

# Manual de Usuario

## Serie InBioPC

Fecha: Agosto 2025

Versión del documento: 1.1

Español

Gracias por elegir nuestro producto. Lea atentamente las instrucciones antes de la operación. Siga estas instrucciones para asegurarse de que el producto funcione correctamente. Las imágenes que se muestran en este manual son solo para fines ilustrativos.



Para obtener más detalles, visite el sitio web de nuestra empresa [www.zkteco.com](http://www.zkteco.com).

## Derechos de autor © 2025 ZKTECO CO., LTD. Todos los derechos reservados.

Sin el consentimiento previo por escrito de ZKTeco, ninguna parte de este manual puede copiarse o enviarse de ninguna manera o forma. Todas las partes de este manual pertenecen a ZKTeco y sus subsidiarias (en adelante, la "Compañía" o "ZKTeco").

### Marca

**ZKTeco** es una marca registrada de ZKTeco. Otras marcas comerciales involucradas en este manual son propiedad de sus respectivos dueños.

### Renuncia

Este manual contiene información sobre la operación y el mantenimiento de los equipos ZKTeco. Los derechos de autor de todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco pertenecen y son propiedad de ZKTeco. El contenido del presente documento no debe ser utilizado ni compartido por el receptor con ningún tercero sin el permiso expreso por escrito de ZKTeco.

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

Es un requisito previo esencial para la operación y el mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido una capacitación completa en la operación y el mantenimiento de la máquina / unidad / equipo. Además, es esencial para el funcionamiento seguro de la máquina/unidad/equipo que el personal haya leído, entendido y seguido las instrucciones de seguridad contenidas en el manual.

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

ZKTeco no ofrece ninguna garantía o representación con respecto a la integridad de la información contenida en este manual o cualquiera de las enmiendas realizadas al mismo. ZKTeco no extiende la garantía de ningún tipo, incluida, entre otras, cualquier garantía de diseño, comerciabilidad o idoneidad para un propósito particular .

ZKTeco no asume responsabilidad por ningún error u omisión en la información o los documentos a los que se hace referencia o están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos al usar la información.

ZKTeco en ningún caso será responsable ante el usuario o cualquier tercero por daños incidentales, consecuentes, indirectos, especiales o ejemplares, incluidos, entre otros, la pérdida de negocios, la pérdida de ganancias, la interrupción del negocio, la pérdida de información comercial o cualquier

pérdida pecuniaria, que surja de, en relación con, o relacionados con el uso de la información contenida o referenciada por este manual, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

Este manual y la información contenida en él pueden incluir inexactitudes técnicas, de otro tipo o errores tipográficos. ZKTeco cambia periódicamente la información aquí contenida que se incorporará en nuevas adiciones/enmiendas al manual. ZKTeco se reserva el derecho de agregar, eliminar, enmendar o modificar la información contenida en el manual de vez en cuando en forma de circulares, cartas, notas, etc. para un mejor funcionamiento y seguridad de la máquina / unidad / equipo. Dichas adiciones o enmiendas están destinadas a mejorar / mejorar las operaciones de la máquina / unidad / equipo y dichas enmiendas no darán derecho a reclamar ninguna compensación o daños bajo ninguna circunstancia.

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

El producto se actualizará de vez en cuando sin previo aviso. Los últimos procedimientos operativos y los documentos relevantes están disponibles en <http://www.zkteco.com>

Si hay algún problema relacionado con el producto, contáctenos.

## Sede de ZKTeco

**Dirección** Parque Industrial ZKTeco, No. 32,  
Industrial Road, Ciudad de Tangxia,  
Dongguan, China.

**Teléfono** +86 769 - 82109991

**Fax** +86 755 - 89602394

Para consultas relacionadas con el negocio, escribanos a:

[sales@zkteco.com](mailto:sales@zkteco.com). Para saber más sobre nuestras sucursales

globales, visite [www.zkteco.com](http://www.zkteco.com).

## Acerca de la empresa

ZKTeco es uno de los mayores fabricantes mundiales de lectores RFID y biométricos (huellas dactilares, faciales, venas dactilares). Las ofertas de productos incluyen lectores y paneles de control de acceso, cámaras de reconocimiento facial de corto y largo alcance, controladores de acceso de ascensores/pisos, torniquetes, controladores de puerta de reconocimiento de matrículas (LPR) y productos de consumo, incluidas las cerraduras de puertas con lectores faciales y de huellas dactilares que funcionan con baterías. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En la planta de fabricación certificada por ISO9001 de última generación de 700,000 pies cuadrados de ZKTeco, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística / envío, todo bajo un mismo techo.

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

## Acerca del manual

Este manual presenta las operaciones del **InBioPC400/InBioPC800**.

Todas las figuras que se muestran son solo para fines ilustrativos. Las cifras de este manual pueden no ser exactamente consistentes con los productos reales.

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






## Convenciones de documentos

Las convenciones utilizadas en este manual se enumeran a continuación:

### Convenciones de GUI

Para software	
Convención	Descripción
<b>Fuente en negrita</b>	Se utiliza para identificar nombres de interfaz de software, por ejemplo, <b>OK</b> , <b>Confirm</b> , <b>Cancel</b> .
>	Los menús de varios niveles están separados por estos corchetes. Por ejemplo, Archivo > Crear > Carpeta.
Para dispositivo	
Convención	Descripción
< >	Nombres de botones o teclas para dispositivos. Por ejemplo, presione <OK>.
[ ]	Los nombres de ventana, los elementos de menú, la tabla de datos y los nombres de campo están entre corchetes. Por ejemplo, abra la ventana [Nuevo usuario].
/	Los menús de varios niveles están separados por barras diagonales de reenvío. Por ejemplo, [Archivo/Crear/Carpeta].

### Símbolo

Convención	Descripción
	Esto representa una nota a la que hay que prestar más atención.
	La información general que ayuda a realizar las operaciones más rápido.
	La información que es significativa.
	Cuidado para evitar peligros o errores.
	La declaración o evento que advierte de algo o que sirve como ejemplo de advertencia.

# Tabla de contenidos

<b>1</b>	<b>SEGURIDAD INSTRUCCIONES.....</b>	<b>7</b>
1.1	Importante Notas.....	7
1.2	Instalación Precauciones .....	8
<b>2</b>	<b>VISIÓN GENERAL .....</b>	<b>10</b>
2.1	Funciones.....	11
2.2	Técnico Características técnicas .....	12
<b>3</b>	<b>DESCRIPCIÓN DEL TERMINAL DEL CONTROLADOR .....</b>	<b>13</b>
3.1	Descripción de los LED en el panel del controlador .....	13
3.2	Apariencia y componentes del sistema .....	15
3.3	Instrucciones de selección de cables .....	17
<b>4</b>	<b>DE10.....</b>	<b>18</b>
4.1	Instrucciones de selección de cables .....	20
<b>5</b>	<b>INSTALACIÓN .....</b>	<b>21</b>
<b>6</b>	<b>CABLEADO DEL CONTROLADOR DE ACCESO.....</b>	<b>23</b>
6.1	Conexión de la fuente de alimentación.....	23
6.2	Conectar una computadora .....	23
6.3	Conexión de DE10 .....	24
6.4	Conexión de salidas auxiliares .....	24
6.5	Conexión de entradas auxiliares .....	24
6.6	Conexión de la alarma .....	25
6.7	Conectando el fuego .....	26
<b>7</b>	<b>DE10 ALAMBRADO .....</b>	<b>27</b>
7.1	Conexión del lector.....	27
7.1.1	Conexión del lector Wiegand .....	27
7.1.2	Conexión del lector RS485 .....	27
7.2	Conexión del sensor .....	28
7.3	Conexión del botón de salida .....	28
7.4	Conexión de la entrada auxiliar.....	29
7.5	Conexión de la salida auxiliar .....	30
7.6	Conexión del interruptor antisabotaje .....	30
7.7	Conexión de la cerradura .....	30
<b>8</b>	<b>SISTEMA DE CONTROL DE ACCESO.....</b>	<b>32</b>
<b>9</b>	<b>INICIAR SESIÓN SERVIDOR WEB.....</b>	<b>33</b>
9.1	PC.....	33
9.2	Teléfono .....	37
<b>10</b>	<b>CONEXIÓN A ZKBIO CVSECURITY .....</b>	<b>38</b>

10.1	Agregar el dispositivo .....	38
10.2	Puerta .....	40
10.3	Lector .....	40
10.4	Auxiliar Entrada .....	41
10.5	Auxiliar Salida.....	42
10.6	Evento Tipo .....	43
10.7	Monitoreo en tiempo real.....	44
10.8	Alarma Monitorización .....	44
10.9	Engranar .....	45
10.10	Ligamiento .....	45
10.11	Anti-Passback.....	46
<b>APÉNDICE 1</b>	.....	<b>47</b>
	Privacidad Política .....	47
	Operación ecológica .....	50



# **1 Instrucciones de seguridad**

## **1.1 Notas importantes**

1. Antes de operar el dispositivo, lea y siga estrictamente todas las instrucciones de seguridad y operación. Mantenga las instrucciones en buenas condiciones para futuras referencias.
2. Utilice los accesorios recomendados por el fabricante o entregados junto con el producto. No se recomienda el uso de ningún otro producto relacionado como sistema de alarma o monitoreo (cámaras, detectores infrarrojos, detectores de humo, etc.). El sistema de alarma o monitoreo debe cumplir con los estándares locales aplicables de prevención de incendios y seguridad.
3. No coloque este dispositivo sobre ninguna mesa inestable, soporte de trípode, terminal o base para evitar que el dispositivo se caiga y se dañe, y cause lesiones personales graves de manera indeseable. Por lo tanto, es importante instalar el dispositivo según las instrucciones del fabricante.
4. Todos los dispositivos periféricos deben estar conectados a tierra.
5. No se pueden exponer cables de conexión externos. Todas las conexiones y los extremos de los cables inactivos deben envolverse con cintas aislantes para evitar que el contacto accidental con los cables expuestos dañe el dispositivo.
6. No intente realizar reparaciones no autorizadas del dispositivo. Es probable que el desmontaje o desprendimiento provoque descargas eléctricas u otros problemas físicos. Todas las reparaciones deben ser realizadas por personal de reparación calificado.
7. En cualquiera de los siguientes casos, desconecte primero la fuente de alimentación del dispositivo y notifique al personal de reparación calificado para su reparación:
  - El cable de alimentación o el conector están dañados;
  - Se filtra líquido o cualquier objeto cae en el dispositivo;
  - El dispositivo se ha mojado o expuesto a la intemperie (lluvia, nieve, etc.);
  - Si el dispositivo no puede funcionar normalmente, aunque funcione según las instrucciones;
  - El dispositivo se cae o su rendimiento cambia obviamente.
8. Si es necesario sustituir un componente, el personal de reparación debe utilizar únicamente los sustitutos especificados por el fabricante.
9. Después de reparar el dispositivo, el personal de reparación debe realizar una inspección de seguridad para garantizar que el dispositivo funcione normalmente.
10. Opere el dispositivo solo con el tipo de fuente de alimentación indicado en la etiqueta. Póngase en contacto con el operador si tiene dudas sobre el tipo de fuente de alimentación.



**La violación de cualquiera de las siguientes precauciones puede provocar lesiones personales o mal funcionamiento del dispositivo. No asumimos ninguna responsabilidad por cualquier daño causado por un mal manejo que esté más allá del uso normal definido en este manual del producto.**

- Antes de la instalación, apague el circuito externo (que suministra energía al sistema).
- Antes de conectar el dispositivo a la fuente de alimentación, asegúrese de que el voltaje de salida esté dentro del rango especificado.
- Nunca conecte el producto a la corriente antes de completar la instalación.

## 1.2 Precauciones de instalación

1. La selección del cable de red debe ser de material de cobre libre de oxígeno de cable de red de categoría 5 por encima de las especificaciones, diámetro nominal del núcleo de 0,5 mm. 100 metros de resistencia de un solo cable es inferior a 10 ohmios. Trate de elegir un cable de red de mayor especificación (como material de cobre libre de oxígeno de categoría 6), reserve suficiente margen para cumplir con los requisitos de carga máxima.
2. Todo el cableado debe tener manguitos, tubería de PVC opcional y tubería galvanizada, para evitar que los ratones muerdan la línea causada por fallas. Aunque el controlador tiene un buen diseño antiestático, a prueba de rayos y fugas, asegúrese de que el chasis del controlador y la conexión a tierra de CA sean perfectos, y que la conexión a tierra de CA esté realmente conectada a tierra.
3. Se recomienda no enchufar y desenchufar los terminales de conexión con frecuencia cuando el sistema está energizado. Asegúrese de desenchufar los terminales de conexión antes de comenzar cualquier trabajo de soldadura relevante.
4. No desconecte ni reemplace ningún chip del panel de control sin permiso porque una operación no profesional puede dañar el panel de control.
5. Se recomienda no conectar ningún otro dispositivo auxiliar sin permiso. Todas las operaciones no rutinarias deben confirmarse con nuestros ingenieros con anticipación.
6. Un panel de control no debe compartir una toma de corriente con ningún otro dispositivo de gran corriente.
7. Es preferible instalar lectores de tarjetas y botones a una altura de 55 pulgadas a 59 pulgadas (1,4 m a 1,5 m) sobre el suelo, sujeto a un ajuste adecuado de acuerdo con la práctica habitual de los clientes.
8. Se recomienda instalar el dispositivo en un lugar fácil de mantener, como una sala de servidores o un pozo débil.
9. Se recomienda encarecidamente que la parte expuesta de cualquier terminal de conexión no tenga más de 0,16 pulgadas (4 mm). Se pueden utilizar herramientas de sujeción profesionales para evitar cortocircuitos o fallas de comunicación resultantes del contacto accidental con cables expuestos excesivos.

10. Si necesita mantener un registro de los eventos de control de acceso, exporte periódicamente los datos desde el controlador.
11. Preparación de contramedidas contra fallas de energía inesperadas, como seleccionar la fuente de alimentación con UPS.
12. Para evitar que la fuerza electromotriz autoinducida generada por la cerradura eléctrica en el momento del encendido y apagado afecte al sistema de control de acceso, es necesario conectar un diodo en paralelo con la cerradura eléctrica (utilice el diodo FR107 suministrado con el sistema) para liberar la fuerza electromotriz autoinducida generada en el momento del encendido y apagado de la cerradura eléctrica durante el cableado del sistema de control de acceso en la aplicación en sitio.
13. Se recomienda utilizar la fuente de alimentación suministrada con el sistema como fuente de alimentación del panel de control.
14. En un lugar con fuertes interferencias magnéticas, se recomiendan tuberías de acero galvanizado o cables blindados, y se requiere una conexión a tierra adecuada.



## 2 Visión general

El controlador principal InBioPC es el pináculo de la tecnología de control de acceso, ya que ofrece una integración perfecta con las unidades de puerta DE-10 y admite hasta 4/8 puntos de acceso. Diseñado para la comunicación TCP/IP de alta velocidad, garantiza una transferencia de datos eficiente y fiable. El servidor web integrado, accesible a través de Wi-Fi, simplifica la configuración del sistema, proporcionando una facilidad de uso sin igual. Compatible con los estándares de alimentación a través de Ethernet (PoE IEEE802.3 y PSE@30W), el InBioPC puede alimentar hasta 4/8 unidades de puerta DE-10, lo que ofrece rendimiento y comodidad.

Este controlador avanzado cuenta con un conjunto de sofisticadas funciones de control de acceso y admite la generación dinámica de códigos QR a través de las aplicaciones móviles ZKBio CVSecurity, lo que mejora la seguridad y la experiencia del usuario. Con soporte para InBioPC ofrece métodos de autenticación versátiles para satisfacer diversas necesidades de seguridad. Su compatibilidad con el protocolo push ZKTeco AC garantiza una comunicación fluida con el software ZKBio CVSecurity.

