MANUAL DE USUARIO

InPulse, Inpulse+
Dispositivos de Control de Acceso

Green Label

Acerca de este manual

Este documento describe las funciones del menú, y la interfaz del usuario de la serie de productos con reconocimiento del patrón venoso de los dedos. Las funciones marcadas con * son opcionales en algunos dispositivos.

Para obtener información no consignada en este documento, por favor consulte el manual de instalación, la guía rápida o al personal técnico de su región.

Aviso importante

Primero que todo queremos agradecerle por haber adquirido este producto. Antes de utilizarlo, por favor lea este manual detenidamente. Le recordamos que el uso adecuado del equipo ayudará a mejorar el rendimiento y la velocidad de verificación.

Nota de privacidad

Sin el previo consentimiento de nuestra empresa, ningún individuo tiene permitido extraer o copiar el contenido de este manual de manera parcial o total, ni distribuirlo en ningún formato.

El producto descrito en el manual tal vez incluye software cuyos derechos de autor son compartidos por los licenciantes incluyendo nuestra empresa. Con excepción de la autorización del titular correspondiente, ningún individuo puede copiar, distribuir, revisar, modificar, extraer, descompilar, desensamblar, desencriptar, invertir ingeniería, transferir o sublicenciar el Software ni realizar otros actos de violación de los derechos de autor, pero se excluyen las limitaciones aplicadas por la ley.

Nos reservamos los derechos finales de modificación e interpretación.

Términos y condiciones

Debido a la constante renovación de productos, la empresa no puede garantizar que el artículo actual consista en su totalidad con la información consignada en este manual. Por favor disculpe los inconvenientes causados debido a los cambios hechos sin notificación.

Contenido

Notas de Orientación

No ubique el dispositivo de cara a la luz solar directa; la fuerte iluminación tiene un impacto adverso en el recolector de imágenes de las venas de los dedos. Cuando hay trabas en la disipación de calor o la temperatura está fuera del rango (0ºC~40ºC), el rendimiento del equipo se puede ver afectado. Si el dispositivo necesita ser utilizado en exteriores por favor utilice una caja de protección o una calefacción.

Recomendamos realizar la instalación del dispositivo a 1.4 m del suelo (recomendación basada en un rango de estaturas de 1.55~1.75 m). La altura de instalación puede ser ajustada teniendo en cuenta la estatura de los usuarios, con el fin de que puedan utilizar el dispositivo cómodamente.

1.1 Funciones del Producto

Identificación de venas de los dedos

La identificación de las venas es una nueva tecnología de reconocimiento de las características biológicas del ser humano. Verifica identidades utilizando imágenes de la distribución de las venas en los dedos; cuenta con una alta veracidad, estabilidad y previene falsificaciones.

Control de Acceso

Un sistema de control de acceso lógico, que cuente con un controlador, tiene las siguientes funciones:

- Fechas válidas para usuarios.
- Períodos de tiempo efectivo para usuarios.
- Múltiples modos de verificación.
- Períodos de tiempo efectivo para puertas.
- Períodos de tiempo para apertura de puertas.
- Festivos.
- Primera apertura normalmente abierta con tarjeta.
- Anti-Passback.
- Archivo de los registros de control de acceso.
- Soporte de entradas auxiliares.
- Soporte de dispositivos esclavos y maestros.

Notas de Orientación

USB

Por medio de la función USB, es posible exportar datos de usuario y registros de control de acceso. También se pueden importar datos de usuarios, fondos de pantalla y otros tipos de imágenes desde la USB.

Comunicación Ethernet o RS485

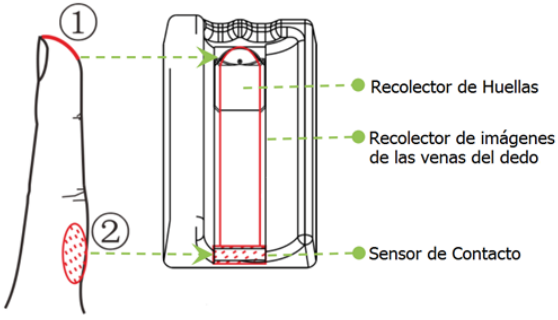
El dispositivo se comunica con el Software Access3.5 por medio del protocolo RS485 o por medio de TCP/IP (Ethernet).

1.2 Modo de Registro/ Verificación de las Huellas* y Venas del Dedo

Nota: Mientras se realiza el registro de las venas del dedo, el dispositivo también recolecta la huella digital.

- Dedos recomendados: índice y medio.
- Ubicación del dedo:

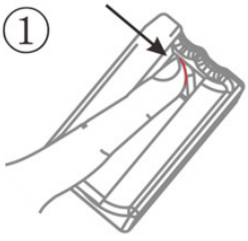
1) Presione el dedo de manera suave, firme y centrado en el recolector de imágenes de las venas de los dedos.



2) Cuando la almohadilla del dedo haga contacto con el sensor, se recolectará al mismo tiempo la huella digital.

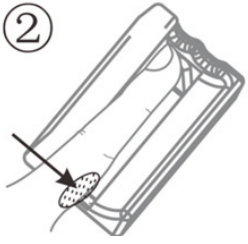
Notas de Orientación

- **Procedimiento para la verificación de venas**

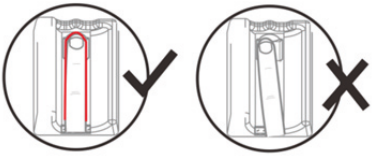


Asegúrese que la yema del dedo se encuentre en la parte superior del recolector de imágenes de venas.

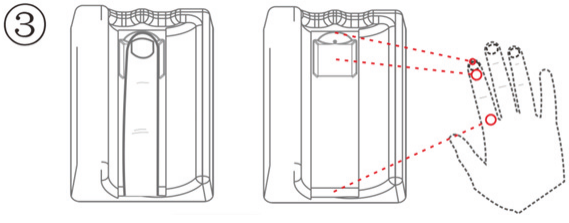
Si la ubicación del dedo es inadecuada, no será posible recolectar las imágenes correctamente.



Presione suavemente el dedo contra el recolector, asegurándose de que se encuentra centrado y que la almohadilla de la parte inferior del dedo haga contacto con el sensor.



La recolección de huellas e imágenes de las venas no pueden ser posibles si el dedo se encuentra inclinado hacia un lado o la almohadilla de la parte inferior del dedo no ha entrado en contacto con el sensor.



Cuando la parte inferior del dedo haga contacto con el sensor, se iniciará el proceso de recolección. Mantenga el dedo en esa posición hasta que el dispositivo haga sonar un bip, indicando que el proceso ha terminado y que ya puede retirar el dedo.

Notas de Orientación

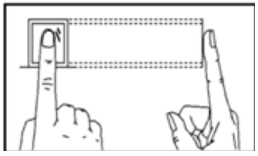
Trate de no doblar o girar el dedo cuando se está recolectando/verificando la huella y las venas.

No necesita presionar con fuerza el dedo contra el recolector.

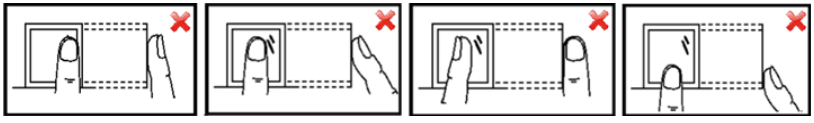
1.3 Ubicación de la huella en el Sensor

Los dedos recomendados son el índice y el corazón. El pulgar, el anular y el meñique no son recomendados (ya que a la hora de ubicarlos en el lector se muestran un poco torpes).

1). Ubicación adecuada del dedo: La huella debe estar firme, de frente y centrada en el lector de huellas.



2). Ubicación incorrecta del dedo: Cuando la huella se encuentra muy cerca o sobre los límites del lector, cuando el dedo está inclinado hacia un lado o cuando se presiona sólo una parte de la huella.



1.4 Uso de la pantalla Táctil

	La forma correcta de presionar la pantalla táctil es utilizando la yema del dedo. Presionar con la punta del dedo o la uña puede ser contraproducente.
	Cuando la lista de opciones es larga y sea necesario desplazarse hacia arriba y hacia abajo, toque la opción o arrastre la barra de movimiento de la parte derecha de la pantalla.

1.5 Modos de Verificación

1.5.1 Verificación de huellas* y venas de los dedos

Verificación 1:N

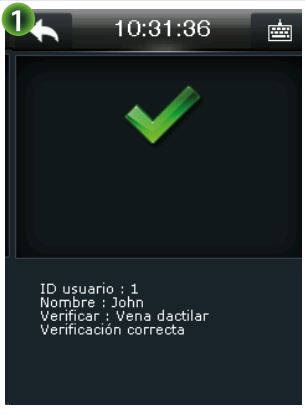
El dispositivo compara la imagen de las venas y la huella actual recolectada con todas las imágenes de venas y huellas almacenadas en el terminal.

1). Ubique el dedo adecuadamente para una correcta lectura. Para más detalles acerca de la postura del dedo en el sensor, por favor consulte el punto 1.2. Y el punto 1.3.

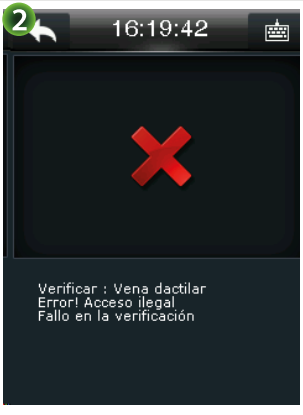
2). Cuando el dedo hace contacto con el sensor, el dispositivo detectará automáticamente las venas del dedo y la huella digital; y procederá a realizar la verificación.

3). Cuando el dispositivo emita un bip, retire el dedo del lector.

Notas de Orientación



Si la verificación es exitosa, la voz guía dirá "Gracias" y el mensaje "Verificación exitosa" será mostrado en pantalla.



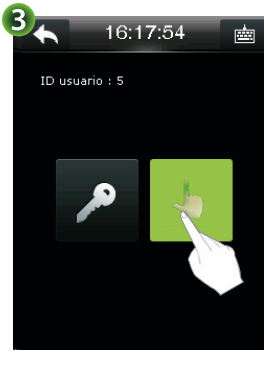
Si la verificación falla, la voz guía dirá "Por favor, intente de nuevo" y el mensaje "Falló la Verificación" será mostrado en pantalla.

Verificación 1:1

En el modo de verificación 1:1; el dispositivo compara la huella y la imagen de las venas del dedo actuales, con la huella y la imagen de las venas pertenecientes al ID de usuario ingresado. Utilice este método únicamente en situaciones en que se dificulte el reconocimiento de la huella digital o las venas.

1). En la interfaz inicial, haga clic en el icono para ingresar su ID de usuario.

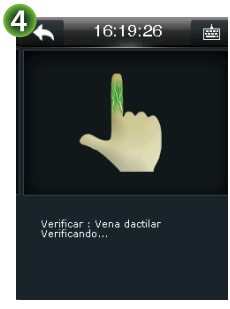
2). Ingrese su ID, haga clic en OK para entrar a otra interfaz y poder escoger el método de verificación.



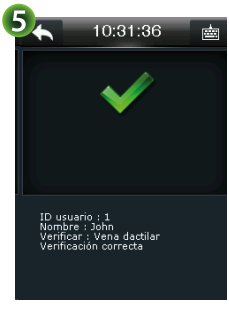
3). Haga clic en el icono de venas del dedo para ingresar a la interfaz de verificación 1:1

Notas de Orientación

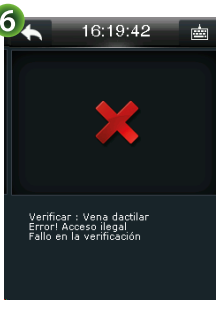
Nota: Si el mensaje "No hay datos de registro" es mostrado en pantalla, es porque el ID de usuario no existe.



4).Ubique el dedo adecuadamente para una correcta lectura. Para más detalles acerca de la postura del dedo en el sensor, por favor consulte el punto 1.2. Y el punto 1.3



5). Cuando el dispositivo emita un bip, retire el dedo del lector. Si la verificación es exitosa, el mensaje "Gracias" sonará y el mensaje "Verificación Exitosa" será mostrado en pantalla (figura 5).

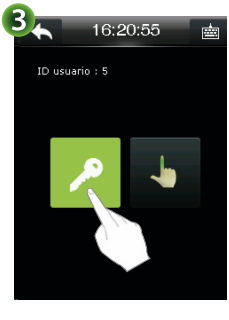


Si la verificación falla, el dispositivo emite el siguiente mensaje de voz " Por favor, inténtelo de nuevo" y el mensaje " Falló la verificación" será mostrado en pantalla (figura 6)

1.5.2 Verificación de Contraseña

1). En la interfaz inicial haga clic en el icono para ingresar su ID de usuario.

2). Ingrese su ID, haga clic en OK para entrar a otra interfaz y poder escoger el método de verificación.

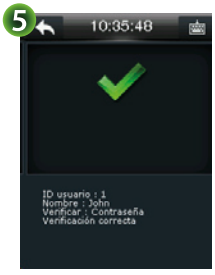


3). Haga clic en el icono de Contraseña para ingresar a la interfaz de verificación de contraseña.

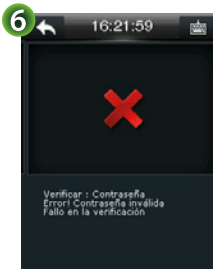
Notas de Orientación

Nota: Si el mensaje "No hay datos de registro" es mostrado en pantalla, es porque el ID de usuario no existe.

4). Ingrese la contraseña y haga clic en OK.

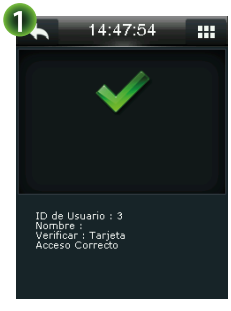


5). Si la verificación es exitosa, el mensaje "Gracias" sonará y el mensaje "Verificación Exitosa" será mostrado en pantalla (figura 5).



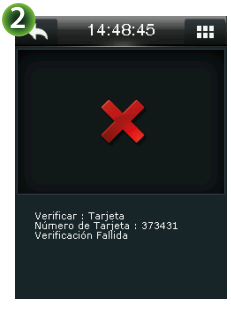
Si la verificación falla, el dispositivo emite el siguiente mensaje de voz " Contraseña Incorrecta" y el mensaje " Falló la verificación" será mostrado en pantalla (figura 6)

1.5.3 Verificación de Tarjeta*



1). La función de tarjeta es opcional. Sólo los productos con módulo de tarjetas integrado pueden realizar verificación por medio de tarjetas. Algunos dispositivos soportan tarjetas ID y MIFARE.

