



Canariascci.com
BioScan Serie BSC-101
Manual de Instrucciones

© 2008 IDTi

Manual de Instrucciones

Control de Acceso BioScan BSC-101

by IDTi

BioScan Serie BSC-101 - Manual de Instrucciones

© 2008 IDTi

Reservados todos los derechos. Ninguna parte de este documento puede ser reproducida en forma alguna ni por medio alguno – gráfica, electrónica o mecánica, incluyendo fotocopiado, grabación, almacenado de la información o sistema de recuperación – sin el permiso por escrito del titular.

Los productos a los que se hace referencia en este documento son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios. Ni el editor ni el autor reclaman nada de estas marcas comerciales.

Si bien se han tomado todas las precauciones posibles en la preparación de este documento, tanto el editor como el autor no asumen responsabilidades por los errores u omisiones, o por aquellos daños resultantes del uso de la información contenida en este documento o del uso de los programas y código fuente que puedan acompañar a dicha documentación. En ningún caso serán ni el editor ni el autor responsables de cualquier posible pérdida de beneficio o de cualquier otro daño comercial producido o supuestamente producido directa o indirectamente por este documento.

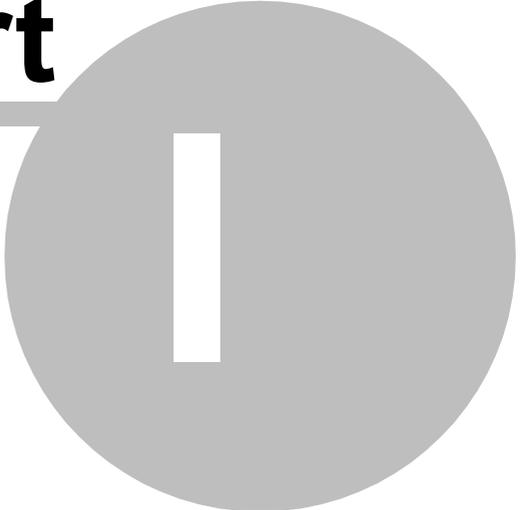
Impreso: en España, en febrero de 2008

Índice de materias

| | | |
|-------|---|----|
| 2 | Inicio rápido..... | 13 |
| 3.1 | Registrar Usuario de Huella Dactilar..... | 24 |
| 3.2 | Registrar usuario de tarjeta..... | 25 |
| 3.3 | Registrar Usuario de Tarjeta & Huella Dactilar..... | 27 |
| 3.4 | Registrar Bloque de Tarjetas de Usuario..... | 28 |
| 3.5 | Registrar Bloque de Tarjetas de Usuario 2..... | 30 |
| 4 | MENÚ DEL SISTEMA 2 – MODIFICAR USUARIO..... | 31 |
| 4.1 | Modificar ID de Usuario..... | 31 |
| 4.2 | Modificar la Huella Dactilar del Usuario..... | 31 |
| 4.3 | Modificar Tarjeta de Usuario..... | 33 |
| 4.4 | Modificar el Nivel de Usuario..... | 33 |
| 4.5 | Modificar el Nombre de Usuario..... | 34 |
| 4.6 | Retropase de usuario..... | 36 |
| 4.7 | Opción (ID)..... | 37 |
| 4.8 | Usuario Dos Personas..... | 37 |
| 5 | MENÚ DEL SISTEMA 3 – VER USUARIO..... | 39 |
| 5.1 | Lista de usuarios..... | 39 |
| 5.2 | Eventos..... | 40 |
| 5.3 | Firmware..... | 41 |
| 5.4 | Versión Escáner Huella..... | 42 |
| 6 | MENÚ DEL SISTEMA 4 – BORRAR USUARIO..... | 45 |
| 6.1 | Borrar Usuario Individual..... | 45 |
| 6.2 | Borrar Todos los Usuarios..... | 45 |
| 7 | MENÚ DEL SISTEMA 5 – CONFIGURACIÓN DEL SISTEMA..... | 45 |
| 7.1 | Hora..... | 45 |
| 7.2 | Modo de funcionamiento..... | 46 |
| 7.2.1 | Establecer el Modo de Funcionamiento..... | 50 |
| 7.3 | Tiempo bloqueo Re..... | 53 |
| 7.4 | Dirección..... | 54 |
| 7.5 | Contraseña de comunicaciones..... | 54 |
| 7.6 | Código de Instalación..... | 57 |
| 7.7 | Reinicio del Sistema..... | 57 |
| 7.8 | Reinicialización de Eventos..... | 59 |
| 7.9 | Velocidad Com..... | 59 |
| 7.10 | Relé de Puerta..... | 60 |
| 7.11 | Dos Personas..... | 60 |
| 7.12 | Retropase..... | 61 |
| 7.13 | Coacción..... | 61 |
| 7.14 | Formato de fecha..... | 63 |
| 7.15 | Visualización personalizada..... | 64 |
| 7.16 | Iluminación de LCD..... | 67 |
| 7.17 | Ocultar PIN..... | 72 |
| 7.18 | Cierre..... | 73 |
| 7.19 | Asistencia..... | 75 |
| 7.20 | Configuración de red..... | 76 |

| | | |
|--------|--|----|
| 7.20.1 | Configuración Dirección IP Dispositivo | 76 |
| 7.21 | Eliminar Evento | 83 |
| 7.22 | Tipo Wiegand | 85 |
| 7.23 | Hora Wiegand..... | 85 |
| 8 | MENÚ DEL SISTEMA 6 – CONFIGURACIÓN DEL ESCANER | 89 |
| 8.1 | Re-Escaneado | 89 |
| 8.2 | Nivel | 89 |
| 8.3 | Condiciones de iluminación | 90 |
| 8.4 | Modo de registro..... | 90 |
| 9 | MENÚ DEL SISTEMA 7 – CONFIGURACIÓN DEL SENSOR | 93 |
| 9.1 | Tipo de entrada | 93 |
| 9.2 | Función | 93 |
| 9.3 | Fallo de línea | 95 |
| 10 | MENÚ DEL SISTEMA 8 – CONFIGURACIÓN DE ALARMAS..... | 76 |
| 10.1 | Configuración de Alarmas..... | 76 |
| 11 | GUÍA DE INSTALACIÓN | 82 |
| 11.1 | Diseño del conector | 82 |
| 11.2 | CN1: Conector de alimentación | 83 |
| 11.3 | CN2: Conector RRE (Wiegand)..... | 84 |
| 11.4 | CN3: Conector de relé | 85 |
| 11.5 | CN5: Conector RS232..... | 86 |
| 11.6 | CN5: Conexión Convertidor RS422..... | 87 |
| 11.6.1 | Red RS422..... | 88 |
| 11.7 | CN8: Conector de sensor..... | 89 |
| 11.8 | Diagrama de instalación | 89 |

Part



1 Introducción general



1.1 Introducción general

Rentable: Una solución integrada que combina un lector biométrico, un lector de proximidad y teclado para el control de acceso. BioScan reduce el coste por puerta de añadir la facilidad y seguridad de la tecnología de verificación de huella dactilar para sistemas de control de acceso.

Tecnología avanzada de sensores: Su capacidad de reconocer huellas dactilares incluso en condiciones adversas, por ejemplo con huellas sucias, hace que BioScan resulte de utilidad en fábricas, plantas, lugares de construcción y entornos similares que previamente no podían desarrollar soluciones de acceso basadas en la biometría.

CARACTERÍSTICAS

- Algoritmo de identificación de huellas líder del sector (1er puesto en Concurso de Verificación de Huellas Dactilares, FVC2004)
- Autenticación 1:1 e Identificación 1:Muchos en menos de 1 segundo (velocidad de procesamiento de 1 segundo por cada 1.000 plantillas)
- Registro de Huella Dactilar seleccionable doble o cuádruple para cada usuario
- Varios modos de seguridad: 11 modos de funcionamiento en total entre los que elegir
- Nombre de presentación de usuario personalizado y mensaje de pantalla en espera personalizado
- Pantalla LCD integrada de 32 caracteres y teclado numérico de 16 posiciones retroiluminado
- Menú incorporado configurable 6 entradas / 2 salidas de Transmisión
- Módulo de Transmisión Remota Externo Opcional para mayor protección de seguridad
- Disponibilidad de puerto de lector externo para funcionalidad de retopase
- Comunicación Individual/de red vía RS232/RS422/TCP/IP
- Interfaz doble de Control de Acceso y software de Horario & Asistencia
- 512 husos horarios
- 365 Vacaciones

ESPECIFICACIONES

CONTROLADOR

| | |
|------------------------------------|---|
| Registro de usuario: | 4,096 Tarjetas / 1.910 Huellas |
| Buffer operaciones: | 16.000 Transacciones con definición de acceso completa |
| Comunicaciones: | Estándar: Wiegand estándar 26-bit y RS232 Opcional: RS422 / RS485 / Ethernet |
| indicador: | LED de estado de 3 colores con zumbador/timbre |
| Requisitos de alimentación: | 12V DC 1A |
| Caract. Físicas: | Dimensiones: H125 * W125 * D22mm Material: ABS (Policarbonato) |
| Ambientales: | Temperatura: -0° ~50° Humedad: 10%~90% |
| Entradas & Salidas: | 6 entradas y 2 salidas, personalizables Opcional: Módulo de Transmisión Remota |

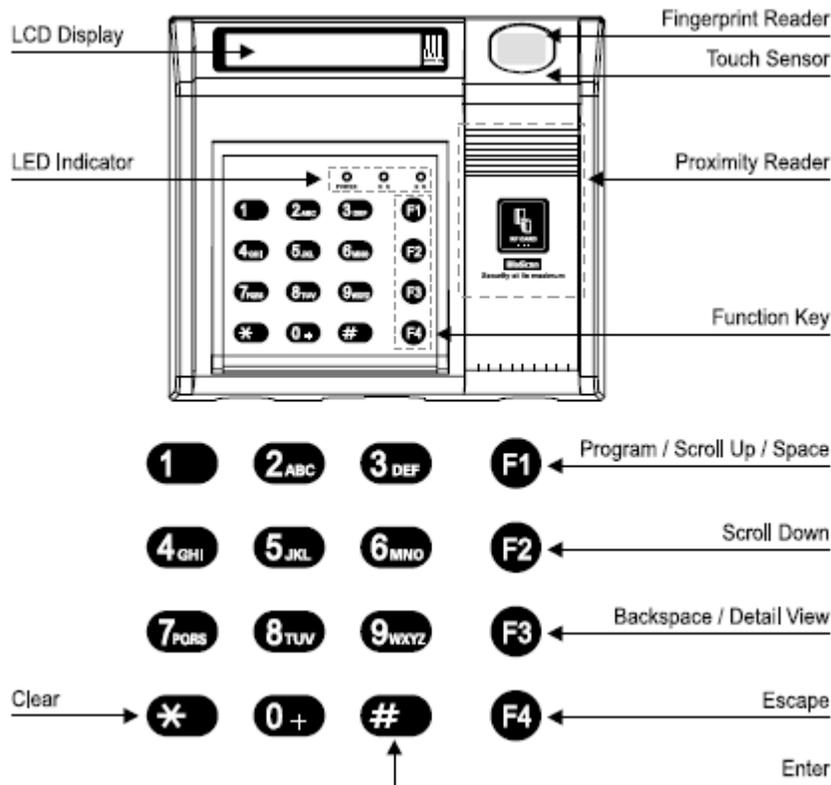
SENSOR HUELLA DACTILAR

| | |
|--------------------------|--|
| CPU: | DSP 400 MHz |
| Memoria Flash: | 1 MB / 4MB |
| FAR | 0.00008% |
| FRR | 0.09% |
| Tamaño plantilla: | 256 ~ 384 Bytes (configurable, predeterminado 384 Bytes) |
| Codificación: | AES 256 bit |
| Tamaño: | 55 x 40 x 8 mm (L x A x Al) |
| Tipo sensor: | Óptico |
| Resolución: | 500 (dpi) |
| Área sensorial: | 16.0 x 19.0 (mm) |
| Tamaño imagen: | 280 x 320 (píxel) |

MÓDULO DE TARJETA

| | |
|-------------------------------------|---------------------|
| Tipo de Lector: | EM / HID / Mifare |
| Tipo de antena: | Bobina |
| Frecuencia: | 125 KHz / 13.56MHz |
| Tipo de frecuencia de radio: | A1D |
| Tipo de comunicaciones: | Tipo individual |
| Tipo de modulación: | Amplitud Modulación |
| Dimensiones de antena: | 45x55mm |
| Interfaz conexión antena: | Fijo |

1.2 Acerca de BSC



1.3 Utilización del Escáner de Huella Dactilar

¿Cuánto hay que presionar para obtener una huella dactilar de buena calidad?

Si se aplica demasiada presión sobre la ventana del sensor, las líneas se pegan unas a otras y hacen que sean indistinguibles. En este caso, el efecto neto es parecido a la dificultad de encontrar detalles minuciosos en la imagen de una huella dactilar mojada. Por el contrario, si se aplica demasiada poca presión, la imagen resultante es parecida a una huella dactilar seca. No obstante, los temas relacionados con la presión son fácilmente resolubles. Todo lo que se necesita es un poco de práctica para que los usuarios se acostumbren. Tocar el sensor como si se estuviera pulsando un botón crea una imagen a la que le faltan datos ricos en información de las huellas dactilares.

1. **Posición:** Si se coloca el dedo alejado del centro del sensor, esto aumenta el índice de rechazos. Los surcos del dedo deben estar en contacto con el sensor de tacto para activar el sensor de huella. El sensor de tacto está ubicado justo debajo del área sensorial.
2. **Rotación:** La rotación del dedo debe mantenerse al mínimo durante el registro y la verificación.
3. **Presión:** Aplicar una presión moderada al hacer contacto con el sensor. Demasiada presión puede provocar que se emborrone la huella dactilar. Demasiada poca presión puede que no permita al sensor reconocer la presencia del dedo. La presión ideal es similar a la que se ejerce para sostener firmemente un bolígrafo.



Posición del dedo

Para capturar el mayor número de datos, maximice la zona de superficie de la huella dactilar sobre la ventana de entrada de la huella, cubriendo el sensor completamente. Es correcto que la punta del dedo se extienda más allá del sensor para que la huella dactilar quede centrada. Durante el proceso de captura, aplique una presión ligera y de forma pareja, sin moverlo. La **Figura2** muestra la posición correcta de la huella dactilar sobre la ventana de entrada. La **Figura1** muestra los errores más comunes que se producen durante la fase inicial del registro.

Cuando la luz **Roja** (Escáner de Huella digital) esté encendida, pase el dedo por el escáner.

1. Coloque el dedo de forma que la primera unión del dedo coincida con el borde del sensor.
2. Baje el dedo sobre el sensor y presione ligeramente.
3. Mantenga el dedo sobre el sensor hasta que se apague la luz **Roja** (escáner de huella digital). Ahora puede retirar el dedo

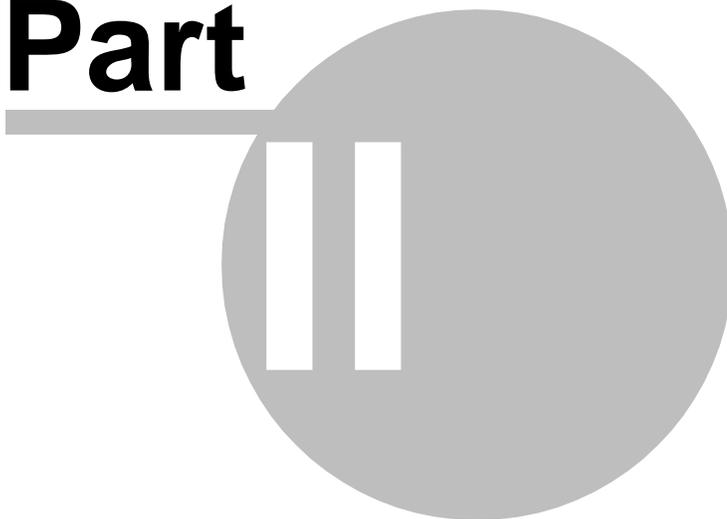
Conseguir buenas imágenes de huellas dactilares

La calidad de una imagen de huella dactilar depende del número de datos minuciosos que se capturen. Si el número y las posiciones de los datos minuciosos son uniformes cuando se escanea y se captura la imagen de la huella dactilar de una persona, la imagen de la huella dactilar coincidirá con la plantilla del dedo que se tenga registrado. Las imágenes de huellas dactilares que no contengan datos minuciosos adecuados no son aceptables como credencial personal y, por tanto, no son válidas. La Figura 3 muestra huellas dactilares de mala calidad, caracterizadas por zonas borrosas, desvaídas o en cualquier caso distorsionadas en la huella dactilar.