Operando dentro de un amplio rango de entrada de voltaje de CA 100V ~ 240V, el InBioPC está diseñado para su implementación global. Incorpora métodos de cifrado de datos de alta seguridad, incluidos HTTP / HTTPS, SSH, AES256 y TLS 2.0, salvaguardando la información confidencial. Compatible con lectores Wiegand (formatos: W26 / W34 / W66) y lectores de tarjetas RS485 (protocolo: ZKTeco RS-485), proporciona opciones de conectividad flexibles.

Además, el InBioPC está diseñado en un tamaño de rack de servidor estándar de 1U, lo que garantiza la compatibilidad con las instalaciones de rack de servidores estándar. Esto lo convierte en una opción ideal para las organizaciones que buscan implementar una solución de control de acceso robusta, escalable y segura.



InBioPC-400



InBioPC-800

## 2.1 Funciones

- Se integra perfectamente con las unidades de puerta DE-10, admitiendo hasta 4/8 puntos de acceso.
- Admite comunicación TCP/IP de alta velocidad para una transferencia de datos eficiente.
- Un servidor web integrado está disponible para la configuración del sistema y se puede acceder a él a través de Wi-Fi.
- Cumple con los estándares IEEE 802.3 en PoE y PSE@30W para alimentar hasta 4/8 unidades de puerta DE-10.
- Equipado con funciones avanzadas de control de acceso para mayor seguridad.
- Admite la generación dinámica de códigos QR con las aplicaciones móviles ZKBio CVSecurity.
- Admite múltiples opciones de credenciales, incluidos biometría, RFID y contraseña.
- Compatible con el protocolo de empuje A&C.
- Funciona con un amplio rango de entrada de voltaje de CA 100V ~ 240V.
- Admite métodos de cifrado de datos de alta seguridad como HTTP / HTTPS, SSH, AES256 y TLS 2.0.
- Admite lectores Wiegand (formatos: W26 / W34 / W66) y lectores de tarjetas RS485 (protocolo: ZKTeco RS- 485)
- Diseñado en tamaño de rack de servidor estándar de 1U para ser compatible con la instalación estándar de rack de servidor.

## 2.2 Especificaciones técnicas

Menú	Descripción
<b>Voltaje de Entrada</b>	CA 110V/240V, 50/60Hz
<b>Número de Puertas</b>	InBioPC-400: 4 puertas InBioPC-800: 8 puertas
<b>Comunicación</b>	TCP/IP, Wi-Fi
<b>Puertos</b>	Interfaz de entrada de fuego *1 Interfaz de salida de alarma *1 Interfaz de entrada auxiliar *1 Interfaz de salida auxiliar *1 Botón de reinicio *1 USB *1 Interfaz Ethernet * 5 (LAN * 1, 4 POE) - InBioPC-400 Interfaz Ethernet * 9 (LAN * 1, 8 POE) - InBioPC-800
<b>Capacidad de Almacenamiento</b>	Capacidad de usuarios: 40,000 Capacidad de huellas dactilares: 4,000 Capacidad de tarjeta: 40,000 Capacidad de registros: 200,000
<b>Software</b>	ZKBio CVSecurity 6.3.0_R o superior
<b>LED</b>	Soportado
<b>Temperatura de funcionamiento</b>	De 0 °C a 45 °C
<b>Temperaturas de almacenamiento</b>	De -40 °C a 70 °C
<b>Humedad de funcionamiento</b>	Del 20% al 80%
<b>Ruido</b>	<60dB

**Dimensión (mm)**

484 mm \* 180 mm \* 44 mm (L\*W\*H)

### 3 Descripción del terminal del controlador

#### 3.1 Descripción de los LED en el panel del controlador

Cuando el controlador de la serie InBioPC está encendido, en condiciones normales, el indicador POWER (rojo) siempre está encendido, el indicador RUN (verde) parpadea (lo que indica un sistema normal) y ninguna de las otras luces está encendida. Sin embargo, en los siguientes casos:



Menú	Color	Descripción
<b>POWER</b>	Rojo	Luz roja siempre encendida (fuente de alimentación normal) Luz roja apagada (fuente de alimentación anormal)
<b>RUN</b>	Verde	La luz verde parpadea lentamente (sistema normal) La luz verde parpadea rápidamente (actualización en curso) Luz verde apagada (muerto)
<b>LAN</b>	Verde	Luz verde siempre encendida (sin interacción de datos) Luz verde parpadeando (con interacción de datos) Luz verde apagada (conexión de red anormal)

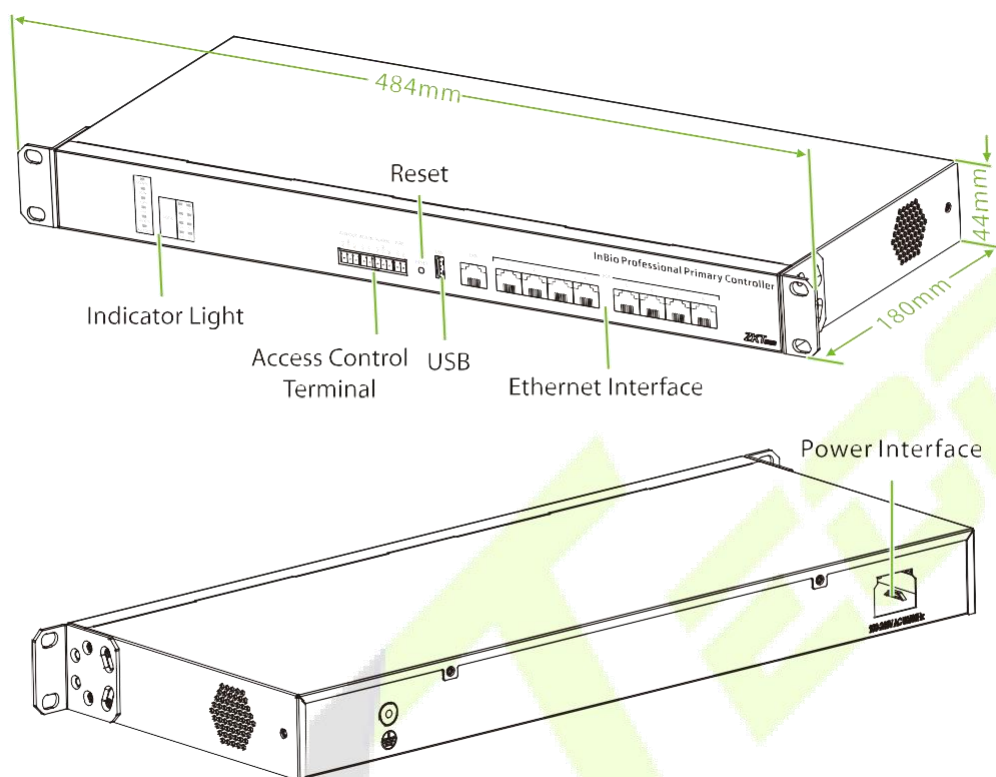
<b>FIRE</b>	Rojo	Luz roja intermitente (con acceso a protección contra incendios y está recibiendo una señal de cortocircuito)
		Luz roja apagada (tiene acceso a la protección contra incendios, pero no está recibiendo señal de cortocircuito)
<b>AUX IN</b>	Rojo	Luz roja parpadeante (hay acceso a la entrada auxiliar y está recibiendo una señal)
		Luz roja apagada (entrada auxiliar accedida pero no se está recibiendo señal)
<b>AUX OUT</b>	Rojo	Luz roja parpadeante (hay acceso a la salida auxiliar y hay señal de salida)
		La luz roja está apagada (la salida auxiliar está conectada, pero no se está recibiendo señal)

Los indicadores para los terminales de control de acceso son los siguientes:







Menú	Color	Descripción
<b>PUERTA</b>	Verde	Luz verde siempre encendida (estado en línea del sensor de puerta apagado / sin sensor de puerta)
		Luz verde parpadeando (estado en línea del sensor de la puerta abierto)
		Luz verde apagada (estado fuera de línea)

## 3.2 Apariencia y componentes del sistema




### Terminal de control de acceso:


No.	Descripción
<p>AUX OUT</p> <p>NO COM NC</p> 	<p>Salida auxiliar, se puede conectar a una alarma o timbre, etc.</p> <p>El voltaje de conmutación máximo del contacto es de 24 V CC, la corriente de conmutación máxima es de 1 A.</p>
<p>AUX IN</p> <p>+ - +</p> 	<p>Entrada auxiliar, se puede conectar a un detector de detección infrarroja del cuerpo humano, alarma de incendio o detector de humo, etc.</p> <p>Voltaje máximo de entrada 12VDC.</p>

<p>ALARMA</p> 	<p>Salida de alarma para conexión de alarma</p> <p>El voltaje de conmutación máximo del contacto es de 24 V CC, la corriente de conmutación máxima es de 1 A.</p>
<p>FUEGO</p> 	<p>Entrada de fuego, botón de disparo externo, activar el botón de disparo, todas las puertas se abren normalmente</p> <p>Voltaje máximo de entrada 12VDC.</p>

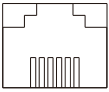
### Restablecimiento:

No.	Descripción
<p>RESET</p> 	<p>Use un pasador de recogida para empujar el dispositivo largo:</p> <ul style="list-style-type: none"> <li>● <math>0 &lt; \text{Actualización de firmware} \leq 5s</math> (Inserte la unidad flash USB con el firmware antes de pinchar el dispositivo con el pin de captación durante mucho tiempo)</li> <li>● <math>5s &lt; \text{Reboot} \leq 10s</math></li> <li>● <math>10s &lt; \text{Restaurar la configuración de fábrica}</math></li> </ul>

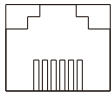
### USB:

No.	Descripción
	<p>Admite la conexión de una unidad flash USB para actualizar el firmware.</p>

### Interfaz Ethernet:

No.	Descripción
<p>LAN</p> 	<p>Conecte un enrutador para la comunicación de red.</p>

POE 1.....8

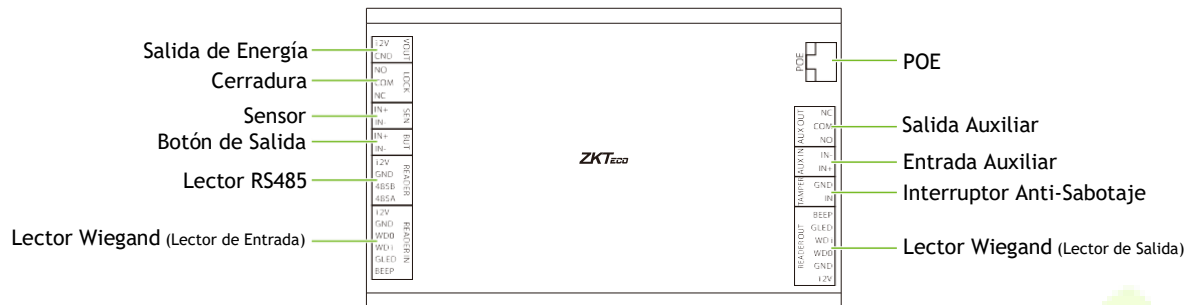







4 interfaces POE (InBioPC-400), 8 interfaces POE (InBioPC-800), a través de esta interfaz de red directamente a la fuente de alimentación del DE10 y la transmisión de datos.

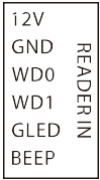
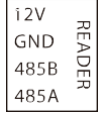
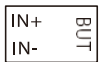


### 3.3 Instrucciones de selección de cables

Nombre	Características técnicas	Distancia máxima
<b>Cable de red</b>	La selección del cable de red debe ser un material de cobre libre de oxígeno de cable de red de categoría 5 por encima de las especificaciones, la resistencia de 100 metros de un solo cable es inferior a 10 ohmios. Trate de elegir una especificación más alta de cable de red (como material de cobre libre de oxígeno de categoría 6), reserve suficiente margen para cumplir con los requisitos de carga máxima.	100 metros

## 4 DE10



Terminal	Descripción
	<p>Interfaces con el controlador de acceso de identificación inteligente de la serie InBioPC.</p> <p>Compatible con el estándar IEEE 802.3at, DE10 recomendó una corriente de salida total inferior a 1,5 A a cargas externas, incluida la salida VOUT, la salida de alimentación del lector 485, la salida de alimentación del lector Wiegand, la salida de bloqueo eléctrico, la salida auxiliar, etc.</p>
	<p>Conéctese a la alarma o al timbre, etc.</p> <p>El voltaje de conmutación máximo del contacto es de 24 VCD, la corriente de conmutación máxima es de 1 A.</p>
	<p>Conecte el detector de sensor infrarrojo del cuerpo humano o el detector de humo, etc.</p> <p>Voltaje de entrada máximo: 12VCD</p>
	<p>Notificación oportuna para detener el desmontaje ilegal del dispositivo.</p> <p>Voltaje máximo de entrada: 12VCD</p>
	<p>Voltaje de salida máximo 12VCD, corriente de salida máxima 0.5A, voltaje de entrada máximo 12VCD</p>

	<p><b>Lector Wiegand (Lector de Entrada)</b></p>	<p>Voltaje de salida máximo: 12VCD Corriente de salida máxima: 0.5A Voltaje de entrada máximo: 12VCD</p>
	<p><b>Lector RS485</b></p>	<p>Voltaje de salida máximo: 12VCD Corriente de salida máxima: 0.5A Voltaje de entrada máximo: 6VCD</p>
	<p><b>Botón de Salida</b></p>	<p>Conexión del botón de salida de la puerta Voltaje de entrada máximo: 12VCD</p>
	<p><b>Sensor</b></p>	<p>Sensor de puerta de conexión Voltaje de entrada máximo: 12VCD</p>
	<p><b>Cerradura</b></p>	<p>Cerradura de puerta de conexión Tensión máxima de conmutación de los contactos: 30VCD Corriente máxima de conmutación: 5A</p>
	<p><b>Salida de Energía</b></p>	<p>Salida de alimentación: 12VCD desde DE10 (conectado a la serie InBioPC directamente a través de POE) Voltaje de salida máximo: 12VCD Corriente de salida máxima: 1A</p>

## 4.1 Instrucciones de selección de cables

Nombre	Características técnicas	Distancia máxima
<b>Wiegand</b>	Adopte un cable blindado de comunicación de 6 núcleos (RVVP 6 * 0.5 mm <sup>2</sup> ) (generalmente de 6 núcleos, 8 núcleos, 10 núcleos, los usuarios pueden elegir según la necesidad del puerto), para reducir la interferencia durante la transmisión	20 m
<b>Cerradura eléctrica</b>	El cable de 4 núcleos (RVV 4 * 0,75 mm <sup>2</sup> , alimentación de 2 núcleos, imán de puerta de 2 núcleos) se utiliza para minimizar el impacto en otros componentes durante el funcionamiento de la cerradura eléctrica	20 m
<b>Botón de salida</b>	Uso de cable de 2 o 4 hilos (RVV 2 * 0,5 mm <sup>2</sup> )	20 m
<b>Lector RS485</b>	Se utiliza un cable de comunicación de 4 núcleos (RVVSP 2 * 2 * 0,5 mm <sup>2</sup> )	20 m con fuente de alimentación del controlador
<b>Cable de red</b>	La selección del cable de red debe ser de material de cobre libre de oxígeno de cable de red de categoría 5 por encima de las especificaciones, diámetro nominal del núcleo de 0,5 mm. 100 metros de resistencia de un solo cable son menos de 10 ohmios. Trate de elegir un cable de red de mayor especificación (como material de cobre libre de oxígeno de categoría 6), reserve suficiente margen para cumplir con los requisitos de carga máxima	100 metros

## 5 Instalación

### ● Instalación en rack

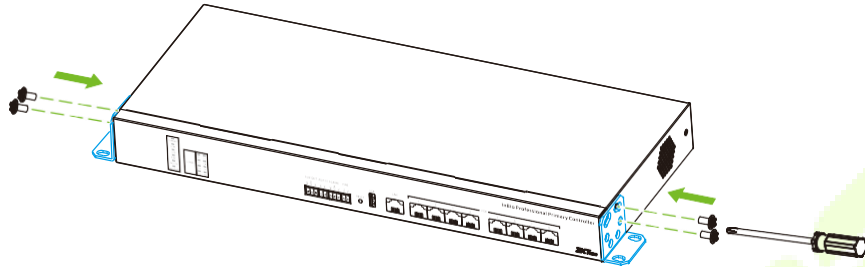
1. Asegure las placas laterales al dispositivo como se muestra en la figura a continuación.
2. Coloque el dispositivo en el rack y asegúrelo con tornillos.



