en adelante, la «Empresa» o «ZKTeco").

Marca Registrada

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

Exención de Responsabilidad

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 ser leído en su totalidad antes de iniciar la operación y mantenimiento del equipo suministrado. Si alguno de los contenidos del manual le 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 totalmente familiarizado con el diseño y que dicho personal haya recibido una formación completa en 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.

Este manual y la información contenida en el mismo pueden incluir imprecisiones técnicas, 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 están destinadas a mejorar el funcionamiento de la máquina/unidad/equipo y dichas modificaciones no darán derecho a reclamar ninguna compensación o indemnización por daños y perjuicios en ninguna circunstancia.

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

El producto se actualizará de vez en cuando sin previo aviso. Los procedimientos de funcionamiento más recientes y los documentos pertinentes están disponibles en **https://www.zktecolatinoamerica.com**

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 del Manual

Este manual introduce las operaciones de M1.
Todas las figuras mostradas son solo para fines ilustrativos. Las figuras en este manual pueden no coincidir exactamente con los productos reales.
Las características 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..... 6
Medidas de seguridad..... 6
1 Instrucciones de uso..... 7
1.1 Interface de espera 7
1.2 Modos de Verificación..... 8
1.2.1 Verificación por Huella Digital..... 8
1.2.2 Verificación por Número de Tarjeta..... 11
1.2.3 Verificación por Contraseña..... 12
1.3 Operación de Entrada de Texto..... 13
1.4 Conexión Wi-Fi..... 14
2 Menú principal..... 17
3 Manual de usuario..... 19
3.1 Buscar usuario..... 19
4 Configuración de comunicación..... 19
4.1 Red Inalámbrica..... 20
4.2 Configuración del Servidor en la Nube..... 22
5 Configuración del Sistema..... 23
5.1 Fecha y hora..... 23
5.2 Configuración de Asistencia..... 24
5.3 Parámetros de Huellas Dactilares..... 25
5.4 Configuración de voz..... 26
5.5 Configuración de Cambio Automático..... 27
5.6 Configuración de seguridad..... 28
5.7 Configuración USB..... 29
5.8 Actualización de Firmware en Línea..... 30
5.9 Restablecimiento de fábrica..... 31
6 Gestión de datos..... 31
7 Registro..... 32
8 Prueba..... 33
9 Información del Sistema..... 34
10 Conectar a la plataforma BioTime Cloud 2.0..... 35
10.1 Iniciar sesión en navegador..... 35
10.2 Agregar dispositivos en la plataforma..... 36
10.3 Agregar empleado en la plaforma..... 37
10.3.1 Agregar empleado..... 37
10.3.2 Sincronizar empleados al dispositivo..... 38
10.4 Registrar Método de Verificación desde el Dispositivo..... 39
10.5 Configuración de la aplicación móvil..... 40

Operación ecológica..... 45

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 Interface de espera

1.Cuando el dispositivo se conecta a la fuente de alimentación y se utiliza por primera vez, entra en la pantalla de espera como se muestra a continuación:



Notas:

1) Este dispositivo debe utilizarse en combinación con la plataforma BioTime Cloud. Una vez que los dispositivos se añadan la plataforma, se podrá gestionar el dispositivo de forma unificada.

2) Para obtener detalles sobre cómo añadir el dispositivo, consulte la sección **10.2 Añadir Dispositivo a la plataforma.**

2. Después de vincular el dispositivo exitosamente, se mostrará la pantalla de espera como se indica a continuación.



Iconos de estado

Icono	Nombre	Descripción
	USB	El dispositivo está conectado a una unidad flash USB.
	Servidor ADMS	La conexión entre el dispositivo y el servidor ADMS es exitosa.
		La conexión entre el dispositivo y el servidor ADMS falló.
	Señal Wi-Fi	La conexión Wi-Fi es normal.
		La conexión Wi-Fi falló.

1.2 Modos de Verificación

En el dispositivo existen tres modos de verificación:

- Verificación por huella digital
- Verificación por número de tarjeta
- Verificación por contraseña

Estos modos de verificación pueden utilizarse para registrar entradas y salidas.

1.2.1 Verificación por Huella Digital

- **Registro de Huellas**

El procedimiento de registro de huellas consiste en capturar la huella digital de un usuario y guardarla como una plantilla asociada al ID correspondiente del usuario. Para mejorar la tasa de autenticación por huella digital, asegúrese de registrar la huella correctamente.

- **Registro de Huellas**

El procedimiento de registro de huellas consiste en capturar la huella digital de un usuario y guardarla como una plantilla asociada al ID correspondiente del usuario. Para mejorar la tasa de autenticación por huella digital, asegúrese de registrar la huella correctamente.

- **Selección de dedo para el registro de huella digital**

◊ Se recomienda utilizar el dedo índice o el dedo medio para registrar su huella digital.

◊ Si las huellas digitales de la mano seleccionada están desgastadas o dañadas, intente utilizar la otra mano.

◊ Si los dedos son pequeños, intente realizar el registro con el pulgar

- **Operación de registro**

◊ Coloque el dedo de manera plana y centrada sobre la superficie del sensor.

◊ Se mostrará la puntuación de cada registro. Asegúrese de que la puntuación sea lo suficientemente alta para garantizar un registro y autenticación adecuados.

◊ Coloque el dedo de manera consecutiva hasta que aparezca el mensaje de éxito. A continuación, se muestra una ilustración:



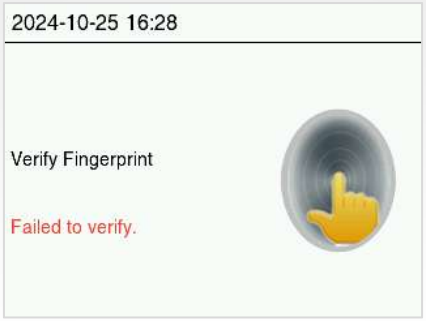
- **Modo de Verificación de Huella Digital 1:N**

El dispositivo compara la huella digital actual, recolectada por el sensor, con todas las huellas almacenadas en el dispositivo. Presione correctamente su dedo sobre el sensor de huellas. Si la huella digital coincide con alguna de las plantillas guardadas, la verificación será exitosa.

Si la verificación es exitosa, se mostrará el siguiente mensaje:



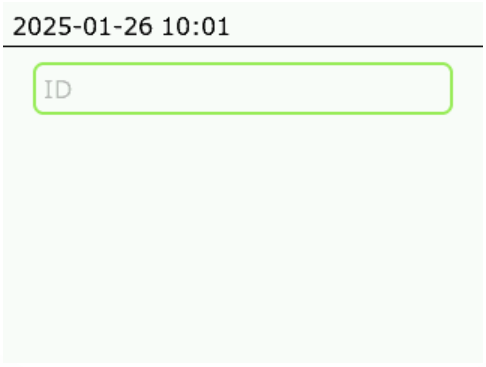
Si la verificación es exitosa, se mostrará el siguiente mensaje::



Si el dispositivo indica "Error en la verificación", presione nuevamente su dedo. Puede intentar la verificación 2 veces más. Si la verificación falla después de estos intentos, el dispositivo volverá a la interfaz de espera.

- **1: 1 Modo de Verificación de Huella Digital**

El dispositivo compara la huella digital actual con las huellas digitales vinculadas al ID de usuario ingresado 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.
Presione las teclas numéricas en el teclado del dispositivo para ingresar al modo de verificación de huella digital 1:1.
1.Ingrese el ID de usuario y presione **M/OK.**



2.Si el usuario ha registrado una tarjeta y una contraseña además de sus huellas digitales, y el método de verificación está configurado en "Verificación de huella digital/tarjeta", aparecerá la siguiente pantalla. Seleccione el ícono de huella digital para ingresar al modo de verificación por huella digital.



3. Coloque el dedo para verificar.

Verificación exitosa:



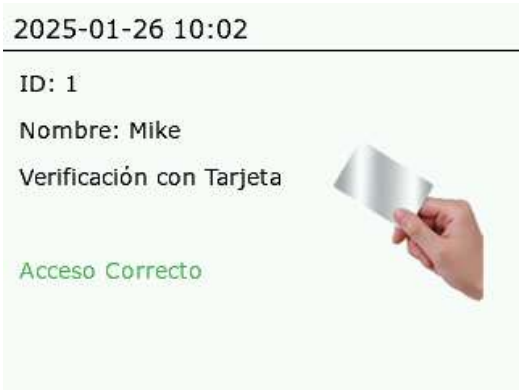
Verificación fallida:



1.2.2 Verificación por Número de Tarjeta

- **Modo de Verificación de Tarjeta 1: N**

El dispositivo compara el número de la tarjeta en el área de inducción de la tarjeta con todos los datos de número de tarjeta registrados en el dispositivo. A continuación se muestra la pantalla de verificación de tarjeta.



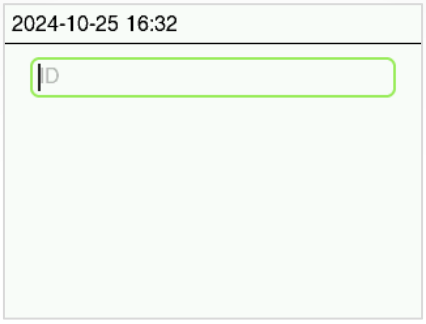
Si la verificación falla, se mostrará el siguiente mensaje:



Modo de Verificación de Tarjeta 1: 1

El modo de verificación 1:1 compara el número de la tarjeta en el área de inducción con el número asociado al ID de usuario del empleado registrado en el dispositivo.
Presione las teclas numéricas en el teclado del dispositivo para ingresar al modo de verificación de tarjeta 1:1.

1. Ingrese el ID de usuario y presione **M/OK.**

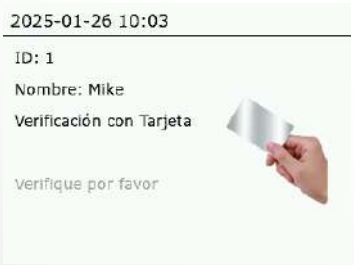


2. Si el usuario ha registrado huella digital y contraseña además de su tarjeta, y el método de verificación está configurado en "Verificación de Contraseña/Huella Digital/Tarjeta", aparecerá la siguiente pantalla. Seleccione el ícono para ingresar al modo de verificación por tarjeta.



3. Coloque la tarjeta en el área de lectura para su verificación.

Verificación exitosa:



Verificación fallida:

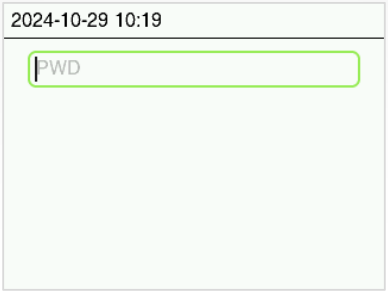


1.2.3 Verificación por Contraseña

El dispositivo compara la contraseña ingresada con la contraseña registrada para el ID de usuario proporcionado.

Presione las teclas numéricas en el teclado del dispositivo para ingresar al modo de verificación de contraseña 1:1. Luego, ingrese el ID de usuario y presione M/OK.

Si el usuario ha registrado una plantilla de huella digital y tarjeta además de la contraseña, y el método de verificación está configurado en "Verificación de Contraseña/Huella Digital/Tarjeta", aparecerá la siguiente pantalla. Seleccione el ícono para ingresar al modo de verificación por contraseña.

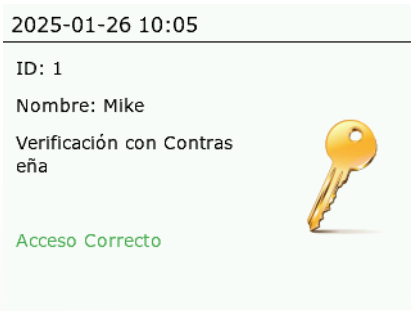


Ingrese la contraseña y presione **M/OK.**



La siguiente pantalla se muestra después de ingresar una contraseña correcta y una incorrecta respectivamente.