Estas condiciones se pueden atribuir a diversos factores, incluyendo una sequedad excesiva o piel húmeda o a cicatrices.

1. Utilice los dedos índice, medio o anular
2. Evite utilizar los dedos pulgar y meñique, ya que resultan difíciles de colocar de forma uniforme sobre el sensor.
3. El mejor funcionamiento se producirá cuando se cubra completamente la zona del sensor con la huella dactilar.

Part



2 Inicio rápido

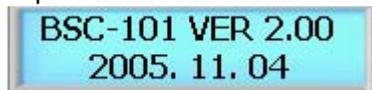
2.1 Lista de comprobación de preinstalación

- Asegúrese de que se han comprobado todos los cables.
- Compruebe el módulo de comunicaciones. Existen diversos tipos de comunicaciones, RS232 / RS422 / Ethernet. Asegúrese de que tiene los módulos de comunicaciones correctos.
- Si está utilizando un convertidor, asegúrese de que TX y RX están cruzados entre el dispositivo y el convertidor.
- Establezca la dirección de red. De forma predeterminada, todos los dispositivos tienen la dirección 1. Si está conectando 2 o más, cambie la dirección de red a 2 y siguientes.
- Si está utilizando tarjetas, defina el código del sitio, conocido también como código de la instalación. Todos los productos IDTi admiten HID Standard 26bit, HID Full 26bit, HID 34bit, Mifare 32bit y EM Standard 26bit.

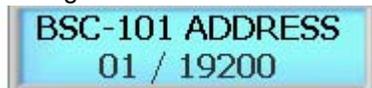
2.2 Secuencia de arranque



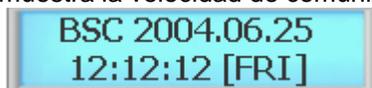
La primera ventana muestra los derechos de autor.



La segunda ventana muestra el número de versión del firmware y su fecha.



Muestra el parámetro de la dirección de red del BSC-101 a la derecha, y a la izquierda muestra la velocidad de comunicación.



La cuarta ventana muestra el dispositivo en posición de espera. A partir de este punto, el dispositivo está completamente operacional.

2.3 Entrada en el Menú del Sistema

Cuando se enciende el lector sin que haya plantillas de huellas dactilares registradas en la unidad, cualquiera puede entrar en el menú del sistema pulsando la tecla F1/p. Si está registrando la primera plantilla de administrador a través del teclado del lector, primero debe determinar el PIN de 1~16 dígitos que utilizará el administrador. Una vez determinado este PIN, el administrador debe estar presente para registrar la huella dactilar en el lector. Tenga en cuenta que esta operación no es válida si ya hay plantillas de administrador en el lector.

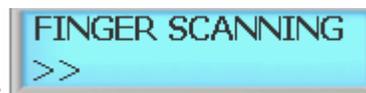
 **NOTE :**

El valor predeterminado de fábrica de BioScan no tiene contraseña de administrador del sistema. Si acaba de adquirir la unidad, debe poder acceder al modo del sistema pulsando la tecla F1. Vaya a Registrar Usuario de Huella Dactilar para registrar una plantilla.

2.3.1 Si ya hay registrado Administrador



1 Pulse la tecla F1/P para entrar en el modo sistema.



4 Aparecerá el mensaje de escaneado de dedo



2 Teclee el ID de administrador, seguido de la tecla #



5 Ahora está en el modo sistema. Pulse la tecla F1 para desplazarse hacia arriba por el menú principal. Pulse la tecla F2 para desplazarse hacia abajo por el menú principal



3 Presente el dedo o la tarjeta, dependiendo de lo que haya registrado el administrador. Por ahora, utilizaremos la huella dactilar

2.3.2 Si todavía no hay registrado Administrador

2.4 Funcionamiento del BioScan

Para usar el BioScan, simplemente introduzca la huella dactilar registrada de un usuario en el escáner. El sensor de tacto activará automáticamente el sensor de huella dactilar cuando el dedo del usuario se coloque en el escáner. Quite el dedo cuando se apague la luz **roja** del escaneado.

En el BioScan existen 11 modos de funcionamiento y, dependiendo del modo que se esté ejecutando, el funcionamiento de BioScan varía.

2.4.1 Funcionamiento con PIN de Usuario



1 Desde el menú en espera, teclee el PIN de usuario y pulse la tecla #.

3 Si la verificación es correcta, aparecerá el mensaje de bienvenida.



2 Introduzca el PIN de usuario y pulse la tecla #.

2.4.2 Funcionamiento con TARJETA de Usuario



1 Desde el menú en espera, pase la tarjeta de usuario por el lector.



2 Si la verificación es correcta, aparecerá el mensaje de bienvenida.

2.4.3 Funcionamiento con HUELLA DACTILAR de Usuario



1 Desde el menú en espera, coloque la huella dactilar del usuario en el escáner. Si el escáner no se pone en marcha, pulse manualmente la tecla # para activarlo.



3 Si la verificación es correcta, aparecerá el mensaje de bienvenida.



FINGER SCANNING
>>

2 Introduzca la huella dactilar del usuario en el escáner.

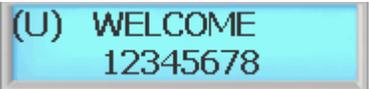
2.4.4 Funcionamiento con PIN & HUELLA DACTILAR

2.4.5 Funcionamiento con TARJETA & HUELLA DACTILAR



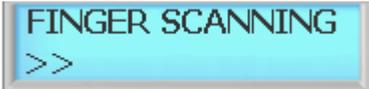
BSC 2004.06.25
12:12:12 [FRI]

1 Desde el menú en espera, pase la tarjeta de usuario por el lector. Una vez verificada la tarjeta, parpadeará la luz roja del escáner de huella dactilar.



(U) WELCOME
12345678

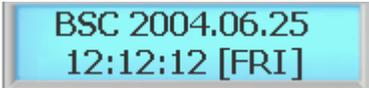
3 Si la verificación es correcta, aparecerá el mensaje de bienvenida.



FINGER SCANNING
>>

2 Introduzca la huella dactilar del usuario en el escáner.

2.4.6 Funcionamiento con PIN & TARJETA



BSC 2004.06.25
12:12:12 [FRI]

1 Desde el menú en espera, teclee el PIN de usuario y pulse la tecla #.

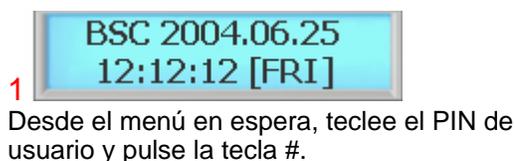


PRESENT CARD

3 Pase la Tarjeta de usuario por el lector.



2.4.7 Funcionamiento con PIN & HUELLA DACTILAR

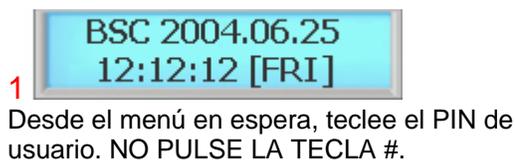


2.5 Funcionamiento de la Tecla de Funciones

Para usar el BioScan, simplemente introduzca la huella dactilar registrada de un usuario en el escáner. El sensor táctil activará el escáner cuando el dedo del usuario se coloque sobre el escáner. Quite el dedo cuando se apague la luz del escaneado.

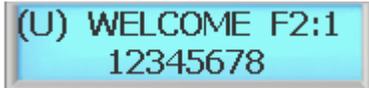
En el BioScan existen 11 modos de funcionamiento y, dependiendo del modo que se esté ejecutando, el funcionamiento de BioScan varía.

2.5.1 Funcionamiento de la Tecla de Función con PIN





2 Una vez introducido el PIN, pulse la tecla de función.

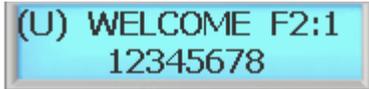


4 Si la verificación es correcta, aparecerá el mensaje de bienvenida con la tecla de función.

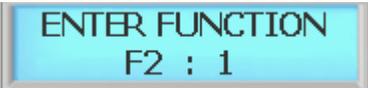
2.5.2 Funcionamiento de la Tecla de Función con TARJETA



1 Desde el menú en espera, pase la tarjeta de usuario por el lector.

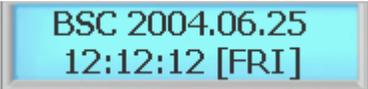


3 Si la verificación es correcta, aparecerá el mensaje de bienvenida con la tecla de función.

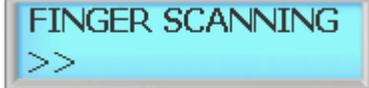


2 Introduzca la tecla de función y, a continuación, presente la tarjeta de usuario.

2.5.3 Funcionamiento de la Tecla de Función con HUELLA DACTILAR



1 Desde el menú en espera, pulse la tecla de función.

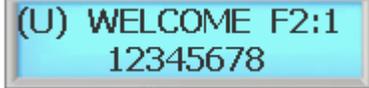


Introduzca la huella dactilar del usuario

3 en el escáner.



2 Introduzca la tecla de función y, a continuación, presente la huella dactilar del usuario.



3 Si la verificación es correcta, aparecerá el mensaje de bienvenida con la tecla de función.

2.5.4 Funcionamiento de la Tecla de Función con TARJETA y HUELLA DACTILAR

1

Desde el menú en espera, teclee la tecla de función.



3 Introduzca la huella dactilar del usuario en el escáner.



2 Pulse la tecla de función y, a continuación, presente la tarjeta de usuario.

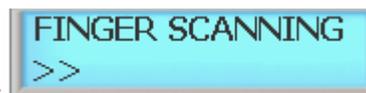


4 Si la verificación es correcta, aparecerá el mensaje de bienvenida con la tecla de función.

2.5.5 Funcionamiento de la Tecla de Función con PIN & HUELLA DACTILAR



1 Desde el menú en espera, teclee el PIN de usuario. NO PULSE LA TECLA #.



4 Introduzca la huella dactilar del usuario en el escáner.



2 Introduzca el PIN de usuario, pero no pulse la tecla #. Una vez introducido el PIN de usuario, introduzca la tecla de función.



5 Si la verificación es correcta, aparecerá el mensaje de bienvenida con la tecla de función.

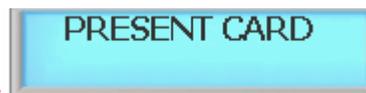


3 Pulse la tecla de función. Introduzca la huella dactilar del usuario.

2.5.6 Funcionamiento de la Tecla de Función con PIN y TARJETA



1 Desde el menú en espera, teclee el PIN de usuario. NO PULSE LA TECLA #.



4 Pase la Tarjeta de usuario por el lector.



2 Introduzca el PIN de usuario, pero no pulse la tecla #.



5

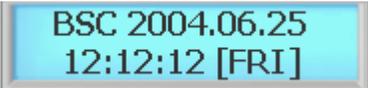
Si la verificación es correcta, aparecerá el mensaje de bienvenida con la tecla de función.



ENTER FUNCTION
F2 : 1

3 Pulse la tecla de función y, a continuación, introduzca la huella dactilar del usuario

2.5.7 Funcionamiento de la Tecla de Función con PIN & TARJETA & HUELLA DACTILAR



BSC 2004.06.25
12:12:12 [FRI]

1 Desde el menú en espera, teclee el PIN de usuario. NO PULSE LA TECLA #.



ENTER USER ID
12345678

2 Introduzca el PIN de usuario, pero no pulse la tecla #.



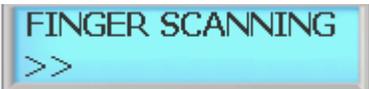
ENTER FUNCTION
F2 : 1

3 Pulse la tecla de función y, a continuación, presente la Tarjeta de usuario.



PRESENT CARD

4 Pase la Tarjeta de usuario por el lector. Parpadeará la luz roja del escáner de huella dactilar.



FINGER SCANNING
>>

5 Introduzca la huella dactilar del usuario en el escáner.



(U) WELCOME
12345678

6 Si la verificación es correcta, aparecerá el mensaje de bienvenida.

Top Level Intro

This page is printed before a new
top-level chapter starts

Part



3 MENÚ DEL SISTEMA 1 – REGISTRAR USUARIO

3.1 Registrar Usuario de Huella Dactilar

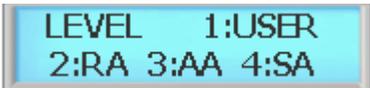
Este comando se utiliza para añadir al lector a los típicos usuarios de sólo huella dactilar, para que puedan entrar al recinto protegido por el lector. En el lector de huella dactilar se pueden guardar hasta 955 usuarios o un total de 1.910 plantillas de huellas digitales, incluyendo las plantillas de huellas digitales administrativas, dependiendo del modelo de lector que tenga. El número total de usuarios depende de cuantas plantillas se apliquen a cada usuario. Esta acción se realiza con la siguiente secuencia de teclas:

1 

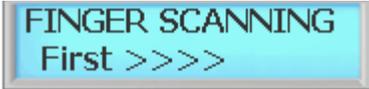
Pulse la tecla # para añadir Plantilla de Huella Digital de usuarios

5 

BioScan tiene una opción para registrar 2 plantillas de huella digital o 4 plantillas de huella digital por cada usuario. Por ahora, seleccionaremos la tecla 2 para registrar 4 plantillas

2 

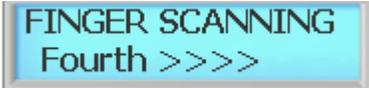
Seleccione el nivel de usuario usando del 1 al 4. Consulte la NOTA acerca de los niveles de usuario

6 

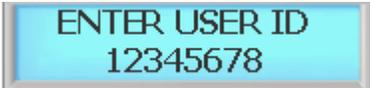
Coloque el primer dedo en el escáner. Quite el dedo cuando se apague la luz roja. Tras la primera, puede volver a registrar la misma huella digital u otra distinta. Repita este proceso hasta registrar la última huella digital

3 

Teclee el ID de usuario, de 1 a 16 dígitos, como se muestra en la siguiente figura

7 

Escaneando la última huella dactilar....

4 

Teclee el ID de usuario, seguido de la tecla #

8 

Registro finalizado. Pulse la tecla # para continuar registrando otra huella dactilar de usuario o pulse cualquier otra para salir del submenú.

Cuando la luz **Roja** (Escáner de Huella digital) esté encendida, pase el dedo por el escáner.

1. Coloque el dedo de forma que la primera unión del dedo coincida con el borde del sensor.
2. Baje el dedo sobre el sensor y presione ligeramente.
3. Mantenga el dedo sobre el sensor hasta que se apague la luz **Roja** (escáner de huella digital). Ahora puede retirar el dedo.
 - Utilice los dedos índice, medio o anular.
 - Evite utilizar el dedo meñique, ya que resulta difícil de colocar de forma uniforme sobre el sensor.
 - El mejor funcionamiento se producirá cuando se cubra completamente la zona del sensor.

NOTE :

Existen cuatro niveles de administración,

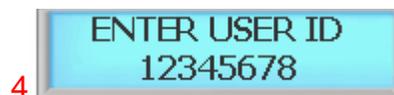
1. **1:USUARIO (Nivel 1)** - Corresponde a un usuario normal. Se pueden verificar, pero no pueden acceder a ninguna función administrativa.
2. **2: RA (Nivel 2)** - Corresponde a un registrador o grabador. Estas plantillas permiten añadir usuarios al sistema y comprobar los usuarios existentes. No obstante, sólo pueden añadir usuarios sin privilegios administrativos (Nivel 1) y no pueden acceder a ninguna otra función administrativa.
3. **AA (Nivel 3)** - Corresponde a un registrador administrador. Estas plantillas permiten añadir administradores de registradores (Nivel 3) pero no administrador del sistema.
4. **SA (Nivel 4)** - Éste es el nivel del administrador del sistema y tiene plenos derechos para configurar el lector.