*Presente la tarjeta en el área del lector, si la verificación es exitosa; el mensaje "Gracias" sonará y el mensaje "Verificación Exitosa" será mostrado en pantalla.

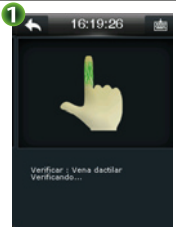
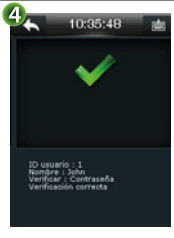


Si la verificación falla, el dispositivo hará sonar mensaje de voz "Ou Ou" y el mensaje "Falló la verificación" será mostrado en pantalla.

1.5.4 Verificación Combinada

El dispositivo soporta verificación combinada, por ejemplo; venas de dedo + contraseña, en la cual dispositivo necesita verificar la contraseña después de que el usuario presente las venas del dedo, y viceversa.

Tomemos como ejemplo la combinación Venas del dedo + Contraseña:

			
Ubique el dedo adecuadamente para una correcta lectura. Para más detalles acerca de la postura del dedo en el sensor, por favor consulte el punto 1.2. Y el punto 1.3.	Cuando el dispositivo emita un bip, retire el dedo del lector. Si la verificación es exitosa, la interfaz de verificación de contraseña se mostrará automáticamente.	Ingrese la contraseña y haga clic en OK.	Cuando la verificación de contraseña es correcta, la interfaz se muestra como en esta imagen

Nota: El usuario puede establecer las combinaciones, según sus necesidades. Para más detalles, por favor consulte el punto 9.1.

1.5.5 Verificación Combinada para Desbloqueo

Nota:

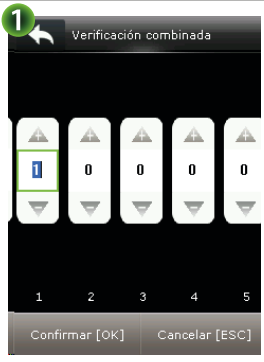
(1). Para consultar más detalles acerca de cómo establecer la verificación combinada para desbloqueo, por favor consulte el punto 9.4.

(2). En la interfaz "Agregar/Eliminar Usuario", el administrador puede especificar el grupo al que pertenece el usuario; y agregarlo al grupo para desbloqueo. Para detalles de la operación, por favor consulte el punto 3.1.7.

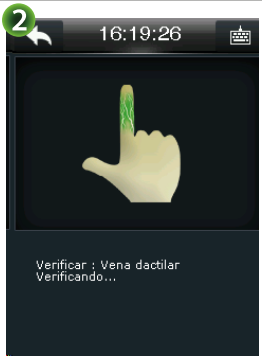
Por ejemplo, agregar una combinación de desbloqueo requiriendo verificación simultánea de grupo de usuarios 1 y grupo de usuarios 2 (figura 1) y agregar usuarios a los grupos para desbloqueo.

Notas de Orientación

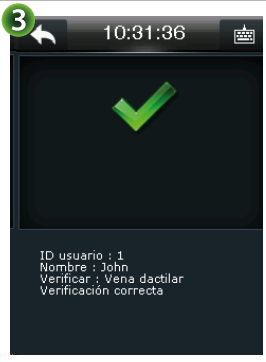
Supongamos que el usuario con el ID de usuario 1, pertenece al grupo 1; y que el usuario con el ID número 2 pertenece al grupo 2.



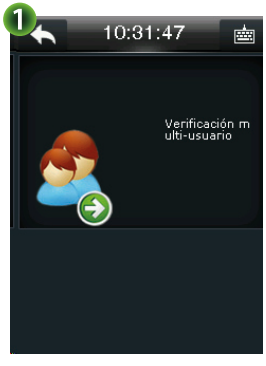
1). El usuario con el ID #1 presenta el dedo en el lector de venas. (detalles en el punto 1.2



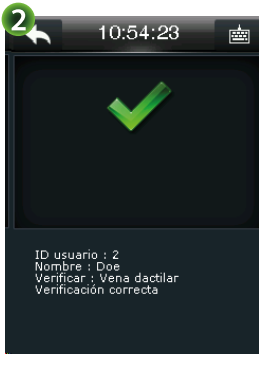
2). Después que el dispositivo hace sonar un bip, el usuario debe retirar el dedo.



3). "Verificación de venas exitosa".



4). Después, el dispositivo muestra el mensaje "Verificación Multi-Usuario



4). Después, el usuario con el ID #2 presenta el dedo en el lector de venas.

- Después que el dispositivo hace sonar un bip, el usuario debe retirar el dedo.

-El mensaje "Verificación de venas exitosa "es mostrado en pantalla y el mensaje "Gracias" es emitido también

Notas de Orientación

1.6 Interfaz Inicial

1). Fecha: Fecha actual.

2). Señal de Alarma: Si una alarma es establecida, se mostrará este icono.

3). Conexión de Red: Muestra el estado de conexión a la red.

4). Alarma Desmantelada: Este ícono se muestra en caso de posible "instalación Incorrecta" o "Desmantelamiento Ilegal"

5). Entrada Auxiliar: Este ícono aparece cuando se utiliza la entrada auxiliar del dispositivo para conectar con un dispositivo auxiliar y este es activado.

6). Hora: Muestra la hora actual. Los formatos de 12 y 24 horas son soportados por el dispositivo. Los usuarios pueden personalizar el estilo de la interfaz principal, para detalles por favor consulte el punto 7.

7). Menú: Presione este ícono para ingresar al menú principal. Si hay administradores establecidos, primero debe pasar la verificación antes de acceder al menú. Si no hay administradores establecidos, cualquier usuario puede acceder al menú principal.

8). Verificación 1:1: Presione este ícono para desplegar el teclado y poder ingresar el ID de usuario para verificación 1:1. Después de ingresar el ID de usuario, presione OK y siglas indicaciones que aparecen en pantalla.

Menú Principal

En la interfaz principal, haga clic en para ingresar al menú principal (Figura 2). Haga clic en para visualizar las opciones que se encuentran más abajo en el menú. (Haga clic otra vez en para desplazarse hacia la parte superior del menú).

Existen 11 opciones en el menú principal del dispositivo:

	Gestión de Usuarios	Usted puede buscar en el dispositivo, la información de los usuarios registrados (ID de usuario, nombre, rol, huella digital, tarjeta, contraseña, foto del usuario); también puede realizar agregar, modificar o eliminar usuarios.
	Privilegios	Se utiliza para establecer los derechos de acceso de los usuarios, a los menús del dispositivo.
	Comunicación	Usted puede establecer los parámetros relacionados con la comunicación entre dispositivo y el PC; incluyendo la dirección IP, comunicación serial, conexión al PC y configuraciones Wiegand
	Sistema	Aquí usted puede establecer la hora y fecha del dispositivo, configurar los registros de acceso, establecer los parámetros de huella digital y las venas del dedo, reiniciar y actualizar el firmware por medio de la USB.
	Personalizar	Con esta opción se pueden realizar cambios respecto a la pantalla, idioma, sonido y timbres.
	Gestión de Datos	Esta opción permite eliminar, realizar copia de seguridad y restaurar datos.

Menú Principal

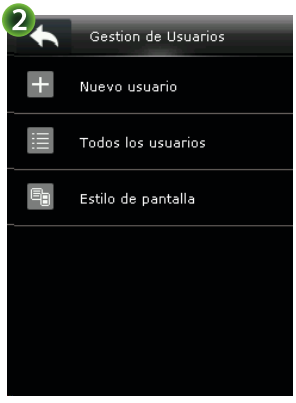
	Control de Acceso	Aquí usted puede establecer los parámetros para de control de acceso, período de tiempo, festivos, verificación combinada y Anti-Passback.
	USB	Aquí usted puede exportar/importar la información de los usuarios y registros de acceso almacenados en una USB a un (o desde un) software relacionado u otro equipo de reconocimiento. En el caso de importación de datos también es posible cargar al dispositivo protectores de pantalla y fondos de escritorio.
	Buscar Datos de Asistencia	Consultar los registros de asistencia guardados en el dispositivo.
	Pruebas	Este sub-menú le permite al sistema verificar que la pantalla, el sensor de huellas, el sonido, el teclado y el reloj estén trabajando correctamente
	Información del Sistema	Consulte aquí la capacidad, la información y el firmware actual del dispositivo

Si hay administradores establecidos, primero debe pasar la verificación antes de acceder al menú. Si no hay administradores establecidos, cualquier usuario puede acceder al menú principal.

Por seguridad recomendamos registrar un administrador cuando el dispositivo vaya a ser utilizado por primera vez.

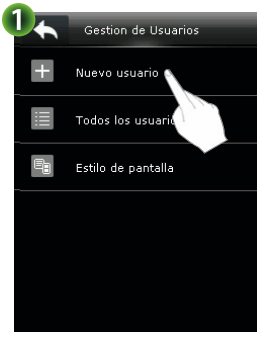
Gestión de Usuarios

A través de este icono, usted puede consultar la información básica del usuario, incluyendo el ID, rol, imágenes de las venas y huellas digitales*, contraseña, número de tarjeta* y nivel de acceso. También agregar, modificar o eliminar la información del usuario.



3.1 Agregar Usuario

En el menú principal elija la opción "Gestión de Usuarios", haga clic en "Nuevo Usuario" e ingrese la información pertinente. Utilice la tecla para visualizar las opciones que se encuentran en la parte inferior de la lista; haga clic de nuevo en para volver a la parte superior de la lista.



Gestión de Usuarios

ID de Usuario: Ingrese un ID de usuario. El sistema soporta de 1 a 9 dígitos.

Nombre: Ingrese un nombre de usuario. El dispositivo soporta hasta 24 caracteres.

Privilegio Usuario: Establezca el privilegio del usuario. El privilegio por defecto es "Usuario Normal", pero también tiene la opción "Administrador". Un usuario normal sólo puede utilizar las funciones de verificación de identidad, mientras que el administrador puede acceder a todas las funciones del menú principal y realizar cambios.

Huella digital y Venas del Dedo: Registrar venas del dedo y huella digital, el dedo índice y el anular son los recomendados.

Contraseña: Registre una contraseña. El sistema soporta hasta 8 dígitos.

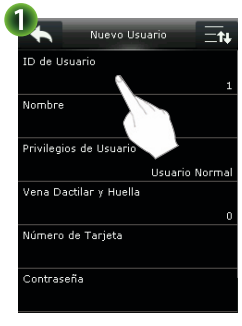
Número de Tarjeta*: Registre una tarjeta.

Nivel de Control de Acceso: Establezca el control de acceso para el usuario (grupo de acceso & horario)

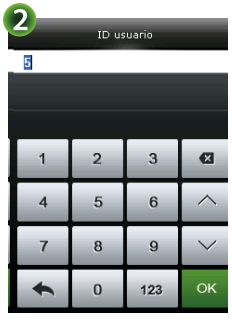
Gestión de Usuarios

3.1.1 Ingresar un ID de Usuario

El dispositivo asigna automáticamente un ID iniciando desde 1 y siguiendo la secuencia. Si usted utiliza el ID asignado por el terminal, puede saltar esta sección.



En la interfaz "Nuevo Usuario" elija la opción "ID de Usuario" y presione [OK]



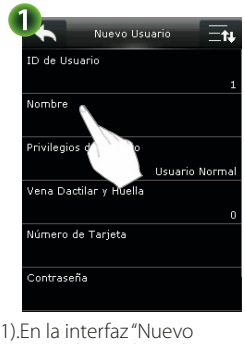
Ingrese el ID de Usuario, presione [OK] para confirmar y volver a la interfaz anterior.

Nota:

- El terminal soporta de 1 a 9 dígitos.
- El ID del usuario no puede ser modificado posteriormente.
- Si el mensaje "El ID de Usuario ya existe" aparece en pantalla; por favor ingrese otro ID

3.1.2 Ingresar Nombre

Ingrese el nombre del usuario utilizando el teclado T9.



1).En la interfaz "Nuevo Usuario", haga clic en la opción "Nombre".

2). Ingrese el nombre. Para detalles sobre el uso del teclado por favor consulte el anexo 1 ubicado en el punto 14 de este manual.

3). Haga clic en OK para guardar los cambios y volver a la interfaz anterior. Para volver a la interfaz anterior sin guardar los cambios, haga clic en

Nota: El dispositivo soporta hasta 24 caracteres.

3.1.3 Privilegio del Usuario

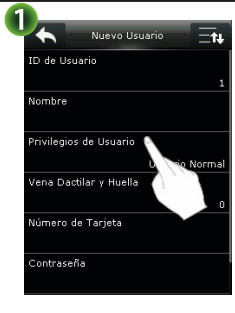
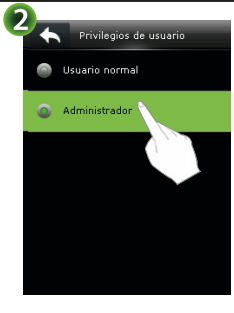
El dispositivo soporta dos tipos de roles: Usuario Normal y Administrador.

Administrador: El súper administrador tiene acceso a todas las funciones del menú del dispositivo.

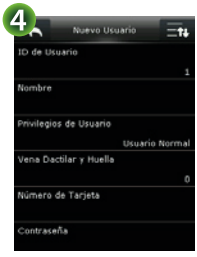
Usuario Normal: Si el sistema tiene un administrador; un usuario normal sólo tiene acceso a la función de verificación de identidad utilizando su huella*, contraseña o tarjeta*. Si el sistema no tiene un administrador; el usuario normal tiene los derechos de operación sobre todas las funciones que ofrece el menú del dispositivo.

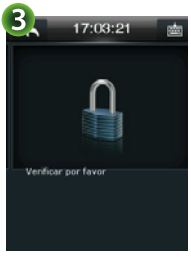
Derechos Especiales: Otras funciones del menú pueden estar disponibles para usuarios normales. El administrador tiene la posibilidad de asignar derechos a otras funciones del menú personalizando el privilegio del usuario.

Este icono indica que el usuario actual es un administrador

	
1). En la interfaz "Nuevo Usuario", haga clic en la opción "Privilegio del Usuario"	2). Seleccione el privilegio correspondiente. El dispositivo volverá automáticamente a la interfaz anterior.

Gestión de Usuarios

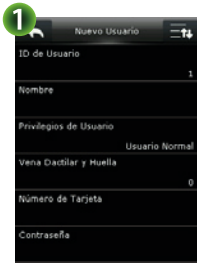




Nota:

Un usuario normal sólo puede utilizar las funciones de verificación de identidad, mientras que el administrador puede acceder a todas las funciones del menú principal y realizar cambios.
Después de haber establecido un administrador (Figura 3), debe realizarse la verificación de administrador antes de poder ingresar al menú principal (Figura 4).