Verificación exitosa:



Verificación fallida:

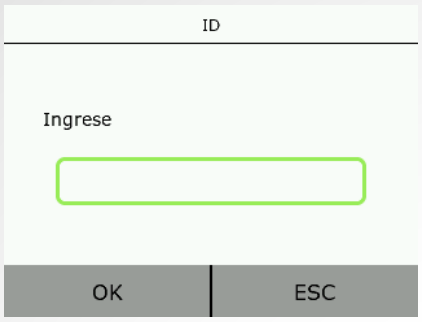


1.3 Operación de Entrada de Texto

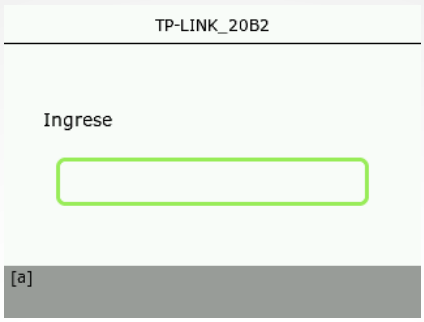
El dispositivo puede reconocer letras en inglés, símbolos y números. Presione > para mostrar el método de entrada y presione > nuevamente para cambiar el método de entrada. Presione la tecla / para desplazarse hacia arriba y hacia abajo. Presione < para borrar la entrada. Presione ESC para salir del método de entrada.

Descripción de la entrada de letras en inglés y símbolos

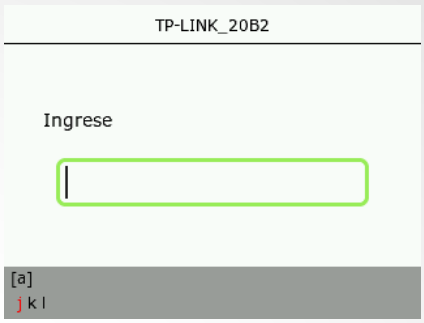
Por ejemplo, ingrese la contraseña: key@M1



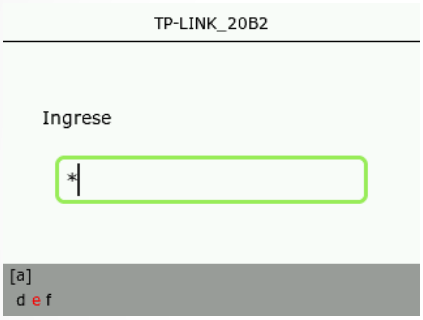
Presione > para mostrar el método de entrada.



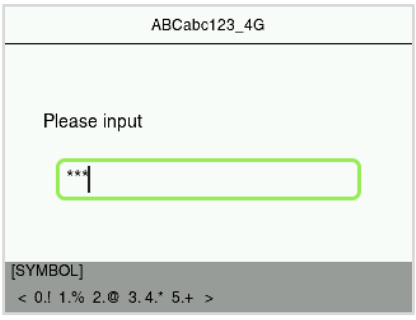
Presione > nuevamente para cambiar el método de entrada. Seleccione Aa, a o A para usar letras mayúsculas y minúsculas según sea necesario.



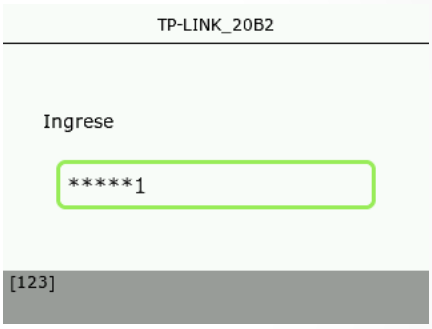
Presione 5JKL dos veces para seleccionar "k".



Presione 3DEF dos veces para seleccionar "e". Complete la entrada de texto de la misma manera.



Presione > nuevamente para cambiar el método de entrada. Seleccione Aa, a o A para usar letras mayúsculas y minúsculas según sea necesario.



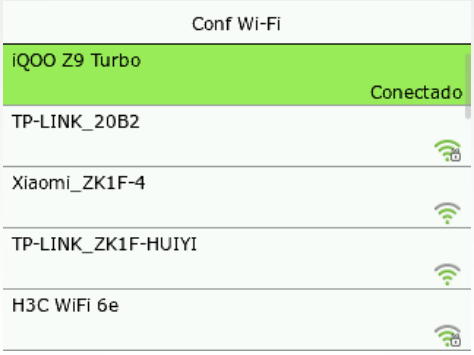
Presione > para cambiar al método de entrada numérico, luego presione 1. Cuando termine, presione ESC para salir. Luego presione M/OK para guardar y salir.

1.4 Conexión Wi-Fi

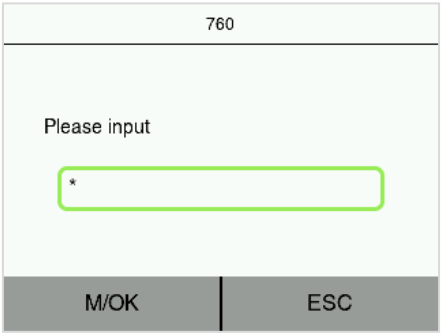
Situación 1: Después de encender el dispositivo, entra directamente en la interfaz de acceso rápido de configuración de Wi-Fi. Siga los siguientes pasos para conectarse a Wi-Fi



1. Al presionar M/OK en esta interfaz de acceso rápido, ingresará directamente a la interfaz de configuración de Wi-Fi. El dispositivo buscará redes Wi-Fi disponibles dentro del alcance de la red.



2. Seleccione la red Wi-Fi disponible de la lista, ingresará a la interfaz de contraseña. Ingrese la contraseña y presione M/OK para conectar.



3. Después de que la conexión Wi-Fi sea exitosa, el ícono de Wi-Fi aparecerá en la barra de estado.



Nota: Si está utilizando el dispositivo por primera vez o si el dispositivo no está vinculado, la interfaz de acceso rápido de Wi-Fi lo llevará directamente a la interfaz SN después de configurar Wi-Fi. En esta pantalla podrá ver el número de serie del dispositivo.

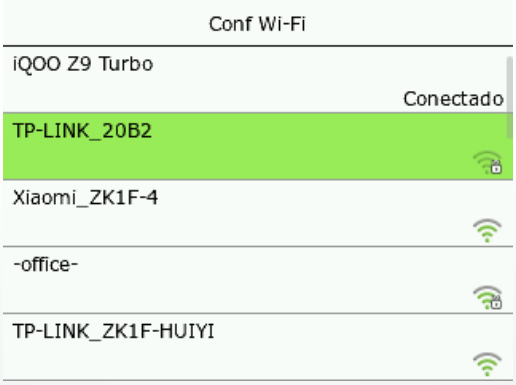
Situación 2: Si ha ingresado a la pantalla del código QR o ha vinculado el dispositivo y accedido a la pantalla de bienvenida, siga los siguientes pasos para conectarse a Wi-Fi.



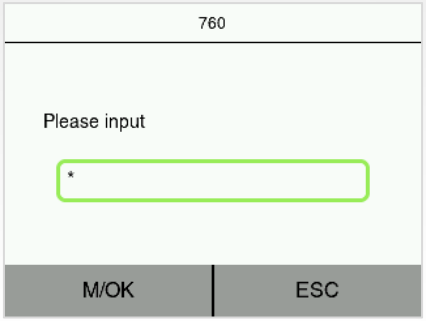
1.Presione M/OK para acceder al Menú Principal si ha vinculado el dispositivo y se encuentra en la pantalla de espera.



2. Luego, haga clic en Comm. > Configuración de Wi-Fi para ingresar a la interfaz de configuración de Wi-Fi. El dispositivo buscará redes Wi-Fi disponibles dentro del alcance de la red.



3. Seleccione la red Wi-Fi disponible de la lista, ingresará a la interfaz de contraseña. Ingrese la contraseña y presione M/OK para conectarse.



4. Después de que la conexión Wi-Fi sea exitosa, el ícono de Wi-Fi aparecerá en la barra de estado.



2 Menú principal

Después de vincular el dispositivo, presione la tecla M/OK en el teclado para ingresar al Menú Principal. Se mostrará la siguiente pantalla:



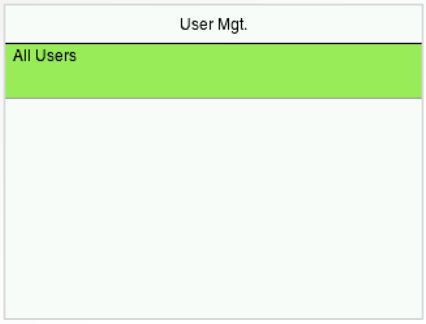
Descripción de Funciones

Menú	Descripción
Gestión de Usuarios	Ver información básica sobre el usuario.
Comunicación	Configurar los parámetros relevantes de la red inalámbrica y del servidor en la nube.
Sistema	Configurar los parámetros relacionados con el sistema, incluidos la fecha y hora, la configuración de asistencia, los parámetros de huella digital, la configuración de audio, la configuración de cambio automático, la configuración de seguridad, la actualización por USB, la actualización de firmware en línea y el restablecimiento a los valores de fábrica.
Gestión de Datos	Eliminar todos los datos relevantes en el dispositivo.
Registros	Consultar los registros de eventos específicos, como los registros de asistencia.
Prueba	Realizar una prueba automática para verificar si cada módulo funciona correctamente, incluidos la pantalla LCD, el audio, el teclado, el sensor de huellas digitales y el reloj en tiempo real.
Información del Sistema	Ver la capacidad de datos, la información del dispositivo y el firmware, así como la política de privacidad del dispositivo.

3 Manual de usuario

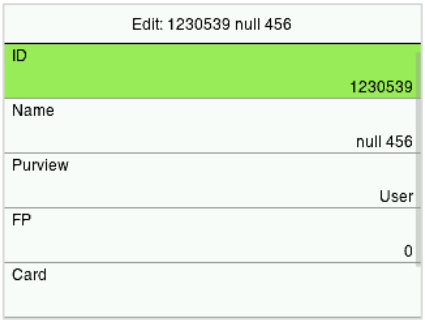
3.1 Buscar usuario

Cuando el dispositivo esté en la interfaz inicial, presione el botón M/OK > [Gestión de Usuarios] > [Todos los Usuarios] para ingresar a la interfaz de Todos los Usuarios. Ingrese el "ID de Usuario" en el cuadro de búsqueda proporcionado para ver el usuario correspondiente.





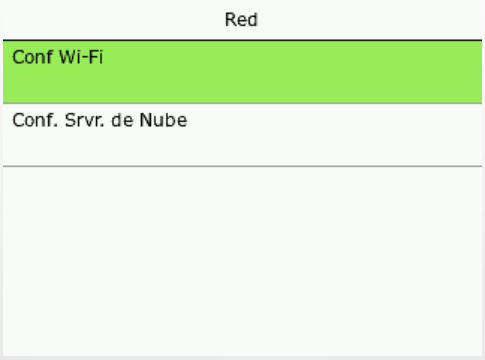




Nota: Solo se puede ver la información básica de todos los usuarios aquí; para editarla, debe operar en Bio-Time Cloud Web. La opción para agregar usuarios se encuentra en 10.3 Agregar Empleado en la plataforma.