3.2 Registrar usuario de tarjeta

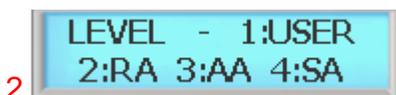
Este comando se utiliza para añadir al lector a los típicos usuarios de sólo tarjeta, para que puedan entrar al recinto protegido por el lector. El número total de usuarios de sólo tarjeta es de 4.096. Si en el sistema hay registrados 500 usuarios de huella dactilar, entonces el número de ranuras para usuarios de tarjeta que queda disponible en el sistema será de 3.596. Los usuarios de huellas dactilares reciben automáticamente una ranura de tarjeta en la memoria del sistema, incluso si no utilizan o registran una tarjeta. El procedimiento de registro es idéntico al de añadir una huella dactilar. Esta acción se realiza con la siguiente secuencia de teclas:



1 Pulse la tecla # para añadir tarjeta de usuario



4 Teclee el ID de usuario, seguido de la tecla #



2 Seleccione el nivel de usuario usando del

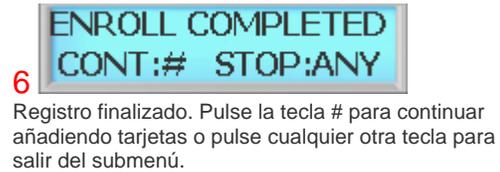
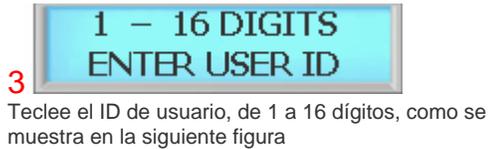


1 al 4

5

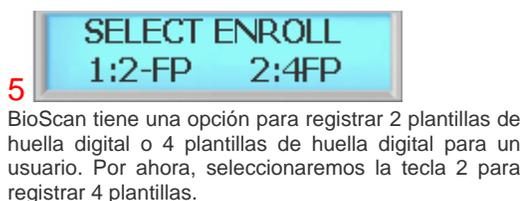
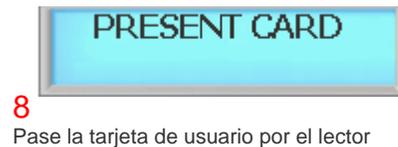
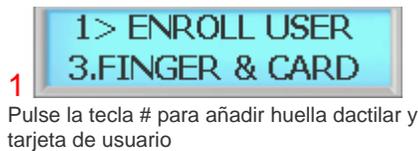
Pase la tarjeta por el lector o teclee manualmente el

número de la tarjeta, seguido de la tecla #



3.3 Registrar Usuario de Tarjeta & Huella Dactilar

Este comando se utiliza para añadir al lector a los usuarios típicos de huella dactilar y tarjeta, para que puedan entrar al recinto protegido por el lector. Esta acción se realiza con la siguiente secuencia de teclas:





3.4 Registrar Bloque de Tarjetas de Usuario

Este comando se utiliza para Registrar un conjunto de tarjetas. La mejor utilización del Registro en bloque de un rango de número de tarjetas se realiza cuando hay una gran cantidad de tarjetas o credenciales cuyos números de ID son secuenciales. Las tarjetas o credenciales no tienen que estar físicamente a mano cuando se registran utilizando el registro en bloque mediante el proceso de grupo de número de tarjetas, pero es necesario disponer del código de la instalación. A continuación se muestra un ejemplo para registrar 100 usuarios cuyo número de tarjeta comienzan en el número 1000. Al ID de Usuario 1000 se le asignará el número de tarjeta 1000, al ID de Usuario 1001 se le asignará el número de tarjeta 1001, etc. Las tarjetas deben ir en orden secuencial para utilizar el Bloque de Tarjetas. Para obtener más información, por favor consulte con su proveedor de tarjetas.

1 1> ENROLL USER
4.CARD BLOCK

Pulse la tecla # para añadir bloque de usuarios de tarjeta.

6 REG. USER NUM

Aparecerá el siguiente mensaje. Introduzca el número total de tarjetas que se van a registrar como se indica a continuación

2 START USER ID

Introduzca el primer número de ID del bloque. Esto será el primer número de ID de la tarjeta como se muestra en la siguiente figura

7 USER COUNT
100

En total se van a registrar 100 tarjetas

3 ENTER USER ID
1000

1000 sería el primer número de ID de usuario

8 ENROLL USER 0001
>>>

Registro de bloque de tarjetas de usuario. Por favor espere hasta que termine el proceso. Esto puede requerir hasta 5 minutos, dependiendo del número total existente en el bloque de tarjetas.

4 START USER CARD

Aparecerá el siguiente mensaje. Introduzca el primer número de tarjeta como se muestra a continuación

9 ENROLL COMPLETED
CONT:# STOP:ANY

Registro finalizado. Pulse la tecla # para continuar añadiendo o pulse cualquier otra para salir del submenú.

5 USER CARD
1000

1000 será el primer número de la tarjeta

NOTE :

Esta opción escribe el bloque de tarjetas en un hueco vacío de la memoria y no borra a los usuarios actualmente registrados. El Bloque de Tarjetas 1 requiere más tiempo que el bloque de tarjetas 2 ya

que tiene que buscar huecos vacíos en la memoria para registrarlos. Utilice el bloque de tarjetas 2 si la memoria está vacía o ya no necesita los datos almacenados.

| | Inicio | | | | Fin | |
|-------------------|--------------|--------------|--------------|--------------|--------------|--------------|
| ID Usuario | ID Usuario 1 | ID Usuario 2 | ID Usuario 3 | ID Usuario 4 | Usuario ID5 | ID Usuario 6 |
| # Tarjeta | Tarjeta # 10 | Tarjeta # 11 | Tarjeta # 12 | Tarjeta # 13 | Tarjeta # 14 | Tarjeta # 15 |
| Sistema | No utilizado | En uso | No utilizado | En uso | No utilizado | No utilizado |
| Memoria | | | | | | |
| Resultado | Sí | No | Sí | No | Sí | Sí |

En este caso sólo se grabarán 4 ID de usuario y 4 tarjetas en el sistema aunque hay registrados 6 usuarios y 6 tarjetas para utilizar el Bloque de Tarjetas. Al utilizar el bloque de tarjetas, el sistema agrupará el ID de usuario y el número de tarjeta juntos. De forma que si el ID de Usuario ya está siendo utilizado en el sistema, la tarjeta correspondiente a ese id de usuario no se grabará y quedará fuera.

3.5 Registrar Bloque de Tarjetas de Usuario 2

Este comando se utiliza para Registrar un conjunto de tarjetas. La mejor utilización del Registro en bloque de un rango de número de tarjetas se realiza cuando hay una gran cantidad de tarjetas o credenciales cuyos números de ID son secuenciales. Las tarjetas o credenciales no tienen que estar físicamente a mano cuando se registran utilizando el registro en bloque mediante el proceso de grupo de número de tarjetas, pero es necesario disponer del código de la instalación. A continuación se muestra un ejemplo para registrar 100 usuarios cuyo número de tarjeta comienzan en el número 1000. Al ID de Usuario 1000 se le asignará el número de tarjeta 1000, al ID de Usuario 1001 se le asignará el número de tarjeta 1001, etc.



1 Pulse la tecla # para añadir bloque de usuarios de tarjeta.

6 Aparecerá el siguiente mensaje. Introduzca el número total de tarjetas que se van a registrar como se indica a continuación



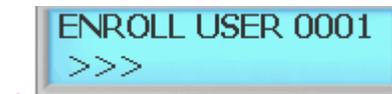
2 Introduzca el primer número de ID del bloque. Esto será el primer número de ID de la tarjeta como se muestra en la siguiente figura



7 En total se van a registrar 100 tarjetas



3 1000 sería el primer número de ID de usuario



8 Registro de bloque de tarjetas de usuario. Por favor espere hasta que termine el proceso. Esto puede requerir hasta 5 minutos, dependiendo del número total existente en el bloque de tarjetas.

A rectangular screen with a light blue background and a black border. The text "START USER CARD" is centered in black, uppercase letters.

4 Aparecerá el siguiente mensaje. Introduzca el primer número de tarjeta como se muestra a continuación

A rectangular screen with a light blue background and a black border. The text "ENROLL COMPLETED" is on the top line and "CONT:# STOP:ANY" is on the bottom line, both in black, uppercase letters.

9 Registro finalizado. Pulse la tecla # para continuar añadiendo o pulse cualquier otra para salir del submenú.

A rectangular screen with a light blue background and a black border. The text "USER CARD" is on the top line and "1000" is on the bottom line, both in black, uppercase letters.

5 1000 será el primer número de la tarjeta

 **NOTE :**

Esta opción escribirá el bloque de tarjetas sin comprobar los huecos en la memoria y borrará los usuarios registrados actualmente. El ID de Usuario existente será reemplazado por Tarjeta y si había registradas huellas dactilares, éstas también se borrarán. El Bloque de Tarjetas 1 requiere más tiempo que el bloque de tarjetas 2 ya que tiene que buscar huecos vacíos en la memoria para registrarlos. Utilice el bloque de tarjetas 2 si la memoria está vacía o ya no necesita los datos almacenados.

Part

IV

4 MENÚ DEL SISTEMA 2 – MODIFICAR USUARIO

4.1 Modificar ID de Usuario

Este comando se utiliza para modificar los ID de usuario existentes accediendo a dicho ID de usuario. Al realizar modificaciones, los administradores sólo pueden realizar cambios al ID de usuario en este menú.



1 Pulse la tecla # para entrar en modificación de ID de usuario



3 Teclee el nuevo ID de usuario, seguido de la tecla #



2 Teclee el ID de usuario que desea modificar, seguido de la tecla #



4 Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.

4.2 Modificar la Huella Dactilar del Usuario

Este comando se utiliza para modificar una Huella Dactilar de usuario existente accediendo a dicho ID de usuario. Al realizar modificaciones, los administradores sólo pueden realizar cambios en la Huella Dactilar de usuario en este menú.



1 Pulse la tecla # para introducir DEDO de usuario



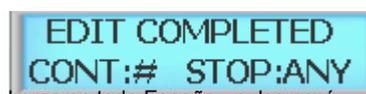
4 Introduzca la primera huella dactilar. Tras la primera, puede añadir la misma huella digital u otra distinta. Repita este proceso hasta registrar la cuarta huella digital.



2 Teclee el ID de usuario que desea modificar, seguido de la tecla #



5 Escaneando el último dedo





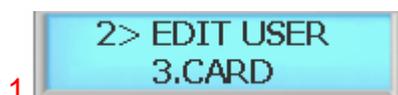
Pulse 1 para añadir 2 plantillas
Pulse 2 para añadir 4 plantillas

6

Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.

4.3 Modificar Tarjeta de Usuario

Este comando se utiliza para modificar una Tarjeta de usuario existente accediendo a dicho ID de usuario. Al realizar modificaciones, los administradores sólo pueden realizar cambios en la Tarjeta de usuario en este menú.



Pulse la tecla # para entrar en modificación de Tarjeta de usuario



Pase la nueva tarjeta que va a registrar o teclee manualmente el número de la tarjeta, seguido de la tecla #. Asegúrese de que la tarjeta no está ya registrada en el BioScan



Teclee el ID de usuario que desea modificar, seguido de la tecla #



Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.

4.4 Modificar el Nivel de Usuario

Este comando se utiliza para modificar el nivel de usuario existente accediendo a dicho ID de usuario. Los niveles de usuario determinan los lugares de validez del usuario. Para modificar el nivel de un usuario existente, siga los siguientes pasos.



Pulse la tecla # para entrar en modificación de NIVEL de usuario



(U) es el nivel actual del usuario. Seleccione el nivel de usuario de 1-4 para aplicar el nuevo nivel.



Teclee el ID de usuario que desea modificar, seguido de la tecla #

4 Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.

! NOTE :

Existen cuatro niveles de administración,

1. **1:USUARIO (Nivel 1)** - Corresponde a un usuario normal. Se pueden verificar, pero no pueden acceder a ninguna función administrativa.
2. **2: RA (Nivel 2)** - Corresponde a un registrador o grabador. Estas plantillas permiten añadir usuarios al sistema y comprobar los usuarios existentes. No obstante, sólo pueden añadir usuarios sin privilegios administrativos (Nivel 1) y no pueden acceder a ninguna otra función administrativa.
3. **AA (Nivel 3)** - Corresponde a un registrador administrador. Estas plantillas permiten añadir administradores de registradores (Nivel 3) pero no administrador del sistema.
4. **SA (Nivel 4)** - Éste es el nivel del administrador del sistema y tiene plenos derechos para configurar el lector.

4.5 Modificar el Nombre de Usuario

Al acceder, BioScan puede mostrar un nombre de usuario personalizado en lugar del ID de usuario. Cuando el BioScan espera un nombre, las teclas de número del teclado se convierten en teclas de letras: se aplican las letras bajo las teclas. Pulse una vez para mostrar la primera letra de encima de la tecla en mayúsculas; pulse cuatro veces para mostrar la letra en minúsculas. Cuando aparezca la letra deseada en la pantalla, pulse el indicador flecha arriba (F1) para pasar a la siguiente letra del nombre.



Pulse la tecla # para introducir NOMBRE



Pulse la tecla # para continuar modificando la opción de presentación. La opción de presentación debe ser configurada para que funcione adecuadamente



Teclee el ID de usuario que desea modificar, seguido de la tecla #



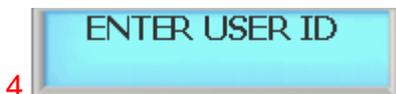
Una vez más, vuelva a introducir el mismo ID que acaba de modificar previamente



Pulse la tecla 1 para introducir el nombre de usuario



Esta vez seleccione #2 para introducir opción de presentación



Teclee el texto como se indica en la siguiente figura. Continúe pulsando la tecla para cambiar de mayúsculas a minúsculas. es decir, para mostrar la



"c" minúscula, pulse la tecla 2 seis veces. Utilice la tecla F1 como espacio

9
Seleccione #2 para mostrar el ID por nombre. Esto permite a

BioScan presentar nombre personalizado de ID en lugar del ID de usuario



5
Teclee el nombre de presentación adecuado y luego pulse la tecla #

10
Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.



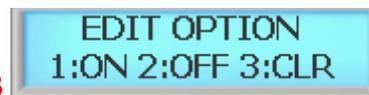
| TECLAS | NÚMERO DE VECES QUE SE PULSA UNA TECLA | | | | | | | |
|--------|--|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | | | | | | | | |
| 2 | A | B | C | a | b | c | | |
| 3 | D | E | F | d | e | f | | |
| 4 | G | H | I | g | h | i | | |
| 5 | J | K | L | j | k | l | | |
| 6 | M | N | O | m | n | o | | |
| 7 | P | Q | R | S | p | q | r | s |
| 8 | T | U | V | t | u | v | | |
| 9 | W | X | Y | Z | w | x | y | z |
| 0 | | | | | | | | |
| * | Borrar | | | | | | | |
| # | Intro | | | | | | | |
| F1 | Espacio | | | | | | | |
| F2 | | | | | | | | |
| F3 | Atrás | | | | | | | |
| F4 | Escape | | | | | | | |

4.6 Retropase de usuario

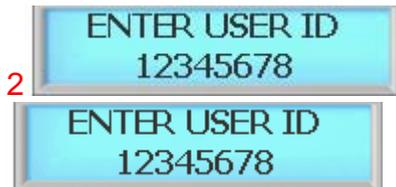
El retropase se utiliza para impedir que dos personas utilicen una sola tarjeta para acceder. Esta función está diseñada para proteger contra dos personas que van a "rebufo". Una vez que se concede el acceso en un lector de ENTRADA, debe presentarse a un lector de SALIDA antes de que otro lector de ENTRADA conceda el acceso. En el caso de que el usuario no pase la tarjeta por un lector de ENTRADA, e intentara salir de una zona, se produciría una violación de retropase. La violación puede simplemente registrar el evento como una condición de alarma, o no permitir que la puerta se abra. Los usuarios que no realizan la lectura de ENTRADA y entran con otros empleados pueden quedar atrapados o encerrados. Debe activarse el Retropase del Sistema para que el Retropase de Usuarios funcione correctamente.



1 Pulse la tecla # para entrar en RETROPASE USUARIO



3 Pulse la tecla 1 para habilitar el retropase
 Pulse la tecla 2 para deshabilitar el retropase
 Pulse la tecla 3 para perdonarlo
 Consulte la NOTA para quitar el retropase



Introduzca ID de usuario en que aplicar retropase



Modificación finalizada. Pulse la tecla # para continuar añadiendo otra huella dactilar de usuario o pulse cualquier otra para salir del submenú.

El retropase debe habilitarse en los parámetros del sistema. Antes de habilitar el retropase en los parámetros de usuario, vaya al menú principal a 5.SYSTEM SETTING/submenú 12.ANTI PASS y habilite el retropase para el sistema

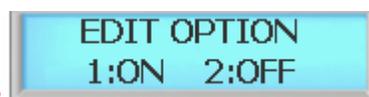
Cuando el sistema detecte un usuario de retropase, el usuario no podrá acceder a ese lugar. El administrador debe quitar a esa persona del retropase entrando en la opción de modificación y reiniciando el retropase seleccionando la opción 3(CLR) de perdón.

4.7 Opción (ID)

Opción ID es un modo especial en el que un usuario puede acceder a la unidad sólo con ID. Cuando se aplica, el usuario puede anular el modo de funcionamiento actual y acceder a la unidad simplemente con un ID (PIN). Esta opción se puede aplicar a aquellos usuarios que no tengan tarjeta. Para aplicar este modo al usuario, siga los siguientes pasos.