3.1.4 Registro de huellas y venas del dedo

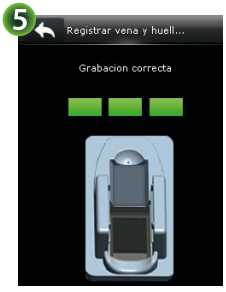
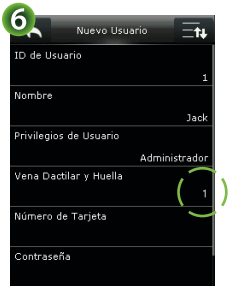
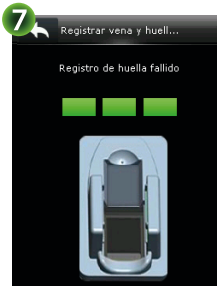


1). En la interfaz "Nuevo Usuario", haga clic en la opción "FV&FP" (Huella digital y Venas del Dedo)

2). Por favor seleccione el dedo que va a registrar.

3). Presione el mismo dedo tres veces en el sensor, siguiendo las indicaciones de la pantalla. Para detalles, consulte el punto 1.2.

Gestión de Usuarios

		
4). Después que se ha presentado la huella digital tres veces en el sensor, el mensaje "Registro Exitoso" aparecerá en pantalla.	5) Después del registro exitoso, el dispositivo vuelve automáticamente a la interfaz "Nuevo Usuario", mostrando la cantidad de Huellas/Imágenes de Venas registradas.	Si el proceso de registro falla, y el mensaje "Registro Fallido", repita el proceso por favor.

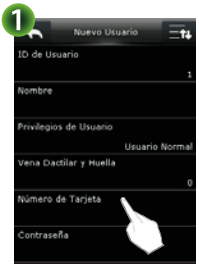
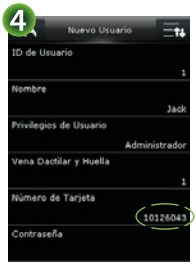
Nota:

• Mientras se realiza el registro de las venas del dedo, el dispositivo registra la huella digital al mismo tiempo.

• Para una mejor recolección de Huellas + Venas, retire el dedo del sensor cada vez que el dispositivo haga sonar un bip; continúe con el registro según las indicaciones mostradas en pantalla.

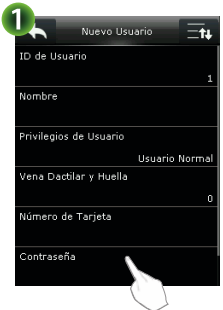
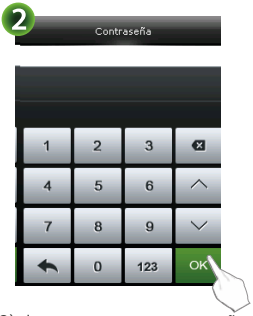
Gestión de Usuarios

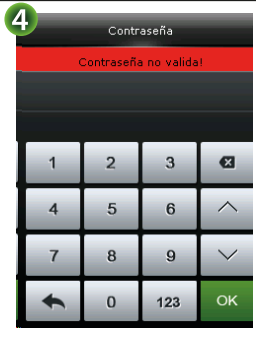
3.1.5 Registrar Número de Tarjeta*

			
1). En la interfaz "Nuevo Usuario", elija la opción "Tarjeta ID"	2). Deslice la tarjeta en el área del lector.	3) Cuando la tarjeta haya sido leída exitosamente, el número se mostrará en pantalla.	4). El dispositivo volverá automáticamente a la interfaz "Nuevo Usuario" y se podrá visualizar el número.

Nota: Algunos dispositivos soportan tarjetas MIFARE e ID.

3.1.6 Registrar una Contraseña

		
1). En la interfaz "Nuevo Usuario", elija la opción "Contraseña".	2). Ingrese una contraseña y oprima OK.	3). Ingrese de nuevo la contraseña y haga clic en Ok. El dispositivo volverá automáticamente a la interfaz "Nuevo Usuario".



Nota:

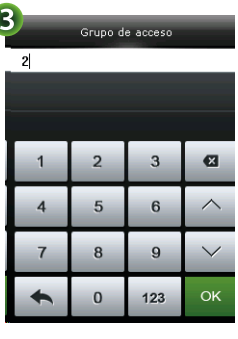
•El sistema soporta contraseñas de hasta 8 dígitos.

•Las contraseñas ingresadas en los puntos 2 y 3 deber ser iguales; de otra manera el mensaje: "Las contraseñas no coinciden", se mostrará en pantalla (Figura 4); el sistema volverá automáticamente a la interfaz "nuevo Usuario", por favor realice el proceso de nuevo.

3.1.7 Configuración del Nivel del Acceso

En la interfaz "Nuevo Usuario", elija la opción "Control de Acceso"

El nivel de control de acceso es utilizado para establecer la apertura de la puerta para cada usuario, incluyendo los grupos de acceso y los horarios.



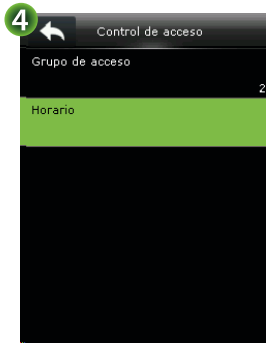
Configurar el Grupo de Acceso: Establezca el grupo al cual pertenece el usuario para facilitar las configuraciones de desbloqueo. El número válido de grupos es de 1 a 99.

1). En la interfaz de control de acceso haga clic en la opción "Grupo de Acceso".
2). Ingrese el número del grupo al cual pertenece el usuario., haga clic en OK

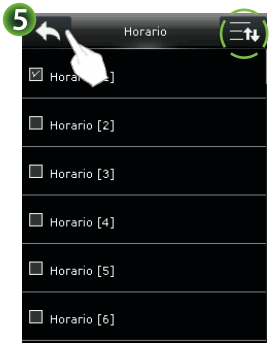
Gestión de Usuarios

(Figura 3) para guardar los cambios regresar a la interfaz "Control de Acceso"

Configurar el Horario: Un máximo de 50 horarios son soportados. El período de tiempo efectivo de apertura de la puerta de un usuario es la sumatoria de los horarios seleccionados.



1). En la interfaz de "Control de Acceso", seleccione la opción "Período de Tiempo". Utilice el icono para desplazarse hacia abajo del menú y haga clic nuevamente para volver a la parte superior.



2). En la lista, seleccione los horarios haciendo clic en ellos (al quedar seleccionados la casilla se muestra así ☑, para quitar la selección haga clic de nuevo). Pulse el icono para guardar los cambios y volver a la interfaz anterior.

3.2 Todos los Usuarios

En la interfaz "Gestión de Usuarios" , haga clic en "Todos los Usuarios". El administrador puede consultar, editar o eliminar usuarios.

Gestión de Usuarios

	Este icono indica que el usuario es administrador
	Indica que el usuario tiene huella digital registrada*
	El usuario tiene una tarjeta registrada*.
	Indica que el usuario tiene registrada una contraseña.
	El usuario tiene registradas las venas del dedo.

Nota: La información de los usuarios registrados es mostrada de acuerdo al "Estilo de Pantalla" establecido. Para más detalles, por favor consulte el punto 3.3.

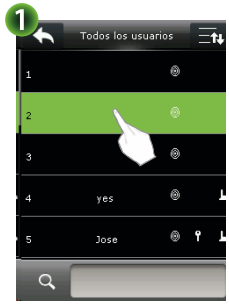
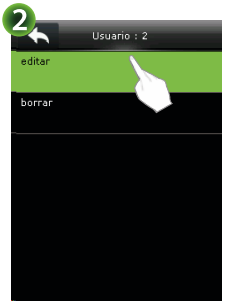
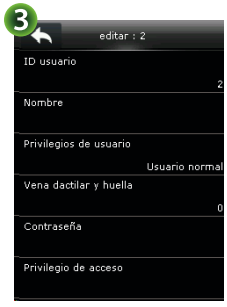
3.2.1 Buscar Usuario

En la interfaz "Gestión de Usuarios"  , seleccione la opción "Todos los Usuarios". Haga clic en la casilla de búsqueda e ingrese el ID o nombre de usuario y haga clic en OK.

3.2.2 Editar/Eliminar Usuarios

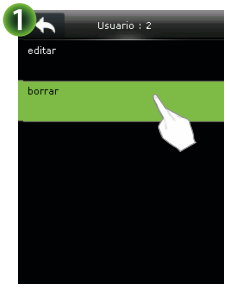
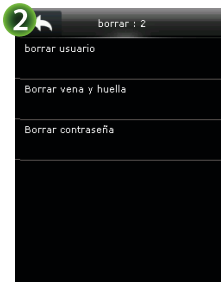
En la interfaz "Gestión de Usuarios"  , seleccione la opción "Todos los Usuarios". Haga clic en la casilla de búsqueda e ingrese el ID o nombre de usuario que desea editar o eliminar y haga clic en OK.

Editar Usuario

		
1). Haga clic en el usuario	2). En la siguiente interfaz, seleccione la opción "Editar".	3). Modifique la información del usuario, haga clic en el icono para guardar los cambios y volver a la interfaz anterior.

Nota: En la edición de usuarios se procede de manera similar a cuando se agrega un nuevo usuario.

Eliminar Usuario

	
1) Haga clic en "Eliminar".	2) En esta interfaz se muestran los ítems según la información registrada, haga clic y en la opción deseada y confirme la acción con "OK". Para cancelar haga clic en "Cancelar"

Nota:

Si elige la opción "Eliminar Usuario" se borrará toda la información del usuario (Nombre, huella*, venas, contraseña, número de tarjeta*)

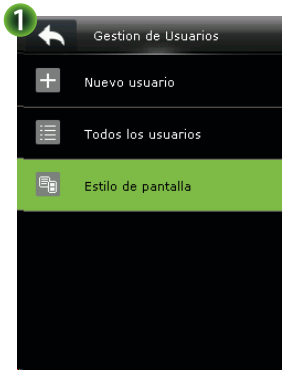
Si el usuario no tiene registrada una contraseña la opción "Eliminar Contraseña" no aparecerá entre las opciones.

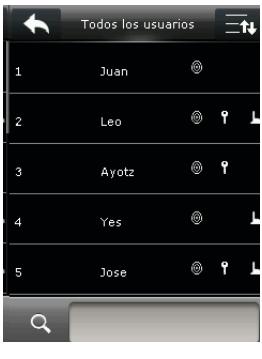
3.3 Estilo de Visualización

En la interfaz "Gestión de Usuarios"  , seleccione la opción "Estilo de Visualización" (Establecer cómo mostrar la información del usuario)

En esta interfaz, usted puede escoger entre las opciones: Línea única, Múltiples Líneas y Línea Combinada.

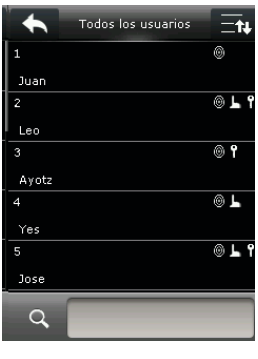
Gestión de Usuarios





Línea única

Múltiples Líneas



Línea Combinada

Privilegio del Usuario-Derechos de Acceso al Menú

Usted puede establecer privilegios de usuarios definidos y asignar niveles de operación a cada uno.

En la lista de privilegios de usuario (Figura 2) seleccione el privilegios a ser editado.

Nota: Los privilegios de usuario definidos, pueden ser establecidos únicamente cuando haya un administrador registrado. (Figura 5)

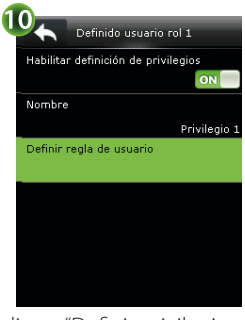
Privilegio del Usuario-Derechos de Acceso al Menú

Habilitar Privilegio Definido: La configuración predeterminada es OFF (Desactivado). Haga clic en ícono para cambiar el estado a ON (Encendido) y viceversa.

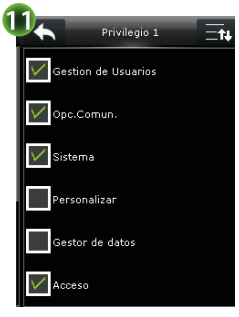
Nombre: Establecer un nombre para el privilegio (Figura 7). Ingrese el nombre mediante el teclado del dispositivo (Figura 8); haga clic en OK (Figura 8) para guardar los cambios y regresar a la interfaz anterior.

Para más detalles, por favor consulte el punto 14, anexo1.

Definir Privilegio del Usuario: Asignar el nivel de operación.



1). Haga clic en "Definir privilegio de Usuario". Utilice el icono para desplazarse hacia abajo del menú y haga clic nuevamente para volver a la parte superior.



2). En la lista, seleccione los iconos del menú haciendo clic en ellos (al quedar seleccionados la casilla se muestra así ☑, para quitar la selección haga clic de nuevo

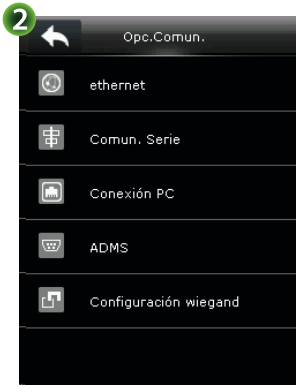
Privilegio del Usuario-Derechos de Acceso al Menú

3). Pulse el icono para guardar los cambios y volver a la interfaz anterior.

Comunicación

Establezca los parámetros de comunicación entre el dispositivo y el PC. Los parámetros incluyen la dirección IP, puerta de enlace, mascara de red, velocidad de transmisión, ID del dispositivo y contraseña de ingreso al sistema.

Menú Principal >> 



5.1 Ethernet

En la interfaz  [Comunicación], y haga clic en la opción [Ethernet].

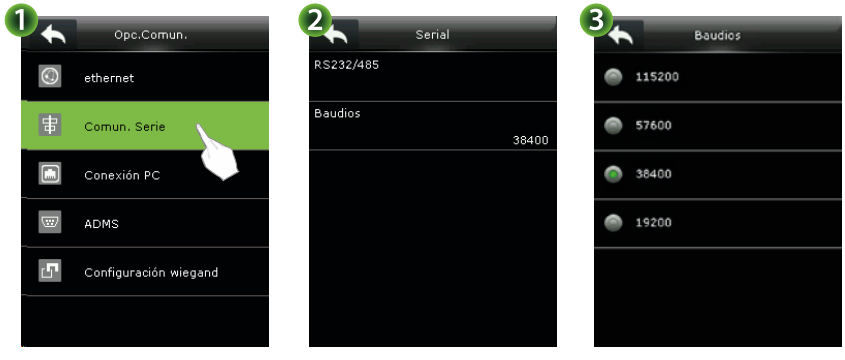
Comunicación

Los parámetros a continuación son los valores de fábrica, por favor ajústelos de acuerdo a la situación de red actual:

Dirección IP: 192.168.1.201
Máscara de Red: 255.255.255.0
Puerta de Enlace: 0.0.0.0
DNS: 0.0.0.0
Puerto de Comunicación TCP: 4370
DHCP: Protocolo de Configuración Dinámica de Host (por sus siglas en inglés) es utilizado para distribuir direcciones IP a clientes vía servidor.
Barra de estado: Utilizado para definir si mostrar o no los iconos de red en la interfaz principal.