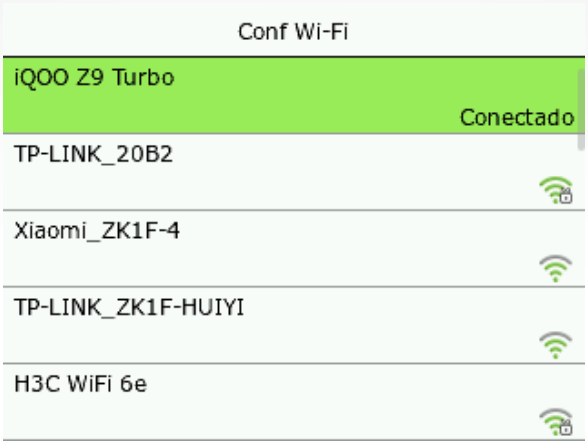
4 Configuración de comunicación

Seleccione Comm. en el Menú Principal para configurar los parámetros relevantes de la Red Inalámbrica y el Servidor en la Nube.



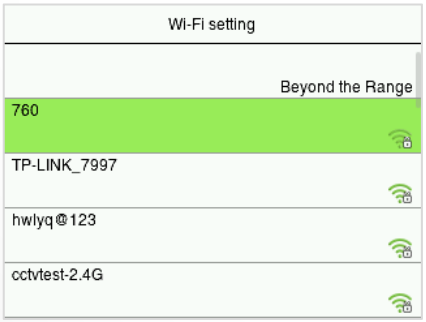
4.1 Red Inalámbrica

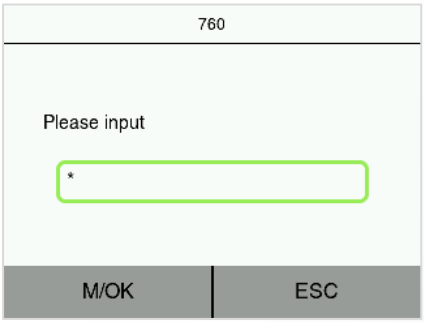
Este dispositivo cuenta con un módulo Wi-Fi integrado. El módulo Wi-Fi permite la transmisión de datos mediante Wi-Fi (Wireless Fidelity) y establece un entorno de red inalámbrica.
Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK > [Comm.] > [Configuración de Wi-Fi]** para configurar las opciones de Wi-Fi.



- **Buscar red Wi-Fi**

◊ El Wi-Fi está habilitado de manera predeterminada en el dispositivo.
◊ Una vez que ingrese a la interfaz de configuración de Wi-Fi, el dispositivo buscará las redes Wi-Fi disponibles dentro del alcance de la red.
◊Elija el nombre de Wi-Fi adecuado de la lista disponible, ingrese la contraseña correcta en la interfaz de contraseña y presione M/OK para conectar.



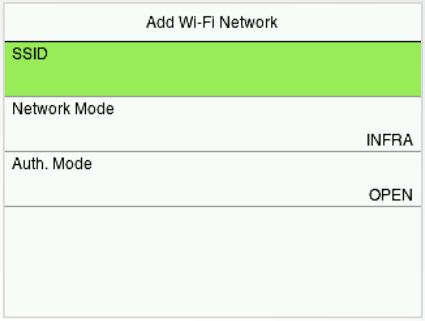


◊ Cuando la conexión Wi-Fi sea exitosa, la interfaz inicial mostrará el ícono de Wi-Fi.

• Agregar una Red Wi-Fi Manualmente

Si la red Wi-Fi deseada no aparece en la lista, puede añadirse manualmente.

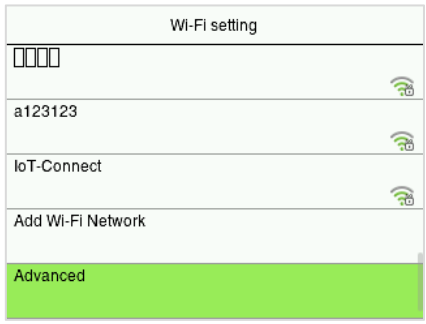


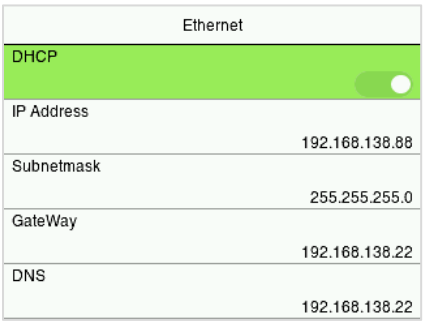


1. Agregue la red Wi-Fi manualmente presionando las teclas de flecha hacia arriba y hacia abajo para seleccionar "Agregar Red Wi-Fi".
2. En esta interfaz, ingrese los parámetros de la red Wi-Fi. (La red añadida debe existir previamente).

Nota: Después de agregar la red Wi-Fi manualmente con éxito, siga el mismo proceso para buscar el nombre de la red añadida.

• Configuración avanzada





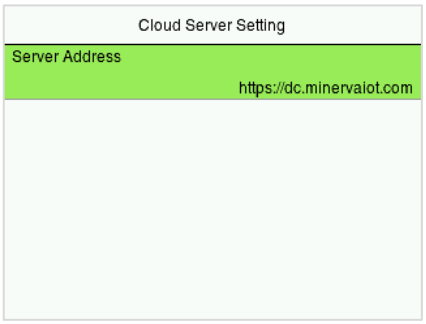
• Descripción de funciones

Menú	Descripción
DHCP	El Protocolo de Configuración Dinámica de Host (DHCP) asigna dinámicamente direcciones IP a los clientes de la red. Si el DHCP está habilitado, no se puede configurar la dirección IP manualmente.
Dirección IP	Dirección IP de la red Wi-Fi, cuyo valor predeterminado es 0.0.0.0. Puede ser modificada según la disponibilidad de la red.
Máscara de subred	La Máscara de Subred predeterminada de la red Wi-Fi es 255.255.255.0. Puede ser modificada según la disponibilidad de la red.

Menú	Descripción
Puerta de enlace	La dirección de la Puerta de Enlace predeterminada es 0.0.0.0. Puede ser modificada según la disponibilidad de la red.
DNS	La dirección DNS predeterminada es 0.0.0.0. Puede ser modificada según la disponibilidad de la red.

4.2 Configuración del Servidor en la Nube

Cuando el dispositivo esté en la interfaz inicial, presione el botón M/OK > [Comm.] > [Configuración del Servidor en la Nube] para ver la dirección del servidor en la nube.

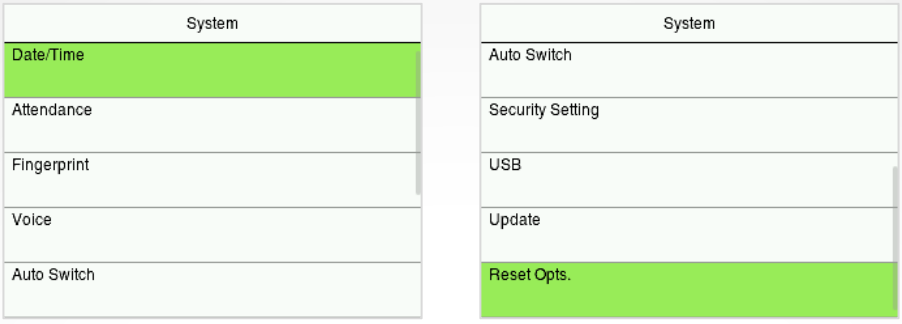


Descripción de la función:

Menú	Descripción
Dirección del servidor	El valor predeterminado es: https://nombredeempresa.biotime.mx

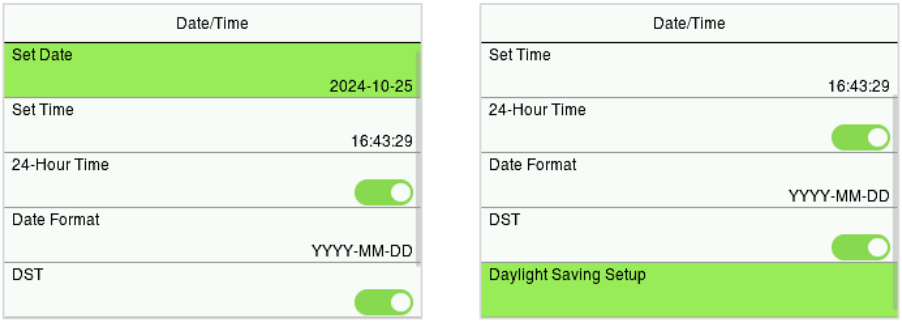
5.Configuración del Sistema

Configure los parámetros relacionados del sistema para optimizar el rendimiento del dispositivo.
Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > **[Sistema]** para configurar los parámetros del sistema y optimizar el rendimiento del dispositivo.



5.1 Fecha y hora

Presione el botón **M/OK** > **[Sistema]** > **[Fecha/Hora]** para configurar la fecha y la hora.



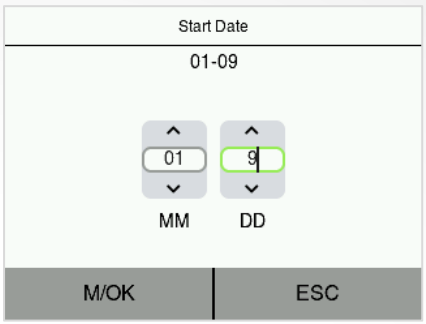
◊ Si los usuarios necesitan configurar la fecha y la hora manualmente, seleccione **Establecer Fecha y Establecer Hora** para ajustarlas, luego presione **M/OK** para guardar.



◊ Presione **M/OK** para controlar el icono de **Hora de 24 horas** y habilitar o deshabilitar este formato. Si está habilitado, seleccione **Formato de Fecha** para configurar el formato de la fecha.

◊ Presione **M/OK** para controlar el icono de **Horario de Verano (DST)** y habilitar o deshabilitar la función de horario de verano. Si está habilitado, presione **Configuración de Horario de Verano** para establecer el tiempo de cambio.



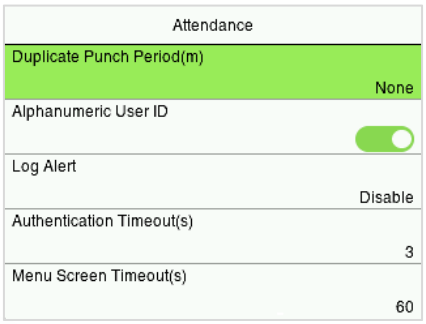


◊ Al restaurar la configuración de fábrica, el formato de hora (24 horas) y de fecha (AAAA-MM-DD) se restaurarán, pero la fecha y hora del dispositivo no se restablecerán.

Nota: Por ejemplo, si el usuario establece la hora del dispositivo (18:35 del 15 de marzo de 2023) en 18:30 del 1 de enero de 2024, después de restaurar la configuración de fábrica, la hora del dispositivo permanecerá en 18:30 del 1 de enero de 2024.

5.2 Configuración de Asistencia

Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > **[Sistema]** > **[Asistencia]** para ingresar a la interfaz de configuración de asistencia.

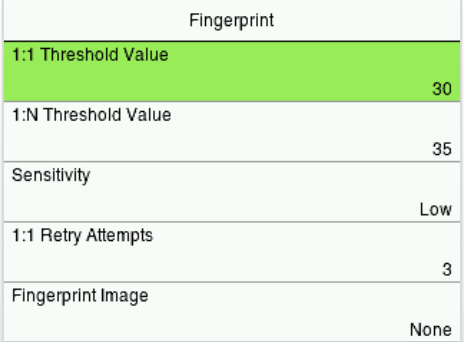


Descripción de la Función:

Menú	Descripción
Periodo de checadas duplicadas	Dentro de un período de tiempo establecido (unidad: minutos), los registros de asistencia duplicados no se conservarán (el rango de valores va de 0 a 999999 minutos).
ID Alfanumérico	Determina si se permite el uso de letras en un ID de Usuario. empleado
Alerta de registro	Cuando el espacio de registro de asistencia alcanza el valor máximo permitido, el dispositivo muestra automáticamente una advertencia sobre el espacio de memoria. Los usuarios pueden deshabilitar esta función o establecer un valor válido entre 1 y 9999
Tiempo de Autenticación (s)	Duración en la que se muestra el mensaje de verificación exitosa. Valor válido: 1~9 segundos.
Tiempo de Espera de la Pantalla del Menú (s)	Se utiliza para configurar el tiempo de retraso antes de salir de la pantalla del menú hacia la pantalla de espera. Los usuarios pueden deshabilitar esta función o establecer un valor válido entre 60 y 99999. 0: Deshabilitar.