Pulse la tecla # para entrar en OPCIÓN (ID)



Pulse la tecla 1 para habilitar la opción ID a este usuario
Pulse la tecla 2 para deshabilitar la opción ID a este usuario



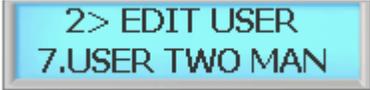
Introduzca ID usuario para aplicar opción ID seguido de tecla #



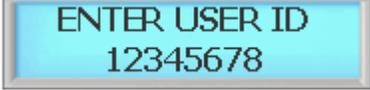
Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.

4.8 Usuario Dos Personas

Este comando impide que un usuario individual entre en una zona de seguridad vacía seleccionada a menos que esté presente otro usuario registrado. Una vez que se registren en la zona los dos usuarios registrados, otro usuario podrá ir y venir individualmente, siempre que haya al menos dos personas en la zona. A la inversa, al salir, los dos últimos ocupantes de la zona de seguridad deben salir juntos. El sistema no permitirá en ningún momento que haya menos de dos usuarios en la zona.

1 

Pulse la tecla # para entrar en USUARIO DOS PERSONAS

2 

Introduzca ID usuario para aplicar función Dos Personas seguido de la tecla.

3 

Pulse 1 para habilitar dos personas a este usuario
Pulse 2 para deshabilitar dos personas a este usuario

4 

Modificación finalizada. Pulse la tecla # para continuar modificando o pulse cualquier otra para salir del submenú.

 **NOTE :**

Dos Personas debe habilitarse en los parámetros del sistema. Tras habilitar la opción Usuario Dos Personas, vaya al menú principal 5.PARÁMETROS SISTEMA / submenú 13.DOS PERSONAS y habilite DOS PERSONAS para el sistema.

Part 5

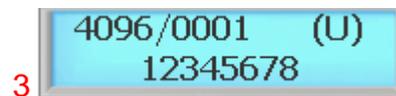
5 MENÚ DEL SISTEMA 3 – VER USUARIO

5.1 Lista de usuarios

En cualquier momento se puede ver una lista de todos los usuarios del sistema. La lista puede ser una lista del conjunto de registros de todos los usuarios del sistema, o puede ser una lista de los usuarios individuales que están físicamente registrados en cualquier lector de huellas digitales individual. El número total de usuarios basado en usuarios de tarjeta es de 4.096. El número total de usuarios de huella de dactilar depende de cuantas plantillas se apliquen a cada usuario.



1 Pulse la tecla # para entrar en ver LISTA USUARIOS



3 Pulse la tecla F3 para ver la vista detallada de usuario



2 Pulse la tecla F1/P para desplazarse por la lista de usuarios
Pulse la tecla F2 para desplazarse hacia abajo por la lista de usuarios



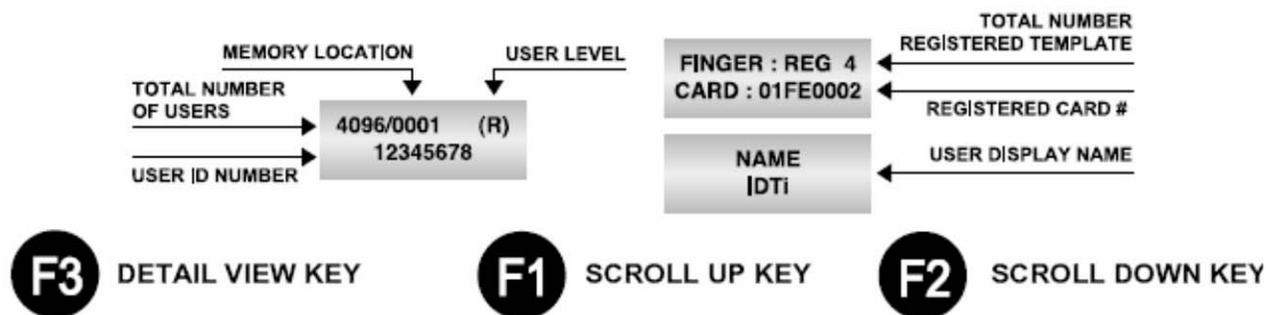
4 Salir de Ver. Pulse la tecla # para continuar viendo otro o pulse cualquier otra para salir del submenú.

Ver la Lista de Usuarios del Sistema

La Lista de Usuarios del Sistema mostrará la siguiente información:

- . El PIN del usuario (ID Plantilla)
- . El nombre del usuario
- . El estatus como administrador del usuario
- . La ubicación en memoria de la plantilla del usuario

NOTE :



Viewing System User List

The System User List will display the following information :

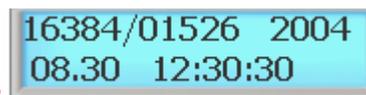
- The user's PIN (Template ID)
- The user's name
- The user's administrator status
- The user's template location in memory

5.2 Eventos

Las transacciones de registro de eventos del sistema se pueden ver en cualquier momento. Un registro creado que contiene información pertinente sobre alguna ocurrencia producida en el control de acceso y en el sistema de monitorización.



1 Pulse la tecla # para entrar en ver EVENTO



3 Aparecerá el siguiente registro de eventos. Pulse la tecla F3 para ver los datos del evento



2 Pulse F1 para desplazarse hacia arriba por registro de eventos
Pulse la tecla F2 para desplazarse hacia abajo por registro de eventos



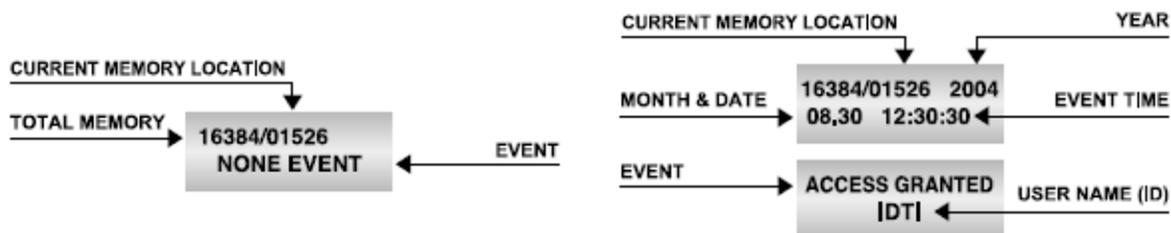
4 Salir de Ver. Pulse la tecla # para continuar viendo otro evento o pulse cualquier otra para salir del submenú.

Ver el Registro de Eventos del Sistema

La Lista de Registro de Eventos del Sistema mostrará la siguiente información:

- La fecha de ocurrencia del evento
- La hora de ocurrencia del evento
- El número total de eventos en registro

NOTE :



DETAIL VIEW KEY



SCROLL UP KEY



SCROLL DOWN KEY

Viewing System Event Log

The System Event Log List will display the following information :

- The date of event occurrence
- The time of event occurrence
- The total number of event log

5.3 Firmware

Esta opción permite ver la versión actual del firmware instalada en BioScan. Otra forma de comprobar el firmware es reiniciando el dispositivo. Al arrancar por primera vez, aparece la versión del firmware.



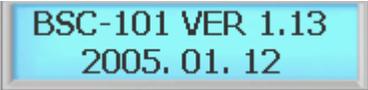
1

Pulse la tecla # para entrar en VERSIÓN DE FIRMWARE



3

Pulse la tecla # para ver otra vez el firmware
Pulse cualquier otra tecla para salir



BSC-101 VER 1.13
2005. 01. 12

2

Aparecerá el número de versión del firmware actual

5.4 Versión Escáner Huella

Esta opción permite ver la versión actual del escáner de huellas dactilares instalado en BioScan.



3> VIEW
4.FINGER VER.

1

Pulse la tecla # para entrar en VERSIÓN ESCANER HUELLA

LIST VIEW EXIT
CONT:# STOP:ANY

3

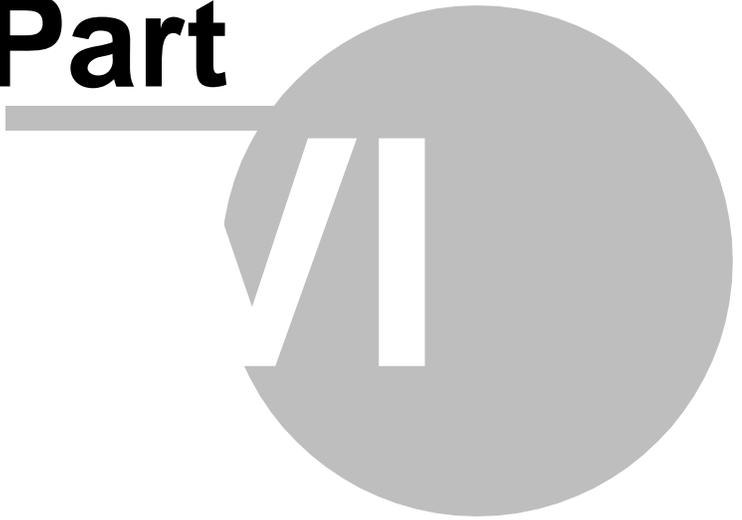
Pulse la tecla # para ver otra vez la versión del escáner
Pulse cualquier otra tecla para salir

2

SFM-3020
VER : V1.4C

Aparecerá el número de versión del módulo de huella
dactilar actual La última versión es V1.6C

Part



6 MENÚ DEL SISTEMA 4 – BORRAR USUARIO

6.1 Borrar Usuario Individual

Borrar una plantilla de huella dactilar de un lector impide que esa plantilla pueda acceder a la zona a través del lector. De un lector de huellas dactilares se puede borrar cualquier plantilla de huella, incluyendo la administrativa y la última plantilla de huella dactilar que quede en el lector. Las plantillas se pueden borrar por usuario individual o todos los usuarios, incluyendo las plantillas administrativas.



1
Pulse la tecla # para entrar en borrar Usuario Individual



3
Introduzca el ID usuario, de 1 a 16 dígitos



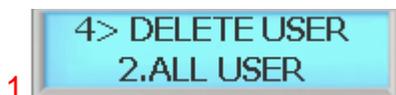
2
Introduzca el ID usuario que desea borrar como se indica a continuación



4
Borrar completado.

6.2 Borrar Todos los Usuarios

Borrar una plantilla de huella dactilar de un lector impide que esa plantilla pueda acceder a la zona a través del lector. De un lector de huellas dactilares se puede borrar cualquier plantilla de huella, incluyendo la administrativa y la última plantilla de huella dactilar que quede en el lector. Las plantillas se pueden borrar por usuario individual o todos los usuarios, incluyendo las plantillas administrativas.



1
Pulse la tecla # para entrar en borrar Todos los Usuarios



3
Borrando. Por favor, espere....

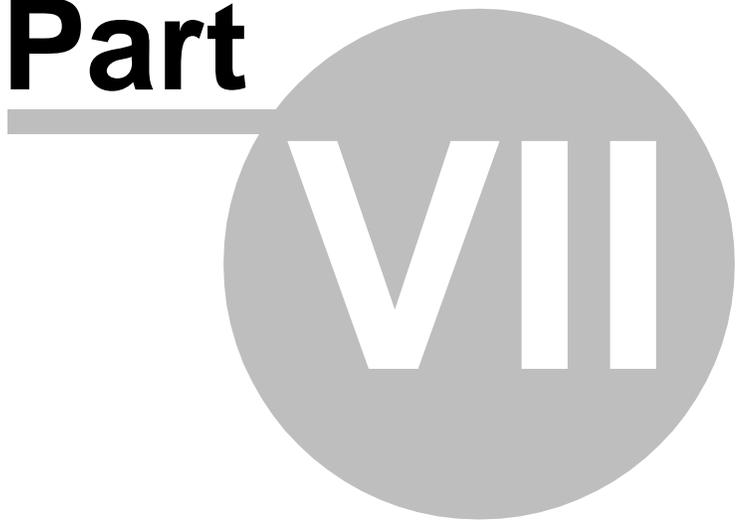


2
Pulse la tecla # para confirmar borrar todo
Pulse cualquier otra tecla para cancelar



4
Borrar completado.

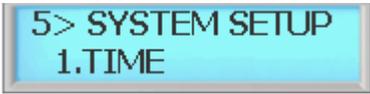
Part



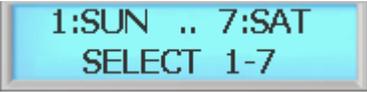
7 MENÚ DEL SISTEMA 5 – CONFIGURACIÓN DEL SISTEMA

7.1 Hora

BioScan dispone de un reloj interno que proporciona la fecha y hora de todos los eventos registrados. Esta sección describe cómo establecer la fecha y hora que usa BioScan para el registro de eventos. Para establecer la hora actual, acceda al sistema de menú y siga estos pasos:

1 

Pulse la tecla # para entrar en Hora del sistema

4 

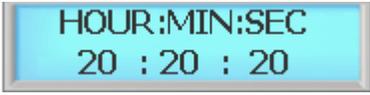
Seleccione el día de la semana. Pulse de 1 a 7 para introducir el día de la semana. Consulte la NOTA

2 

Introduzca la fecha actual

5 

Pulse la tecla # para confirmar

3 

Introduzca la hora actual en formato de tipo militar, es decir, 20:20:20

6 

La configuración ha finalizado

NOTE :

Time format can be displayed in 3 types, Asian Time, European Time, and American Time. After setting the current time, go to page and customized the time display option to view local time display.

Select the day of the week :

| | | | |
|-----------|---|----------|---|
| Sunday | 1 | Thursday | 5 |
| Monday | 2 | Friday | 6 |
| Tuesday | 3 | Saturday | 7 |
| Wednesday | 4 | | |

-  CLEAR KEY
-  ENTER KEY
-  ESCAPE KEY
-  BACK SPACE KEY

7.2 Modo de funcionamiento

BioScan tiene un total de 11 modos de funcionamiento. A continuación se muestra la vista detallada de los modos de funcionamiento disponibles en BioScan.



CD / FP
F1:UP F2:DN

- 1 **[CD / FP] – TARJETA o HUELLA DACTILAR**
El usuario puede acceder al dispositivo mediante tarjeta o huella dactilar. Al funcionar en este modo, simplemente introduzca la tarjeta o la huella dactilar en el dispositivo.



ID & FP / CD
F1:UP F2:DN

- 2 **[ID&FP/CD] – PIN & HUELLA DACTILAR o TARJETA**
En este modo, el usuario puede acceder al dispositivo mediante PIN con huella dactilar o simplemente una tarjeta. Para funcionar en este modo, el usuario debe introducir primero el PIN antes de introducir el dedo o presentar la tarjeta de usuario.



ID & CD & FP
F1:UP F2:DN

- 3 **[ID&CD&FP] - PIN & TARJETA & HUELLA DACTILAR**
El usuario debe utilizar los tres elementos para poder pasar. Es el modo de mayor seguridad disponible en BioScan. Para funcionar en este modo, primero introduzca el PIN de usuario y pulse la tecla #, a continuación presente la tarjeta de usuario seguido de la huella dactilar del usuario.



ID / CD / FP
F1:UP F2:DN

- 4 **[ID/CD/FP] - PIN o TARJETA o HUELLA DACTILAR (CUALQUIER MODO)**
El usuario puede acceder al dispositivo mediante cualquiera de los elementos disponibles. Este modo es el más cómodo pero el de menos seguridad de BioScan. Para funcionar en este modo, simplemente utilice cualquiera de los elementos.

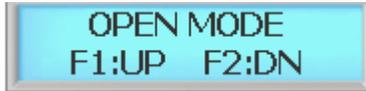


CD & FP
F1:UP F2:DN

- 7 **[CD&FP] – Tarjeta & Huella dactilar**
El usuario debe entrar utilizando la tarjeta de usuario & Huella dactilar para acceder a la unidad. Para funcionar en este modo, introduzca la tarjeta seguido de la huella dactilar del usuario.

- 8 **[ID&FP OR ID&CD] – PIN & Huella dactilar o PIN & Tarjeta**
En este modo, el usuario puede acceder al dispositivo introduciendo el PIN de usuario y la huella dactilar o el PIN de usuario y la tarjeta. Este modo es útil cuando están conectados en red con lectores de proximidad.

- 9 **[ID&FP OR CARD&FP] – PIN & Huella dactilar o Tarjeta & Huella dactilar**
En este modo, el usuario puede acceder al dispositivo mediante PIN con huella dactilar o simplemente una tarjeta.



OPEN MODE
F1:UP F2:DN

- 10 **[ABIERTO] – SIEMPRE ABIERTO**
El punto de acceso permanecerá abierto para caso de emergencia, por ejemplo, incendio.