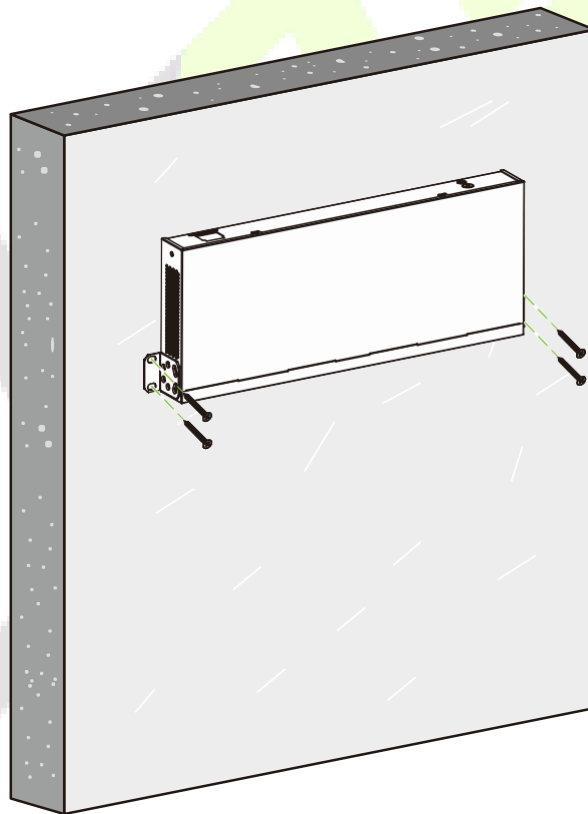
- **Montaje en pared**

1. Asegure las placas laterales al dispositivo como se muestra en la figura a continuación.
2. Asegure el dispositivo a la pared con tornillos.

1



2



## 6 Cableado del controlador de acceso

### 6.1 Conexión de la fuente de alimentación

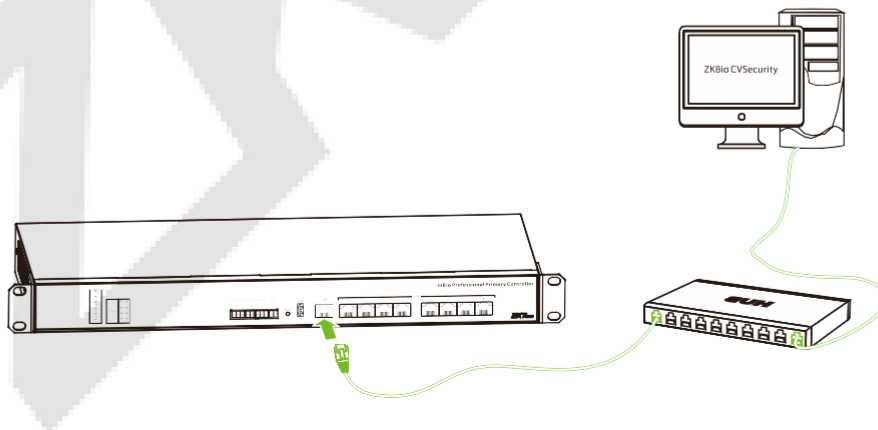
Utilice la fuente de alimentación configurada para el controlador de la serie InBioPC para suministrar energía desde la fuente de alimentación suministrada de 100-240 V, AC50/60 Hz.



**Nota:** Antes de conectar la fuente de alimentación, asegúrese de que la tierra del chasis del controlador esté bien conectado y que la tierra de CA esté realmente conectada a tierra.

### 6.2 Conectar una computadora

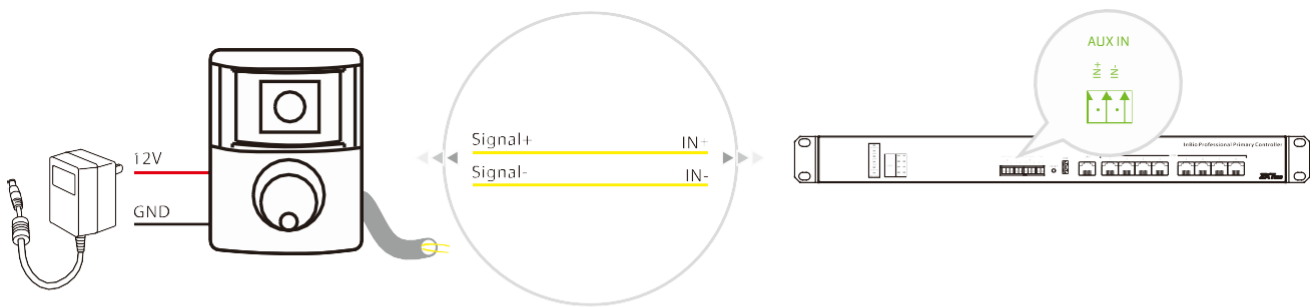
Conecte el controlador de la serie InBioPC al software para PC a través de un cable Ethernet. El cableado se muestra a continuación:



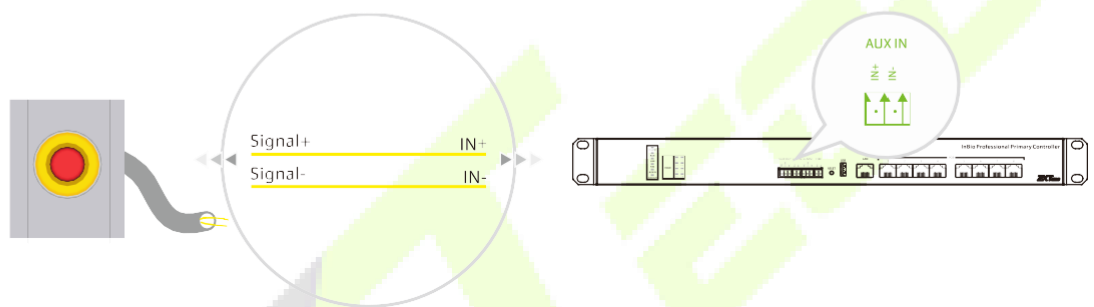
**Nota:** La dirección IP predeterminada de la NIC principal es **192.168.1.201**.



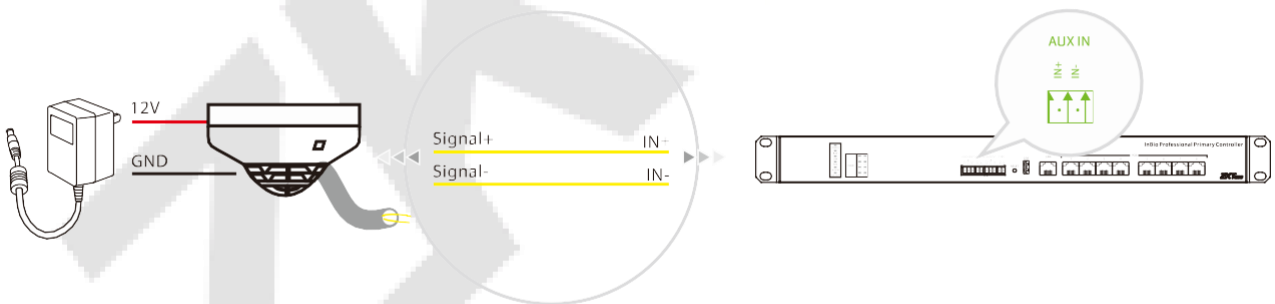
- **Detector de sensor infrarrojo del cuerpo humano**



- **Fuego**

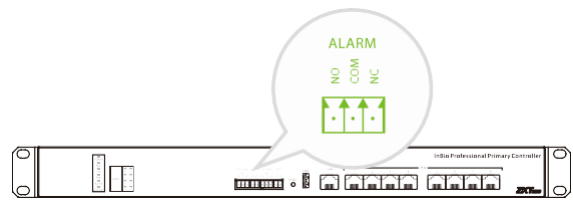
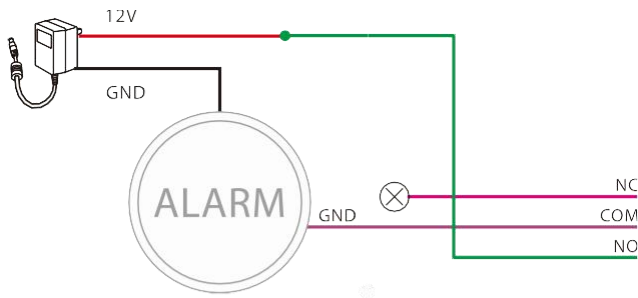


- **Detector de humo**



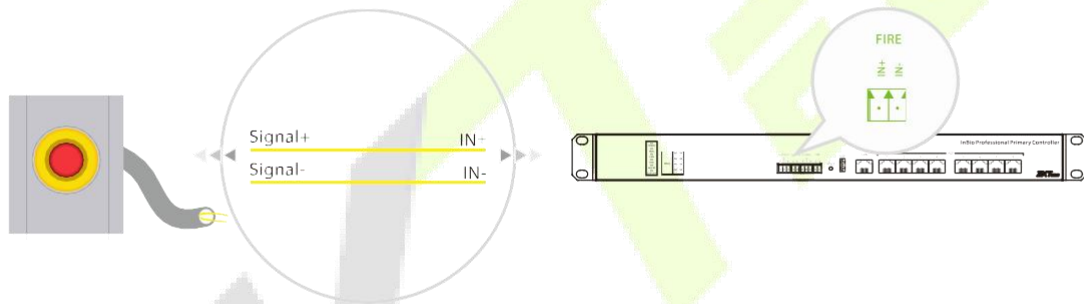
## 6.6 Conexión de la alarma

La alarma suena cuando se reciben señales como alarmas de incendio o robos.



## 6.7 Conectando el fuego

Cuando la interfaz de entrada de protección contra incendios está en cortocircuito, todas las puertas de la unidad entran automáticamente en el estado normalmente abierto, la alarma y la función de enlace global (deben estar activadas). Cuando el equipo se reinicia, no afecta el funcionamiento normal de la interfaz de extinción de incendios.

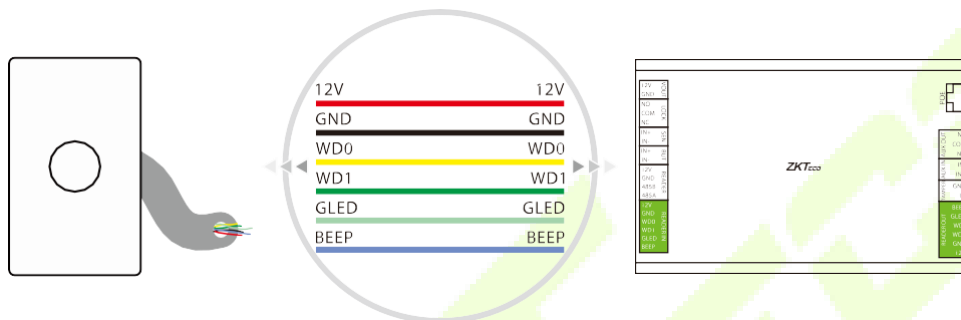


## 7 Cableado DE10

### 7.1 Conexión del lector

#### 7.1.1 Conexión del lector Wiegand

Tomando como ejemplo el lector ProID10B, después de que la serie InBioPC se conecte correctamente al DE10, conecte la interfaz Wiegand entre el DE10 y el ProID10B.

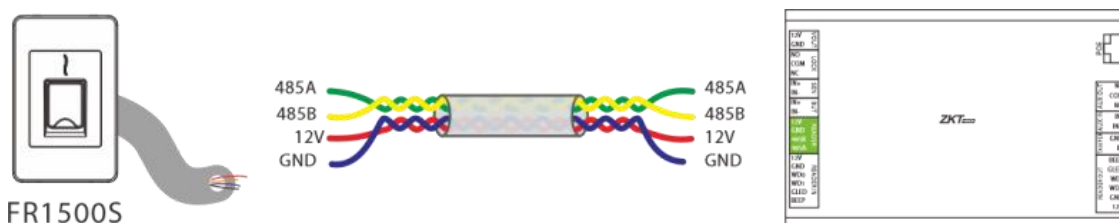


#### **Nota:**

1. Un DE10 tiene dos interfaces de lector Wiegand, se pueden conectar hasta 2 lectores Wiegand y se puede configurar una puerta bidireccional de una sola puerta.
2. El lector debe instalarse a unos 1,4 m del suelo y a 30 ~ 50 mm del borde de la puerta.

#### 7.1.2 Conexión del lector RS485

1. Se deben utilizar cables blindados de par trenzado, que son reconocidos internacionalmente. El tipo recomendado de cable de par trenzado blindado es RVVSP4 \* 0.5. El uso de cable de par trenzado blindado ayuda a reducir y eliminar la capacitancia distribuida entre las dos líneas de comunicación 485, así como la interferencia de modo común generada alrededor de las líneas de comunicación.
2. Las líneas de datos 485A y 485B deben estar trenzadas, DE10 GND, 485A, 485B se conectaron al lector RS485 GND, 485A, 485B. El cableado debe ser un cable de par trenzado multifilar blindado. Multifilar para el respaldo en caso de trozarse; el blindaje es para depuración cuando surge una situación especial; trenzado debido a la comunicación 485 que utiliza el principio de comunicación en modo diferencial, trenzado anti-interferencia de lo mejor.