5.2 Comunicación Serial

En la interfaz [Comunicación], y haga clic en la opción [Comunicación Serial].



Cuando el Puerto serie (RS232/RS485) es utilizado para la comunicación entre el dispositivo y el PC, las siguientes configuraciones necesitan ser revisadas:

RS232/485: Habilitar o desactivar la comunicación RS485.
Velocidad de Transmisión: Hay cinco opciones: 19200, 38400,57600 y 115200(predeterminada). Entre más alta es la velocidad de transmisión, la velocidad de comunicación es más veloz, pero menos estable. En general una alta velocidad de transmisión puede ser utilizada para distancias cortas; pero cuando la distancia de comunicación es larga, elija una velocidad de transmisión más lenta.

5.3 Contraseña de Conexión al PC

Para mejorar la seguridad de los datos, es necesario establecer una contraseña de conexión entre el dispositivo y el PC. La contraseña de conexión se utiliza cuando el Software de PC se conecta al dispositivo para leer los datos.

Clave de Comunicación: La contraseña predeterminada del sistema es 0 (no hay contraseña). Establezca la clave de comunicación y haga clic en OK (figura3) para guardar los cambios y volver a la interfaz anterior. El sistema soporta claves de 1 a 6 dígitos.

ID del Dispositivo: El número de identificación del dispositivo puede estar en un rango de 1 a 254. Ingrese el ID y haga clic en OK para guardar los cambios y volver a la interfaz anterior.
Si la comunicación RS232 es utilizada, este ID necesita ser ingresado en la interfaz de comunicación del software.

5.4 Configuración Wiegand

Menú Principal>>  >>

5.4.1 Entrada Wiegand

Establecer el formato Wiegand de un lector conectado externamente.

Comunicación

Formato Wiegand: El dispositivo soporta los siguientes formatos: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a y Wiegand 50. El estado "Sin Usar" significa que ese formato no está siendo utilizado.

Ancho de Pulso (us): El ancho de pulso enviado por medio de Wiegand. El valor predeterminado es de 100 microsegundos, pero puede ser ajustado dentro de un rango de 20 a 100.

Intervalo de Pulso (us): El valor predeterminado es de 100 microsegundos, pero puede ser ajustado en dentro de un rango de 200 a 20.000.

Tipo de ID: Contenido de entrada incluido en la señal de entrada wiegand. El ID de Usuario o Número de Tarjeta puede ser elegido.

Definiciones de los formatos Wiegand:

Formato Wiegand	Definición
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 26 bits de código binario. El 1er bit es el bit de paridad par de los bits del 2º al 13º, mientras que el bit 26º es el bit de paridad impar del 14º al 25º. Los bits del 2º al 25º son los del número de tarjeta.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consiste de 26 bits de código binario. El 1er bit es el bit de paridad par de los bits del 2do al 13ro, mientras que el bit 26 es el bit de paridad impar de los bits del 14to al 25to. Los bits del 2do al 9no son los códigos del sitio y los bits del 10mo al 25to son los números de tarjeta.

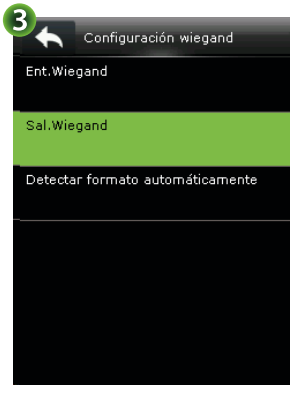
Comunicación

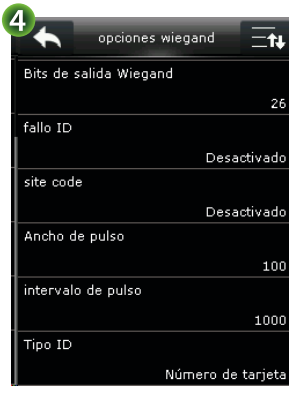
Wiegand 34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits de código binario. El 1er bit es el bit de paridad par del 2do al 17mo bit, mientras que el 34to bit es el bit de paridad impar del 18vo al 33er bit. Los bits del 2do al 25to son el número de tarjeta.
Wiegand 34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits de código binario. El 1er bit es el bit de paridad par del 2do al 17mo bit, mientras que el 34to bit es el bit de paridad impar del 18vo al 33er bit. Los bits del 2do al 19no son el código del sitio, mientras que del 10mo al 25to bit son el número de tarjeta.
Wiegand 36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consiste de 36 bits de código binario. El 1er bit es el bit de paridad impar del 2do al 18vo bit, mientras que el 36to bit es el bit de paridad par del 19no al 35to bit. Los bits del 2do al 17mo son el código del dispositivo, los bits del 18vo al 33er son el número de tarjeta, y los bits 34to y 35to son el código del fabricante.
Wiegand 36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consiste de 36 bits de código binario. El 1er bit es el bit de paridad par del 2do al 18vo bit, mientras que el 36to bit es el bit de paridad impar del 19no al 35to bit. Los bits del 2do al 19no son el código del dispositivo y del 20mo al 35to bit son el número de tarjeta.
Wiegand 37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consiste de 37 bits de código binario. El 1er bit es el bit de paridad impar del 2do al 18vo bit, mientras que el 37mo bit es el bit de paridad par del 19no al 36to bit. Del 2do al 4to bit son el código del fabricante, del 5to al 16to son el código del sitio y del 21ro al 36to son el número de tarjeta.
Wiegand 37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consiste de 37 bits de código binario. El 1er bit es bit de paridad par del 2do al 18vo bit, mientras que el 37mo bit es el bit de paridad impar del 19no al 35to bit. Del 2do al 4to bit son el código del fabricante, del 5to al 14to bit son el código del dispositivo, del 15to al 20mo bit son el código del sitio, y del 21er al 36to bit son el número de tarjeta.
Wiegand 50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 50 bits de código binario. El 1er bit es el bit de paridad par del 2do al 25to bit, mientras que el 50mo bit es el bit de paridad impar del 26to al 49no bit. Del 2do al 17mo bit son el código del sitio y del 18vo al 49 son el número de tarjeta

Nota:

C denota el número de tarjeta, **E** el bit de paridad par, **O** el bit de paridad impar, **f** código del dispositivo, **M** código de fabricante, **P** paridad par y **S** código de sitio.

5.4. 2 Salida Wiegand





Formato Wiegand: Consulte las definiciones de los formatos Wiegand soportados por el sistema en el punto 5.4.1; el actual formato es determinado por los bits de salida wiegand.

Bits de Salida Wiegand: Cantidad de bits de los datos wiegand. Después de elegir la opción [Bits de Salida Wiegand], el dispositivo utilizará la cantidad de bits establecidos para encontrar el formato wiegand adecuado.
Por ejemplo, si son seleccionados el 26Bit/Wiegand26, 34Bit/Wiegand34a, 36Bit/Wiegand36, 37Bit/Wiegand 37a y 50Bit/Wiegand 50; pero los bits de salida Wiegand están establecidos en 36, el formato 36-Bit Wiegand36 es adoptado.

ID Fallido: Está definido como el valor de salida de la verificación de usuario fallida. El formato de salida depende de la configuración del [Formato Wiegand]. El rango predeterminado es de 0 a 65535.

Código de Sitio: Es similar al ID del dispositivo, excepto porque este puede ser establecido manualmente y puede repetirse en varios dispositivos.

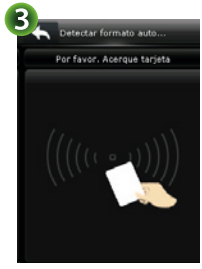
Ancho de Pulso (us): El ancho de pulso enviado por medio de Wiegand. El valor predeterminado es de 100 microsegundos, pero puede ser ajustado dentro de un rango de 20 a 100.

Intervalo de Pulso (us): El valor predeterminado es de 100 microsegundos, pero puede ser ajustado en dentro de un rango de 200 a 20.000.

Tipo de ID: Contenido de salida incluido en la señal de salida wiegand. El ID de Usuario o Número de Tarjeta puede ser elegido.

5.4.3 Detección Automática del tipo de Tarjeta

La [Detección Automática del Tipo de Tarjeta] es una función que permite la rápida detección del tipo de tarjeta y su formato correspondiente. Varios formatos de tarjetas están preestablecidos en el dispositivo. Después de deslizar la tarjeta, el sistema detectará los diferentes números de tarjeta de acuerdo a cada formato; el usuario sólo requiere escoger el ítem equivalente al actual número de tarjeta, y establecer el formato como el formato Wiegand para el dispositivo. Esta función aplica también a la función de lectura de tarjetas y lector wiegand auxiliar.

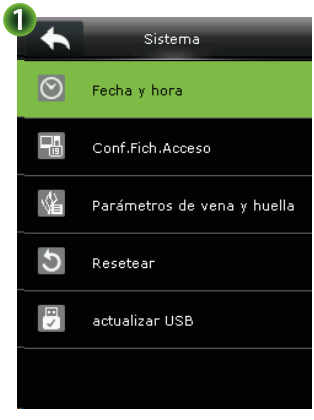
		
En la interfaz [Detección Automática del Tipo de Tarjeta], deslice la tarjeta (en este dispositivo o en el lector).	El formato wiegand y el número de tarjeta serán detectados automáticamente.	Seleccione el número consistente con el actual número de tarjeta, y el formato correspondiente es el formato Wiegand que debe ser seleccionado para leer este tipo de tarjeta.

Configuración del Sistema

Los parámetros del sistema incluyen la fecha y hora del dispositivo, registros de acceso*, parámetros de huella digital y venas de los dedos, restauración de los valores de fábrica y actualización del firmware.

6.1 Hora/Fecha

Configurar la hora y la fecha del dispositivo. Menú principal>> Sistema>> Fecha/Hora.



Configuración del Sistema

Establecer Fecha y Hora: Este parámetro es utilizado para establecer la hora y la fecha del dispositivo.

Formato de 24 Horas: Este parámetro es utilizado para establecer el formato de la hora del dispositivo. Si la función está encendida la hora se mostrará en formato de 24 horas. Si la opción está apagada la hora se mostrará en formato de 12 horas.

Formato de Fecha: Este parámetro permite definir el formato en que se va a mostrar la fecha en el dispositivo.

6.1.1 Horario de verano

Horario de Verano: El DST, también llamado Horario de Verano; se utiliza con el fin de ahorrar energía. Es un sistema que adoptan algunos países en verano y consiste en adelantar el horario 1 hora.

Para satisfacer las necesidades del DST, una opción especial ha sido personalizada en nuestro dispositivo; haciendo que la el horario se adelante 1 hora en X minuto, X hora y X día y vuelva al estado normal en X minuto, X hora, X día y X si es necesario.

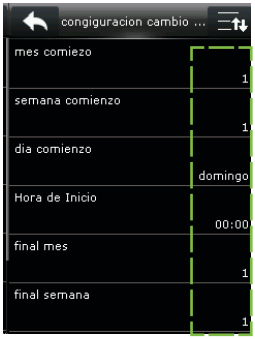
	Active la función [Horario de verano] ON ; al activarla aparecerán las opciones [Modo del Horario de Verano] y [Configuración del Horario de Verano]. Modo del horario de verano: Usted puede establecer el modo fecha/día o modo semana/fecha. Configuración del Horario de verano: Establezca el inicio y el fin del horario de verano.

Ejemplo

Establezcamos que el reloj se adelante una hora a las 08:00 el 1ro de abril y el 1ro de octubre retroceda 1 (es decir, que la hora volverá al estado normal)

- **Modo semana/fecha:**

•Modo Semana/Fecha:



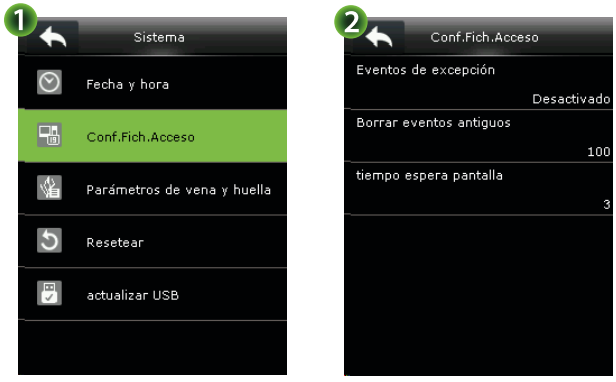
Nota:

1). Si el mes en el que inicia el horario de verano es más tarde que la fecha de finalización; significa que el horario de verano abarcará un período de ocupa dos años diferentes. Por ejemplo: Fecha de inicio (nov-01-2012), fecha final (abril-01-2013)

2). Asumamos que el Modo Semana/Fecha ha sido seleccionado y que el horario de verano inicia desde el domingo de la sexta semana de septiembre de 2013. De acuerdo con el calendario, en septiembre de 2013 no tiene seis semanas, pero tiene cinco. En ese caso, en 2013, inicia en el punto de tiempo correspondiente al último domingo de septiembre.

3). Supongamos que el horario de verano inicia desde el lunes de la primera semana de septiembre de 2012. De acuerdo con esto, la primera semana de septiembre no tiene lunes. En este caso, el DST inicia desde el primer lunes de septiembre de 2012.

6.2 Configuración de los Registros de Acceso*



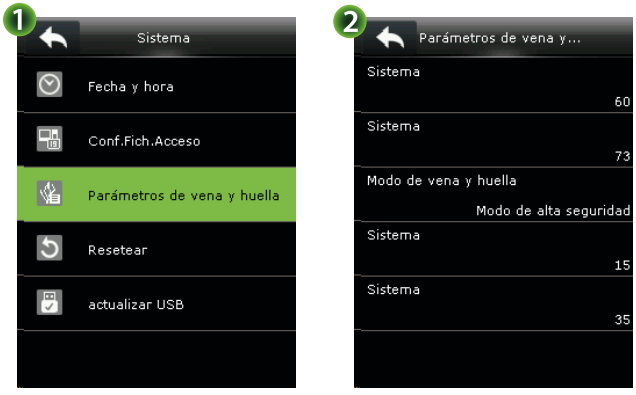
Menú principal>> Sistema>> Config. Registros de Acceso.

Alerta de Espacio Insuficiente: Cuando la capacidad de registros restante sea menor que el valor preestablecido, el dispositivo generará un mensaje indicando la capacidad de registros restante. Usted puede activar/desactivar esta función; cuando la active el rango es de 1 a 9999.