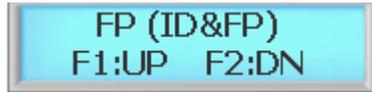


CLOSED MODE
F1:UP F2:DN

48

5

B



ions Manual

[F P O ID / FP] – SÓLO DEDO ó ID

11

[CERRADO] – SIEMPRE CERRADO



& DEDO

El lector de huella dactilar será el único dispositivo disponible y los usuarios deben entrar usando la huella dactilar. El resto de los elementos estarán deshabilitados. Esto es una verificación 1:1 o 1:N. El usuario también tiene la opción de acceder introduciendo el PIN de usuario e introduciendo la huella dactilar para más rapidez. Para funcionar en este modo, introduzca la huella dactilar del usuario o PIN y Huella dactilar de usuario

El punto de acceso permanecerá cerrado para una emergencia, como por ejemplo, intrusión.



6

[ID&FP] – PIN & Huella dactilar

El usuario debe entrar utilizando el PIN de usuario & Huella dactilar para acceder a la unidad. Para funcionar en este modo, introduzca el PIN de usuario seguido de la huella dactilar.

12

[MODO PRUEBA] – MODO PRUEBA

Es una buena idea probar la unidad en este modo cuando se instala por primera vez.

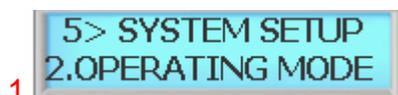
&: significa "Y"

/: significa "O"

(): significa "O"

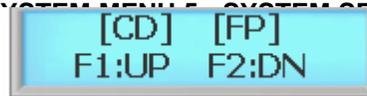
7.2.1 Establecer el Modo de Funcionamiento

Esta sección proporciona información sobre cómo seleccionar el modo de funcionamiento. ID/CD/FP (TODO) es el modo de funcionamiento predeterminado.



1

Pulse la tecla # para añadir plantilla de huella dactilar de usuarios



3

Pulse la tecla # para seleccionar el modo de funcionamiento. Consulte la Nota para ver los modos de funcionamiento disponibles.



2

Pulse la tecla F1 para desplazarse hacia arriba por el menú de modos
Pulse la tecla F2 para desplazarse hacia abajo por el menú de modos



4
Configuración finalizada

! NOTE :

FINGERPRINT MODE [FINGER]

Note that the maximum time required to identify a fingerprint is directly proportional to the number of templates enrolled at the reader. The reader can compare fingerprints at an approximate rate of 1,000 fingerprints per second. If no match is found, then the maximum time elapses before the red LED lights due to the reader having to try every template in the database before determining that there is no match.

SELECT MODE
F1:UP F2:DN

List of operating modes to choose from. Select from the following list.

CD / FP
F1:UP F2:DN

ID & FP / CD
F1:UP F2:DN

ID & CD & FP
F1:UP F2:DN

ID / CD / FP
F1:UP F2:DN

FP (ID&FP)
F1:UP F2:DN

ID & FP
F1:UP F2:DN

CD & FP
F1:UP F2:DN

ID & FP / ID & CD
F1:UP F2:DN

ID & FP / CD & FP
F1:UP F2:DN

OPEN MODE
F1:UP F2:DN

CLOSED MODE
F1:UP F2:DN

.TESTING MODE.
F1:UP F2:DN

7.3 Tiempo bloqueo Re

Es la duración máxima que se activará el relé de liberación del bloqueo. El relé se desactiva si la puerta se abre antes de que haya expirado este tiempo. El tiempo de bloqueo se puede establecer en el rango de 01~99 segundos. No se puede establecer un tiempo de bloqueo de 0 segundos. El valor predeterminado es 4 segundos.

1 **5> SYSTEM SETUP**
3.RE-LOCK TIME

Pulse la tecla # para introducir Tiempo Bloqueo Relé

3 **SETUP COMPLETED**
F1:UP F2:DN

La configuración ha finalizado



Introduzca Tiempo Bloqueo Relé, de 1 a 99 segundos, seguido de la tecla #. C indica tiempo establecido actual, el ejemplo indica 4 segundos.

7.4 Dirección

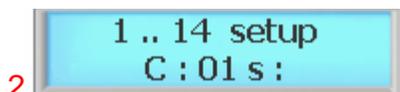
Las opciones de comunicaciones permiten a BioScan comunicarse con un PC y con otros equipos de control de puerta. En las aplicaciones en red, las unidades BioScan se comunican con un PC conectado. Esto requiere que cada unidad tenga un código de identificación único. Para asignar un ID de Red, siga los siguientes pasos: Repita este procedimiento por cada unidad conectada en red, asignando a cada unidad un código de identificación único. La dirección predeterminada es 1.



Pulse la tecla # para introducir Dirección



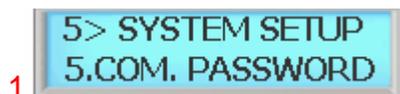
La configuración ha finalizado



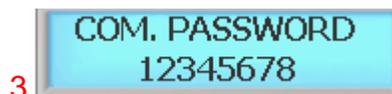
Introduzca 1 ~ 14 seguido de la tecla #. Puede asignar ID de red de 1 a 14. C Indica el parámetro actual, el ejemplo muestra la dirección 1. El parámetro de dirección predeterminado es 1.

7.5 Contraseña de comunicaciones

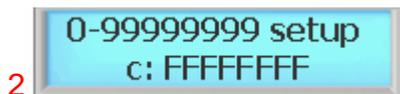
La contraseña de comunicaciones se utiliza durante la comunicación en red. Esto salvaguarda la información enviada durante la transmisión y también evita que se cuelen en el sistema.



Pulse la tecla # para introducir la Contraseña de Comunicaciones



Introduzca la contraseña de 8 dígitos y pulse la tecla # para confirmar la nueva contraseña



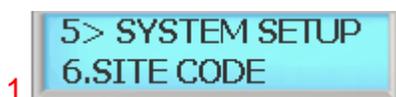
Aparece la contraseña actual. Introduzca la nueva contraseña como se muestra en la siguiente figura.

4

La configuración ha finalizado

7.6 Código de Instalación

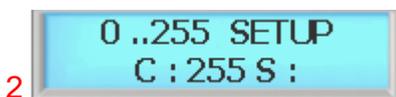
El código de instalación, que a veces se le llama código de servicio, diferencia a un grupo de tarjetas de usuario de otro. El código de instalación es un código integral que se programa en la tarjeta en el momento de su fabricación. El código adicional asegura que aunque los números de tarjeta fueran duplicados por el fabricante, las tarjetas no funcionarán en el edificio de otra persona que tenga un código de instalación distinto. La limitación inherente en el proceso de facturación de las tarjetas da como resultado la capacidad de crear sólo un número finito de tarjetas, tras lo cual se duplican los códigos. Los códigos de instalación superan esta limitación añadiendo un segundo código, que es comprobado por el lector. Si el código de instalación no coincide con el código programado, se deniega la entrada.



1 Pulse la tecla # para introducir Código de Instalación



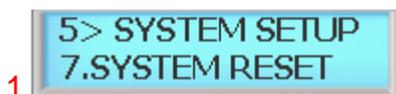
3 La configuración ha finalizado



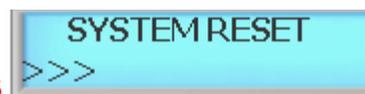
2 "C" indica código de instalación actual, que es 255. Introduzca número de 0 a 255 y pulse la tecla #. El parámetro predeterminado es 255

7.7 Reinicio del Sistema

Dentro de BioScan hay dos bases de datos, Base Datos del Sistema & Base Datos de Eventos. La Base Datos del Sistema almacena la información de configuración del sistema. Cuando se ejecuta, el sistema restaura los parámetros predeterminados en fábrica.



1 Pulse la tecla # para entrar en Reinicialización del Sistema

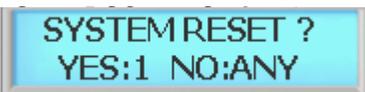


3 Mensaje de reinicialización del sistema. Esto puede llevar desde unos segundos a un minuto, dependiendo del tamaño de la base de datos



58

B **ions Manual**



2

Pulse 1 para reinicializar el sistema
Pulse cualquier otra tecla para cancelar

4

La configuración ha finalizado

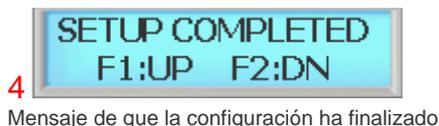
7.8 Reinicialización de Eventos

7.9 Velocidad Com.

Este comando establece la velocidad de transmisión con la que el BioScan se comunicará con el dispositivo conectado al puerto serie. El cambio de la velocidad de comunicación será efectivo inmediatamente tras la ejecución del comando. La velocidad de comunicación predeterminada es 19.200.

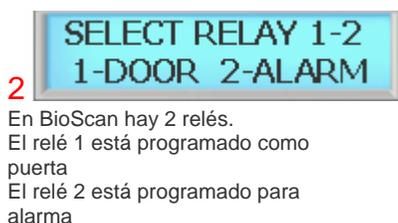
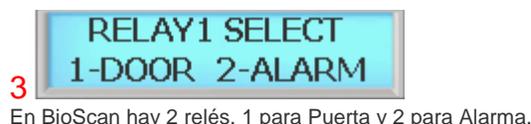
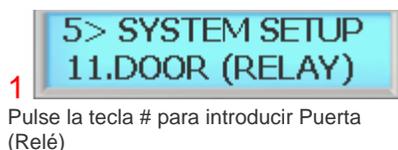


Existen 4 velocidades de comunicación distintas. Seleccione la mejor configuración para su red. La velocidad predeterminada está establecido a 4800 baudios.
Vaya al Panel de Control y asegúrese de que la velocidad de transmisión del PC está sincronizada con BioScan



7.10 Relé de Puerta

La configuración del relé es Normalmente Abierto (N.A.), y se cambia a cortado cuando lo activa un evento, como una autenticación o ausencia de ID. El relé se puede utilizar para enviar alimentación a elementos conmutados como pulsadores de puertas eléctricas, pomos de puertas, cierres magnéticos o indicadores.



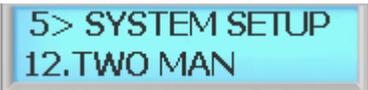
Para que funcione el relé, en la Configuración de Alarma, uno de los relés tiene que establecerse como alarma y al menos una de las alarmas tiene que establecerse como relé.

El valor predeterminado en fábrica del relé 1 es Puerta (cerrado)

El valor predeterminado en fábrica del relé 2 es Alarma

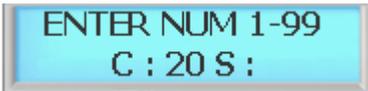
7.11 Dos Personas

Este comando impide que un usuario individual entre en una zona de seguridad vacía seleccionada a menos que esté presente otro usuario registrado. Una vez que se registren en la zona los dos usuarios registrados, otro usuario podrá ir y venir individualmente, siempre que haya al menos dos personas en la zona. A la inversa, al salir, los dos últimos ocupantes de la zona de seguridad deben salir juntos. El sistema no permitirá que en ningún momento haya menos de dos usuarios en la zona.



5> SYSTEM SETUP
12.TWO MAN

1
Pulse la tecla # para entrar en Dos
Personas



ENTER NUM 1-99
C : 20 S :

3
Esto es el límite de tiempo que tiene el segundo usuario
para realizar la verificación en el lector una vez
verificado el primer usuario. "C" indica el parámetro
actual.
Teclee de 1 a 99 segundos y pulse la tecla #.

4
La configuración ha finalizado



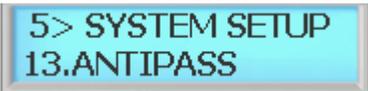
ENABLE TWOMAN
1:YES 2:NO

2
Pulse la tecla 1 para habilitar dos
personas
Pulse la tecla 2 para deshabilitar dos
personas

7.12 Retropase

El retropase se utiliza para impedir que dos personas utilicen una sola tarjeta para acceder. Si el acceso se deniega debido a esto, se enviará un mensaje de alarma a la impresora. También puede provocar que se active un relé, si se ha programado de esta forma.

Esto es un parámetro de anti pase del sistema y el parámetro de anti pase de usuario debe estar habilitado para que funcione adecuadamente.



5> SYSTEM SETUP
13.ANTIPASS

1
Pulse la tecla # para entrar en Retropase



SETUP COMPLETED
F1:UP F2:DN

3
La configuración ha finalizado



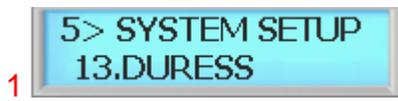
ENABLE ANTIPASS?
1:YES 2:NO

2
Pulse la tecla 1 para habilitar el retropase
Pulse la tecla 2 para deshabilitar el retropase

7.13 Coacción

Coacción es una condición en la que un usuario se puede ver confrontado por un intruso que intenta acceder a una zona de seguridad. Mediante la puesta en práctica de la función de coacción, el usuario puede indicar "de forma secreta" a seguridad que está entrando en una zona de seguridad bajo "coacción". Para que funcione, esta función debe utilizarse con una tecla de función.

62 BioScan BSC-101 Series Operations Manual



Pulse la tecla # para entrar en Coacción



Introduzca de 0 a 9 seguido de la tecla #.

2



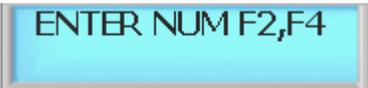
Pulse la tecla 1 para habilitar coacción
Pulse la tecla 2 para deshabilitar coacción

5



Configuración finalizada

3



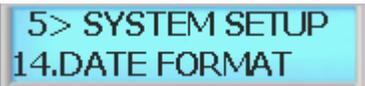
Introduzca F2 o F4 para asignar la tecla de coacción.
Por ahora, introduciremos la tecla F2

Para utilizar la coacción, pulse F2 - 2 y luego introduzca Tarjeta o PIN dependiendo del modo de funcionamiento actual.

7.14 Formato de fecha

BioScan permite seleccionar el formato de fecha disponible para el horario de Asia, horario de EE.UU. y horario de Europa. Aquí es donde el usuario puede personalizar el formato horario. Esta sección describe cómo seleccionar el formato de hora.

1



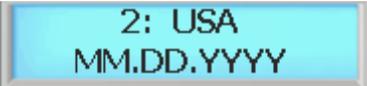
Pulse la tecla # para entrar en Formato de Hora

2



Pulse la tecla F1 para desplazarse hacia arriba por la lista
Pulse la tecla F2 para desplazarse hacia abajo por la lista

3




Seleccione el formato de hora adecuado para su región. Para utilizar mensaje personalizado, vaya a Presentación Personalizada en siguiente página.



Se ha establecido el formato de Hora

NOTE :



Formato presentación Hora de ASIA



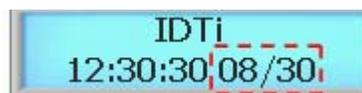
Formato presentación Hora de EE.UU.



Formato presentación Hora de EUROPA



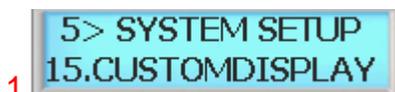
PERSONALIZADO 1 Aparecerá el mensaje personalizado con formato de fecha europeo. El día aparece antes que el mes



PERSONALIZADO 2 Aparecerá el mensaje personalizado con hora con formato de fecha americano. El mes aparece antes que el día

7.15 Visualización personalizada

BioScan dispone de la opción de personalizar la visualización (display). BioScan Allows permite mostrar hasta 32 caracteres. Aquí es donde el usuario puede personalizar la ventana principal de visualización. Esta sección describe cómo modificar la visualización personalizada.