5.3 Parámetros de Huellas Dactilares

Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > [**Sistema**] > [**Huellas Dactilares**] para ingresar a la interfaz de configuración de huellas dactilares.

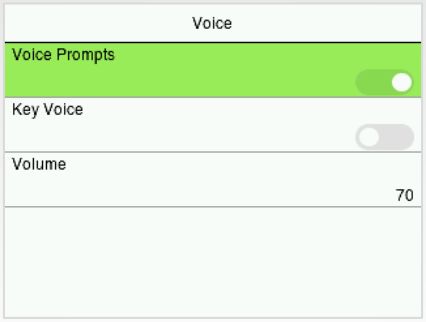


Descripción de la Función:

Menú	Descripción
Valor Umbral 1:1	En el método de verificación 1:1, la verificación será exitosa solo cuando la similitud entre los datos de huella dactilar adquiridos y la plantilla de huella dactilar asociada con el ID de usuario ingresado en el dispositivo sea mayor que el valor establecido.
Valor Umbral 1:1	En el método de verificación 1:N, la verificación será exitosa solo cuando la similitud entre los datos de huella dactilar adquiridos y las plantillas de huellas dactilares registradas en el dispositivo sea mayor que el valor establecido.
Sensibilidad	Para ajustar la sensibilidad en la adquisición de huellas dactilares. Se recomienda usar el nivel predeterminado **"Medio (Mid)".** Cuando el ambiente es seco y esto ralentiza la detección de huellas, puede configurar el nivel en **"Alto (High)"** para aumentar la sensibilidad; si el ambiente es húmedo y dificulta la identificación de huellas, puede configurarlo en **"Bajo (Low)".**
Intentos de Reintento 1:1	En la verificación 1:1, los usuarios pueden olvidar la huella dactilar registrada o colocar el dedo incorrectamente. Para reducir el proceso de volver a ingresar el ID de usuario, se permite el reintento.
Imagen de Huella Dactilar	Esta función está deshabilitada por defecto. Al deshabilitarla, la imagen de la huella dactilar no se mostrará durante el registro ni la verificación de huellas. La interfaz del menú permite habilitar o deshabilitar esta función, con avisos de seguridad al cambiar la configuración. Hay cuatro opciones disponibles: • **Mostrar para registro:** muestra la imagen de la huella dactilar en la pantalla solo durante el registro. • **Mostrar para verificación:** muestra la imagen de la huella dactilar en la pantalla solo durante la verificación. • **Mostrar siempre:** muestra la imagen de la huella dactilar en la pantalla durante el registro y la verificación. • **Ninguna:** no muestra la imagen de la huella dactilar en ningún momento.

5.4 Configuración de voz

Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > [**Sistema**] > [**Voz**] para configurar los ajustes de voz.

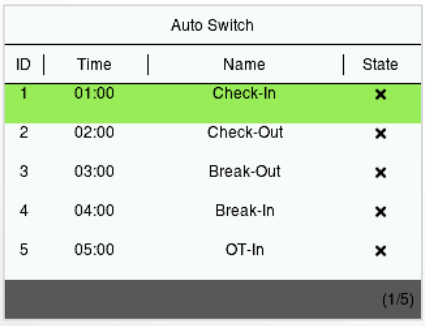


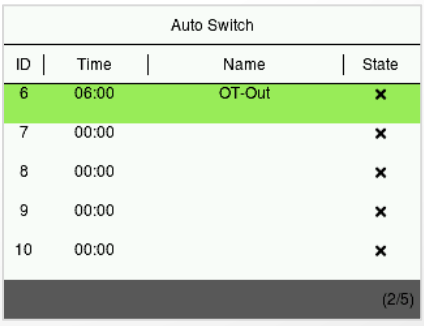
Descripción de la función:

Menú	Descripción
Indicación de Voz	Toggle to enable or disable the voice prompts during function operations.
Sonido de Teclas	Activar o desactivar los sonidos del teclado.
Volumen	Ajustar el volumen del dispositivo, con un rango de configuración entre 0 y 100.

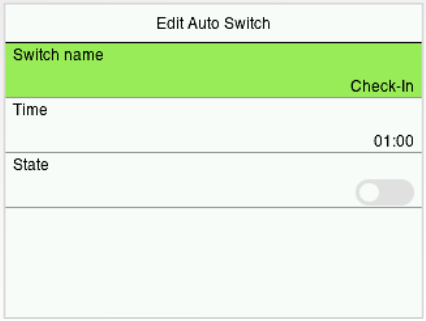
5.5 Configuración de Cambio Automático

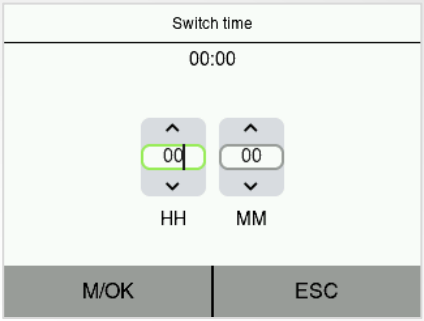
Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > [**Sistema**] > [**Cambio Automático**] para ingresar a la interfaz de configuración.





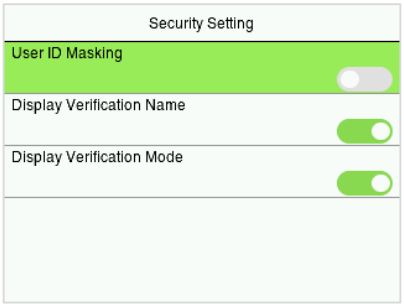
Al activar el cambio automático y configurar la hora de cambio, dentro del tiempo establecido, la plantilla de la interfaz en espera mostrará automáticamente el estado de registro.





5.6 Configuración de seguridad

Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > [**Sistema**] > [**Configuración de Seguridad**] para ingresar a la interfaz de configuración.

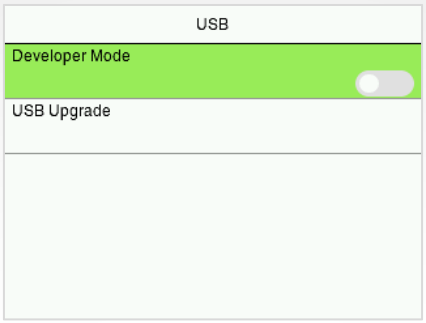


Descripción de funciones

Menú	Descripción
Ocultamiento del ID de Usuario	Al habilitar esta función, el ID de Usuario se mostrará parcialmente después del resultado de la verificación del personal (solo se aplica a IDs de Usuario con más de 2 dígitos). Esta opción está habilitada por defecto.
Mostrar Nombre en Verificación	Al habilitar esta función, el nombre del usuario se mostrará después del resultado de la verificación del personal. Si se desactiva, el resultado de la verificación no mostrará el nombre.
Mostrar Modo de Verificación	Al habilitar esta función, el resultado de la verificación del personal mostrará el modo de verificación del usuario. Si se desactiva, el resultado de la verificación no mostrará el modo de verificación.

5.7 Configuración USB

Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > [**Sistema**] > [**USB**] para ingresar a la interfaz de configuración de USB.



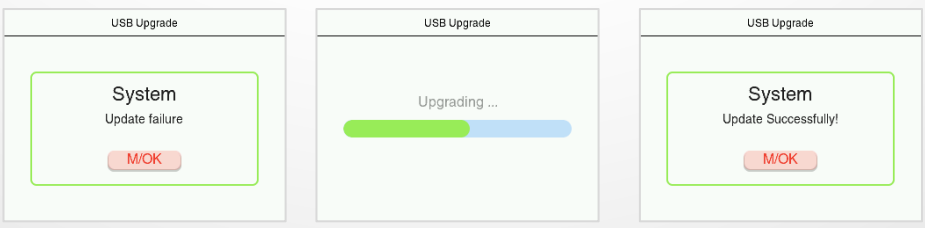
Descripción de funciones

Menú	Descripción
Modo Desarrollador	Al activarlo, el dispositivo entra en modo desarrollador, momento en el cual la función de actualización por USB se desactiva.
Actualización por USB	Actualiza el firmware mediante un disco USB. **Nota:** Este elemento del menú no se mostrará cuando el **Modo Desarrollador** esté activado.

- **Actualización por USB**

El firmware del dispositivo puede actualizarse utilizando el archivo de actualización en una unidad USB. Antes de realizar esta operación, asegúrese de que la unidad USB contenga el archivo de actualización correcto y esté correctamente insertada en el dispositivo. Luego seleccione [Actualización por USB] y haga clic en M/OK para actualizar.

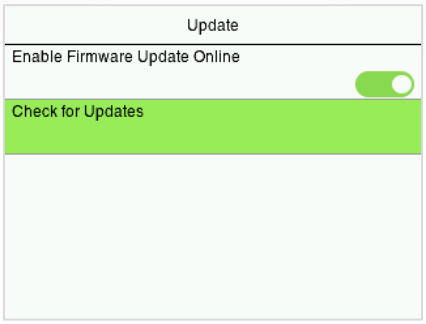
Si no se ha insertado una unidad USB, el sistema mostrará el mensaje "PenDrive not found" después de seleccionar Actualización por USB en la interfaz del sistema.



Nota: Si necesita el archivo de actualización, comuníquese con nuestro soporte técnico. La actualización del firmware no se recomienda en circunstancias normales.

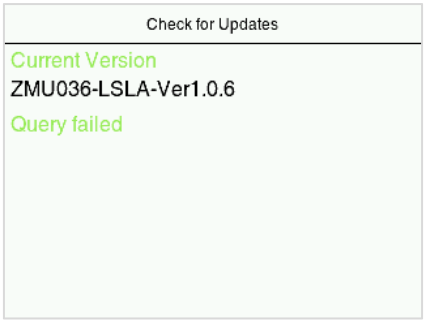
5.8 Actualización de Firmware en Línea

Cuando el dispositivo esté en la interfaz inicial, presione el botón M/OK > [Sistema] > [Actualizar] para ingresar a la interfaz de configuración.
Presione el botón M/OK para habilitar la función Actualizar Firmware en Línea. El dispositivo mostrará un aviso indicando que la actualización podría conllevar algunos riesgos de seguridad de datos, lo que requiere una confirmación manual por parte del usuario (si la función de configuración de seguridad está desactivada, no se mostrará la advertencia de riesgo al habilitar la actualización en línea).

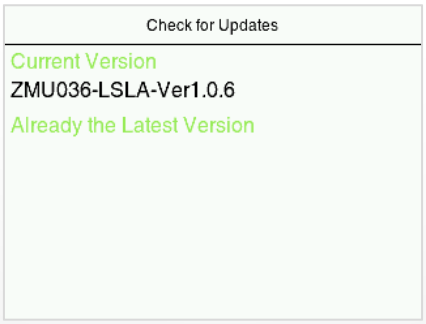


Seleccione [**Buscar Actualizaciones**]; esto puede dar lugar a los siguientes 3 escenarios:

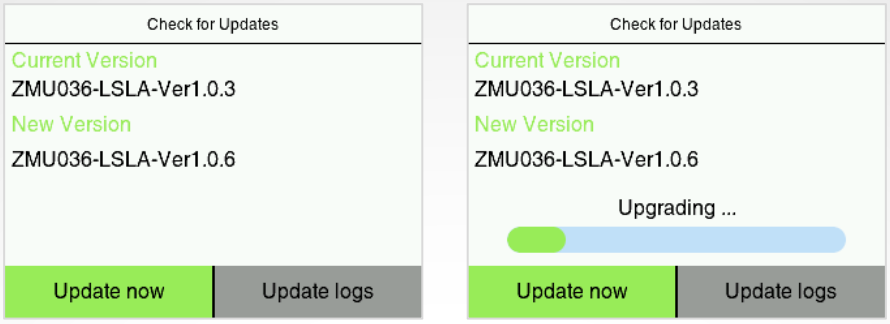
◊ **Si la consulta falla**, la interfaz mostrará el mensaje **"Consulta fallida"**



◊ **Si la versión del firmware del dispositivo es la más reciente**, se mostrará un aviso indicando que la versión actual del firmware ya está actualizada.