Limpieza Periódica de Registros de Asistencia: Especificar el máximo de registros de entradas que pueden ser eliminados (el rango es de 1 a 999) en el momento que el número de registros alcance la capacidad máxima. Esta función puede ser desactivada.

Duración de Pantalla de Confirmación: Especifique el tiempo para mostrar el resultado de la autenticación en la pantalla. El rango es de 1 a 9 segundos.

6.3 Parámetros de Huellas Digitales* y Venas del dedo



Menú principal>> Sistema>> Parámetros Huella & Venas

Umbral 1:1 VD (Venas del Dedo): Examina la similitud entre la imagen de verificación actual y la imagen de las venas del dedo registradas por el usuario (almacenada en el dispositivo). El valor preestablecido es 60, pero usted puede modificarlo dentro de un rango de 55 a 75. Cuando la similitud alcance el nivel establecido, la verificación es exitosa. Entre más alto sea el umbral más bajo es el error de cálculo y más alto el índice de rechazo, y viceversa.

Umbral 1: N VD (Venas del Dedo): Examina la similitud entre la imagen de verificación actual y todas las imágenes de las venas del dedo almacenadas en el dispositivo. El valor preestablecido es 70, pero usted puede modificarlo dentro de un rango de 65 a 85. Cuando la similitud alcance el nivel establecido, la verificación es exitosa. Entre más alto sea el umbral más bajo es el error de cálculo y más alto el índice de rechazo, y viceversa.

Umbrales de verificación recomendados:

Tasa de rechazo por error	Tasa de error de cálculo	Umbral de Coincidencia	
		1:N	1:1
Alto	Bajo	85	75
Medio	Medio	70	60
Bajo	Alto	65	55

Configuración del Sistema

Modo H&V (Huella & venas): El modo Huella digital & Venas del Dedo está preestablecido. Usted puede seleccionar el modo Huella o Venas también.

• **Modo Huella o Venas:** La verificación pasa cuando la huella o las venas del dedo (cualquiera de las dos) son verificadas como positivas.

• **Modo Huella & Venas:** La verificación pasa únicamente cuando la huella y las venas (ambas) son verificadas positivamente

Nota: El modo HD&VD (Huella Digital & Venas del Dedo) sólo puede ser modificado cuando no hay datos existentes en el sistema. Si existen datos, usted debe eliminarlos para poder modificar el modo HD&VD.

• **Umbral 1:1 HD* (Huella Digital):** Examina la similitud entre la huella de verificación actual y la plantilla de la huella registrada por el usuario (almacenada en el dispositivo). El valor preestablecido es 15, pero usted puede modificarlo dentro de un rango de 10 a 35. Cuando la similitud alcance el nivel establecido, la verificación es exitosa. Entre más alto sea el umbral más bajo es el error de cálculo y más alto el índice de rechazo, y viceversa.

• **Umbral 1: N HD* (Huella Digital):** Examina la similitud entre la huella de verificación actual y todas las plantillas de huellas almacenadas en el dispositivo. El valor preestablecido es 35, pero usted puede modificarlo dentro de un rango de 25 a 45. Cuando la similitud alcance el nivel establecido, la verificación es exitosa. Entre más alto sea el umbral más bajo es el error de cálculo y más alto el índice de rechazo, y viceversa.

Umbrales de verificación recomendados:

Tasa de rechazo por error	Tasa de error de cálculo	Umbral de Coincidencia	
		1:N	1:1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

6.4 Reinicio

Menú principal>> Sistema>> Reinicio

Nota: Después de reiniciar el dispositivo, la información de los usuarios y las configuraciones de la interfaz de control de acceso no serán eliminadas.

6.5 USB Actualización del Firmware

Por medio de esta función usted puede actualizar el Firmware del dispositivo, utilizando un archivo de actualización en una USB.
Inserte la USB en el puerto del dispositivo y haga clic en [Actualización USB].

Configuración del Sistema

Menú principal>>  Sistema>> Actualización USB.

Nota:

1). Si hace clic en la opción [Actualización USB] pero no hay una USB conectada, se mostrará en pantalla el mensaje "¡Error! Lectura de la USB falló" (Figura 2).

2). Si requiere del archivo de actualización, por favor contacte a nuestro equipo técnico más cercano. Bajo circunstancias normales, actualizar el equipo no es recomendado.

Personalizar

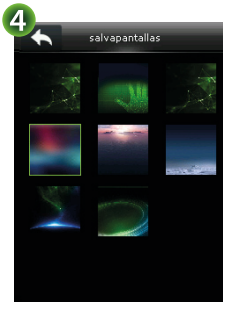
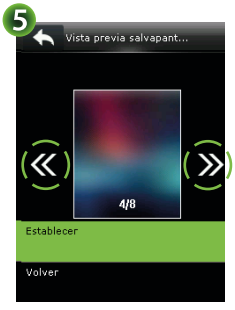
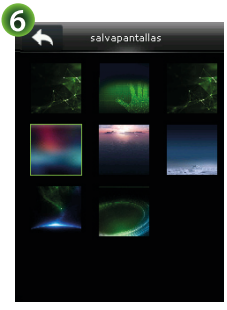
Menú principal>> Personalizar.

7.1 Interfaz de Usuario

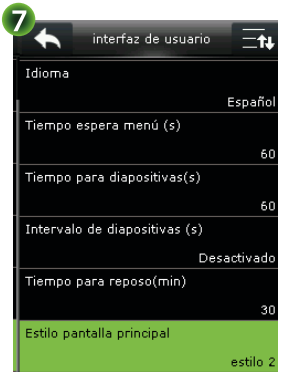
En la interfaz [Personalizar] haga clic en la opción [Interfaz de Usuario]. Haga clic en el icono para desplazarse hacia abajo del menú, y haga clic de nuevo en el icono para volver a la parte superior.

Personalizar

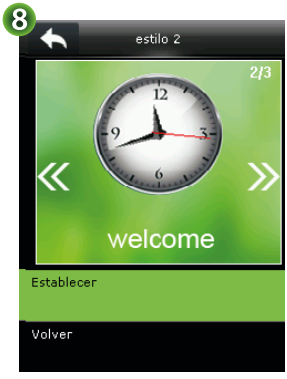
Fondo de Pantalla: Seleccione el fondo de escritorio de la pantalla principal. El dispositivo cuenta con varios estilos.

		
Menú principal I > Personalizar > Interfaz de Usuario > Papel tapiz: El dispositivo cuenta con 8 imágenes.	Haga clic en la imagen para pre visualizarla. Utilice los iconos y para consultar las demás imágenes. Haga clic en "Establecer" para seleccionar la imagen. Para salir sin hacer cambios, utilice la opción "Salir".	Haga clic en para guardar los cambios y volver a la interfaz anterior.

Idioma: Seleccionar el idioma del dispositivo.
Tiempo de Espera del Menú (S): El dispositivo vuelve automáticamente a la interfaz inicial si habiendo abierto el menú no se ha hecho ninguna operación dentro de X período de tiempo (el rango es de 60 a 99999 segundos). Esta función puede ser desactivada.
Tiempo de Espera para Diapositivas (s): La presentación es mostrada cuando no se estén realizando operaciones en la interfaz inicial. El rango de tiempo es de 3 a 999 segundos; esta función puede ser desactivada.
Intervalo de tiempo para Dispositivas (s): Este parámetro es utilizado para establecer el tiempo de duración de las diapositivas en pantalla. El rango de tiempo es de 0 a 999 segundos.
Tiempo para Reposo (m): Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Usted sacar al dispositivo del modo reposo presionando cualquier tecla. El rango de espera es de 1 a 999 minutos. Si esta función de encuentra en modo "Desactivado" el dispositivo no entrará nunca en estado de reposo.
Estilo de la Pantalla Principal: Seleccione el estilo de la pantalla de inicio.



Menú principal l > Personalizar > Interfaz de Usuario > Estilo de la pantalla de inicio



Utilice los iconos ⏪ y ⏩ para consultar los estilos. Haga clic en "Establecer" para seleccionar, para salir sin hacer cambios, utilice la opción "Salir".

7.2 Sonido

Menú principal l >> Personalizar >> Sonido.

Personalizar

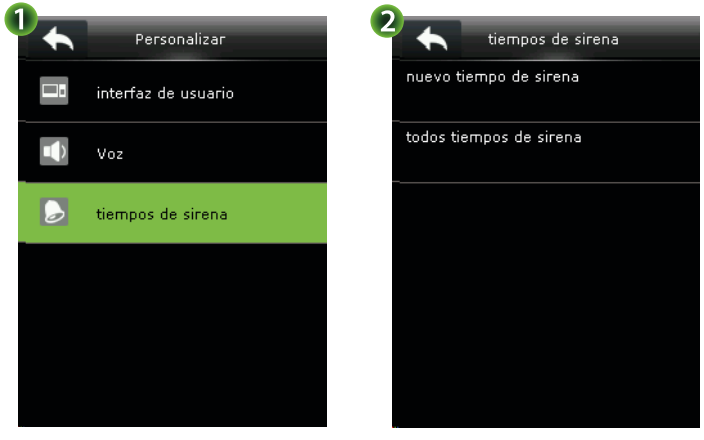
Voz Guía: Activar o desactivar los mensajes auditivos del dispositivo. Por defecto, esta función se encuentra encendida ON; para desactivarla haga clic en el icono de estado ON y este cambiará a OFF(desactivado).

Tono del Teclado: Activar o desactivar el sonido del teclado. Por defecto, esta función se encuentra encendida ; para desactivarla haga clic en el icono de estado y este cambiará a (desactivado).

Volumen: Con esta función puede ajustar el volumen de la voz guía y los sonidos. Por defecto, el valor está establecido en 70. Haga clic en [Volumen], utilice los iconos y para bajar y subir el volumen (Figura 4); luego, haga clic en [Confirmar/OK] para guardar los cambios y volver a la interfaz anterior.

7.3 Timbre

Muchas empresas necesitan un timbre para señalar la hora de inicio/fin de la jornada laboral. Algunos utilizan timbres manuales y otros electrónicos. Para ahorrar costos y brindar un mejor rendimiento, nosotros integramos las funciones de timbre en el dispositivo. Usted puede establecer la hora de timbre: cuando llegue la hora establecida, el dispositivo activará la señal del relevador y hará sonar el timbre elegido. El timbre sonará en el lapso de tiempo establecido por el usuario.



Menú principal >> Personalizar >> Timbre

7.3.1 Nuevo Timbre

Menú principal >> Personalizar >> Timbre >> Nuevo Timbre (Figura 4).

Estado del Timbre: Activar / Desactivar este timbre. Por defecto, esta función se encuentra desactivada OFF; para activarla haga clic en el icono de estado OFF y este cambiará a ON (activado).

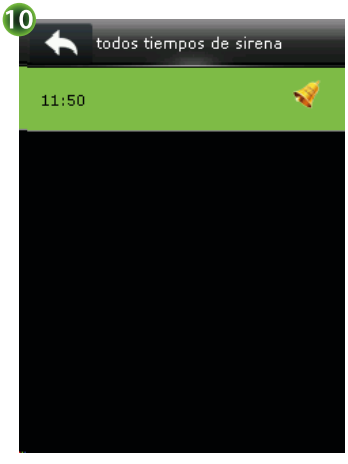
Nota: El timbre sonará sólo si la opción [Estado del Timbre] se encuentra activada.

Hora del Timbre: Establecer la hora en la que debe sonar el timbre. Haga clic en [Hora del timbre]; utilice los iconos ▲ y ▼ pasa aumentar/disminuir los números; haga clic en [Confirmar/OK] (Figura 5) para guardar los cambios y volver a la interfaz anterior.

Repetir: Especificar los días de la semana en los que debe sonar el timbre. Por defecto, la opción "Nunca "está seleccionada. En la lista (Figura 6), seleccione los días de la semana haciendo clic en ellos (al quedar seleccionados la casilla se muestra así ☑, para quitar la selección haga clic sobre ellos nuevamente). Para guardar los cambios y salir de la interfaz, haga clic en ↩.

Duración del Timbre: Especificar la duración del timbre. El rango es desde 1 a 999 segundos.

7.3.2 Todos los timbres



Menú principal l >> Personalizar >> Timbre >> Todos los Timbres.

En esta interfaz, usted puede visualizar todos los timbres establecidos. También tiene la opción de editarlos o eliminarlos.

Editar Timbre:
En la interfaz [Todos los Timbres] (Figura 10), haga clic en el timbre que desea editar; en la siguiente interfaz haga clic en la opción [Editar]. Establezca los cambios y utilice el icono para guardar los cambios y volver a la interfaz anterior.

Eliminar Timbre:
En la interfaz [Todos los Timbres] (Figura 10), haga clic en el timbre que desea eliminar; en la siguiente interfaz haga clic en la opción [Eliminar]. En el cuadro de diálogo emergente, confirme que desea eliminar ese timbre haciendo clic en la opción [Si]; después de esto el dispositivo vuelve automáticamente a la interfaz anterior.

Gestión de Datos

Menú principal>>  Gestión de Datos

8.1 Eliminar Datos

Menú principal>> Gestión de Datos >> Eliminar Datos.
Haga clic en el icono para desplazarse hacia abajo del menú, y haga clic de nuevo en el icono para volver a la parte superior.

Eliminar Registros de Acceso*: Eliminar todos los registros de acceso.

Eliminar Todos los Datos: Eliminar toda la información del personal; incluyendo imágenes de las venas, huellas digitales*, etc.

Eliminar Privilegio de Administrador: Cambiar todos los administradores a usuarios normales.

Eliminar Control de Acceso: Restaurar las configuraciones de control de acceso (Días festivos, privilegios, horarios) a los valores de fábrica. Los registros de acceso no serán eliminados.

Eliminar Fondo de Pantalla: Eliminar uno, varios o todos los fondos de pantalla.

Gestión de Datos

(1). Haga clic en [Eliminar Fondo de Pantalla].

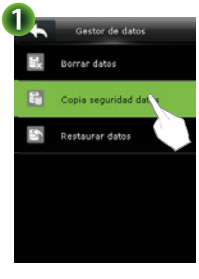
(2). En la interfaz [Eliminar Fondo de Pantalla], utilice los iconos y para visualizar los fondos de pantalla uno a uno, las opciones [Eliminar esta imagen] y [Eliminar todas las Imágenes] se mostrarán en cada caso (figura 5).

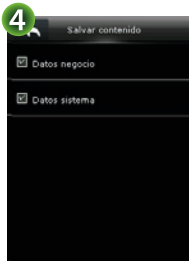
Eliminar Protectores de Pantalla: Elimine todas las imágenes cargadas desde la USB al terminal. (Para detalles sobre la carga de imágenes, por favor consulte el punto 10.2)

Eliminar Copia de Seguridad: Eliminar los datos pertenecientes a la copia de seguridad.