Pulse la tecla # para entrar en Visualización Personalizada



Continúe escribiendo el mensaje donde lo dejó en la figura 2



Introduzca la letra y pulse la tecla F1 para pasar a la siguiente letra. Para conseguir una minúscula, continúe pulsando la tecla hasta que aparezca la letra en



minúsculas: Si el nombre es más largo de 16, pulse la tecla # tras introducir la última letra (la 16). Esto continuará en el siguiente paso

5

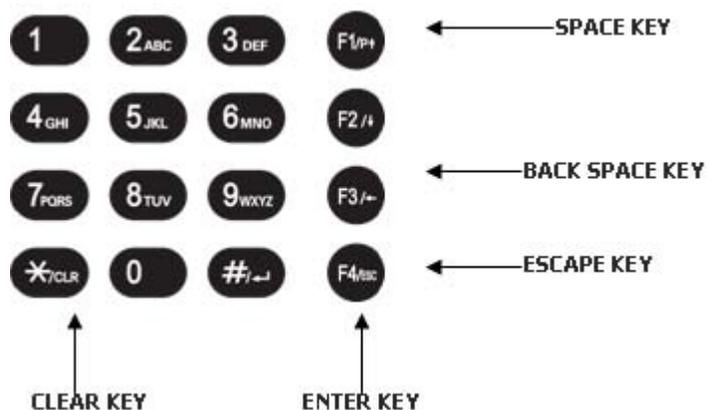
Finalizada modificación de mensaje personalizado

EDIT CONTINUE?
1: YES 2: NO

3 Si el mensaje contiene más de 16 dígitos, pulse la tecla 1 para continuar escribiendo el mensaje. En caso contrario, pulse 2 para finalizar la escritura del mensaje personalizado

NOTE :

Se pueden introducir hasta 32 dígitos. El LCD irá desplazando el mensaje si tiene más de 16 dígitos. Para ver la visualización personalizada, vaya a Formato de Fecha y establezca la opción de visualización a Personalizado 1 o Personalizado 2, dependiendo del formato de fecha.



| TECLA | NÚMERO DE VECES QUE SE PULSA TECLA | | | | | | | |
|-------|------------------------------------|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | | | | | | | | |
| 2 | A | B | C | a | b | c | | |
| 3 | D | E | F | d | e | f | | |
| 4 | G | H | I | g | h | i | | |
| 5 | J | K | L | j | k | l | | |
| 6 | M | N | O | m | n | o | | |
| 7 | P | Q | R | S | p | q | r | s |
| 8 | T | U | V | t | u | v | | |
| 9 | W | X | Y | Z | w | x | y | z |
| 0 | | | | | | | | |

| | |
|----|---------------|
| * | Borrar |
| # | Intro |
| F1 | Espacio |
| F2 | |
| F3 | Espacio Atrás |
| F4 | Escape |

7.16 Iluminación de LCD

BioScan permite seleccionar si el visualizador aparecerá iluminado o sin luz. De forma predeterminada, cuando se utiliza, el visualizador se ilumina durante 5 segundos. La iluminación del visualizador permite una mejor visualización en zonas oscuras, mientras que dejar apagado el visualizador ahorra energía. Esta sección proporciona información sobre cómo establecer las opciones de iluminación del visualizador del BioScan.

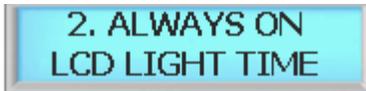


Pulse la tecla # para entrar en la opción Luz LCD



Pulse la tecla # para establecerla como hora predeterminada
Pulse F1 para desplazarse hacia arriba por el menú
Pulse F2 para desplazarse hacia abajo por el menú

2.2



Pulse la tecla # para establecerlo como siempre encendida
Pulse F1 para desplazarse hacia arriba por el menú
Pulse F2 para desplazarse hacia abajo por el menú

2.3



Pulse la tecla # para establecerla como personalizar
Pulse F1 para desplazarse hacia arriba por el menú
Pulse F2 para desplazarse hacia abajo por el menú

3



Terminado edición horario retroiluminación LCD

3



Terminado edición horario retroiluminación LCD

2.4



Definir hora de inicio de LCD. LCD se encenderá conforme a este parámetro de hora. Introduzca la hora en formato militar. Por ejemplo, 15:15:15 (3:15:15 PM)

2.5



Definir hora de fin de LCD. LCD se apagará conforme a este parámetro de hora. Introduzca la hora en formato militar. Por ejemplo, 15:15:15 (3:15:15 PM). Pulse la tecla # cuando haya terminado

3



Terminado edición horario
retroiluminación LCD

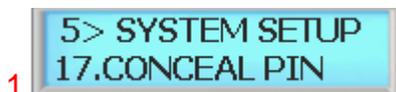
NOTE :

Existen 3 opciones de LCD:

1. Predeterminada: el LCD permanecerá encendido durante 5 segundos.
2. Siempre encendido: LCD estará iluminado en todo momento. Esto reducirá la vida de la pantalla LCD.
3. Personalizado: Puede programar el horario en el que el LCD se apagará y encenderá.

7.17 Ocultar PIN

BioScan permite ocultar el PIN de usuario al entrar en el dispositivo. Para ocultar el PIN de usuario al entrar en el dispositivo, siga las siguientes instrucciones.



1 Pulse la tecla # para entrar en Ocultar PIN



3 La configuración ha finalizado



2 Pulse la tecla 1 para habilitar Ocultar PIN
Pulse la tecla 2 para cancelar Ocultar PIN

 **NOTE :**

(U) WELCOME
00002

Vista Normal



ENTER USER ID
*****1

Vista real en entrada



(U) WELCOME

Vista PIN oculto de usuario

7.18 Cierre

BioScan dispone de una opción para utilizar un relé auxiliar para armar/desarmar un sistema de alarma externo llamado el cierre. Esta sección describe como habilitar el dispositivo de cierre.



1 5> SYSTEM SETUP
19. LOCK DOWN

Pulse la tecla # para entrar en Cierre

3 FUNC KEY ENABLE ?
1:YES 2:NO

Pulse la tecla 1 para habilitar la tecla de función
Pulse la tecla 2 para deshabilitar la tecla de función

2 LOCK DN ENABLE ?
1:YES 2:NO

Pulse la tecla 1 para habilitar Cierre
Pulse la tecla 2 para cancelar Cierre

4 SETUP COMPLETED
F1:UP F2:DN

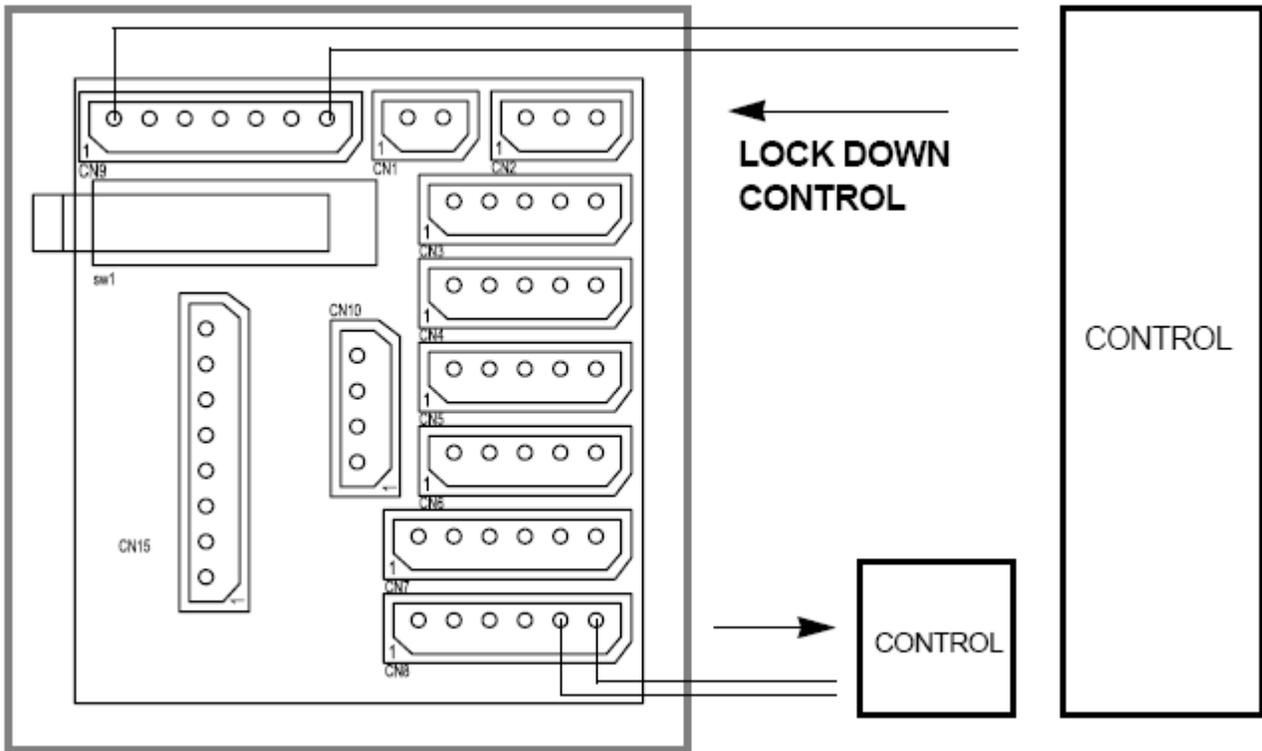
La configuración ha finalizado

! NOTE :

[S] L.D On F2:0
01234

[S] L.D Off F4:0
01234

[U] L.D BK
06789



7.19 Asistencia

BioScan dispone de la opción de mostrar ENTRADA o SALIDA al utilizar teclas de función. El usuario debe ser consciente del modo de asistencia actual que aparece en el visualizador en modo de espera. El último modo de asistencia utilizado será el modo predeterminado hasta que se utilice el siguiente. Si la última vez se utilizó F2-0, entonces a menos que un segundo usuario utilice una tecla de función distinta, aparecerá como F2-0 incluso si el segundo usuario no pulsa ninguna tecla de función. Esta sección muestra cómo personalizar la tecla de función que muestra el visualizador.



Pulse la tecla # para entrar en Formato de Hora



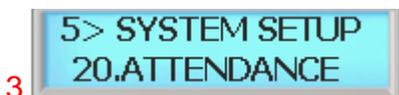
Pulse 1 para configurar asistencia
Pulse 2 para cancelar la configuración



Pulse la tecla F1 para desplazarse hacia arriba por la lista
Pulse la tecla F2 para desplazarse hacia abajo por la lista



La configuración ha finalizado



3 Pulse la tecla # para entrar en Asistencia

STANDBY LCD DISPLAY

| | | |
|------|------------------------------------|---------------------|
| F2-0 | IN 2005.12.27 16:17:59 [TUE] | IN |
| F4-0 | OUT 2005.12.27 16:17:59 [TUE] | OUT |
| F2-1 | E-IN 2005.12.27 16:17:59 [TUE] | 2 ND IN |
| F2-2 | E-OUT 2005.12.27 16:17:59 [TUE] | 2 ND OUT |

ACCESS GRANTED DISPLAY

| | | |
|---|------------------------------------|---------------------|
| 0 | (U) < I N > F2:0 123456 | IN |
| 0 | (U) < O U T > F4:0 123456 | OUT |
| 1 | (U) < E X - I N > F2:1 123456 | 2 ND I I |
| 2 | (U) < E X - O U T > F2:2 123456 | 2 ND O I |

7.20 Configuración de red

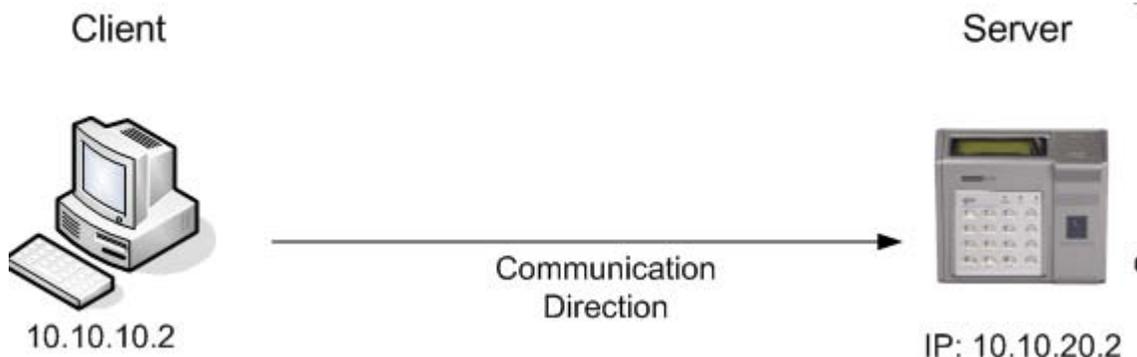
Dentro de este menú hay dos submenús, Dirección IP y Ver Dirección IP.

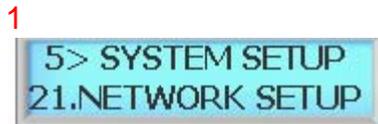
7.20.1 Configuración Dirección IP Dispositivo

BioScan puede funcionar como Servidor o como Cliente. Si se establece como Servidor, entonces el software se debe establecer como Cliente y si se establece como Cliente, entonces el software se debe establecer como Servidor.

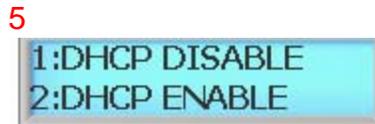
7.20.1.1 Modo Servidor Manual

En el Modo Servidor, el software se conecta al dispositivo. Ésta es la configuración ideal de red ya que el software se reconectará automáticamente si se pierde la conexión.





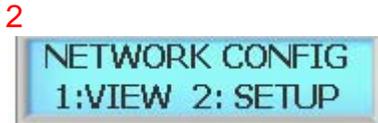
Seleccionar configuración de red desde el menú del sistema
5.



Pulse 1 para deshabilitar el modo DHCP



Introduzca el número de puerto del dispositivo y pulse la tecla #.



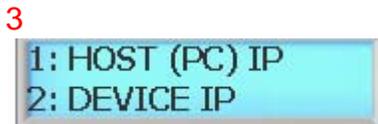
Pulse la tecla 2 para configurar la red.



Introduzca la dirección IP y pulse la tecla #.
(Ej. 192.168.0.10) Introduzca la tecla 192168000010#

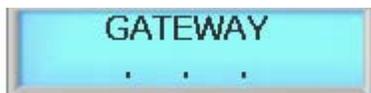


Configuración finalizada.

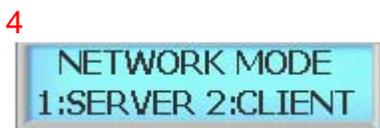


Pulse 2 para introducir la dirección IP del dispositivo.

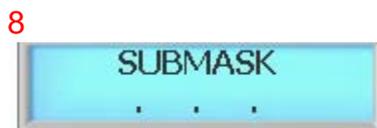
7



Introduzca la dirección IP de la puerta de salida y pulse la tecla #.
(Ej. 192.168.0.1) Introduzca la tecla 192168000001#



Pulse 1 para seleccionar el Modo Servidor

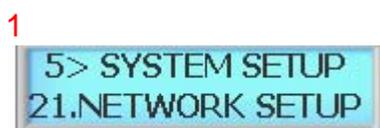
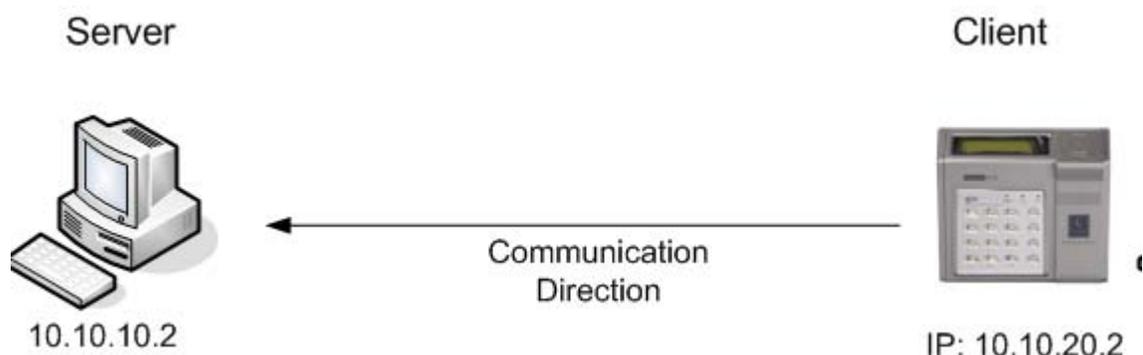


Introduzca la dirección IP de submáscara y pulse la tecla #.
(Ej. 255.255.255.0) Introduzca la tecla 255255255000#

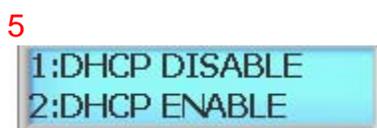
Consulte el manual de software para obtener la configuración Host PC.

7.20.1.2 Modo Cliente Manual

En el Modo Cliente, el dispositivo se conecta al software. Esta es una red más práctica pero puede perder conexiones; sería la configuración de red ideal ya que el software se reconectará automáticamente si se pierde la conexión.



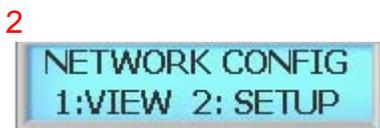
Seleccionar configuración de red desde el menú del sistema 5.



Pulse 1 para deshabilitar el modo DHCP



Introduzca el número de puerto del dispositivo y pulse la tecla #.



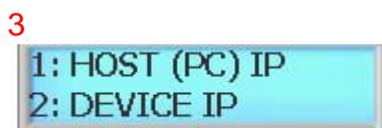
Pulse la tecla 2 para configurar la red.