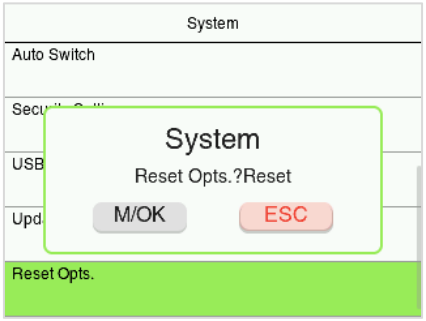


◊ Si la versión del firmware del dispositivo no es la más reciente, se mostrarán el número de versión y el registro de cambios de la última versión disponible. Los usuarios podrán elegir si desean actualizar a la última versión del firmware.



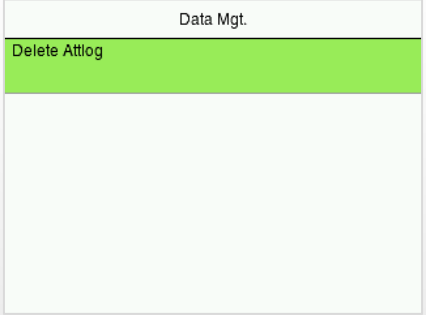
5.9 Restablecimiento de fábrica

La función de Restablecimiento de Fábrica restaura la configuración del dispositivo, como la configuración de comunicación y del sistema, a los valores predeterminados de fábrica (esta función no elimina los datos de los usuarios registrados).
Seleccione [Opciones de Restablecimiento] en la interfaz del sistema y luego presione M/OK para restaurar la configuración de fábrica predeterminada.

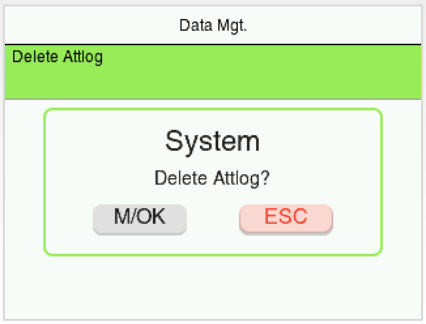


6. Configuración del Sistema

Cuando el dispositivo esté en la interfaz inicial, presione el botón M/OK > [Gestión de Datos] > [Eliminar Registro de Asistencia] para eliminar los registros de asistencia especificados.

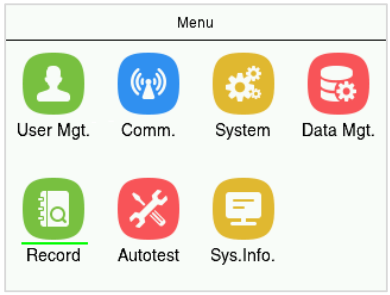


Seleccione [**Eliminar Registro de Asistencia**] en la interfaz de gestión de datos y, en la ventana de confirmación emergente, haga clic en **M/OK** para eliminar todos los registros de asistencia.

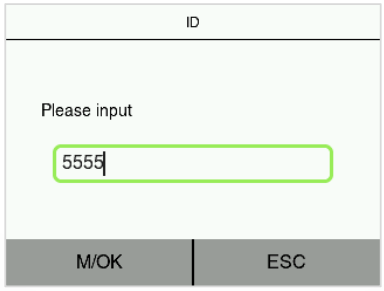


7. Registro

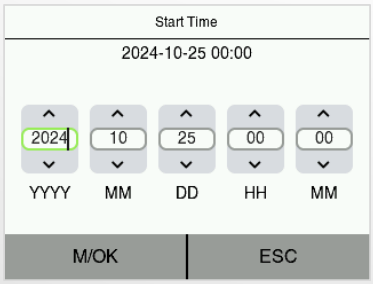
Una vez que se verifica la identidad de un usuario, los registros de eventos se guardan en el dispositivo. Esta función permite a los usuarios consultar sus registros de asistencia.
Cuando el dispositivo esté en la interfaz inicial, presione el botón M/OK > [Registro] para buscar el registro de asistencia requerido.

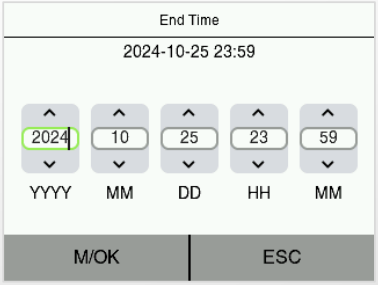


1.Ingrese el ID de usuario que desea buscar y haga clic en M/OK. Si desea buscar registros de todos los usuarios, haga clic en M/OK sin ingresar ningún ID de usuario.

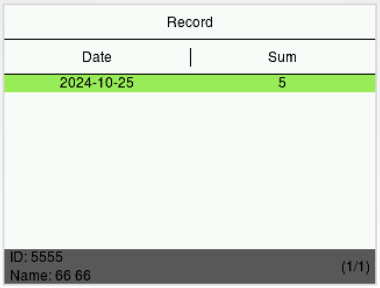


2.Seleccione el rango de tiempo en el que se deben buscar los registros.

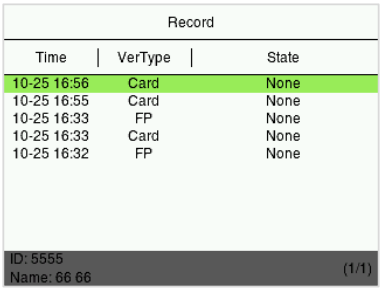




3.Una vez que la búsqueda del registro sea exitosa, seleccione el registro resaltado en verde para ver sus detalles.

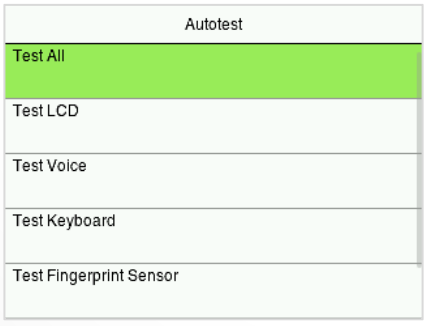


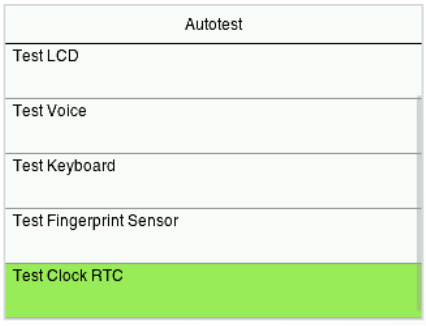
4.La figura a continuación muestra los detalles del registro seleccionado.



8. Prueba

Cuando el dispositivo esté en la interfaz inicial, presione el botón M/OK > [Prueba] para realizar automáticamente una prueba que verifique si todos los módulos del dispositivo funcionan correctamente. Esto incluye la pantalla LCD, el sistema de voz, el teclado y el reloj en tiempo real (RTC).





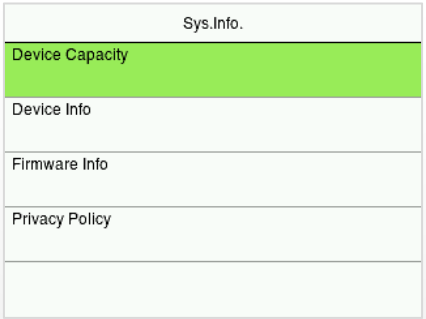
Descripción de funciones

Menú	Descripción
Probar Todo	Realiza automáticamente pruebas para verificar si la pantalla LCD, el audio, la cámara y el RTC funcionan correctamente.

Probar LCD	Realiza automáticamente una prueba del efecto de visualización de la pantalla LCD mostrando colores completos, blanco puro y negro puro para comprobar si la pantalla muestra los colores de manera normal.
Probar Voz	Realiza automáticamente una prueba para verificar si los archivos de audio almacenados en el dispositivo están completos y si la calidad de la voz es buena.
Probar Teclado	El terminal verifica si cada tecla del teclado funciona correctamente. Presione cualquier tecla en la interfaz de prueba del teclado para comprobar si la tecla presionada coincide con la que se muestra en pantalla. Las teclas son de color gris oscuro antes de ser presionadas y se vuelven azules después de ser presionadas.
Probar Sensor de Huellas	Prueba el sensor de huellas colocando un dedo en el escáner para verificar si la imagen de la huella adquirida es clara. Al presionar un dedo en el escáner, la imagen de la huella se mostrará en la pantalla.
Probar Reloj RTC	Prueba el reloj en tiempo real (RTC). El dispositivo verifica si el reloj funciona normalmente y con precisión utilizando un cronómetro. Toque la pantalla para iniciar el conteo y vuelva a presionarla para detener el conteo.

9. Información del Sistema

Cuando el dispositivo esté en la interfaz inicial, presione el botón **M/OK** > [**Info. del Sistema**] para ver el estado de almacenamiento, la información de la versión del dispositivo, los datos del firmware y la política de privacidad.



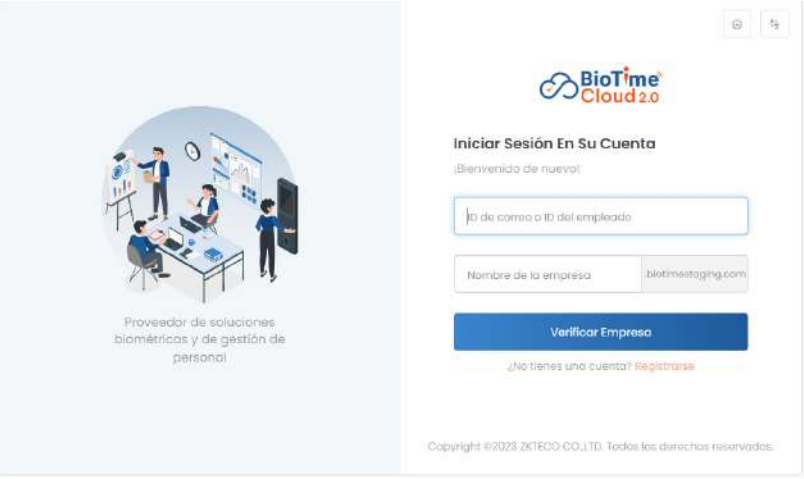
Descripción de funciones

Menú	Descripción
Capacidad del Dispositivo	Muestra el número de usuarios registrados, administradores, contraseñas, huellas dactilares, tarjetas y registros de asistencia.
Información del Dispositivo	Muestra el nombre del dispositivo, número de serie, dirección MAC, algoritmo de huella dactilar, información de la plataforma y proveedor.
Información del Firmware	Muestra la versión del firmware del dispositivo.
Política de Privacidad	Muestra el contenido de la política de privacidad.