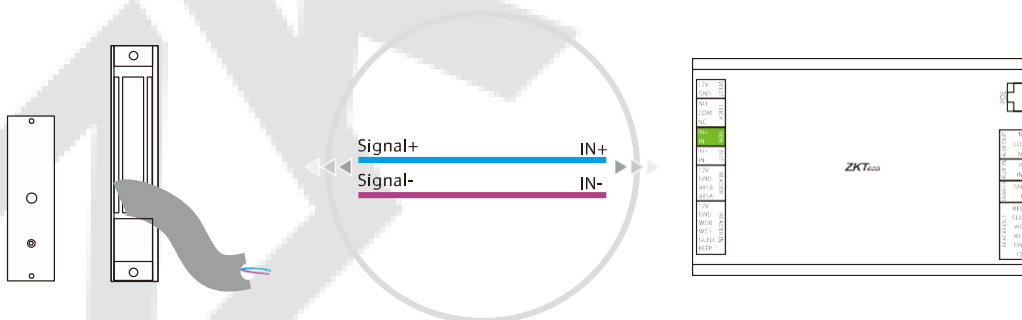


### Nota:

1. Un DE10 tiene una interfaz de lector RS485 y se pueden conectar hasta 2 lectores RS485, los códigos de dirección RS485 deben ser 1 y 2.
2. El lector debe instalarse a unos 1,4 m del suelo y a 30 ~ 50 mm del marco del borde de la puerta.
3. Cuando DE10 no está conectado al puerto POE del controlador que está configurado como modo maestro-esclavo o DE10 está en estado predeterminado de fábrica sin conexión previa al controlador, la validación de cualquier tarjeta, contraseña, huella digital o código QR en lectores conectados externamente desbloqueará con éxito la cerradura de la puerta durante 5 segundos, no se guardarán registros de acceso. (El modo de puerto POE del controlador se puede configurar en el servidor web)

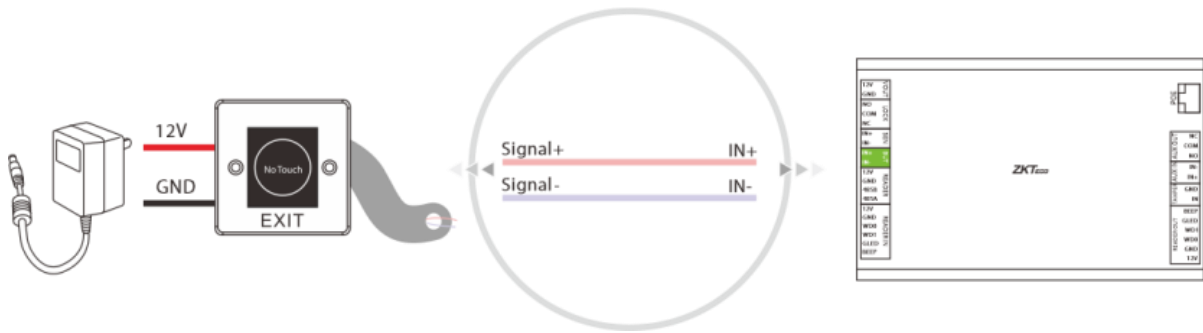
## 7.2 Conexión del sensor

El sensor de puerta se utiliza para detectar el estado de la puerta, el controlador de acceso puede detectar que la puerta se abre ilegalmente a través del interruptor del sensor de puerta y luego se emitirá la alarma. Además, después de abrir la puerta en más de un período de tiempo específico y no cerrar la puerta, el controlador de acceso también activará la alarma. Se recomienda elegir alambre de dos núcleos, diámetro de alambre de 0,22 milímetros cuadrados o más. Si no es necesario conocer el estado de conmutación de la puerta en línea y no es necesario dejar la puerta abierta durante mucho tiempo de alarma, alarma de intrusión y enclavamiento y otras funciones, es posible que el sensor de la puerta no esté conectado.



## 7.3 Conexión del botón de salida

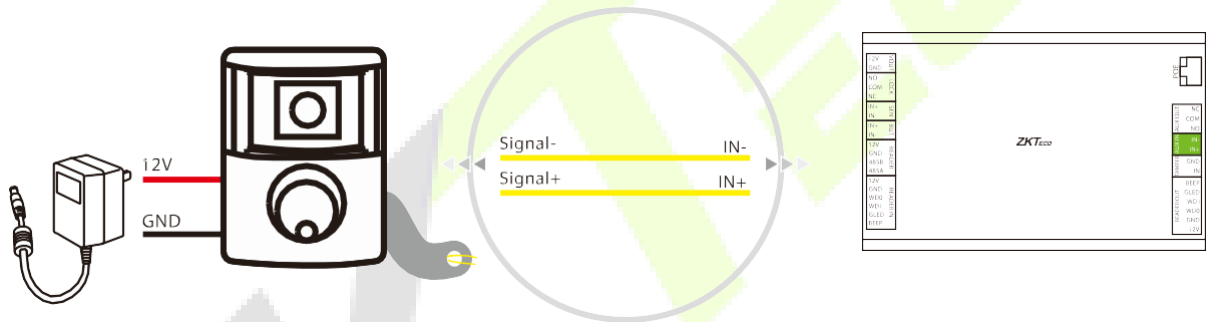
El botón de salida es un dispositivo de conmutación para abrir la puerta instalado dentro de la habitación, y la puerta se puede abrir cuando el botón de salida está cerrado. El botón de salida se fija a aproximadamente 1,4 metros del suelo, y debe asegurarse de que la posición del botón de salida sea correcta, sin distorsión, y que el cableado sea preciso y firme (pellizque el extremo expuesto de los cables no utilizados y envuélvalos con cinta aislante). Tenga cuidado de evitar interferencias de sensores electrónicos (como: interruptores de iluminación, computadoras, etc.). Se recomienda utilizar cables de dos núcleos con un área de sección transversal de 0,3 mm<sup>2</sup> o más para los cables que conectan el botón de salida al controlador.



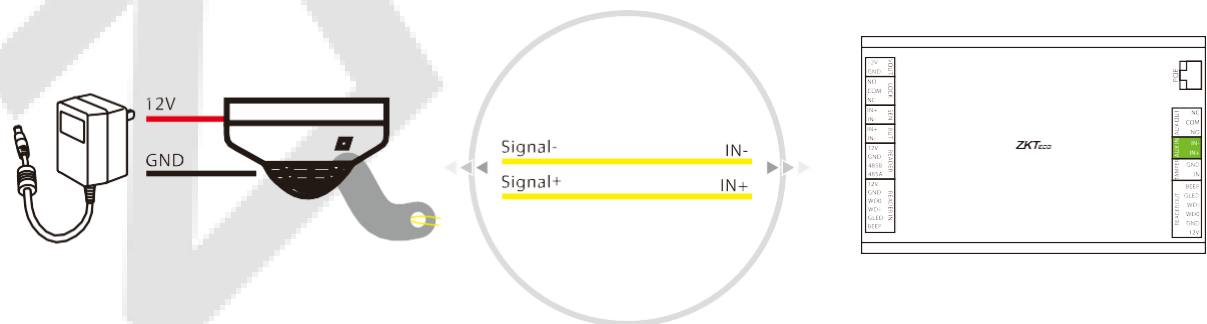
## 7.4 Conexión de la entrada auxiliar

El DE10 proporciona 1 puerto de entrada auxiliar para conectar detectores de detección de cuerpos infrarrojos o detectores de humo, etc.

- **Detector de sensor infrarrojo del cuerpo humano**

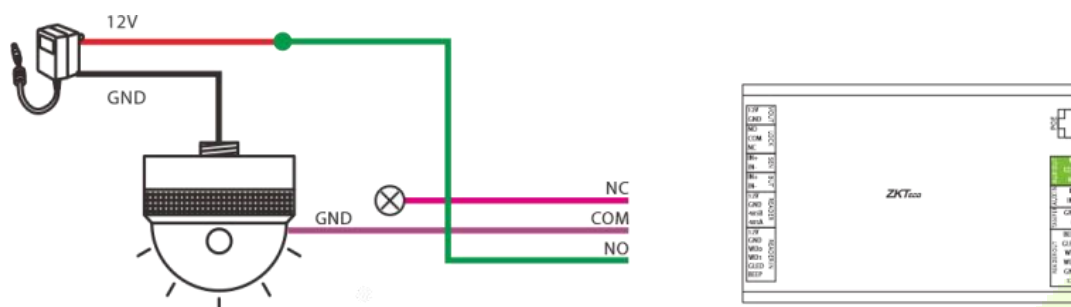


- **Detector de humo**



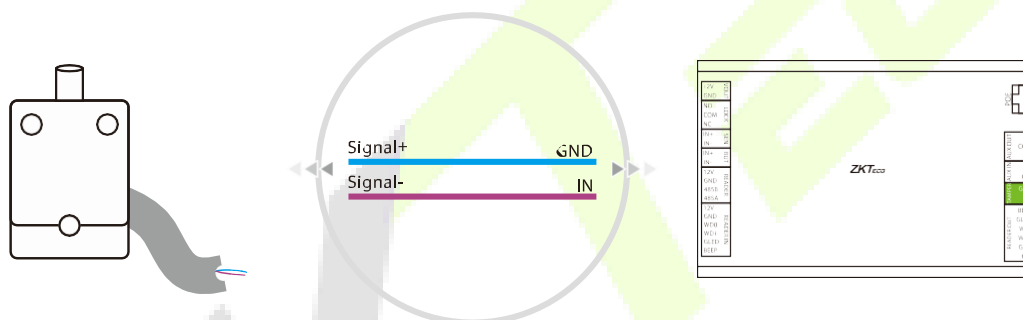
## 7.5 Conexión de la salida auxiliar

El DE10 proporciona 1 conector de salida auxiliar para conectar una alarma audible y visual.



## 7.6 Conexión del interruptor anti-sabotaje

La señal de manipulación del DE10 está conectada al interruptor de manipulación del gabinete.



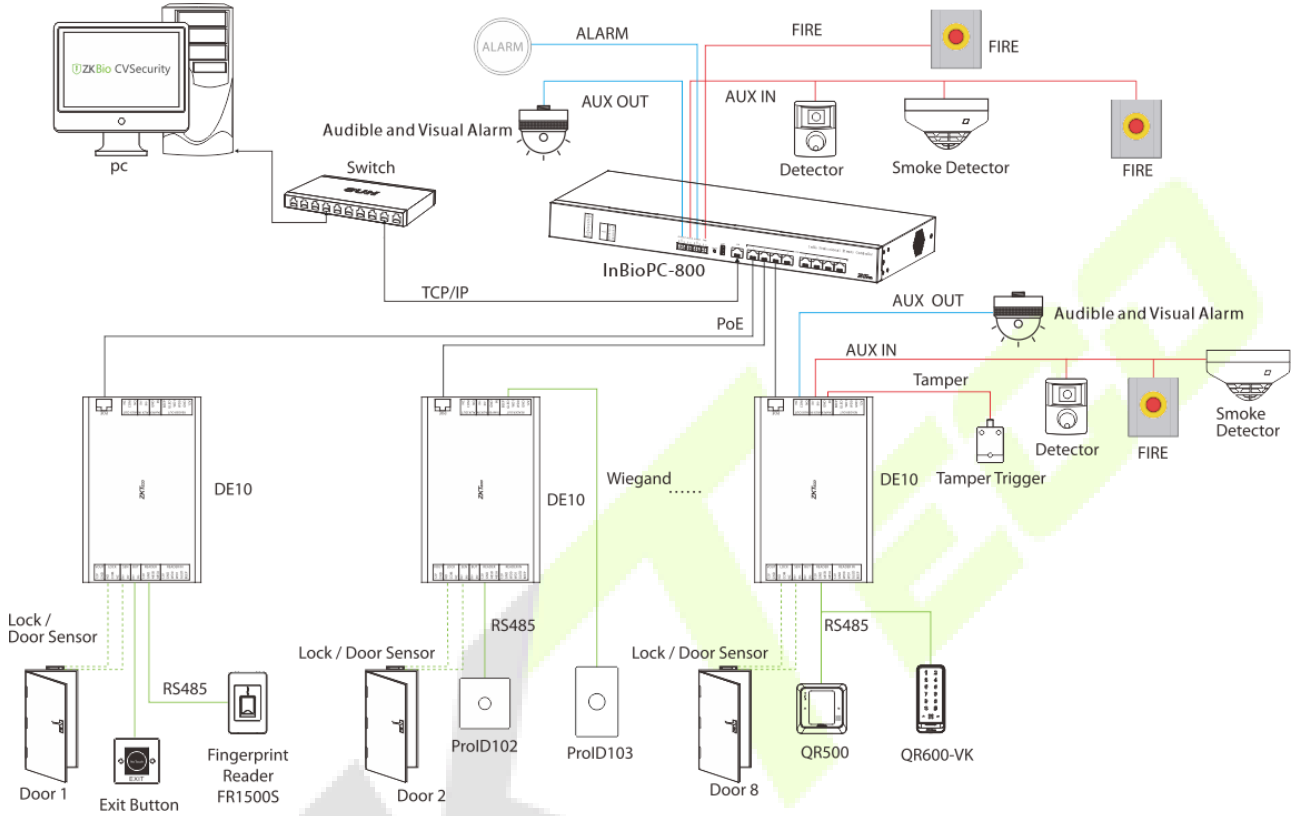
## 7.7 Conexión de la cerradura

1. Un DE10 admite el control de una cerradura para puerta .
2. El sistema admite tanto la cerradura normalmente abierta como la cerradura normalmente cerrada. El bloqueo NO (normalmente abierto cuando está encendido) está conectado con los terminales 'NO1' y 'COM', y el bloqueo NC (normalmente cerrado cuando está encendido) está conectado con los terminales 'NC1' y 'COM'.
3. Para evitar que la cerradura eléctrica genere una fuerza electromotriz autoinducida en el sistema de control de acceso en el momento de la conmutación, es necesario conectar un diodo en paralelo con la cerradura eléctrica (utilice el FR107 suministrado con el sistema) para liberar la fuerza electromotriz autoinducida durante el cableado de la aplicación de campo del sistema de control de acceso.
4. El terminal VOUT del DE10 puede suministrar energía a la cerradura eléctrica, pero el consumo de corriente de la cerradura debe ser inferior a 800 mA.



## 8 Sistema de control de acceso

Utilice la fuente de alimentación configurada para el controlador de la serie InBioPC para suministrar energía desde la fuente de alimentación suministrada de 100-240 V, AC50/60 Hz.

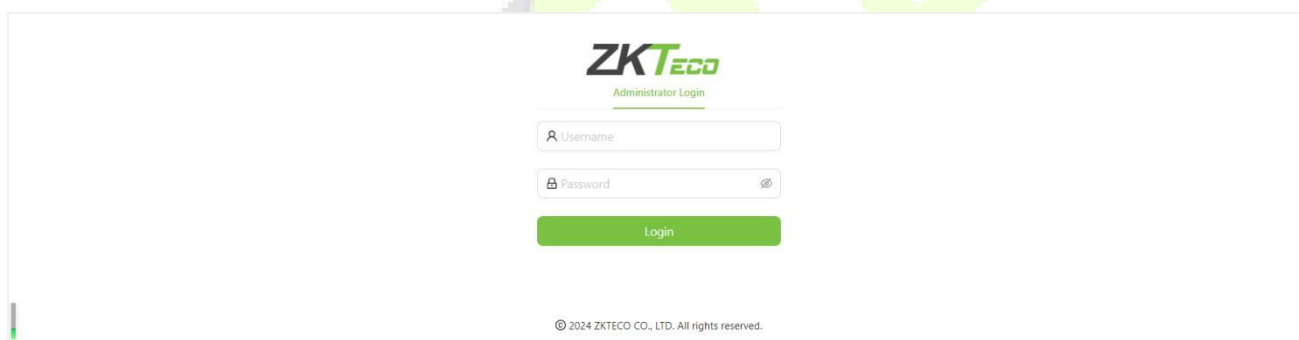
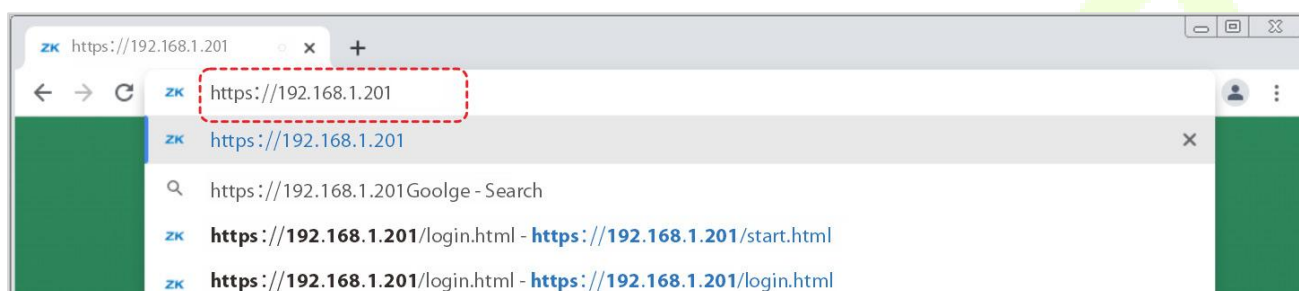


## 9 Iniciar sesión WebServer

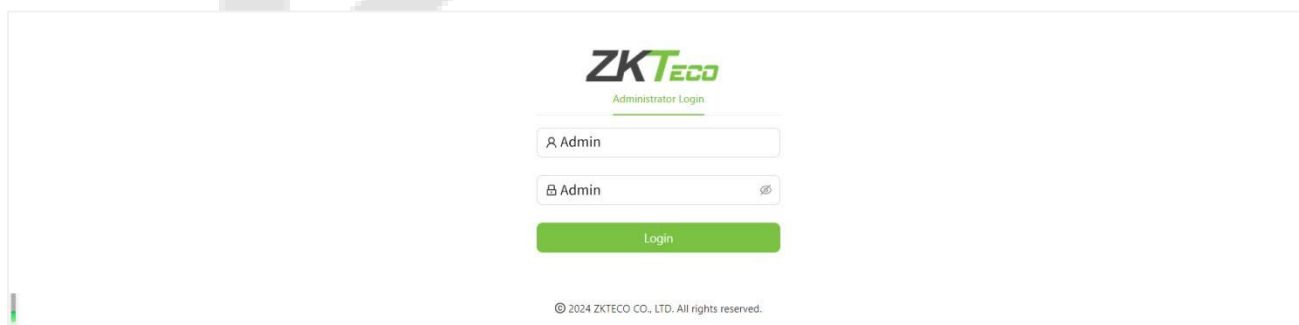
El dispositivo tiene un servidor web incorporado, que admite la configuración de parámetros del dispositivo y la verificación del estado del dispositivo, etc. en PC y teléfono celular.