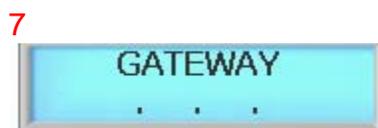
Introduzca la dirección IP y pulse la tecla #.
(Ex. 192.168.0.10) Introduzca teclas 192168000010#



Configuración finalizada.

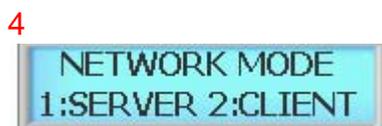


Pulse 2 para introducir la dirección IP del dispositivo.

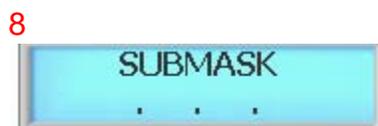


Introduzca la dirección IP de la puerta de salida y pulse la tecla #.

(Ej. 192.168.0.1) Introduzca la tecla 19216800001#



Pulse 2 para seleccionar el Modo Cliente

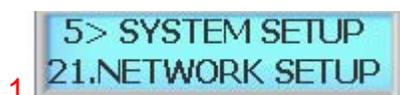


Introduzca la dirección IP de submáscara y pulse la tecla #.

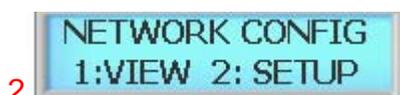
(Ej. 255.255.255.0) Introduzca la tecla 255255255000#

Los dispositivos cliente necesitan información del Host PC para poder realizar la conexión con el PC host. Una vez introducida la información IP del dispositivo, por favor, vaya a Configuración de Dirección del Host PC y configure la dirección IP de Host PC.

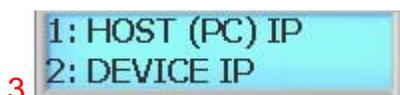
7.20.1.2.1 Configuración de Dirección IP de Host PC



Seleccionar configuración de red desde el menú del sistema 5.



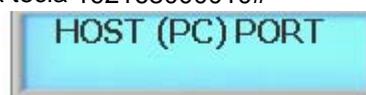
Pulse la tecla 2 para configurar la red.



Pulse 1 para introducir la dirección IP del PC Host.

4

Introduzca la dirección IP y pulse la tecla #. (Ej. 192.168.0.10) Introduzca la tecla 192168000010#



5

Introduzca el número de puerto de Host PC y pulse la tecla #.



6

Configuración finalizada.

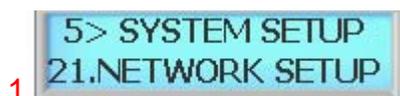
7.20.1.3 Modo DHCP

El Protocolo de Configuración Dinámica de Host (DHCP) es un conjunto de reglas que utiliza un dispositivo de comunicaciones para permitir que el dispositivo solicite y obtenga una dirección IP de un servidor, que dispone de una lista de direcciones disponibles para su asignación.

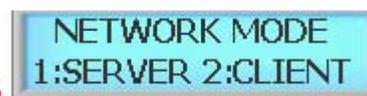
DHCP es un protocolo utilizado por los dispositivos para obtener de un servidor DHCP una dirección IP única y otros parámetros tales como router predeterminado, máscara de subred, y direcciones IP para los servidores DNS. DHCP se puede utilizar tanto en Modo Servidor, como en Modo Cliente.

Dependiendo de la implementación del servidor DHCP, el dispositivo podría perder su dirección IP. Puede intentar la reconexión reiniciando el dispositivo o asignando manualmente una dirección IP; en caso contrario, por favor, póngase en contacto con su administrador de red.

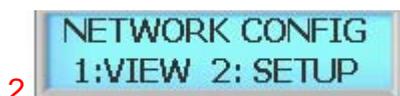
7.20.1.3.1 Modo Servidor DHCP



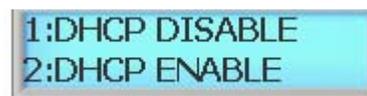
1 Seleccione configuración de red desde el menú del sistema 5.



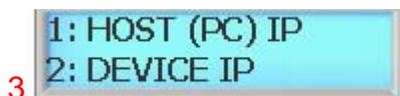
5 Pulse 1 para entrar en el Modo Servidor



2 Pulse la tecla 2 para configurar la red.



6 Pulse 2 para habilitar el Modo Servidor DHCP.

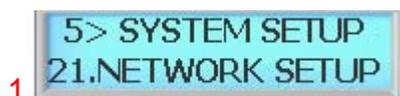


3 Pulse 2 para introducir la dirección IP del dispositivo.

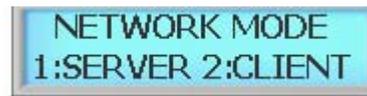


7 Configuración finalizada.

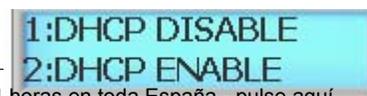
7.20.1.3.2 Modo DHCP Cliente

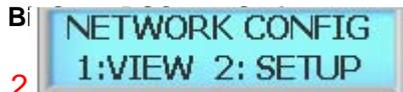


1 Seleccione configuración de red desde el menú del sistema 5.



5 Pulse 2 para entrar en el Modo Cliente

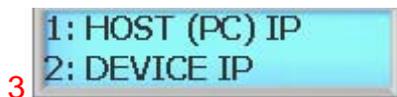




Pulse la tecla 2 para configurar la red.

6

Pulse 2 para habilitar el Modo DHCP Cliente.

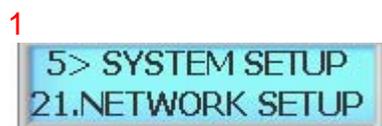


Pulse 2 para introducir la dirección IP del dispositivo.

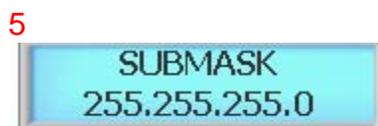
Configuración finalizada.

7.20.2 Ver Configuración IP

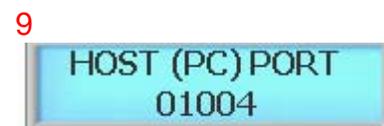
Ver Configuración IP muestra los parámetros actuales de red del dispositivo para las dos configuraciones IP de Dispositivo y PC Host.



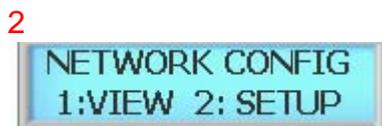
Seleccionar configuración de red desde el menú del sistema 5.



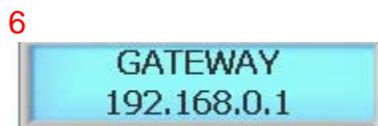
Muestra la Submáscara actual



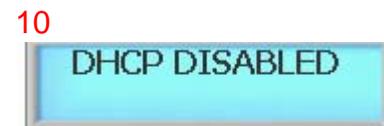
Muestra el número actual de puerto de PC Host



Pulse la tecla 2 para configurar la red.



Muestra la Puerta de Enlace actual



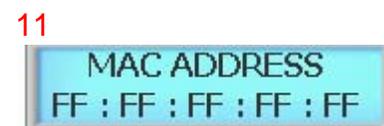
Muestra información DHCP



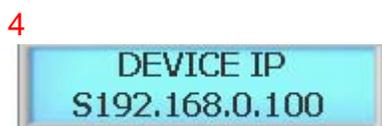
Pulse 2 para introducir la dirección IP del dispositivo.



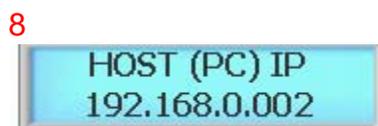
Muestra el puerto IP actual del dispositivo



Muestra la dirección MAC del dispositivo

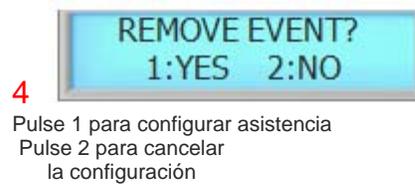
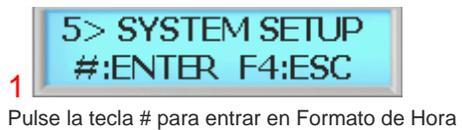


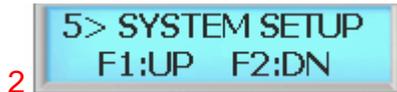
Pulse 1 para seleccionar el Modo Servidor



Muestra la dirección IP actual de PC Host

7.21 Eliminar Evento





- 2
Pulse la tecla F1 para desplazarse hacia arriba por la lista
Pulse la tecla F2 para desplazarse hacia abajo por la lista

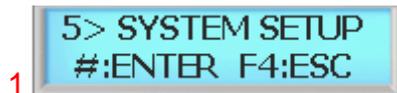


- 5
La configuración ha finalizado



- 3
Pulse la tecla # para entrar en Asistencia

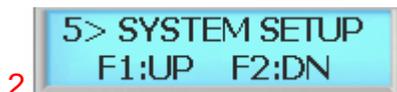
7.22 Tipo Wiegand



- 1
Pulse la tecla # para entrar en Formato de Hora



- 4
Pulse 1 para configurar asistencia
Pulse 2 para cancelar la configuración



- 2
Pulse la tecla F1 para desplazarse hacia arriba por la lista
Pulse la tecla F2 para desplazarse hacia abajo por la lista

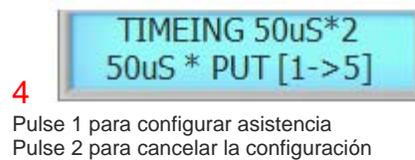
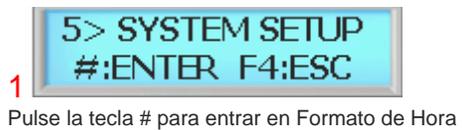


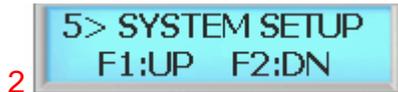
- 5
La configuración ha finalizado



- 3
Pulse la tecla # para entrar en Asistencia

7.23 Hora Wiegand





Pulse la tecla F1 para desplazarse hacia arriba por la lista
Pulse la tecla F2 para desplazarse hacia abajo por la lista



La configuración ha finalizado



Pulse la tecla # para entrar en Asistencia

Top Level Intro

This page is printed before a new
top-level chapter starts

Part



VIII

8 MENÚ DEL SISTEMA 6 – CONFIGURACIÓN DEL ESCANER

8.1 Re-Escaneado

Esto es un modo operacional en el que el lector intenta repetidamente identificar una huella dactilar en la unidad óptica. El acceso no se concede o se deniega a menos que se coloque un dedo en la unidad óptica. El parámetro predeterminado es de 3 veces, y puede reescanear hasta 9 veces.



Pulse la tecla # para entrar en Reescaneado



Configuración finalizada



"C" indica el parámetro actual. Introduzca de 1 a 9

8.2 Nivel

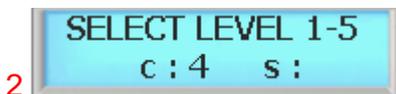
Este comando establece el nivel de seguridad que el lector utilizará tanto al verificar las huellas dactilares como al identificar las huellas dactilares. Los niveles de seguridad van de 1 a 7, siendo 5 el valor normal para verificación. El parámetro más alto de seguridad es 7 y el parámetro de menor seguridad es 1. Normalmente, un acceso de mayor seguridad requiere un parámetro de mayor seguridad. Para un funcionamiento adecuado, el nivel de seguridad de identificación debe establecerse a un valor superior al nivel de seguridad de verificación.



Pulse la tecla # para entrar en Reescaneado



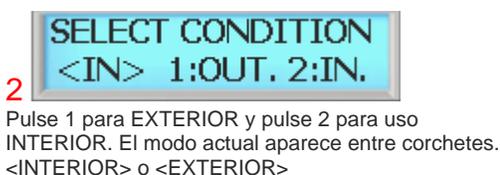
Configuración finalizada



"C" indica el parámetro actual. Introduzca de 1 a 7. El nivel predeterminado es 5.

8.3 Condiciones de iluminación

Esto es un modo operacional en el que el escáner establece las condiciones ambientales. Hay 2 condiciones disponibles, EXTERIOR e INTERIOR. Dependiendo del modo, el escáner se ajusta automáticamente al entorno para mejorar la capacidad de escaneado. El establecimiento del modo adecuado reduce enormemente el índice de falsos rechazos.



8.4 Modo de registro

8.5 Velocidad de identificación

El uso de una nueva Velocidad de Identificación puede acelerar hasta 10 veces la identificación, con una degradación relativamente baja de la precisión de autenticación. La Velocidad de Identificación tiene 6 niveles distintos, desde el modo 1 al 6.

1 
Pulse la tecla # para introducir CONDICIÓN DE ILUMINACIÓN

3 
Configuración finalizada

2 
"C" indica el parámetro actual. Introduzca de 1 a 6. El nivel predeterminado es 5.

Aunque la degradación de funcionamiento no es demasiada, el modo rápido no es necesario que se utilice en la identificación de pequeñas bases de datos, digamos de menos de 100 plantillas. En ese caso, la diferencia de identificación entre un modo normal y uno rápido no es significativa.

Top Level Intro

This page is printed before a new
top-level chapter starts

Part



IX

9 MENÚ DEL SISTEMA 7 – CONFIGURACIÓN DEL SENSOR

9.1 Tipo de entrada

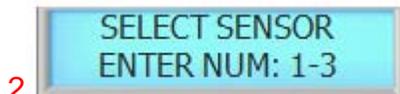
Las entradas del sensor vienen predeterminadas de fábrica a Normalmente Abierto (N.A.). Esta sección indica cómo cambiar la entrada del sensor a N.A o N.C.



1
Pulse la tecla # para introducir el Tipo de Entrada



3
Pulse la tecla 1 para N/A (significa Normal Abierto)
Pulse la tecla 2 para N/C (significa Normal Cerrado)



2
Seleccione del 1 a 6 seguido de la tecla #.



4
Configuración finalizada

9.2 Función

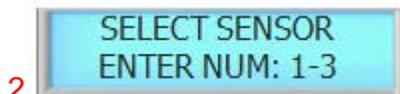
Éstas son las entradas del sensor que se encuentran en el panel de control de BioScan y que controlan los dispositivos externos. Hay 6 entradas de sensor en BioScan y todas se pueden programar para manejar distintos tipos de sensores externos desde el menú del sistema.



1
Pulse la tecla # para introducir Función



4
Pulse la tecla F1 para desplazarse hacia arriba por la lista de funciones
Pulse la tecla F2 para desplazarse hacia abajo por la lista de funciones. Consulte la Nota para obtener la lista completa de funciones. Una vez seleccionada, pulse la tecla #



2
Seleccione el sensor del 1 al 6. Consulte la nota sobre el sensor



5
La configuración ha finalizado

SENSOR1 1.EXIT
1:SETUP 2:CANCEL

3

El predeterminado está configurado a SALIDA. Se puede personalizar la función como se indica en la nota

NOTE :

Configuración predeterminada en fábrica de los sensores. Para obtener el diagrama de conexión, consulte el Conector de Sensor.

SENSOR 1: SALIDA

SENSOR 2: ALARMA (CONFIGURACIÓN ALARMA: SENSOR ALARMA)

SENSOR 3: ALARMA INCENDIO (CONFIGURACIÓN ALARMA: ALARMA INCENDIO)

SENSOR 4: BLOQUEO (CONFIGURACIÓN ALARMA: BLOQUEO MANTENIDO)

SENSOR 5: CONTACTO PUERTA (CONFIGURACIÓN ALARMA: FORZAR ABIERTO / SOSTENER PUERTA)

SENSOR 6: INTRUSIÓN (CONFIGURACIÓN ALARMA: INTRUSIÓN)

Los sensores se utilizan en conjunción con la configuración de las alarmas. Una vez activado el sensor, vaya a Configuración de Alarma y configure el tipo de salida. Los sensores se pueden reprogramar dependiendo de la instalación.

9.3 Fallo de línea

Cuando se supervisa el fallo de línea, se monitorizan constantemente las comunicaciones o los cortes causados por fallos de cableado o intrusión. Cuando se detecta un error, se envía al operador un informe con los problemas. Los sistemas están disponibles con o sin entradas supervisadas de alarma. El resultado de las alarmas debe configurarse en 7. Configuración de Alarma /7. Fallo de línea.