8.2 Copia de Seguridad

Menú principal>> Gestión de Datos >> Copia de Seguridad.





Copia de Seguridad al Dispositivo:

En la interfaz [Copia de Seguridad] (Figura 2), haga clic en [Copia de seguridad al dispositivo]; al hacer esto, ingresará a la interfaz mostrada en la Figura 3.

Configure los parámetros:

Contenido de la Copia: Figura 4; seleccione las opciones haciendo clic en ellas (al quedar seleccionados la casilla se muestra así ☑, para quitar la selección haga clic sobre ellos nuevamente). Para guardar los cambios y salir de la interfaz, haga clic en .

Gestión de Datos

Apuntes de Apoyo:

Haga clic en la pantalla (Figura 5) y se desplegará un teclado. Ingrese el texto y haga clic en OK (Figura 6) para guardar el teclado, después haga clic en Confirmar /OK (Figura 7) para guardar los cambios y volver a la interfaz "Copia de Seguridad al Dispositivo".

Iniciar Copia: Haga clic en esta opción para iniciar el proceso.

Copia de Seguridad a la USB
(1). Antes de dar clic en esta opción, por favor inserte una USB en el puerto del dispositivo y siga las instrucciones.
(2). Cuando se pasen los datos al PC, el sistema reemplazará la copia de seguridad anterior por la más reciente.

8.3 Restaurar Datos

Menú principal>> Gestión de Datos >>Restaurar Datos.

Gestión de Datos

Restaurar Datos desde el Dispositivo
(1). Haga clic en [Restaurar datos desde el dispositivo] (Figura 2).
(2). Haga clic en [Iniciar Restauración] y haga clic en [Si], Figura 3.
(3). Después de restaurar los datos (Figura 4) el dispositivo se reiniciará, haga clic en OK.

Restaurar Datos desde USB
En la interfaz [Restaurar Datos] elija la opción "Restaurar Datos desde USB", el procedimiento es similar al de "Restaurar Datos desde el Dispositivo".

Nota: Antes de elegir la opción "Restaurar los Datos desde la USB", por favor inserte una USB con los datos en el puerto del dispositivo.

Menú Principal >> Control de Acceso.

Para obtener acceso, el usuario registrado debe cumplir con las siguientes condiciones:

(1). La hora de acceso del usuario debe estar dentro del horario del personal o del horario del grupo.
(2). El grupo del usuario debe estar en la combinación de acceso (Cuando hay otros grupos en la mismo combinación de acceso, la verificación de los miembros de ese grupo también son requeridos para desbloquear la puerta)

En la configuración de fábrica, todos los usuarios nuevos son ubicados dentro del primer grupo con el horario y la combinación de acceso predeterminada como "1".

9.1 Opciones de Control de Acceso

En la interfaz de control de acceso, haga clic en "Opciones de Control de Acceso"; Utilice el icono para desplazarse hacia abajo del menú, y haga clic de nuevo en el icono para volver a la parte superior.

Control de Acceso

Establezca los parámetros de bloqueo y dispositivos relacionados.

Retraso de Bloqueo de la puerta(s): El período de tiempo de desbloqueo (Desde la apertura al cierre) después de que la cerradura eléctrica recibe la señal de apertura enviada desde el dispositivo. El rango es de 0 a 10 segundos.

Retraso de Sensor de Puerta (s): Cuando la puerta es abierta, el sensor de puerta revisará el estado de la puerta después de cierto tiempo; si el estado de la puerta es inconsistente con el modo establecido, se emitirá una alarma. El rango de tiempo es de 0 a 255 segundos.

Tipo de Sensor de Puerta: Incluye Ninguno Normalmente Abierto (NO) y Normalmente Cerrado. (NC) significa que el sensor no está en uso, "Normalmente Abierto" significa que la puerta es abierta cuando la electricidad está encendida, y "Normalmente Cerrado" significa que la puerta es cerrada cuando la electricidad está encendida.

Modo de Verificación: Usted puede seleccionar entre Contraseña/Venas, Sólo Tarjeta*, Contraseña, Venas, Contraseña & Venas, Tarjeta/Huella*, Sólo Huella*, Huella & Contraseña, Tarjeta &Contraseña*, Tarjeta & Huella, o Tarjeta & Huella & Contraseña*.

Horario de Puerta Habilitada: Establezca aquí el horario válido para que los usuarios abran la puerta.

Horario de Puerta NO: Establezca un horario para el modo Normalmente Abierto (NO) de la puerta.

Utilizar como Maestro: Mientras se realiza la configuración de dispositivos esclavos y maestros, usted puede establecer el estado maestro como "Entrada" o "Salida".

Salida: Un registro de verificación en el dispositivo maestro es un registro de Salida

Entrada: Un registro de verificación en el dispositivo maestro es un registro de Salida

Ajuste de Entrada Auxiliar*: Establezca el "Tiempo de Apertura de Puerta/ Auxiliar" o el "Ajuste de Salida Auxiliar" (Ninguno, Abrir Puerta, Activar Alarma, Abrir Puerta & Activar Alarma).

Alarma Altavoz: Cuando esta opción está activada, el altavoz del dispositivo emitirá una alarma en caso de que sea desmontado.

Resetear la Configuración de Acceso: Resetear los parámetros de Retraso de Bloqueo de la Puerta, Retraso del Sensor de Puerta, Tipo de Sensor de Puerta, Horario de puerta NO, y la configuración de la Entrada Auxiliar; excluyendo los registros de acceso (Los Datos de Acceso se eliminan desde la opción "Gestión de Datos").

Parámetros de Acceso	Valores de Fábrica
Retraso de Bloqueo de la Puerta	5s
Retraso del Sensor de Puerta	10s
Tipo de Sensor de Puerta	NO
Horario de Puerta NO	Ninguno
Tiempo de Apertura de Puerta (Auxiliar)	255s

Nota: Después de configurar el Horario de Puerta NO; por favor cierre bien la puerta, de otro modo puede que la alarma se active durante este período de tiempo.

9.2 Configuración de Horario

Un horario; es la mínima unidad de las configuraciones de control de acceso; hay disponibles 50 horario en el sistema. Cada horario consiste de 7 secciones (una semana) y 3 secciones de tiempo para días festivos. Cada sección de tiempo es el tiempo válido dentro de las 24 horas.

Usted puede establecer un máximo de 3 períodos de tiempo para cada sección de tiempo. La relación entre estos períodos de tiempo es "o". Cuando el tiempo de verificación cae en cualquiera de estos períodos de tiempo, la verificación es válida. El formato del período de tiempo es HH:MM - HH:MM en sistema de 24 horas con precisión de minutos.

En la interfaz de Control de Acceso, haga clic en "Configuración de Horarios" para ingresar a la interfaz "Horarios". Utilice el icono  para desplazarse hacia abajo del menú, y haga clic de nuevo en el icono para volver a la parte superior.

Control de Acceso

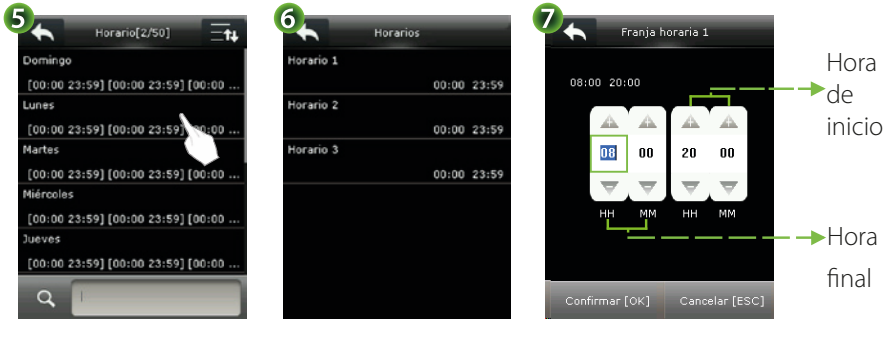
Editar Horario

Un administrador puede editar los horario.

(1). Haga clic en la casilla de búsqueda (figura 2).

(2). Ingrese un número de horario, haga clic en OK (Figura 3).

(3). En la lista de secciones de tiempo (Figura 4), haga clic en un día o sección de tiempo (Figura 5) para ingresar a la interfaz de periodos de tiempo (Figura 6) haga clic en uno de los tres e ingrese la hora de inicio y la hora final (Figura 7).



(4). Después de la configuración, haga clic en Confirmar (OK) para guardar los cambios y volver a la interfaz anterior.

Nota:

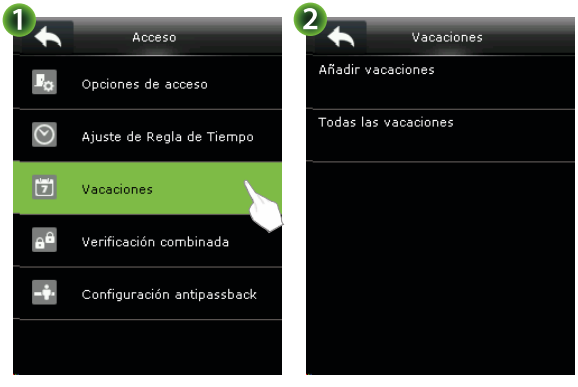
• Utilice los iconos ▲ y ▼ para aumentar/disminuir los dígitos (Figura 7).

• Cuando la Hora Final es más temprana que la Hora de Inicio (por ejemplo, 23:57~23:56) significa que cerrará todo el día. Cuando la Hora Final es después de la Hora de inicio (por ejemplo, 00:00~23:59) significa que este período de tiempo es válido.

• Por defecto, el horario 01 indica "funcionamiento todo el día".

9.3 Días Festivos

Agregar control de acceso a festivos y establecer los horarios. El dispositivo controlará el acceso en los festivos de acuerdo a la configuración establecida.



Menú Principal >> Control de Acceso>> Festivos.

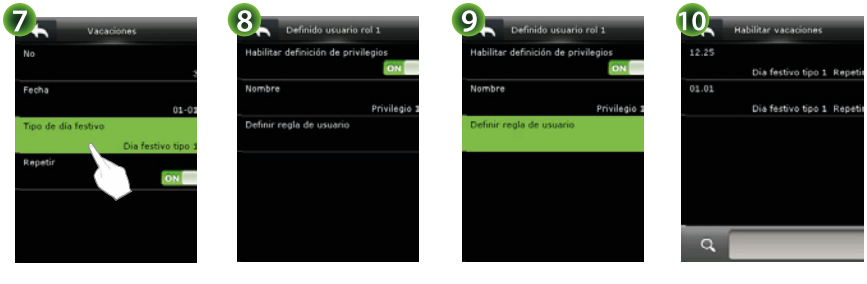
9.3.1 Agregar Día Festivo

Menú Principal >> Control de Acceso>> Día Festivos>> Agregar Día Festivo. (Figura 4)

Nº: El dispositivo asignará automáticamente un número al día festivo (Figura 5). Haga clic en OK para guardar los cambios y volver al menú anterior. Nota: el Rango de Nº de festivos es de 1 a 24.

Fecha: Establezca la fecha del día festivo. Utilice los iconos y para aumentar/disminuir el mes/día. Haga clic en OK (Figura 6) para guardar los cambios y volver al menú anterior.

Tipo de Día Festivo: Seleccione el tipo de día festivo y haga clic en (Figura 8) para guardar los cambios y volver al menú anterior.



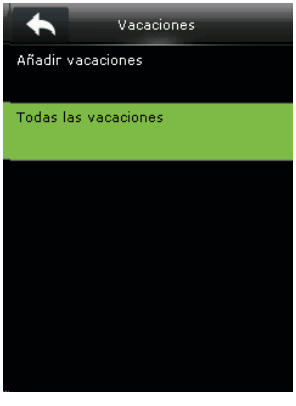
Repetir: El estado predeterminado es ON, para cambiar el estado haga clic sobre el icono ON y este pasará a OFF.

Para días festivos fijos cada año; como por ejemplo el día de año nuevo (1ro de enero), active ON la función "Repetir" para repetir este día festivo. Para festivos no fijos, como por ejemplo el día de la madre (el 2do domingo de mayo), el día puede cambiar; por favor desactive OFF la función "Repetir".

Por ejemplo, cuando la fecha de un festivo es establecida en Enero/01/2016 y el tipo de día festivo es el número 1, el control de acceso el 1ro de enero es llevado a cabo según con la configuración establecida en el día festivo Tipo 1 en lugar de las configuraciones de tiempo para los días viernes (el día viernes fue el 1ro de enero).

Después de realizar las configuraciones utilice el icono para guardar los cambios y volver a la interfaz anterior. Figura 9.

9.3.2 Todos los Días Festivos



Menú Principal >> Control de Acceso>> Día Festivo >> Todos los Días Festivos.

Haga clic en Todos los Días Festivos, en la siguiente interfaz (Figura 10) se mostrarán todos los días festivos establecidos, usted puede dar clic en ellos y editarlos o eliminarlos.

Nota: Los parámetros de edición son los mismos que cuando se agrega un nuevo día festivo. Para eliminar, de clic en la opción "Eliminar" y confirme la acción dando clic en "Si".

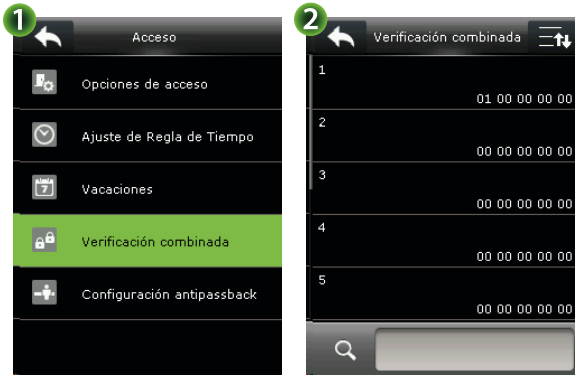
9.4 Configuración de Verificación Combinada

Nota:

(1). El Software Access 3.5no es requerido si el dispositivo es utilizado por primera vez. Usted puede establecer la verificación combinada en el dispositivo directamente.

(2). Después que la verificación combinada es establecida en el Software Access 3.5 y las configuraciones son enviadas al dispositivo, el dispositivo soportará sólo las configuraciones enviadas desde el Software Access 3.5 y la verificación combinada ya no podrá establecerse en el dispositivo.

Combine dos o más miembros para mejorar la verificación múltiple y la seguridad. En la verificación combinada, el rango de usuarios es de 1 ~ 5, los usuarios pueden pertenecer máximo a 5 grupos diferentes:



Menú Principal >> Control de Acceso>> Verificación Combinada.