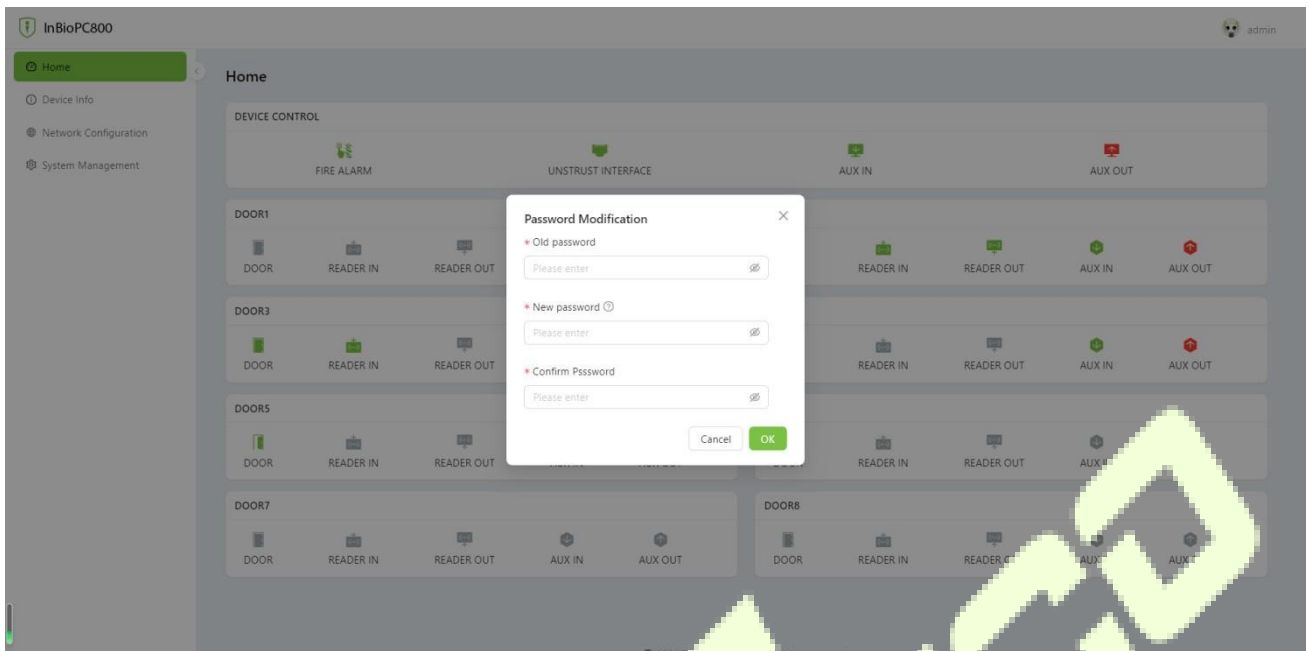
### 9.1 PC

1. Una vez que el dispositivo esté conectado a la corriente y a la red, abra un navegador e inicie sesión en el servidor web ingresando la dirección, que es la “**https://[Dirección IP]**”. Por ejemplo: <https://192.168.1.201>.



2. Ingrese la cuenta y la contraseña del servidor web, la cuenta predeterminada es: **admin**; y la contraseña es: **admin**.

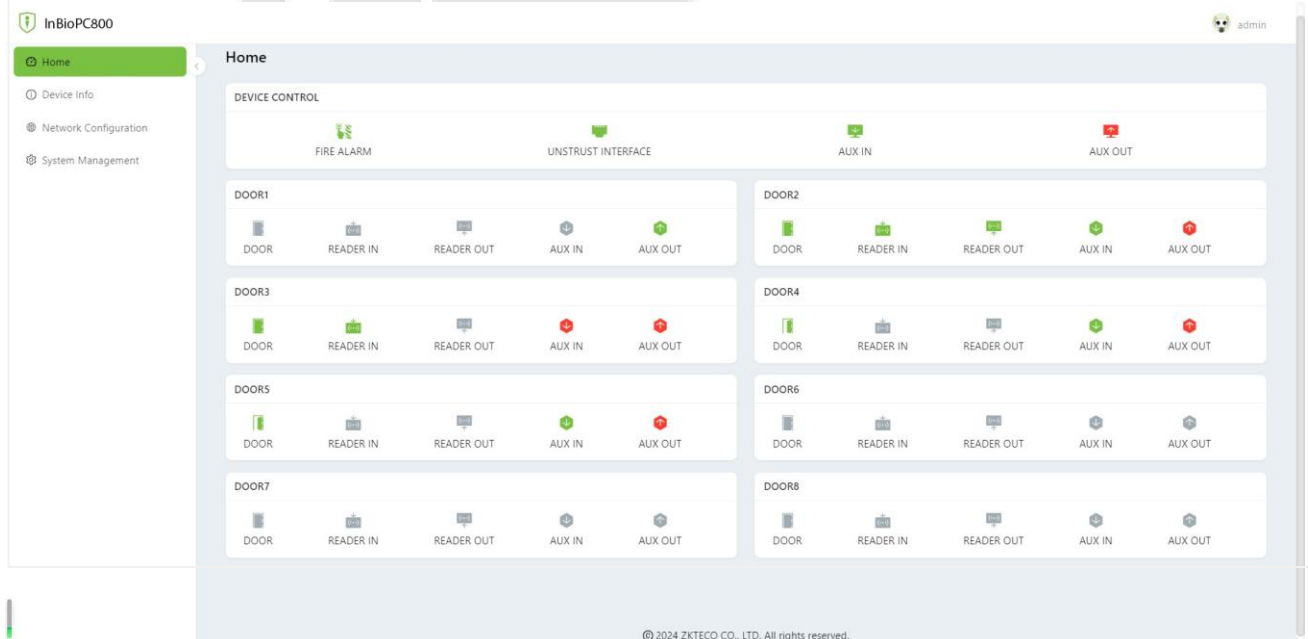




**Nota:** El sistema tiene la contraseña predeterminada, si el usuario inicia sesión o visita la página de inicio, el sistema le recuerda que debe modificar la contraseña; si la modificación es exitosa, debe volver a iniciar sesión.

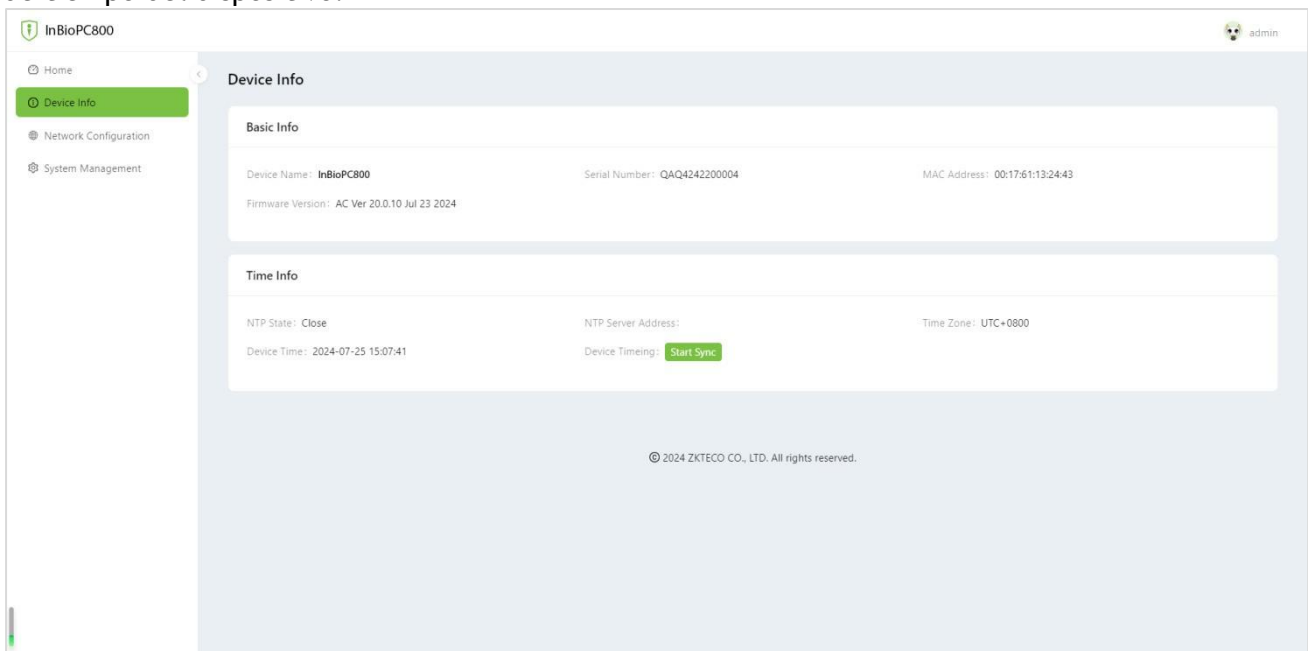
## Información de estado

En la página del servidor web abierta, haga clic en **[Inicio]** para ver la información de estado de todos los dispositivos periféricos conectados al dispositivo, como el lector, la entrada auxiliar, la salida auxiliar, la red y la puerta.



## Información del dispositivo

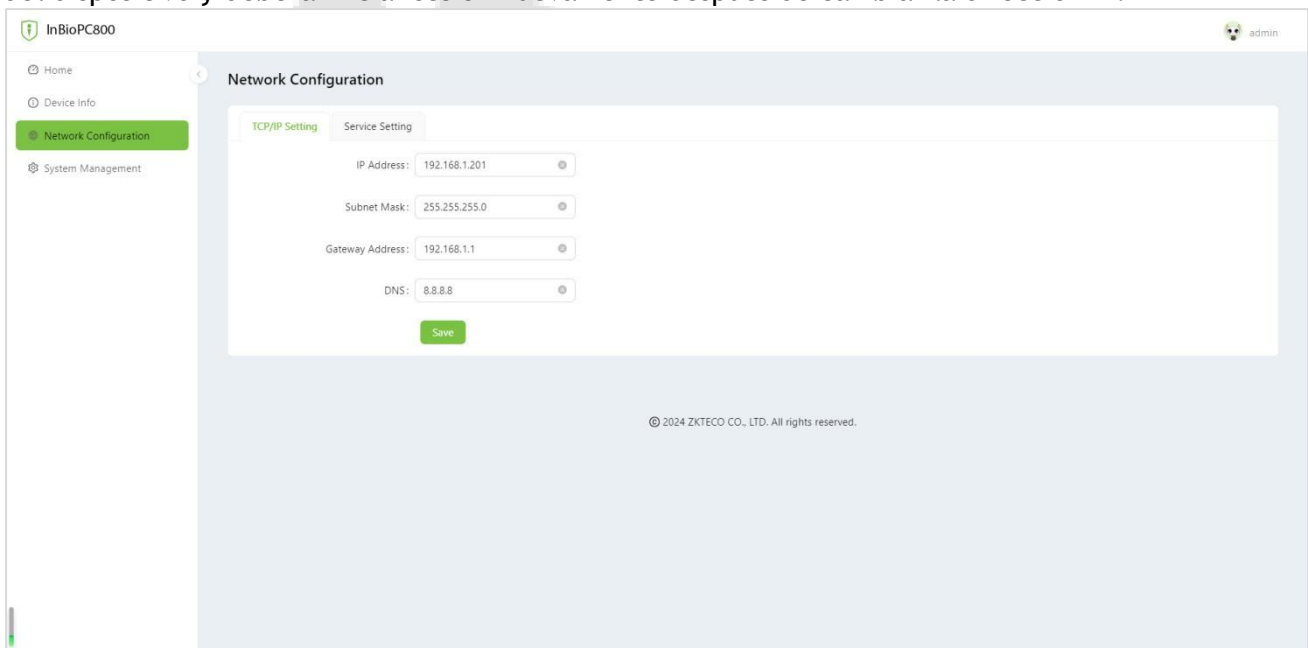
Haga clic en **[Información del dispositivo]** para examinar la información básica y la información de tiempo del dispositivo.



The screenshot shows the 'Device Info' page of the InBioPC800 web interface. The page is divided into two main sections: 'Basic Info' and 'Time Info'. The 'Basic Info' section displays the following details: Device Name: InBioPC800, Serial Number: QAQ4242200004, MAC Address: 00:17:61:13:24:43, and Firmware Version: AC Ver 20.0.10 Jul 23 2024. The 'Time Info' section displays: NTP State: Close, NTP Server Address: (empty), Time Zone: UTC+0800, Device Time: 2024-07-25 15:07:41, and Device Timing: Start Sync (indicated by a green button). The page footer contains the copyright notice: © 2024 ZKTECO CO., LTD. All rights reserved.

## Configuración de red

Haga clic en **[Configuración de red]** > **[Configuración TCP/IP]** para cambiar la dirección IP del dispositivo y deberá iniciar sesión nuevamente después de cambiar la dirección IP.



The screenshot shows the 'Network Configuration' page of the InBioPC800 web interface. The page is divided into two tabs: 'TCP/IP Setting' (selected) and 'Service Setting'. The 'TCP/IP Setting' tab displays the following configuration fields: IP Address: 192.168.1.201, Subnet Mask: 255.255.255.0, Gateway Address: 192.168.1.1, and DNS: 8.8.8.8. A green 'Save' button is located below the fields. The page footer contains the copyright notice: © 2024 ZKTECO CO., LTD. All rights reserved.

Haga clic en **[Configuración de red]** > **[Configuración de servicio]** para configurar el servidor con la IP y puerto del software, como ZKBio CVSecurity.

The screenshot shows the 'Network Configuration' page for the InBioPC800 device. The 'Service Setting' tab is active. The configuration fields are as follows:

Field	Value
Server Mode	IP Mode
Connection Method	HTTPS
IP Address	192.168.1.50
Port	8088

A green 'Save' button is located below the fields. The footer of the page reads: © 2024 ZKTECO CO., LTD. All rights reserved.

## Gestión del sistema

Haga clic en **[Administración del sistema]** para admitir la configuración del modo de puerto POE del dispositivo, la configuración del punto de acceso Wi-Fi y reiniciar/restaurar la configuración de fábrica/actualización del dispositivo.