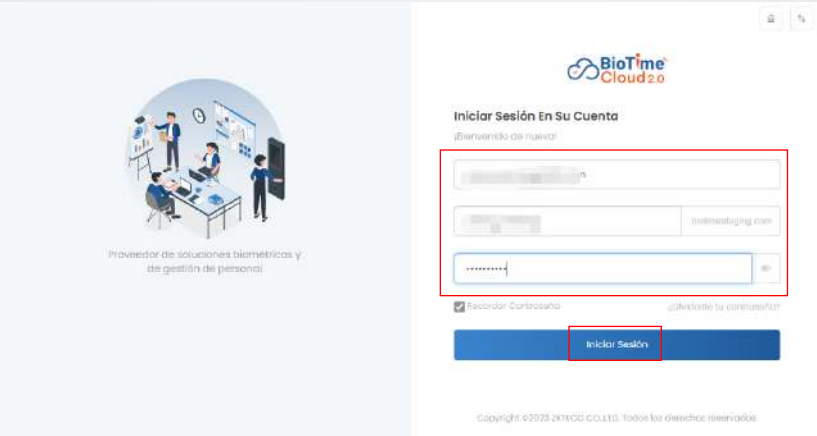
10. Conectar a la plataforma BioTime Cloud 2.0

10.1 Iniciar sesión en navegador

1. Abra el navegador recomendado e ingrese la dirección para acceder a la web de BioTime Cloud.
2. En la página de inicio de sesión, ingrese el ID de correo electrónico y el Nombre de la empresa. Luego haga clic en [Verificar Empresa].

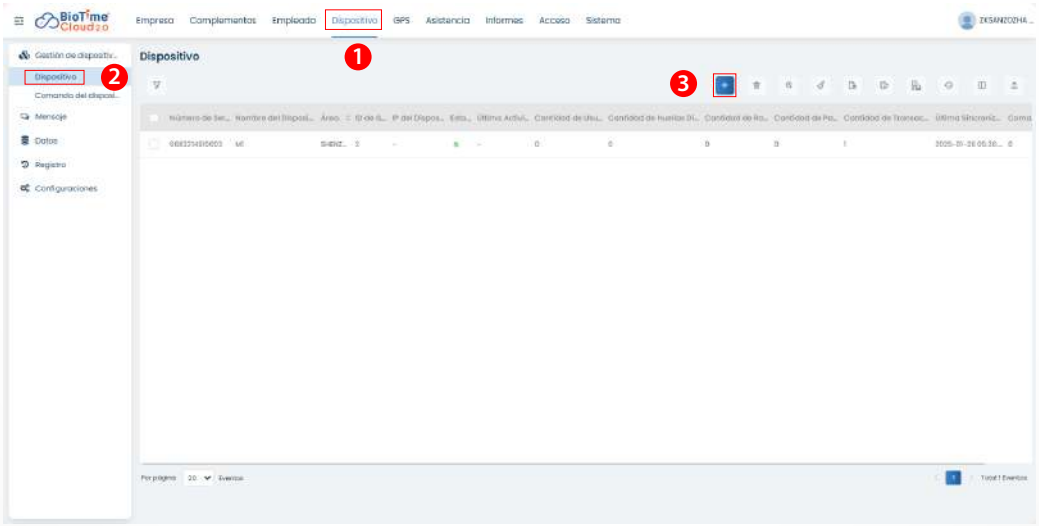


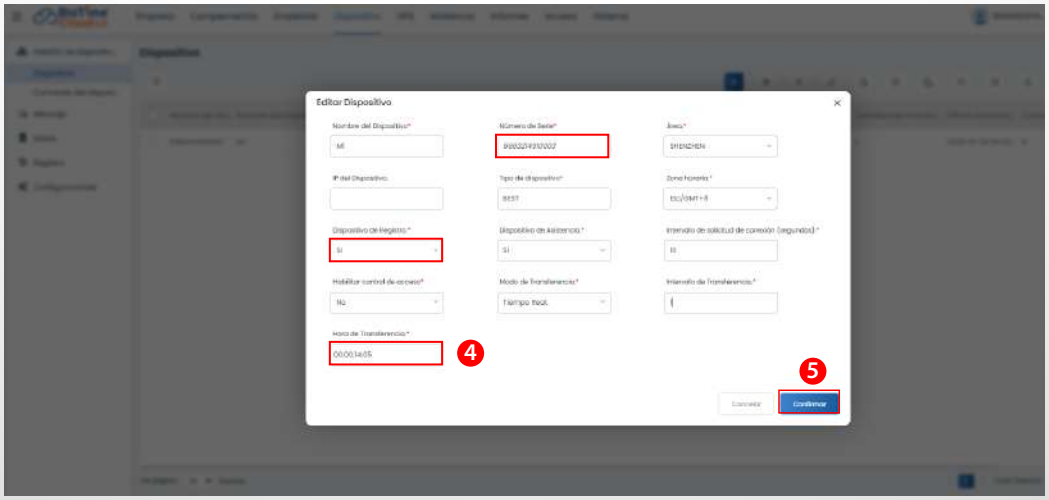
3. Ingrese la contraseña y haga clic en **[Iniciar sesión].**



10.2 Agregar dispositivos en la plataforma

1.Haga clic en [**Dispositivo**] para ingresar a la interfaz de gestión de dispositivos.
2.Luego haga clic en el ícono + y complete los parámetros relevantes en la ventana emergente para agregar el dispositivo.
3.Una vez que haya terminado de ingresar, haga clic en [**Confirmar**] para guardar y salir





Descripción de la Función:

• **Número de Serie:** Verifique la etiqueta del número de serie en la parte posterior del dispositivo. O haga clic en el botón **M/OK** para ingresar al **Menú Principal,** luego haga clic en [**Info. del Sistema**] > [**Info. del Dispositivo**] > [**Número de Serie**] para ver el número de serie.

• **Área:** Una vez que se seleccione un área, todo el personal en esa área se sincronizará automáticamente con el dispositivo.

• **Dispositivo de Registro:** Seleccione Sí para habilitar el registro remoto.

• **Tipo de Dispositivo:** Configure el tipo de dispositivo como BEST.

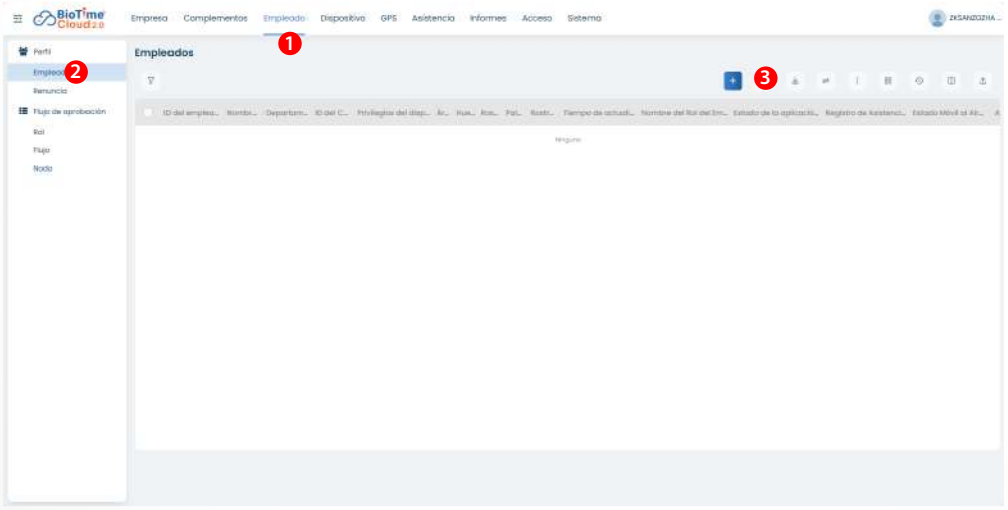
10.3 Agregar dispositivos en la plataforma

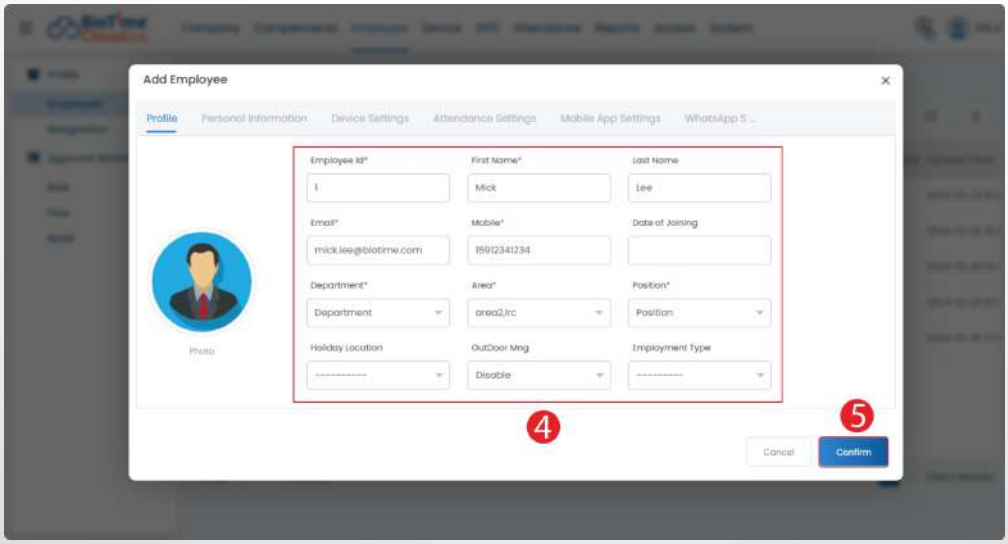
10.3.1 Agregar empleado

1.Haga clic en [Empleado] > [Empleados] para ingresar a la interfaz de configuración de empleados.

2. Luego haga clic en el ícono + y complete los parámetros relevantes en la ventana emergente para agregar a la persona.

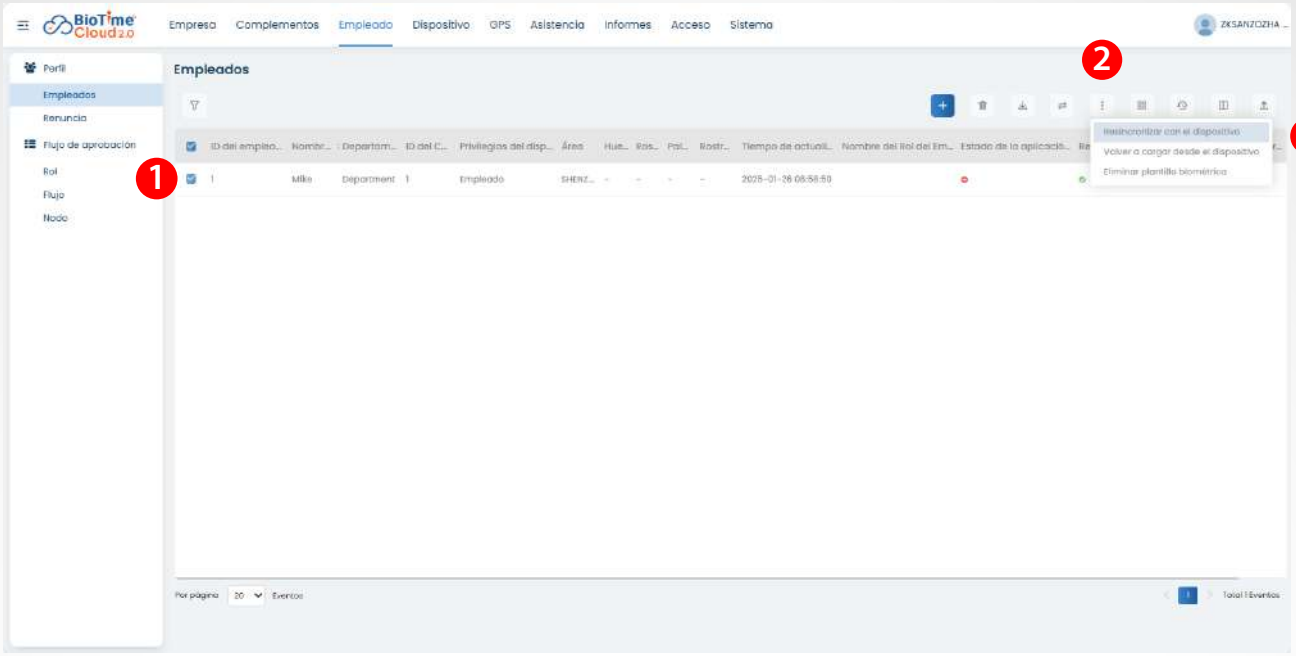
3.Una vez que haya terminado de ingresar los datos, haga clic en **[Confirmar]** para guardar y salir.