Por defecto, el dispositivo soporta 10 combinaciones de desbloqueo. Los usuarios pueden modificar la configuración de la verificación combinada.

(1). En la interfaz de Verificación Combinada (Figura 2) haga clic en una combinación para modificarla.

(2). (Figura 3) Utilice los iconos y para aumentar/disminuir los números para establecer el ID de un grupo de usuarios. Haga clic en OK para guardar los cambios y volver al menú anterior.

Después de realizar la configuración exitosamente (figura 4), una puerta puede ser abierta sólo después que un usuario del grupo de usuarios 1 y un usuario del grupo de usuarios 2 pasen la verificación.

Nota:

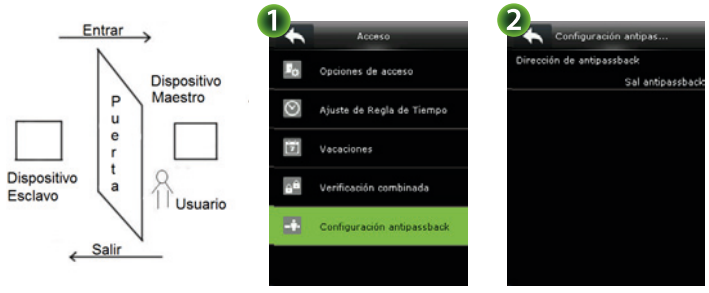
(1). Una combinación de desbloqueo soporta un máximo de 5 grupos de usuarios. Eso significa que en una combinación de desbloqueo, una puerta puede ser abierta sólo después de que un máximo de 5 usuarios pasen la verificación.

(2). Después que una combinación de desbloqueo (figura 5) es establecida, una puerta puede ser abierta sólo después que un usuario en el grupo de usuarios 2 y dos usuarios en el grupo de usuarios 1 pasen la verificación.

(3). Una combinación de desbloqueo es eliminada cuando los ID del grupo de usuarios sean establecidos en 0.

9.5 Anti-Passback

Para evitar que algunas personas sigan a los usuarios para ingresar por una puerta sin autorización, la función Anti-Passback puede ser establecida. Los registros de Check-in: Entrada deben coincidir con los de Check –Out: Salida para abrir la puerta. Esta función requiere que dos dispositivos trabajen juntos: Uno es instalado en el lado de adentro de la puerta (Dispositivo Maestro) y el otro es instalado en la parte de afuera (Dispositivo Esclavo). Los dos dispositivos se comunican por medio de señal Wiegand. El formato Wiegand y el tipo de salida (ID de usuario/Tarjeta) adoptado por los dispositivos Esclavo y Maestro deben coincidir.



Dirección del Anti-Passback (Figura 2)

No Anti-passback: Desactivar la función Anti-Passback. Significa que pasar la verificación del dispositivo esclavo o el maestro puede desbloquear la puerta. El estado de asistencia no es reservado.

Anti-Passback de Salida: Cuando un usuario hace Check-Out (Salida); sólo si el último registro es un Check-in (Entrada), el usuario puede hacer Check-Out (Salida) otra vez; de otra manera la alarma sonará. Sin embargo, el usuario puede hacer Check-in (Entrada) libremente.

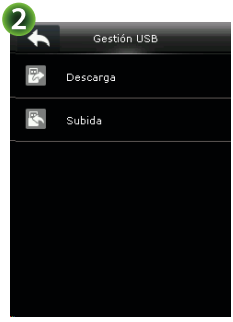
Anti-Passback de Entrada: Cuando un usuario hace Check-in (Entrada); sólo si el último registro es un Check-Out (Salida), el usuario puede hacer Check-in (Entrada) otra vez; de otra manera la alarma se disparará. Sin embargo, el usuario puede hacer Check-Out (Salida) libremente.

Anti-Passback de Entrada/Salida: Sólo si el último registro es un Check-Out (Salida) el usuario puede hacer Check in otra vez; y sólo si el último registro es un Check-in (Entrada) el usuario puede hacer Check-Out (Salida) otra vez; de otra manera la alarma de disparará.

USB

El dispositivo tiene la función de importar y exportar datos desde o a una USB. Datos como la información del usuario, plantillas de huella, imágenes de las venas y datos de verificación, entre otros.

Antes de cargar o descargar información desde o a una USB, inserte la USB en el puerto del dispositivo.



Menú Principal>> USB.

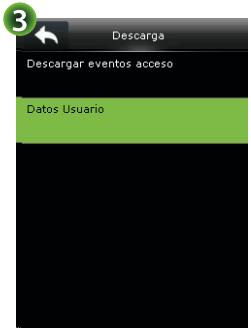
10.1 Exportar a la USB

Descargue los registros de control de acceso* y datos de usuario a una USB.

Descargar Registros de Acceso*: Almacene los registros de control de acceso en una USB.

Datos de Usuarios: Descargar toda la información de los usuarios e información de venas de los dedos a una USB.

Ejemplo:



Menú Principal>> USB>> Descargar>> Datos de Usuario. Haga clic en "Datos de Usuario" para iniciar la descarga.

Después de que el proceso termina el mensaje "Descarga Completa" es mostrado en pantalla (Figura 4).

Retire la USB y haga clic en el icono para volver a la interfaz anterior.

10.2 Importar Datos desde la USB

Cargue al dispositivo datos de usuario, protectores de pantalla y papel tapiz almacenados en una USB.

Menú Principal>> USB>> Cargar.

USB

Datos de Usuario: Cargar toda la información de los usuarios desde una USB al dispositivo.

Protector de Pantalla:

Cargar al dispositivo protectores de pantalla almacenados en una USB. Después que el dispositivo entre al modo de reposo los protectores de pantalla cargados se mostrarán en pantalla.

(1). Haga clic en "Protector de Pantalla" (Figura 6).

(2). Utilice los iconos y para visualizar uno a uno los protectores de pantalla y haga clic en "Cargar esta imagen" para cargar esa imagen al dispositivo. También puede dar clic en la opción "Cargar todas las imágenes" para cargar al dispositivo todas las imágenes que llenen los requerimientos.

(3). Después de la carga exitosa, el mensaje "Carga completa "es mostrado en pantalla. Haga clic en para volver al menú anterior.

Fondo de Pantalla:

Cargar al dispositivo los fondos de pantalla almacenados en una USB. Este proceso es igual al descrito en "Protector de Pantalla".

Nota:

•Antes de cargar los protectores de pantalla, ubique las imágenes en la carpeta "Advertise" (Anuncio) de la USB.

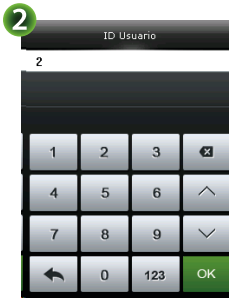
•Antes de cargar los fondos de escritorio, ubique las imágenes en la carpeta "Wallpaper" (fondo de pantalla) de la USB.

•Las imágenes deben estar en formato PNG, JPG o BMP; con un tamaño no mayor a 30KB.

•Los nombres de las imágenes no deben poseer más de 20 caracteres.

Buscar Registro de Asistencia

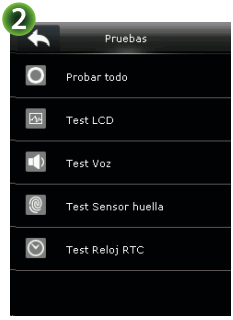
Los registros de asistencia de los empleados se guardarán en el dispositivo. Para poder consultarlos de una manera sencilla, la opción "Buscar Asistencia" está disponible en el menú principal.

		
Menú Principal>> Buscar Asistencia.	Ingrese el ID del usuario a consultar y haga clic en [OK].	Seleccione el lapso de tiempo que desea consultar y haga clic en [OK]. Los registros relacionados al usuario y al lapso de tiempo escogido se mostrarán en pantalla

Nota: Si el campo "ID de Usuario" es dejado en blanco, aparecerán en pantalla todos los empleados.

Pruebas

Las pruebas automaticas permiten al dispositivo comprobar el funcionamiento de varios módulos, incluyendo la pantalla, sonido, sensor* y el reloj.



Probar Todo: El dispositivo examinará automáticamente el LDC, el sonido, el sensor de huella*y el reloj. Durante la revisión presione la pantalla para continuar con el próximo o haga clic en para salir de la prueba.

Probar LCD: El terminal verificará los efectos de color de la pantalla mostrando imágenes en colores vivos, blanco y negro para comprobar si la pantalla está funcionando adecuadamente. Durante la revisión presione la pantalla para continuar con el próximo o haga clic en para salir de la prueba.

Probar Sonido: Esta función revisará si los archivos de voz están completos, y que la calidad del sonido sea la adecuada reproduciendo los archivos de sonido almacenados en el terminal. Durante la revisión presione la pantalla para continuar con el próximo o haga clic en para salir de la prueba.

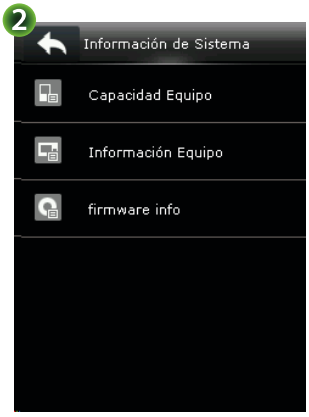
Probar Sensor de Huellas: El terminal examinará automáticamente si el sensor se encuentra funcionando con normalidad y revisa también que la calidad de las imágenes sea clara y apta. Cuando el usuario presente el dedo en el sensor, la imagen de la huella será mostrada en tiempo real. Haga clic en o toque la pantalla para salir de la prueba.

Probar Reloj: El terminal revisará el rendimiento del reloj por medio del cronómetro. Haga clic en o toque la pantalla para salir de la prueba.

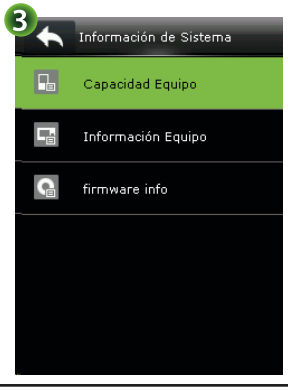
Información del Sistema

Con este parámetro usted puede verificar el estado de almacenamiento, la información del Firmware y la versión del dispositivo.

Menú Principal>> Información del Sistema.



Capacidad del Dispositivo: El número de usuarios inscritos, administradores, contraseñas, huellas, venas, tarjetas* y los registros de control de acceso almacenados en el dispositivo.

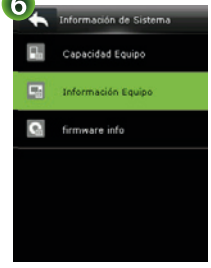


Información del Sistema

Información del Dispositivo: Nombre del dispositivo, número serial, dirección MAC, algoritmo de huella digital, algoritmo de venas del dedo*, información de la plataforma, versión MCU*, fecha de fabricación y fabricante.

Utilice el icono para desplazarse hacia abajo del menú y haga clic nuevamente para volver a la parte superior.

6

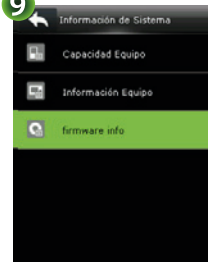


7

8

Información del Firmware: Versión del firmware, Bio service, Servicio Pull y Dev service.

9



10

Anexos

Anexo 1: Ingreso de Texto

Anexo 2: USB

El dispositivo sirve como USB Host, que puede ser conectado a una USB para intercambio de datos.

Los dispositivos tradicionales de reconocimiento de venas soportan transmisión de datos por medio de RS485 o Ethernet. Cuando la cantidad de datos es grande, la transmisión es lenta y tarda mucho tiempo debido a las condiciones físicas. La velocidad de transmisión por medio de USB es mucho más rápida que cualquier modo de transmisión tradicional.

Inserte la USB en el puerto del dispositivo para la descarga de datos (Utilice la opción USB del menú principal); después inserte la USB al PC para cargar los datos. El dispositivo soporta transmisión de información del usuario y plantillas de venas de los dedos entre dos dispositivos, eliminando el tedioso proceso de conexión mediante cables.

Anexo 3: Wiegand, Introducción

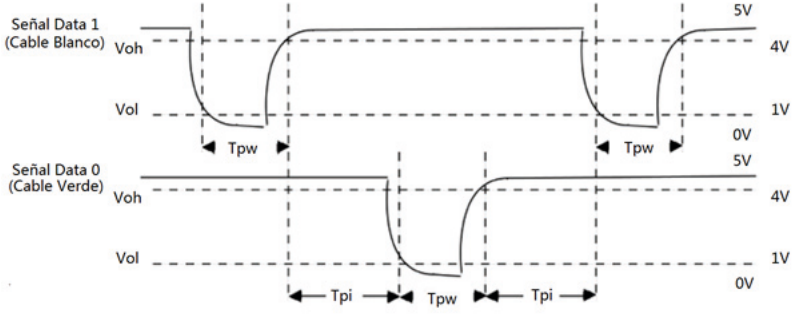
El protocolo Wiegand fue diseñado para conseguir una tecnología que permitiera transmitir datos entre dos dispositivos alejados entre sí; como por ejemplo, un lector y un controlador de accesos. Es utilizado mayormente en la industria de la seguridad, control de acceso, gestión de asistencia y otros sectores relacionados.

Señal Digital

La figura 1 muestra el diagrama de secuencia del lector de tarjetas enviando la señal digital en bits al controlador. El Wiegand en este diagrama sigue el protocolo estándar de control de acceso SIA (Asociación de la Industria de la Seguridad, por sus siglas en inglés), que tiene como objetivo un lector de tarjetas Wiegand de 26 bits (Con una duración de pulso de 20 µs. a 100 µs y un salto de frecuencia de 200 µs a 20 ms). Las señales Data 1 y data 0 son de alto nivel (Superior que VOH), hasta que el lector de tarjetas está listo para enviar un flujo de datos. El lector de tarjetas envía un pulso asíncrono bajo (menor que VOL), transmitiendo flujo de datos vía Data 1 y Data 0 a la caja de control de acceso (Como en la onda de sierra en la figura1). Los pulsos de Data 1 y Data 0 no se superponen o sincronizan. La figura 1 muestran el ancho de pulso mínimo y máximo (Pulso consecutivo) y el tiempo de salto de frecuencia (El tiempo entre dos pulsos) permitidos por la serie de terminales de control de acceso de huella digital.

Símbolo	Definición	Valores normales del lector de tarjetas
Tpw	Ancho de Pulso	100 µs
Tpi	Intervalo de Pulso	1ms

Figura 1: Diagrama de Secuencia



Anexo 3.1 Wiegand26, Introducción.