The screenshot shows the 'System Management' page for the InBioPC800 device. The 'Port Setting' tab is active. The configuration fields are as follows:

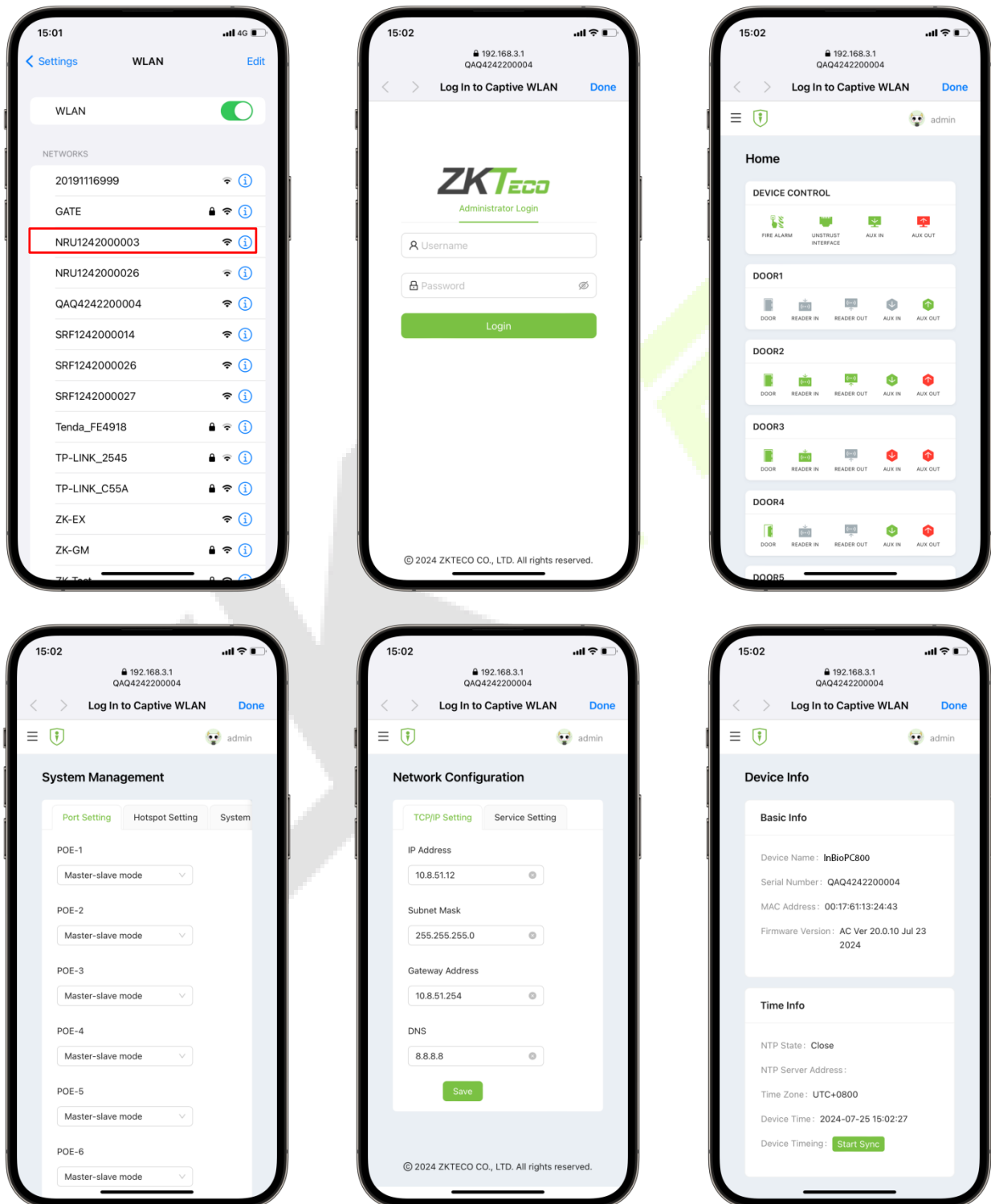
Port	Mode
POE-1	Master-slave mode
POE-2	Master-slave mode
POE-3	Master-slave mode
POE-4	Master-slave mode
POE-5	Master-slave mode
POE-6	Master-slave mode
POE-7	Master-slave mode
POE-8	Master-slave mode

A green 'Save' button is located at the bottom. A note at the bottom of the page reads: The switch of network port mode requires a restart of the changed network port to take effect, which will cause the POE power supply and network to be disconnected for a few seconds before automatically recovering!

**Nota:** El puerto POE se puede configurar como modo maestro-esclavo o modo de switch. El cambio del modo de puerto de red requiere un reinicio del puerto de red cambiado para que surta efecto, lo que hará que la fuente de alimentación POE y la red se desconecten durante unos segundos antes de recuperarse automáticamente.

## 9.2 Teléfono

No es necesario ingresar la dirección IP del dispositivo en el teléfono celular. Después de que el dispositivo esté conectado a la fuente de alimentación y a la red, el teléfono celular debe estar cerca del dispositivo, buscar el punto de acceso del dispositivo (de forma predeterminada, es el número de serie del dispositivo) y luego hacer clic en él, ya conectado te abrirá una ventana emergente en la cual se deberá ingresar la cuenta y la contraseña del servidor web.

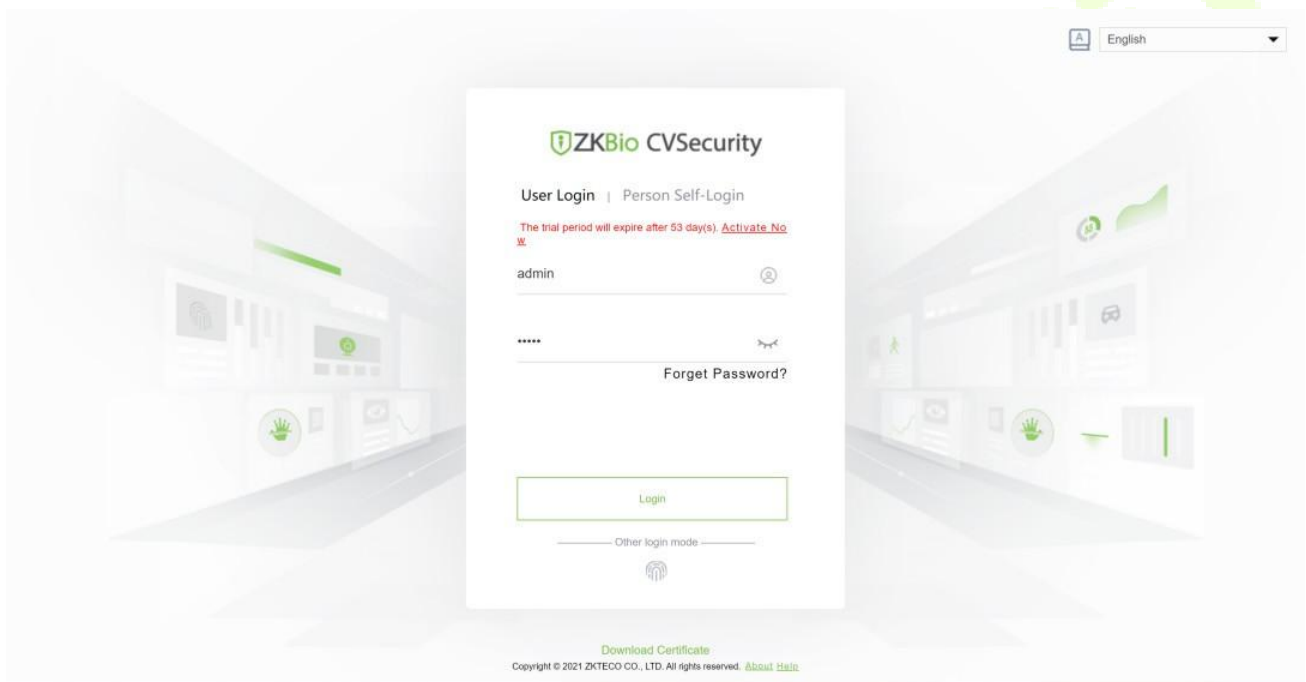


## 10 Conexión a ZKBio CVSecurity

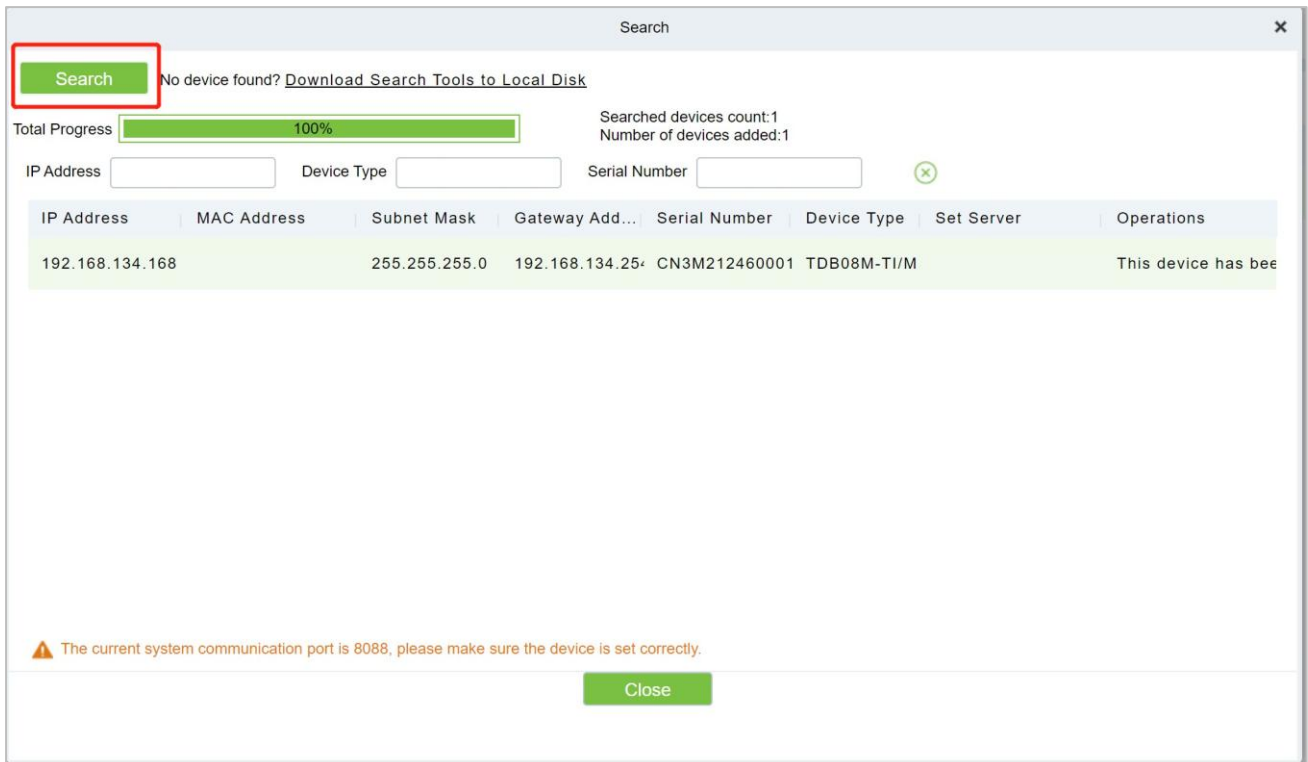
El dispositivo se conecta a ZKBio CVSecurity configurando la información del servidor en [Configuración web] > [Configuración del servidor] del servidor web (no es necesario configurar si el dispositivo y el servidor están en el mismo segmento de red). El dispositivo puede agregar módulos, configurar reglas de control de acceso, configurar anti-passback global, vinculación, enclavamiento y otras operaciones de control de acceso en ZKBio CVSecurity.

### 10.1 Agregar el dispositivo

1. Abra ZKBio CVSecurity e inicie sesión en ZKBio CVSecurity ingresando el nombre del usuario y contraseña.



2. En el módulo de **Control de Acceso**, seleccione [**Dispositivo**] > [**Dispositivo de Control de Acceso**].
3. En la interfaz del dispositivo, haga clic en el botón [**Buscar**] para que aparezca un cuadro de búsqueda.
4. Haga clic en [**Iniciar Búsqueda**] en el cuadro de búsqueda para mostrar los **dispositivos de control de acceso** que se pueden agregar, como se muestra en la figura a continuación.



5. Opcional: Modifique la dirección IP del dispositivo de **Control de Acceso**, haga clic en **[Modificar Dirección IP]**, el dispositivo se reiniciará después de modificar la dirección IP y la modificación de la dirección IP se completará después del reinicio.
6. Para los dispositivos de control de acceso buscados, haga clic en el botón **[Agregar]** en la barra de operaciones para agregar el dispositivo.

## 10.2 Puerta


1. En el módulo de **Control de Acceso**, seleccione **[Dispositivos] > [Puerta]**.
2. En la interfaz de administración de la puerta, haga clic en el botón **[Editar]** en la barra de operación de la puerta para abrir el cuadro de configuración de parámetros de la puerta.
3. En la interfaz de configuración de parámetros de puerta, complete los parámetros correspondientes de acuerdo con los requisitos de adición, como se muestra en la figura a continuación.

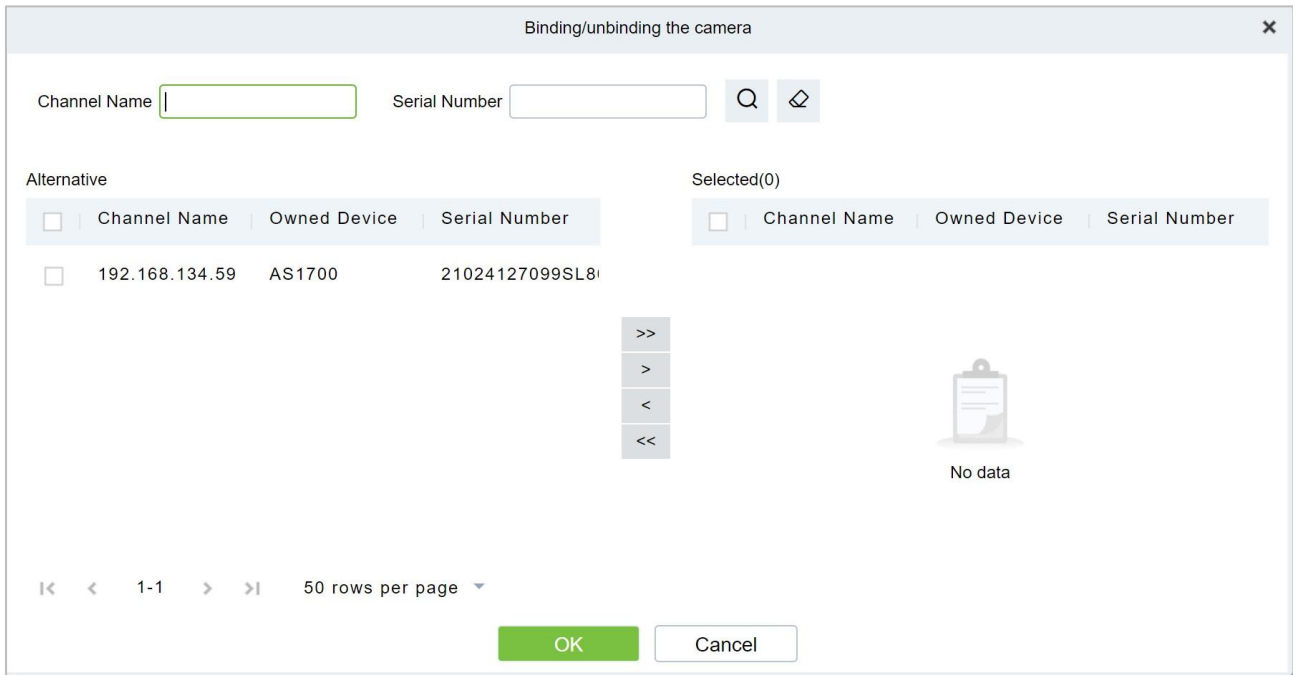
The screenshot shows a configuration window titled "Edit" with a close button (X) in the top right corner. The window is divided into two columns of settings:

- Left Column:**
  - Device Name\*: ZKT\_Korea
  - Door Name\*: ZKT\_Korea-1
  - Verification Mode\*: Automatic Identification (dropdown)
  - Operate Interval\*: 0 second(0-254)
  - Anti-Passback Duration of Entrance: 0 minute(0-120)
  - Duress Password: (Maximum 6 Bit Integer)
  - Emergency Password: (8 Bit Integer)
  - Disable Alarm Sounds:
- Right Column:**
  - Door Number\*: 1
  - Active Time Zone\*: 24-Hour Accessible (dropdown)
  - Lock Open Duration\*: 5 second(1-254)
  - Door Sensor Type\*: None (dropdown)
  - Door Sensor Delay: (second(1-254))
  - Passage Mode Time Zone: (dropdown)
  - Multi-Person Operation Interval\*: 10 second(5-60)

At the bottom, there is a text field: "The above settings are copied to" followed by a dropdown menu. At the very bottom, there are two buttons: "OK" (green) and "Cancel" (white).