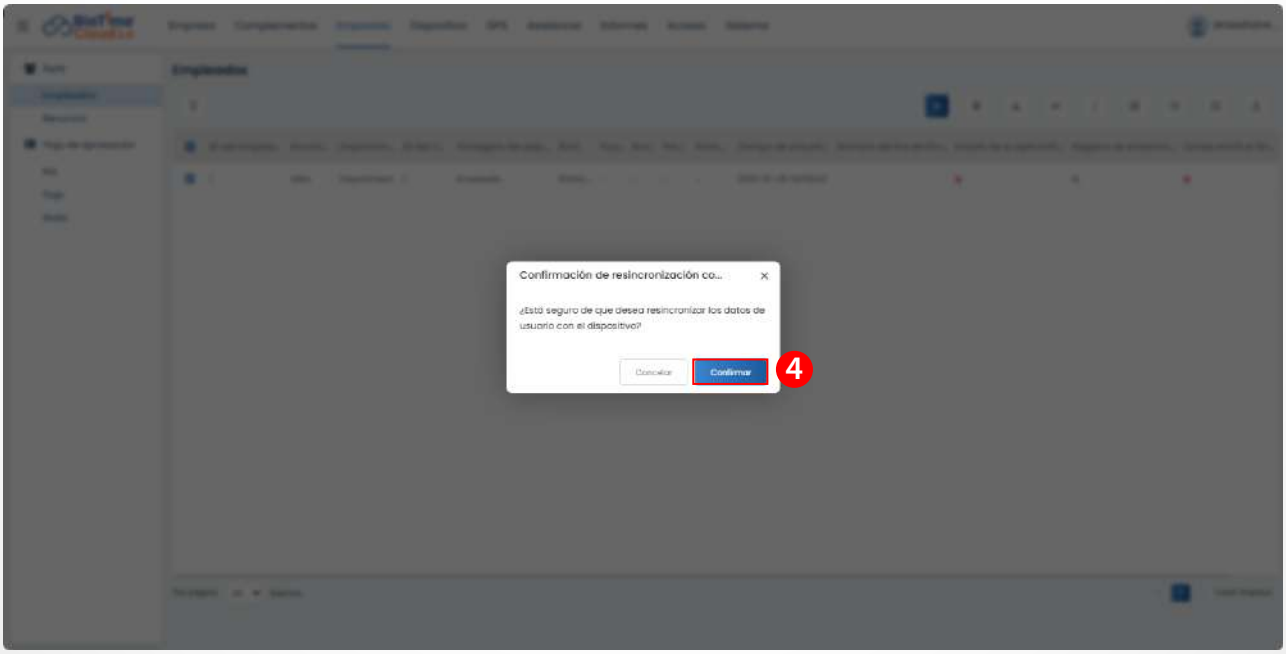




10.3.2 Sincronizar empleados al dispositivo

Seleccione el dispositivo al que desea sincronizar a las personas en la lista de dispositivos, haga clic en el ícono ⋮ y seleccione **[Sincronizar al dispositivo]** en el menú emergente. Luego, haga clic en **[Confirmar]** en la ventana emergente para confirmar.





10.4 Registrar Método de Verificación desde el Dispositivo

Después de sincronizar exitosamente a la persona en el dispositivo, puede registrar a la persona con información biométrica. El dispositivo soporta verificación por tarjeta y huella dactilar. Solo se ilustrará el registro de huella dactilar como ejemplo.

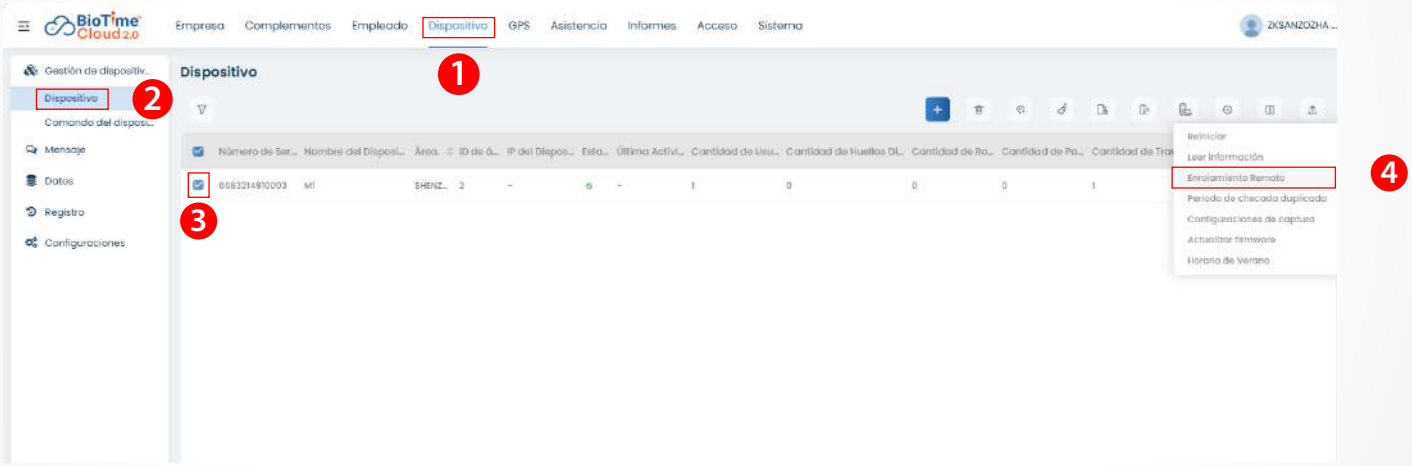
1.Haga clic en [Dispositivo] > [Dispositivo] para ingresar a la interfaz de lista de dispositivos.

2.Seleccione el dispositivo y haga clic en el ícono +. Seleccione [Registrar Remotamente] en el menú desplegable que aparece.

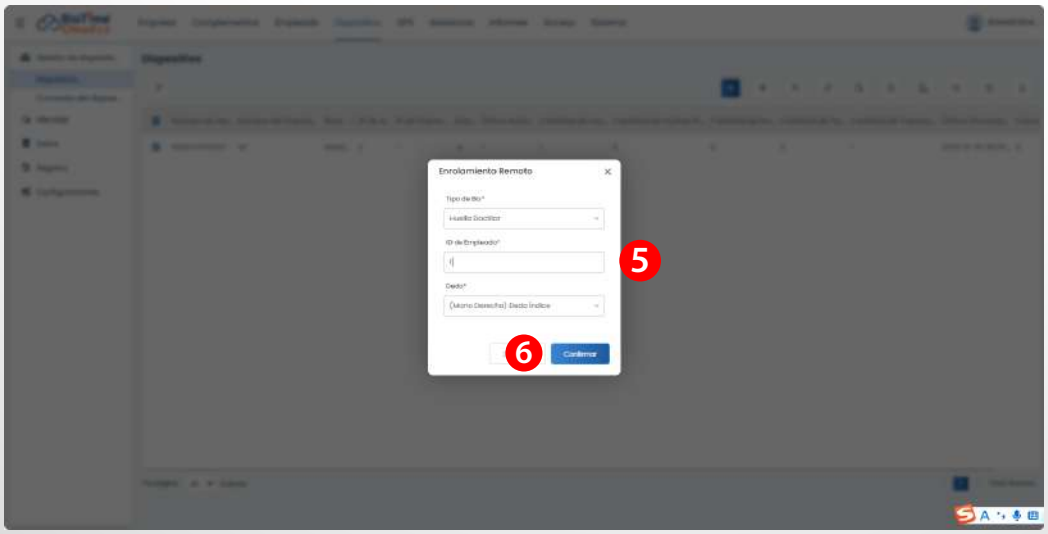
3.Luego, en la ventana emergente, configure el tipo de bioinformación como Huella Dactilar, ingrese el número de identificación del empleado y seleccione el dedo que se va a registrar (Cuando registre una tarjeta, configure el tipo de bioinformación como Tarjeta MF e ingrese el número de identificación del empleado). Como se muestra en la figura a continuación.

4.Al mismo tiempo, el dispositivo ingresará a la pantalla de registro de huellas dactilares. Según las indicaciones, coloque su dedo en el lector de huellas y presione 3 veces. Cuando la interfaz muestre "Registro Exitoso" , significa que la huella dactilar se ha registrado correctamente.

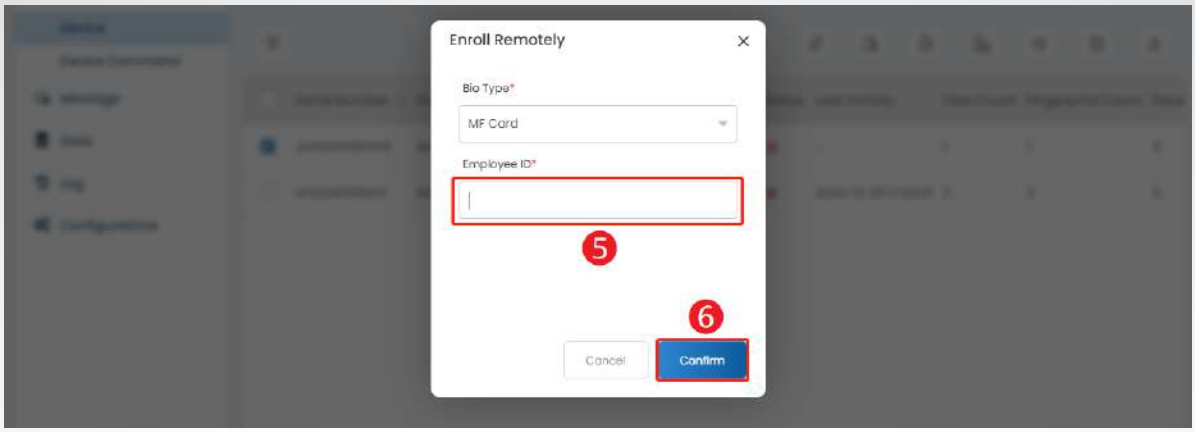
Puede repetir la operación anterior para registrar otros dedos..