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

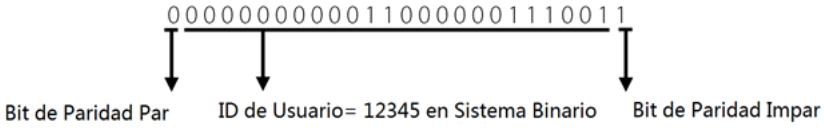
1	2 25	26
Bit de Paridad Par	ID de Usuario/ Número de Tarjeta	Bit de Paridad Impar

La siguiente tabla describe los campos:

Bit de Paridad Par	El bit de paridad par es determinado por los bit 2~13. Si ahí hay un número par de 1's, el bit de paridad par es 0. Si hay un número impar de 1's, el bit de paridad par es 1.
ID de Usuario/ Número de tarjeta (Bit 2 a través de bit 25	El ID de usuario/Número de tarjeta (Código de tarjeta, 0-16777215) y el bit 2 indica el bit más significativo (MSB)
Bit de Paridad Impar	El bit de paridad impar es determinado por los bit 14~25. Si ahí hay un número par de 1's, el bit de paridad impar es 1. Si hay número impar de 1's, el bit de paridad impar es 0.

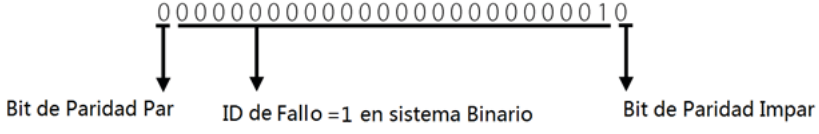
Ejemplo: Un usuario con el ID 12345 tiene el número de tarjeta 0013378512 y el ID de fallo es establecido en 1.

(1). Cuando el contenido de salida es establecido para ID de Usuario, la salida wiegand del sistema es la siguiente después que el usuario pasa la verificación:



(2). Cuando el contenido de salida es establecido para número de tarjeta, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:

(3). Cuando la verificación falla, la salida Wiegand del sistema es la siguiente:



Nota: Cuando el contenido de salida esté por encima del rango predeterminado del formato Wiegand, los últimos bit son reservados y los primeros bits son descartados. Por ejemplo, si un ID de usuario es 888 888 888 que es 110 100 111 110 110 101 111 000 111 000 en sistema binario, los últimos 24 bits (111 110 110 101 111 000 111 000) son emitidos y los primeros 6 bits (110 100) son descartados porque el formato Wiegand 26 sólo soporta 24 bits de salida de contenido.

Anexo 3.2 Wiegand34, Introducción.

Composición del formato Wiegand 34: 2 bit de paridad y 31 bit de salida de contenido (Id de Usuario o número de tarjeta). Los 32 bits en código binario pueden indicar 4 294 967 296 (0-4 294 297 295) diferentes valores.

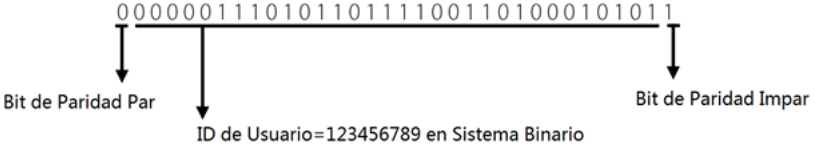
1	2 33	34
Bit de Paridad Par	ID de Usuario/ Número de Tarjeta	Bit de Paridad Impar

La siguiente tabla describe los campos:

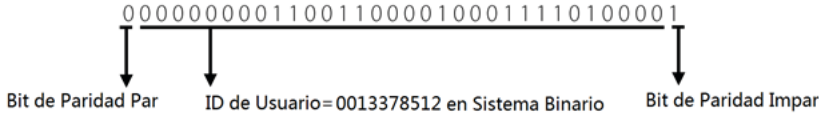
Bit de Paridad Par	El bit de paridad par es determinado por los bit 2~17. Si ahí hay un número par de 1's, el bit de paridad par es 0. Si hay un número impar de 1's, el bit de paridad par es 1.
D de Usuario/ Número de tarjeta (Bit 2 a través de bit 25	El ID de usuario/Número de tarjeta (Código de tarjeta, 0-4 294 967 295) y el bit 2 indica el bit más significativo (MSB)
Bit de Paridad Impar	El bit de paridad impar es determinado por los bit 18~33. Si ahí hay un número par de 1's, el bit de paridad impar es 1. Si hay número impar de 1's, el bit de paridad impar es 0.

Ejemplo: Un usuario con el ID 123456789 tiene el número de tarjeta 0013378512 y el ID de fallo es establecido como 1.

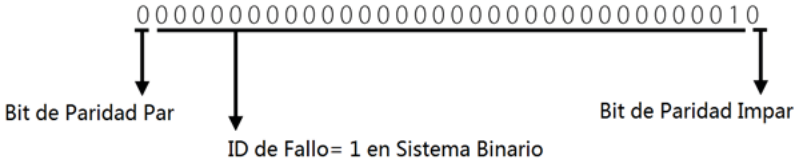
(1). Cuando el contenido de salida es establecido para ID de usuario, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:



(2). Cuando el contenido de salida es establecido para número de tarjeta, la salida Wiegand del sistema es la siguiente después que el usuario pasa la verificación:

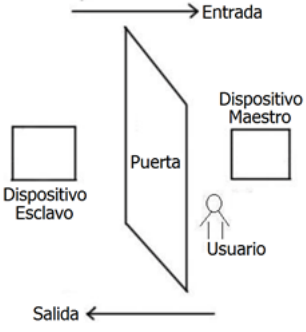


(3). Cuando la verificación falla, la salida Wiegand del sistema es la siguiente:



Anexo 4 Configuración del Anti-Passback

Para evitar que algunas personas sigan a los usuarios para ingresar por una puerta sin autorización, la función Anti-Passback puede ser establecida. Los registros de Check-in (Entrada) deben coincidir con los de Check –Out (Salida) para abrir la puerta. Esta función requiere que dos dispositivos trabajen juntos: Uno es instalado en el lado de adentro de la puerta (Dispositivo Maestro) y el otro es instalado en la parte de afuera (Dispositivo Esclavo). Los dos dispositivos se comunican por medio de señal Wiegand. El formato Wiegand y el tipo de salida (ID de usuario/Tarjeta) adoptado por los dispositivos Esclavo y Maestro deben coincidir.



Anexos

[Principio de Funcionamiento]

El dispositivo maestro soporta la señal de entrada Wiegand y el dispositivo esclavo soporta la señal de salida Wiegand. Después que el puerto de salida wiegand del dispositivo esclavo es conectado al puerto de entrada wiegand del dispositivo maestro, la señal wiegand emitida por el dispositivo esclavo no puede contener el ID del dispositivo y los números enviados al maestro deben existir en el dispositivo maestro. Esto significa que la información del usuario en el dispositivo esclavo, soportando la función Anti-Passback debe corresponder a la información del usuario en el dispositivo maestro.

[Descripción de las Funciones]

El dispositivo detecta el Anti-Passback basado en el último registro Check-in (Entrada)/ Check –out (Salida) de los usuarios. El registro Check-in (Entrada) debe coincidir con el último registro Check –out (Salida). El dispositivo soporta Anti-Passback de Salida, Anti-Passback de Entrada y Anti-Passback de Entrada/Salida.

Cuando el **Anti-Passback de Salida** es establecido para un usuario en el dispositivo maestro, el último registro del usuario debe ser un Check-in (Entrada) si el usuario necesita hacer Check-in (Entrada)/out libremente. De lo contrario, el usuario no puede hacer el Check –out (Salida). y la petición de Check –out (Salida). es rechazada por el Anti-Passback. Por ejemplo; si el primer reciente registro del usuario es un Check-in (Entrada), el segundo registro puede ser un Check-in (Entrada) o un Check –out (Salida). pero el tercer registro debe ser basado en el segundo, asegurando que el Check-in (Entrada) coincida con el Check-out.

Nota: Si el usuario no tiene registro, sólo puede hacer Check-in (Entrada).

Cuando el **Anti-Passback de Entrada** es establecido para un usuario en el dispositivo maestro, el último registro del usuario debe ser un Check –out (Salida). si el usuario necesita hacer Check-in (Entrada)/Check –out (Salida). libremente. De lo contrario, el usuario no puede hacer Check-in (Entrada) y la petición de los usuarios es rechazada debido al Anti-Passback.

Nota: Si un usuario no tiene registro, sólo puede hacer Check –out (Salida)..

Cuando el Anti-Passback de Entrada/Salida es establecido en el dispositivo maestro, si el último registro del usuario es un Check –out (Salida). el siguiente registro debe ser un Check-in (Entrada) y viceversa; para que el usuario pueda realizar el próximo Check-in (Entrada)/Check –out (Salida). sin problemas. Esto significa, que los registros de Check-in (Entrada) y Check-out Check –out (Salida). deben coincidir siempre.

[Descripción de la Operación]

(1). Selección del Modelo

Dispositivo Maestro: Dispositivos que soportan la función Wiegand de entrada, excepto el lector F10.

Dispositivo Esclavo: Dispositivos que soportan la función de salida Wiegand.

(2). Configuraciones del Menú

Dirección del Anti-Passback

Las opciones de dirección del Anti-Passback incluyen Anti-Passback de Entrada/Salida, Anti-Passback de Salida, Anti-Passback de Entrada y No Anti-Passback.

- Anti-Passback de Salida: Sólo si el último registro es un Check-in (Entrada) el usuario puede realizar el Check-out (Salida) de nuevo.
- Anti-Passback de Entrada: Sólo si el último registro es un Check-out (Salida) el usuario puede hacer Check-in (Entrada) de nuevo.

Estado del Dispositivo

Las opciones del estado del dispositivo incluyen: Ninguno, Salida y Entrada.

- Ninguno: Desactivar la función Anti-Passback.
- Salida: Todos los registros en el dispositivo son registros Check-out (Salida).

- Entrada: Todos los registros en el dispositivo, son registros Check-in.

(3). Modificar el Formato de Salida Wiegand del Dispositivo

Cuando dos dispositivos se comunican entre sí, sólo las señales Wiegand que no contentan el ID del Dispositivo son aceptables. En el dispositivo usted puede utilizar la opción Menú Principal>> configuración Wiegand o acceda al Software y elija las opciones Configuración Básica >> Gestión de Dispositivos >> Wiegand y establezca los parámetros Definir Formato para Wiegand 26-bits o Wiegand26 Sin ID de Dispositivo.

(4). Registro de Usuario

Los ID de los usuarios deben existir en ambos dispositivos (esclavo y maestro) y deben coincidir. Por lo tanto, los usuarios deben ser registrados en los dos dispositivos.

(5). Descripción del Cableado

Los dispositivos esclavo y maestro se comunican entre sí por medio de Wiegand y el cableado es el siguiente:

Dispositivo Maestro	Dispositivo Esclavo
IWD0	WD0
IWD1	WD1
GND	GND

Privacidad

Apreciado consumidor:

Gracias por elegir las soluciones diseñadas y fabricadas por el equipo ZK. Como proveedor líder en el mercado de productos y soluciones biométricas, nos esforzamos por cumplir los estatutos relacionados con los derechos humanos & privacidad de cada país. Por esta razón consignamos en este documento la siguiente información:

1.Todos dispositivos de reconocimiento de huella digital ZKTeco para uso civil, sólo recogen puntos característicos de las huellas digitales, no imágenes como tal. Gracias a esto no se suscitan problemáticas que involucren o violen la privacidad de los usuarios.

2. Los puntos característicos de las huellas digitales recolectadas por nuestros dispositivos no pueden ser utilizadas para reconstruir la imagen original de la huella.

3. ZKTeco como proveedor de los equipos, no se hace legalmente responsable directa o indirectamente por ninguna consecuencia generada debido al uso de nuestros productos.

4. Por cualquier inconveniente que involucre los derechos humanos o la privacidad de los mismos cuando se utilicen nuestros productos, por favor contacte directamente a su empleador directamente.

Nuestros otros equipos de huella digital de uso policíaco u herramientas de desarrollo, pueden proporcionar la función de recolección de las imágenes originales de las huellas digitales de los ciudadanos. Cuando considere que este tipo de recolección de huellas infringe su privacidad, por favor contacte al gobierno local o al proveedor final. ZKTeco como el fabricante original de los equipos, no se hace legalmente responsable de ninguna infracción generada por esta razón.

Nota: Las siguientes son regulaciones ligadas a las leyes de la República popular de China acerca de la libertad personal:

1.Detención, reclusión o búsqueda ilegal de ciudadanos de la República Popular de China es una violación a la intimidad de la persona, y está prohibida.

2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.

Privacidad

3. El hogar de los ciudadanos de la República Popular de China es inviolable.

4. La libertad y privacidad correspondiente a los ciudadanos de la República Popular de China están protegidos por la ley.

Recalcamos que los biométricos, como avanzada tecnología de reconocimiento, será aplicada en diversos sectores; incluyendo el comercio electrónico, sistemas bancarios, aseguradoras y cuestiones legales. Cada año alrededor del mundo, una gran cantidad de personas sufren inconvenientes causados por la inseguridad de las contraseñas.

En la actualidad, el reconocimiento de huellas digitales es utilizado para una protección adecuada de la identidad de las personas brindando un ambiente de alta seguridad en todo tipo de empresa.

Descripción Medio Ambiental

El EFUP (Periodo de Uso Amigable con Medio Ambiente, por sus siglas en inglés) marcado en este producto, se refiere al periodo de seguridad en el cual el producto es utilizado bajo las condiciones establecidas en las instrucciones del mismo, sin riesgo de fuga de sustancias nocivas o perjudiciales.

El EFUP de este producto no cubre las partes consumibles que necesiten ser reemplazadas regularmente, como por ejemplo, las baterías. El EFUP de las baterías es de 5 años.

Nombre y concentración de sustancias o elementos nocivos						
Nombre de las piezas	Sustancias o elementos nocivos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Resistencia	X	O	O	O	O	O
Condensado	X	O	O	O	O	O
Inductor	X	O	O	O	O	O
Diodo	X	O	O	O	O	O
Componentes ESD	X	O	O	O	O	O
Buzzer	X	O	O	O	O	O
Adaptador	X	O	O	O	O	O
Tornillos	O	O	O	X	O	O

O: Indica que esta sustancia tóxica o nociva está presente en todos los materiales homogéneos de esta pieza, por debajo de los límites requeridos en SJ/T11363-2006.

X: Indica que esta sustancia tóxica o nociva está presente en al menos uno de los materiales homogéneos de esta pieza, por encima de los límites requeridos en SJ/T11363-2006.

Nota: El 80% de las partes de este producto están fabricadas con materiales ecológicos. Las sustancias o elementos nocivos contenidos, no pueden ser reemplazados por materiales ecológicos por razones técnicas o restricciones económicas.

Green Label

www.zkteco.com

www.zktecolatinoamerica.com