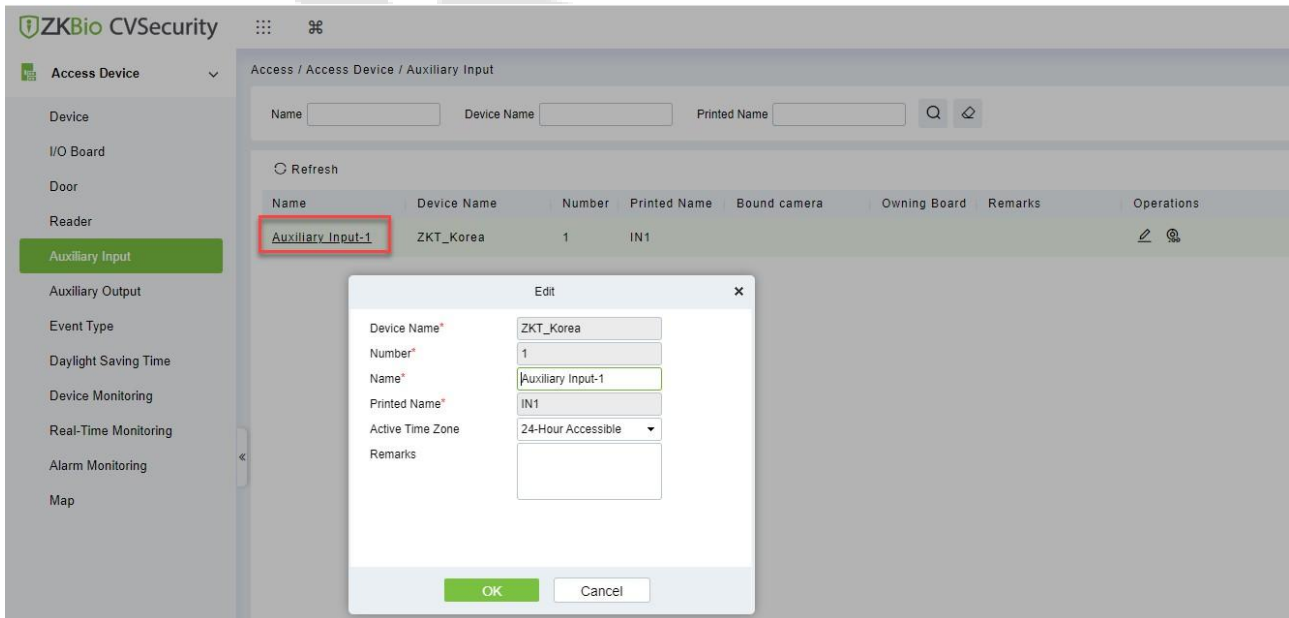
## 10.3 Lector

1. En el módulo de **Control de Acceso**, seleccione **[Dispositivo] > [Lector]**.
2. En la columna Operación del lector correspondiente, haga clic en . Se muestra la página de vinculación/desvinculación de la cámara.
3. En la pantalla Seleccionar lector, configure el lector según sea necesario, como se muestra en la figura siguiente.



## 10.4 Entrada auxiliar

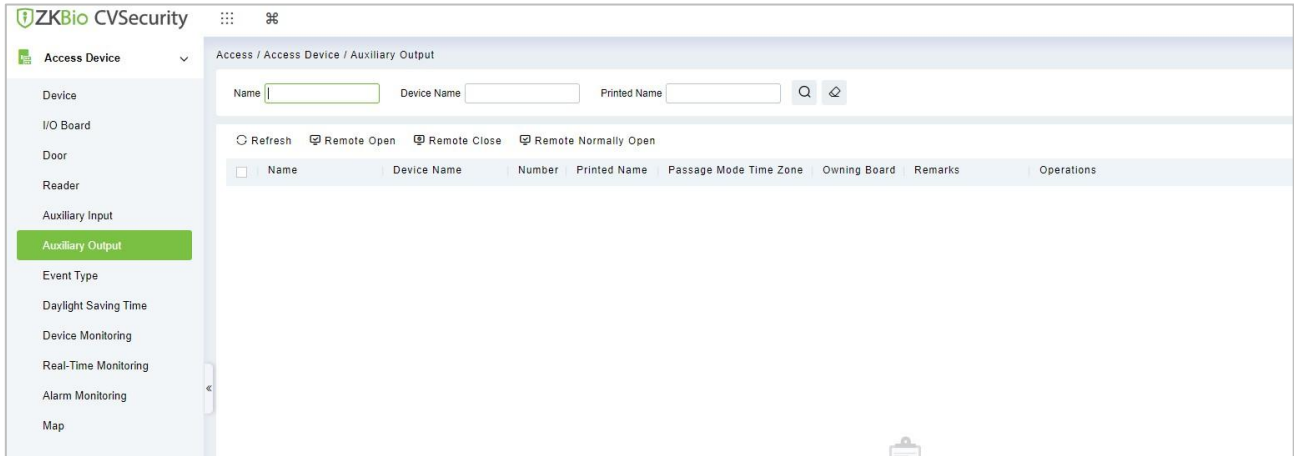
1. Haga clic en **[Dispositivo de Acceso] > [Entrada Auxiliar]** en el menú de acciones para acceder a la interfaz que se muestra a continuación.
2. Haga clic en **[Nombre]** o **[Editar]** para modificar los parámetros como se muestra a continuación:



3. Haga clic en **[Aceptar]** para guardar el nombre y el comentario y salir.

## 10.5 Salida auxiliar

1. Haga clic en **[Dispositivo de Acceso]** > **[Salida Auxiliar]** en el menú de acciones para acceder a la siguiente interfaz:



2. Haga clic en **[Editar]** para modificar los parámetros.

The 'Edit' dialog box contains the following fields:

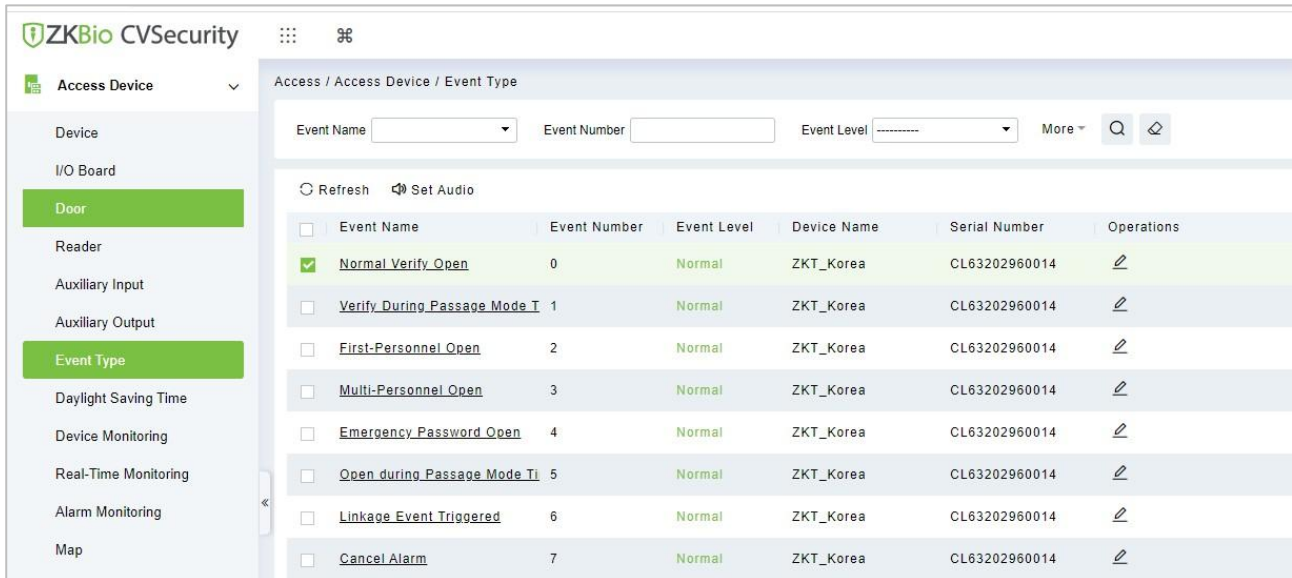
- Device Name\*: 192.168.12.155
- Number\*: 1
- Name\*: Auxiliary Output-1
- Printed Name\*: OUT1
- Passage Mode Time Zone: -----
- Remark: (empty text area)

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

3. Haga clic en **[Aceptar]** para guardar el nombre y el comentario y salir.

## 10.6 Tipo de evento

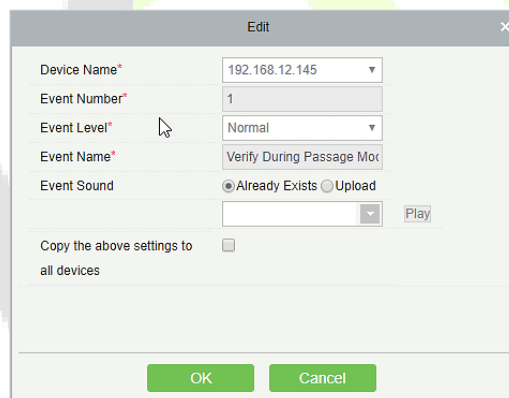
1. Clic [**Dispositivo de Acceso**] > [**Evento**] para acceder a la siguiente página:



The screenshot shows the ZKBio CVSecurity web interface. On the left is a navigation menu with 'Event Type' selected. The main area shows a table of event types for device 'ZKT\_Korea' (serial 'CL63202960014').

<input type="checkbox"/>	Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
<input checked="" type="checkbox"/>	Normal_Verify_Open	0	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	Verify_During_Passage_Mode_T	1	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	First-Personnel_Open	2	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	Multi-Personnel_Open	3	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	Emergency_Password_Open	4	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	Open_during_Passage_Mode_T	5	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	Linkage_Event_Triggered	6	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>
<input type="checkbox"/>	Cancel_Alarm	7	Normal	ZKT_Korea	CL63202960014	<a href="#">✎</a>

2. Clic [**Editar**] o haga clic en el nombre del tipo de evento que desea editar.

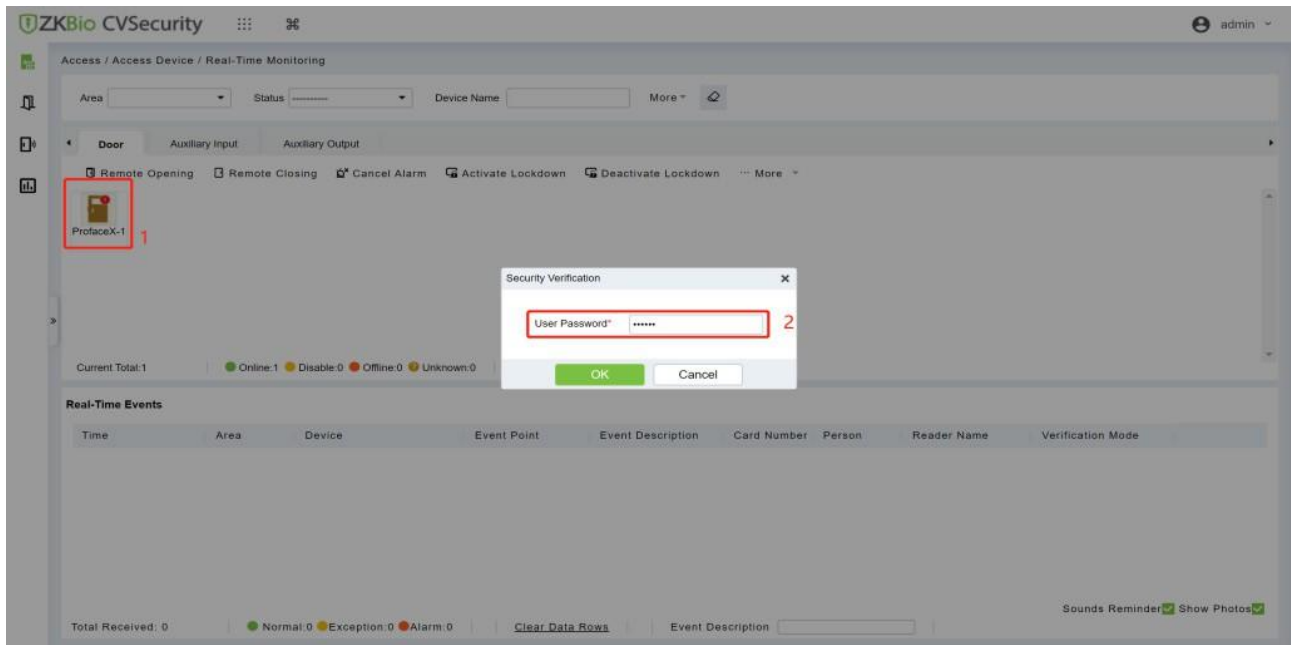


The 'Edit' dialog box contains the following fields and options:

- Device Name\*: 192.168.12.145
- Event Number\*: 1
- Event Level\*: Normal
- Event Name\*: Verify During Passage Mo...
- Event Sound:  Already Exists  Upload
- Play button
- Copy the above settings to all devices:
- OK and Cancel buttons

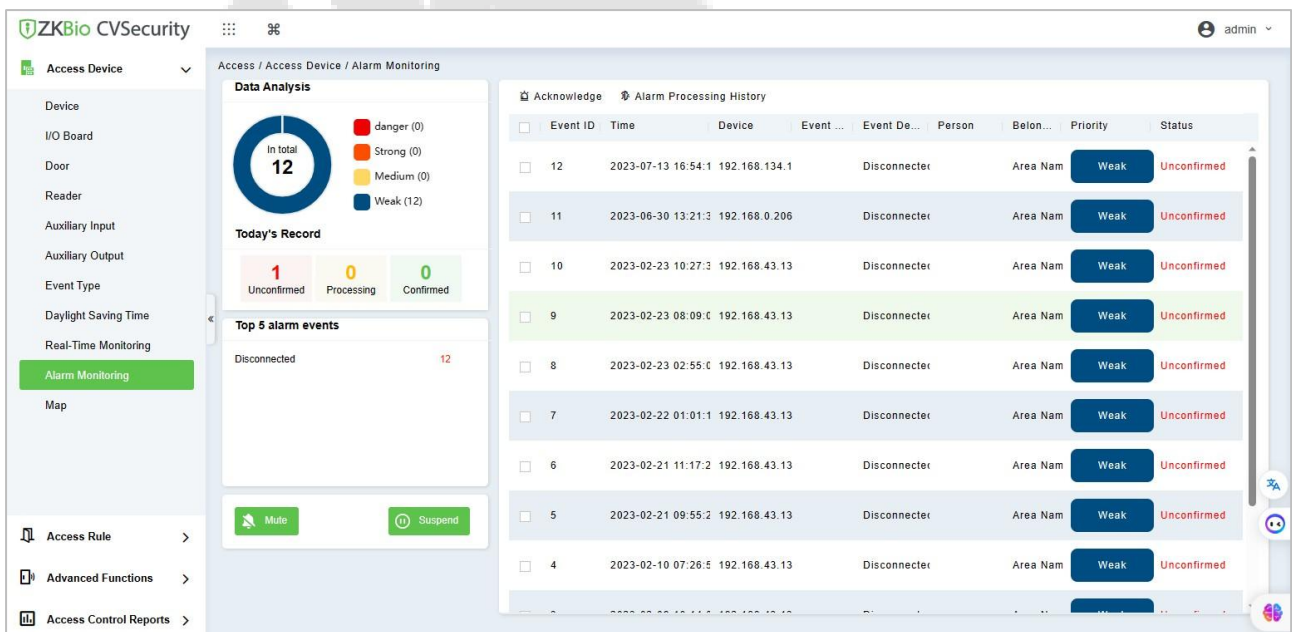
## 10.7 Monitoreo en tiempo real

1. En el módulo de **Control de Acceso**, elija **[Dispositivo de Control de Acceso] > [Monitoreo en Tiempo Real]**.
2. Compruebe si el estado del icono del dispositivo agregado está en línea.