Registro de huella digital:



Registro de tarjeta:



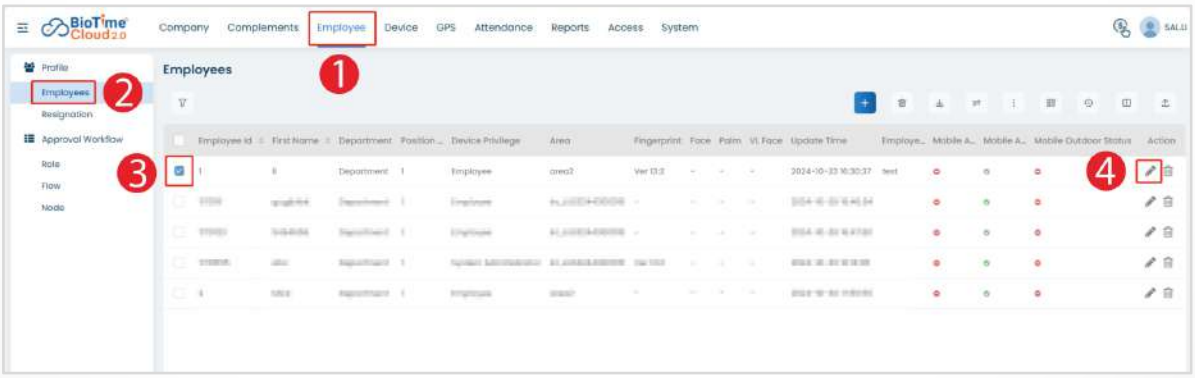
10.5 Configuración de la aplicación móvil

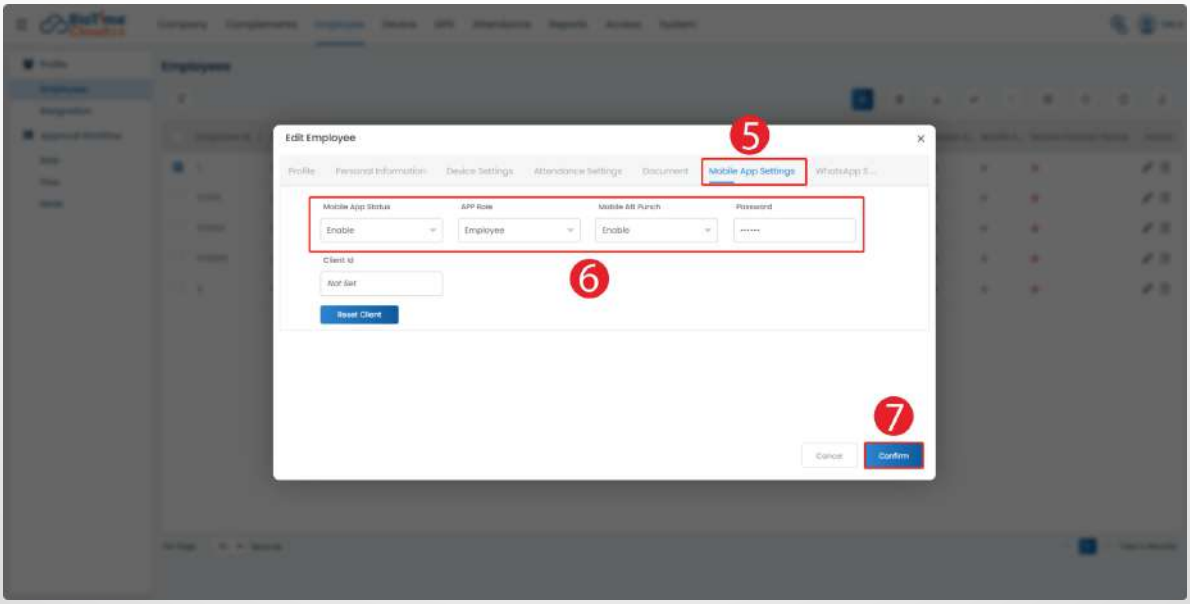
1.Haga clic en [Empleado] > [Empleados] para ingresar a la interfaz de lista de empleados.

2.Seleccione al empleado y haga clic en el ícono de editar para ingresar a la interfaz de edición de empleado.

3.Luego, haga clic en [Configuración de la App Móvil] para configurar los parámetros relevantes e ingrese la contraseña. Haga clic en [Confirmar] para guardar y salir.

4.Una vez completada la configuración, el empleado podrá usar su cuenta y contraseña para iniciar sesión en la BioTime Cloud App para registrar su asistencia.





Política de Privacidad

Aviso:
Para ayudarle a usar mejor los productos y servicios de ZKTeco (en adelante, "nosotros", "nuestro" o "nos"), un proveedor de servicios inteligentes, recopilamos constantemente su información personal. Dado que comprendemos la importancia de su información personal, tomamos su privacidad muy en serio y hemos formulado esta política de privacidad para protegerla. A continuación, le mostramos las políticas de privacidad para que comprenda de manera precisa las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes.

Antes de usar nuestros productos y servicios, lea cuidadosamente y comprenda todas las reglas y disposiciones de esta Política de Privacidad. Si no está de acuerdo con el acuerdo relevante o cualquiera de sus términos, deberá dejar de usar nuestros productos y servicios.

I. Información Recopilada
Para garantizar el funcionamiento normal del producto y ayudar a la mejora del servicio, recopilaremos la información proporcionada voluntariamente por usted o proporcionada con su autorización durante el registro y el uso, o generada como resultado de su uso de los servicios.

1. Información de Registro del Usuario: En su primer registro, el template de características (template de huella dactilar / template de rostro / template de palma) se guardará en el dispositivo de acuerdo con el tipo de dispositivo seleccionado para verificar la similitud única entre usted y el ID de usuario registrado. Puede ingresar opcionalmente su nombre y código. La información mencionada es necesaria para que pueda usar nuestros productos. Si no proporciona dicha información, no podrá usar algunas funciones del producto regularmente.

2. Información del Producto: De acuerdo con el modelo del producto y su permiso concedido al instalar y usar nuestros servicios, se recopilará la información relacionada con el producto en el que se usan nuestros servicios cuando el producto se conecte a la plataforma, incluida la versión del modelo del producto, el número de versión del firmware, el número de serie del producto y la información de capacidad del producto. Cuando conecte su producto a la plataforma, lea cuidadosamente la política de privacidad de la plataforma.

I. Seguridad y Gestión del Producto

1. Cuando utilice nuestros productos por primera vez, deberá configurar el privilegio de Administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que configure el privilegio de Administrador al ingresar a la interfaz del menú principal. Si aún no configura el privilegio de Administrador después de recibir la notificación del sistema, debe ser consciente del posible riesgo de seguridad (por ejemplo, los datos pueden ser modificados manualmente).

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

3. Solo se muestra su ID de usuario por defecto. Puede configurar si desea mostrar otra información de verificación del usuario (como nombre, departamento, foto, etc.) bajo el privilegio de Administrador. Si elige mostrar dicha información, asumimos que está consciente de los posibles riesgos de seguridad (por ejemplo, su foto se mostrará en la interfaz del dispositivo).

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

5. Todos los datos recopilados por nuestros productos están cifrados con el algoritmo AES 256. Todos los datos subidos por el Administrador a nuestros productos se cifran automáticamente con el algoritmo AES 256 y se almacenan de manera segura. Si el Administrador descarga datos de nuestros productos, asumimos que usted necesita procesar los datos y que está al tanto de los riesgos de seguridad potenciales. En tal caso, será responsable de almacenar los datos. Debe saber que algunos datos no pueden ser descargados por razones de seguridad.

6. Toda la información personal en nuestros productos puede ser consultada, modificada o eliminada. Si ya no utiliza nuestros productos, por favor elimine sus datos personales.

II. Cómo Tratamos la Información Personal de Menores

Nuestros productos, sitio web y servicios están diseñados principalmente para adultos. Sin el consentimiento de los padres o tutores, los menores no deben crear su propia cuenta. Si usted es menor de edad, le recomendamos que pida a sus padres o tutores que lean esta política cuidadosamente, y solo utilice nuestros servicios o la información proporcionada por nosotros con el consentimiento de sus padres o tutores.

Solo utilizaremos o divulgaremos la información personal de menores recopilada con el consentimiento de sus padres o tutores si dicha utilización o divulgación está permitida por la ley o hemos obtenido el consentimiento explícito de los padres o tutores, y dicha utilización o divulgación tiene como propósito proteger a los menores.

Al notar que hemos recopilado información personal de menores sin el consentimiento previo de los padres verificables, eliminaremos dicha información lo antes posible.

III. Otros

Puede visitar

https://www.zkteco.com/en/index/Index/privacyprotection.html para obtener más información sobre cómo recopilamos, usamos y almacenamos de manera segura su información personal. Para mantenernos al día con el rápido desarrollo de la tecnología, ajustes de operaciones comerciales y para atender las necesidades de los clientes, constantemente deliberaremos y optimizaremos nuestras medidas y políticas de protección de privacidad. Le invitamos a visitar nuestro sitio web oficial en cualquier momento para conocer nuestra última política de privacidad

Operación ecológica



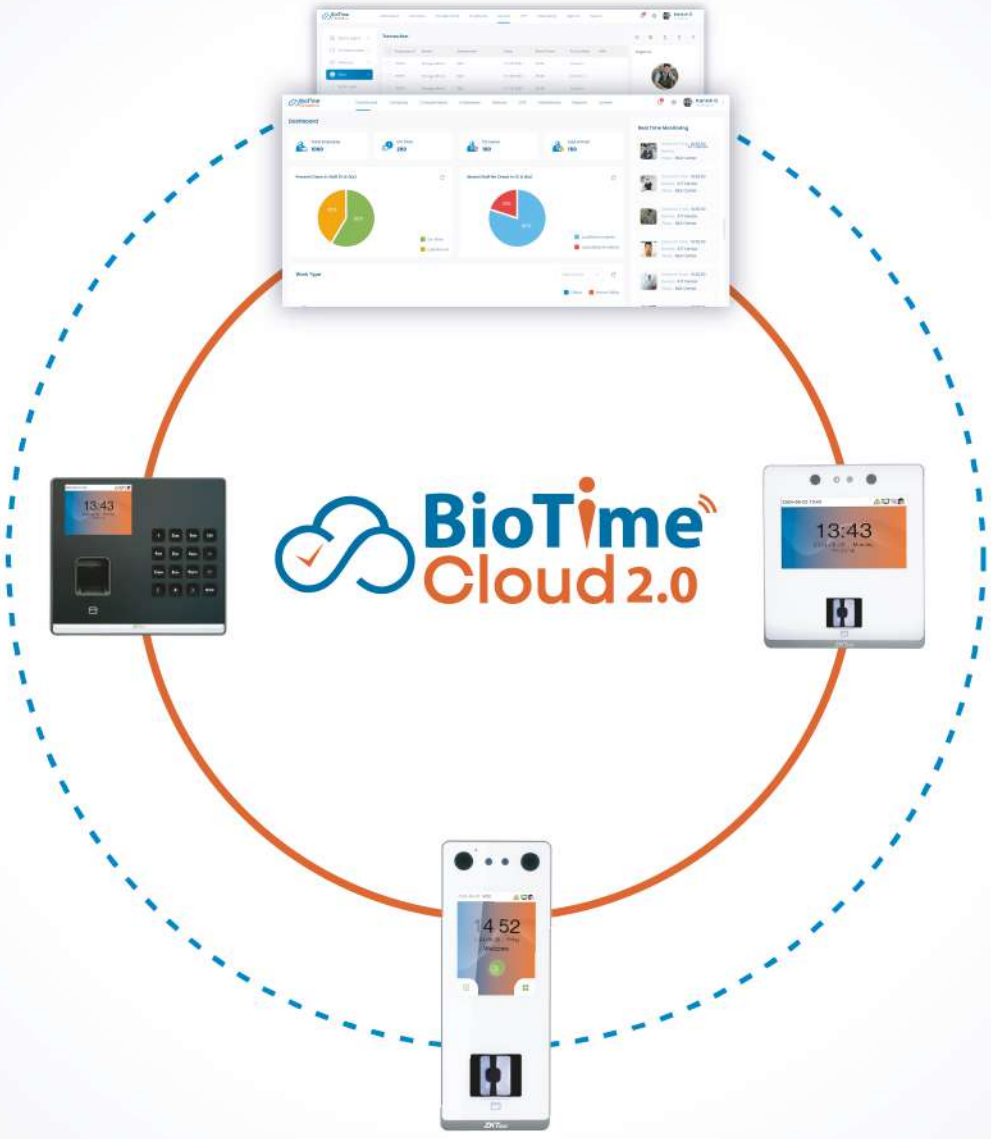
El "periodo de operación ecológica" del producto se refiere al tiempo durante el cual este producto no liberará sustancias tóxicas o peligrosas cuando se utilice de acuerdo con los requisitos establecidos en este manual.
El periodo de operación ecológica especificado para este producto no incluye baterías 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

Copyright © 2024 ZKTeco CO., LTD. All rights reserved.
ZKTeco may, at any time and without prior notice, make changes or improvements to its products and services, or cease their production or marketing.
The ZKTeco logo and brand are the property of ZKTeco CO., LTD