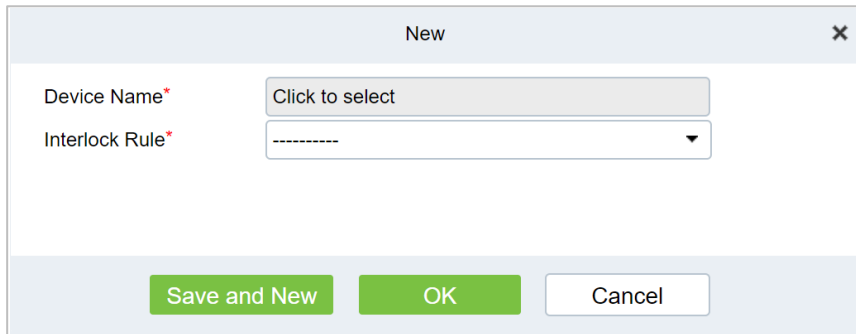
## 10.8 Monitoreo de alarmas

Monitoreará el estado y los eventos en tiempo real de las puertas debajo de los paneles de control de acceso en el sistema en tiempo real, incluidos los eventos normales y los eventos anormales.



## 10.9 Esclusamiento

Establezca el control de esclusamiento entre dos o más puertas en el dispositivo de control de acceso: Para verificar la apertura de una puerta, asegúrese de que todas las demás puertas estén cerradas; de lo contrario, la puerta no se puede abrir. En el módulo de **Control de Acceso**, elija **[Control de Acceso] > [Esclusamiento]** y haga clic en **[Nuevo]**.

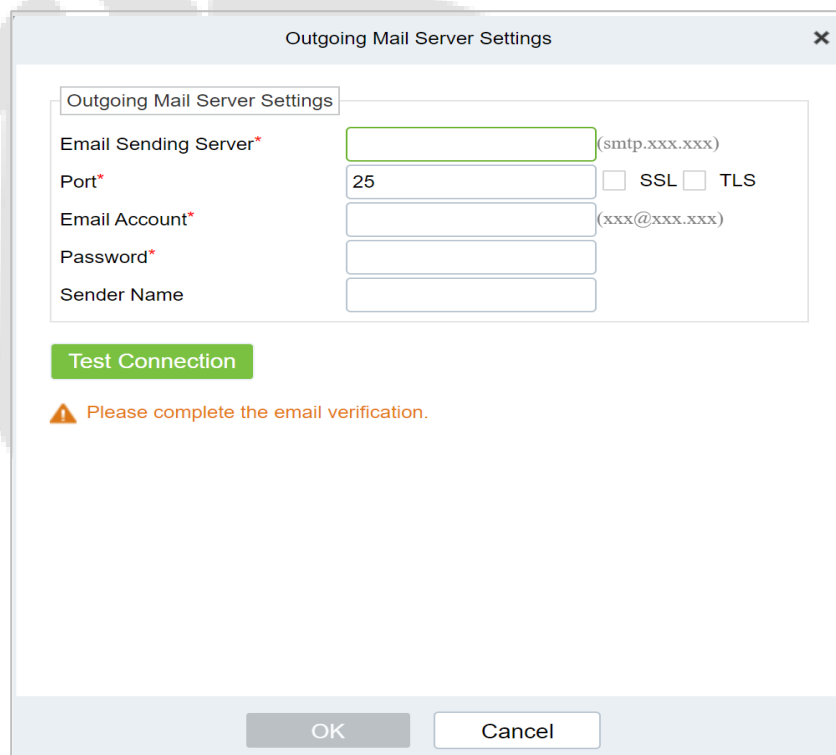


The 'New' dialog box contains the following fields and buttons:

- Device Name\***: A text input field with the placeholder text 'Click to select'.
- Interlock Rule\***: A dropdown menu with a single visible option '-----'.
- Buttons**: 'Save and New' (green), 'OK' (green), and 'Cancel' (white).

## 10.10 Vínculo

El método de uso y el escenario de vinculación son flexibles. Después de que un punto de entrada en el sistema de **Control de Acceso** active un evento específico, se generará una acción de enlace en el punto de salida especificado para controlar eventos como la apertura de verificación, la alarma y la anomalía en el sistema. Agregue Configuración para vincular cámaras a dispositivos de control de acceso, puntos de entrada, puntos de salida y lector.

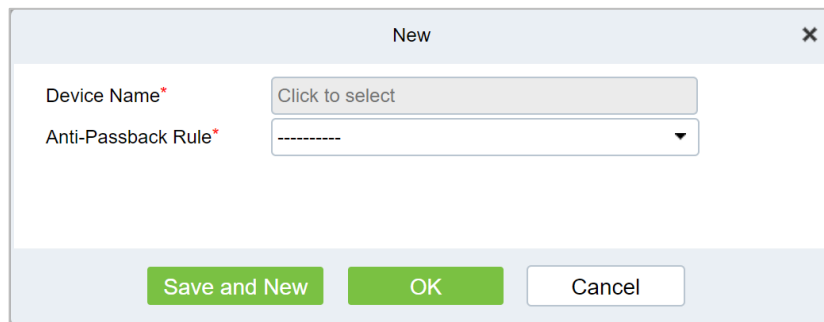


The 'Outgoing Mail Server Settings' dialog box contains the following fields and elements:

- Outgoing Mail Server Settings**: A title bar with a close button.
- Email Sending Server\***: A text input field with a placeholder '(smtp.xxx.xxx)'.
- Port\***: A text input field with the value '25' and checkboxes for 'SSL' and 'TLS'.
- Email Account\***: A text input field with a placeholder '(xxx@xxx.xxx)'.
- Password\***: A text input field.
- Sender Name**: A text input field.
- Test Connection**: A green button.
- Warning**: A red triangle icon followed by the text 'Please complete the email verification.'
- Buttons**: 'OK' (grey) and 'Cancel' (white).

## 10.11 Anti-Passback

Algunas ocasiones requieren que el personal que cepilla la tarjeta verifique, la tarjeta de cepillo que entra por una puerta debe cepillar la tarjeta para salir por otra puerta, el registro de la tarjeta de cepillo debe ingresar una correspondencia estricta. Esta función se puede utilizar cuando los usuarios la habilitan en la configuración. Generalmente se utiliza en unidades especiales, investigación científica, bóvedas bancarias y otras ocasiones. En el módulo **Control de Acceso**, seleccione **[Control de Acceso]** > **[Anti-Passback]** y haga clic en **[Nuevo]**.



The image shows a 'New' dialog box with a close button (X) in the top right corner. It contains two fields: 'Device Name\*' with a 'Click to select' button, and 'Anti-Passback Rule\*' with a dropdown menu showing '-----'. At the bottom, there are three buttons: 'Save and New' (green), 'OK' (green), and 'Cancel' (white).

Para obtener información más detallada sobre el uso de ZKBio CVSecurity, consulte el Manual de Usuario de ZKBio CVSecurity.

# **Apéndice 1**

## **Política de privacidad**

### **Nota:**

Para ayudarlo a utilizar mejor los productos y servicios de ZKTeco (en adelante, "nosotros", "nuestro" o "nos"), un proveedor de servicios inteligentes, recopilamos constantemente su información personal. Dado que entendemos la importancia de su información personal, tomamos su privacidad con sinceridad y hemos formulado esta política de privacidad para proteger su información personal. Hemos enumerado las políticas de privacidad a continuación para comprender con precisión las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes.

**Antes de utilizar nuestros productos y servicios, lea atentamente y comprenda todas las reglas y disposiciones de esta Política de privacidad. Si no está de acuerdo con el acuerdo correspondiente o cualquiera de sus términos, debe dejar de usar nuestros productos y servicios.**

### **I. Información recopilada**

Para garantizar el funcionamiento normal del producto y ayudar a mejorar el servicio, recopilaremos la información proporcionada voluntariamente por usted o proporcionada según lo autorizado por usted durante el registro y el uso o generada como resultado de su uso de los servicios.

- 1. Información de registro de usuario:** En su primer registro, la plantilla de funciones (**plantilla de huella digital/plantilla de rostro/plantilla de palma**) se guardará en el dispositivo de acuerdo con el tipo de dispositivo que haya seleccionado para verificar la similitud única entre usted y el ID de usuario que ha registrado. Opcionalmente, puede ingresar su nombre y código. La información anterior es necesaria para que pueda utilizar nuestros productos. Si no proporciona dicha información, no podrá utilizar algunas funciones del producto con regularidad.
- 2. Información del producto:** De acuerdo con el modelo del producto y el permiso otorgado cuando instala y utiliza nuestros servicios, la información relacionada del producto en el que se utilizan nuestros servicios se recopilará cuando el producto se conecte al software, incluido el modelo del producto, el número de versión del firmware, el número de serie del producto y la información de capacidad del producto. **Cuando conecte su producto al software, lea atentamente la política de privacidad del software específico.**

### **II. Seguridad y gestión de productos**

- 1.** Cuando utilice nuestros productos por primera vez, deberá establecer el privilegio de

administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que establezca el privilegio de administrador cuando ingrese a la interfaz del menú principal. **Si aún no establece el privilegio de administrador después de recibir el mensaje del sistema, debe tener en cuenta el posible riesgo de seguridad (por ejemplo, los datos pueden modificarse manualmente).**

2. Todas las funciones de visualización de la información biométrica están desactivadas en nuestros productos por defecto. Puede elegir Menú > Configuración del sistema para establecer si desea mostrar la información biométrica. Si habilita estas funciones, asumimos que es consciente de los riesgos de seguridad de la privacidad personal especificados en la política de privacidad.
3. De forma predeterminada, solo se muestra su ID de usuario. Puede establecer si desea mostrar otra información de verificación de usuario (como Nombre, Departamento, Foto, etc.) bajo el privilegio de administrador. **Si elige mostrar dicha información, asumimos que es consciente de los posibles riesgos de seguridad (por ejemplo, su foto se mostrará en la interfaz del dispositivo).**
4. La función de cámara está desactivada en nuestros productos de forma predeterminada. Si desea habilitar esta función para tomar fotografías de sí mismo para grabar la asistencia o tomar fotografías de extraños para el control de acceso, el producto habilitará el tono rápido de la cámara. **Una vez que habilite esta función, asumimos que es consciente de los posibles riesgos de seguridad.**
5. Todos los datos recopilados por nuestros productos están encriptados mediante el algoritmo AES 256. Todos los datos cargados por el Administrador en nuestros productos se cifran automáticamente mediante el algoritmo AES 256 y se almacenan de forma segura. Si el Administrador descarga datos de nuestros productos, asumimos que necesita procesar los datos y que conoce el riesgo potencial de seguridad. En tal caso, usted asumirá la responsabilidad de almacenar los datos. Debes saber que algunos datos no se pueden descargar por el bien de la seguridad de los datos.
6. Toda la información personal de nuestros productos puede ser consultada, modificada o eliminada. Si ya no utiliza nuestros productos, borre sus datos personales.

### III. **Cómo manejamos la información personal de menores**

Nuestros productos, sitio web y servicios están diseñados principalmente para adultos. Sin el consentimiento de los padres o tutores, los menores no pueden crear su propia cuenta. Si es menor de edad, se recomienda que pida a sus padres o tutores que lean detenidamente esta Política y que solo utilicen nuestros servicios o la información proporcionada por nosotros con el consentimiento de sus padres o tutores.

Solo usaremos o divulgaremos información personal de menores recopilada con el

consentimiento de sus padres o tutores si y en la medida en que dicho uso o divulgación esté permitido por la ley o hayamos obtenido el consentimiento explícito de sus padres o tutores, y dicho uso o divulgación sea con el fin de proteger a los menores. Al notar que hemos recopilado información personal de menores sin el consentimiento previo de los padres verificables, eliminaremos dicha información lo antes posible.

#### **IV. Otros**

Puede visitar [https://www.zkteco.com/en/index/Index/privacy\\_protection.html](https://www.zkteco.com/en/index/Index/privacy_protection.html) para aprender más información sobre cómo recopilamos, usamos y almacenamos de forma segura su información personal. Para seguir el ritmo del rápido desarrollo de la tecnología, el ajuste de las operaciones comerciales y para hacer frente a las necesidades de los clientes, deliberaremos y optimizaremos constantemente nuestras medidas y políticas de protección de la privacidad. Bienvenido a visitar nuestro sitio web oficial en cualquier momento para conocer nuestra última política de privacidad.



## Operación ecológica



El "período operativo ecológico" del producto se refiere al tiempo durante el cual este producto no descargará ninguna sustancia tóxica o peligrosa cuando se usa de acuerdo con los requisitos previos de este manual.

El período operativo ecológico especificado para este producto no incluye baterías u otros componentes que se desgastan fácilmente y deben reemplazarse periódicamente. El período operativo ecológico de la batería es de 5 años.

### Sustancias peligrosas o tóxicas y sus cantidades

Nombre del componente	Sustancia/elemento peligroso/tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio (Cd)	Cromo hexavalente (Cr6+)	Bifenilos polibromados (PBB)	Éteres de difenilo polibromados (PBDE)
Resistencia de chip	×	○	○	○	○	○
Condensador de chip	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componente ESD	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Tornillos	○	○	○	×	○	○

Esta tabla se prepara de acuerdo con las disposiciones de SJ / T 11364.

○ indica que la cantidad total de contenido tóxico en todos los materiales homogéneos está por debajo del límite especificado en GB/T 26572.

× indica que la cantidad total de contenido tóxico en todos los materiales homogéneos excede el límite especificado en GB / T 26572.

**Nota:** El 80% de los componentes de este producto se fabrican con materiales no tóxicos y ecológicos. Los componentes que contienen toxinas o elementos nocivos se incluyen debido a las limitaciones económicas o técnicas actuales que impiden su sustitución por materiales o elementos no tóxicos.

Parque Industrial ZKTeco, No. 32,  
Industrial Road, Ciudad de Tangxia,  
Dongguan, China.

Fax : +86 755 - 89602394

[www.zkteco.com](http://www.zkteco.com)