1
Pulse la tecla # para entrar en Fallo de Línea



3
Mensaje de configuración finalizada

LINE SENSING ?
1:YES 2:NO

Pulse la tecla 1 para habilitar la monitorización de la línea
Pulse la tecla 2 para deshabilitar la monitorización de la línea

Top Level Intro

This page is printed before a new
top-level chapter starts

Part



X

10 MENÚ DEL SISTEMA 8 – CONFIGURACIÓN DE ALARMAS

10.1 Configuración de Alarmas

En el BSC-101 hay 6 entradas de sensor y 2 relés. Para el bloqueo se utilizan uno o dos relés, dependiendo de la configuración, y el relé de repuesto se puede utilizar para alarmas de anuncio u otra forma de control.

No hay función de programación para las alarmas; lo que se programe es lo que ocurrirá cuando se produzca una alarma determinada. Como resultado de una alarma pueden ocurrir dos cosas:

- una alarma puede dar como resultado el envío de un mensaje al altavoz (Timbre).
- una alarma también puede hacer que se active un relé (Relé).

BSC-101 tiene una salida para activar un generador sonoro pero también está equipado con relés que se pueden controlar desde una estación de control, mediante algún tipo de actividad del sistema. Estas entradas & relés de sensor permiten realizar muchas funciones, tales como sensor de movimiento o como medio de interactuar con un sistema de automatización doméstico. Sólo se activarán los sensores internos a menos que haya otros sensores conectados y configurados en Configuración de Sensores. Para usar la alarma, el relé debe estar conectado. Consulte Conector de relé.



- 1** Hay un total de 12 alarmas. Para obtener la lista completa, consulte la **Figura 1** a la izquierda. Pulse la tecla # para entrar en Abrir Carcasa



- 2** Pulse la tecla 1 para configurar Alarma.
Pulse la tecla número 2 para cancelar



- 3** Pulse la tecla F1 para desplazarse hacia arriba por la lista de funciones
Pulse la tecla F2 para desplazarse hacia abajo por la lista de funciones



- 4** Hay un total de 4 opciones de sonido. Consulte las opciones de la lista de sonidos en la **figura 2**. Por ahora, seleccionaremos 1 Timbre & Relé y después pulse la tecla #



- 5** Finalizada la configuración de la alarma

NOTE :

Figura 1

8> ALARM SETUP
F1:UP F2:DN

(Figura 1) Lista de alarmas. Seleccione de la siguiente lista

8> ALARM SETUP
1.CASE OPEN

Manejado por sensor interno.

8> ALARM SETUP
2.INTRUSION

Pre-programado a sensor 6 (INTRUSIÓN).

8> ALARM SETUP
3.FORCE OPEN

Pre-programado a sensor 5 (CONTACTO PUERTA).

8> ALARM SETUP
4.ALARM SENSOR

Pre-programado a sensor 2 (ALARMA).

Figura 2

SELECT FUNCTION
F1:UP F2:DN

(Figura 2) Lista de funciones de salida. Seleccione de la siguiente lista

BUZZER&RELAY
1.BUZZER&RELAY

El Timbre y el Relé se activarán una vez que se active la alarma.

BUZZER&RELAY
2.BUZZER ONLY

El Timbre se activará una vez que se active la alarma. No se enviará salida de relé.

BUZZER&RELAY
3. RELAY ONLY

El Relé se activará una vez que se active la alarma. No se oirá sonido alguno.

La Alarma está inactiva. El Evento se producirá y será registrado incluso si las alarmas están inactivas. Para deshabilitar las alarmas completamente, deshabilite el sensor que está supervisando la alarma activada.



8> ALARM SETUP
5.FIRE

Pre-programado a sensor 3 (ALARMA DE INCENDIO).

8> ALARM SETUP
6.DURESS

Manejado por Configuración del Sistema / 13 Coacción. Debe habilitarse en Coacción.

8> ALARM SETUP
7.LINE TROUBLE

Manejado por Fallo de Línea en Configuración de Sensor / 3. Fallo de Línea. Debe habilitarse en Fallo de Línea en Configuración de Sensor.

8> ALARM SETUP
8.BOLT OPEN

Manejado por sensor interno.

8> ALARM SETUP
9.DOOR HELD

Pre-programado a sensor 5 (CONTACTO PUERTA).

8> ALARM SETUP
10.LOCK HELD

Pre-programado a sensor 4 (BLOQUEO).

8> ALARM SETUP
11.ALARM TIME

Duración del tiempo de la alarma. Tiempo de alarma se aplicará a todas las alarmas.

8> ALARM SETUP
12.ALARM OFF

Deshabilitar alarma. El evento se producirá y se registrará incluso si las alarmas están inactivas. Para deshabilitar completamente las alarmas, deshabilite el sensor que está supervisando la alarma activada.

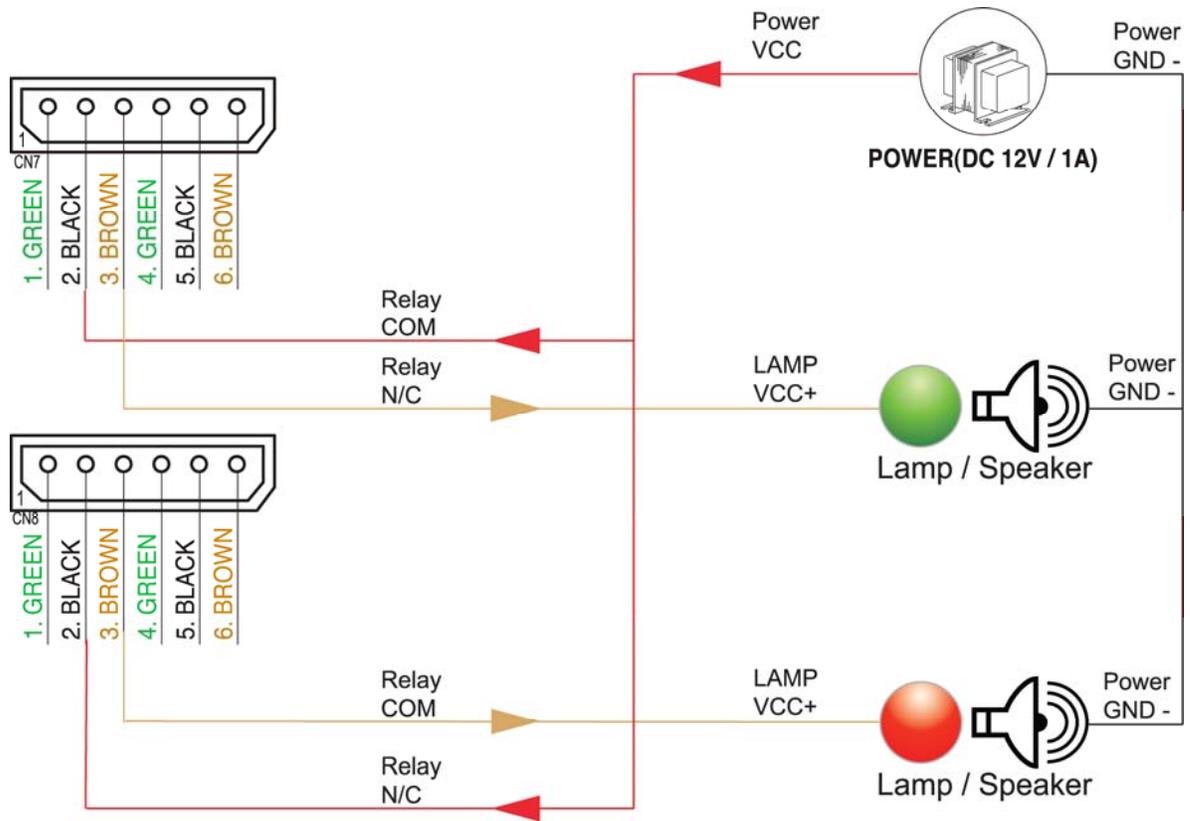
8> ALARM SETUP
13. ALARM BELL

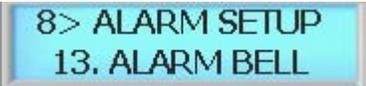
Maneja el timbre de la alarma.

10.2 Conexión de Luz & Alarma externas

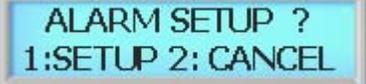
10.2.1 Diagrama de conexión de alarma

Para conectar un altavoz o una luz externos, utilice la conexión de Luz Roja (CN8). Luz Roja está asociado al relé 2, establecido como alarma.



1 

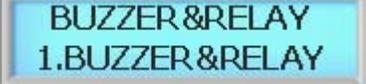
Pulse la tecla # para entrar en Configuración Alarmas

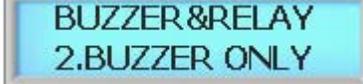
2 

Pulse 1 para configurar timbre de alarma y 2 para cancelar

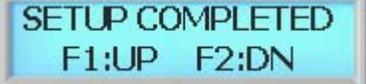
3 

Pulse la tecla F1 para desplazarse hacia arriba por la lista y la tecla F2 para desplazarse hacia abajo. Hay un total de 4 opciones.

4 



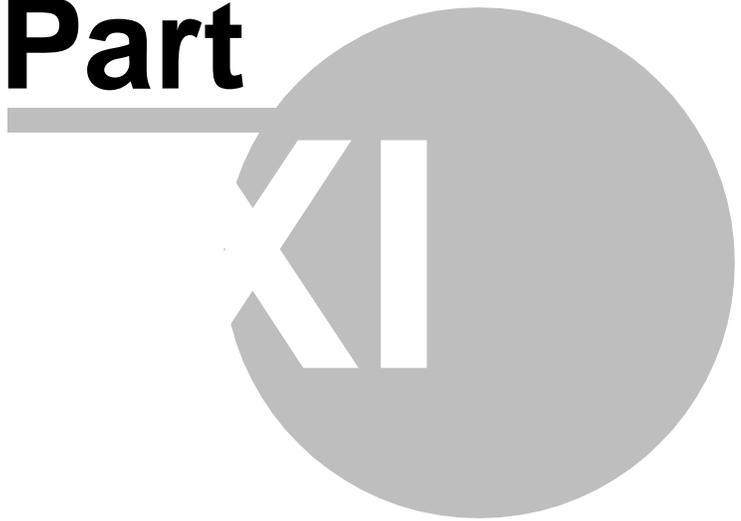
Seleccione de la lista pulsando la tecla #

5 

Configuración finalizada.



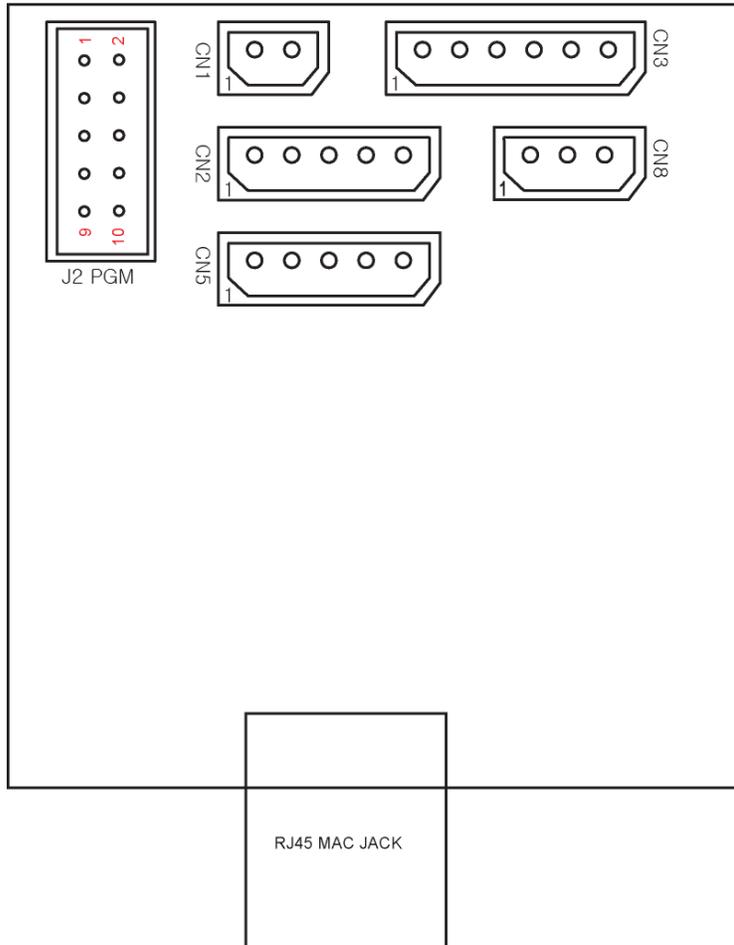
Part





11 GUÍA DE INSTALACIÓN

11.1 Diseño del conector



CN1: POWER

- 1: VCC (12V)
- 2: GND

CN2: WIEGAND OUT

- 1: VCC (12V)
- 2: GND
- 3: DATA0 OUT
- 4: DATA1 OUT
- 5: SENSOR 3

CN3: RELAY

- 1: N/C 1
- 2: COM 1
- 3: N/O 1
- 4: N/C 2
- 5: COM 2
- 6: N/O 2

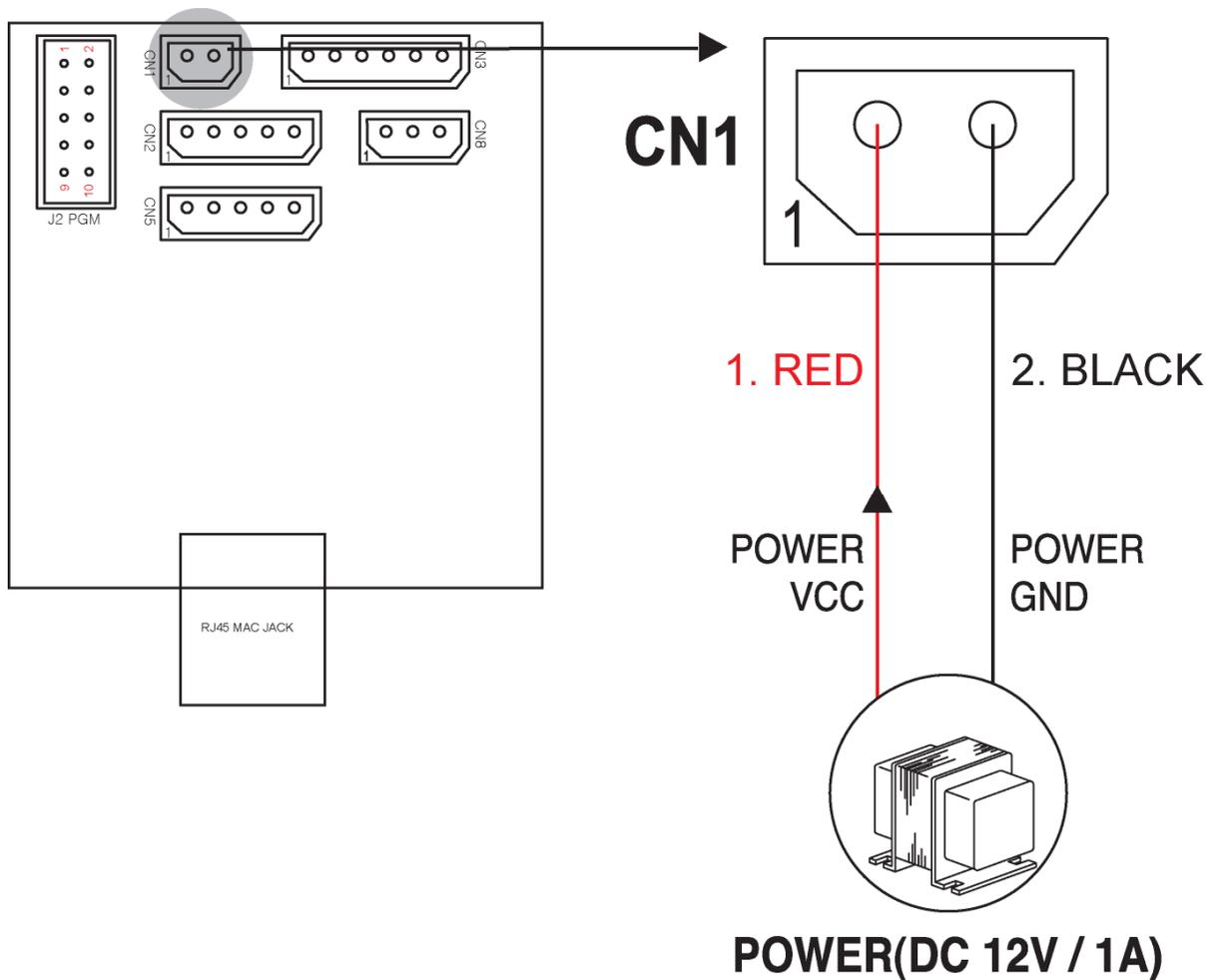
CN5: 232

- 1: VCC OUT(12V)
- 2: RX
- 3: TX
- 4: ENABLE
- 5: GND

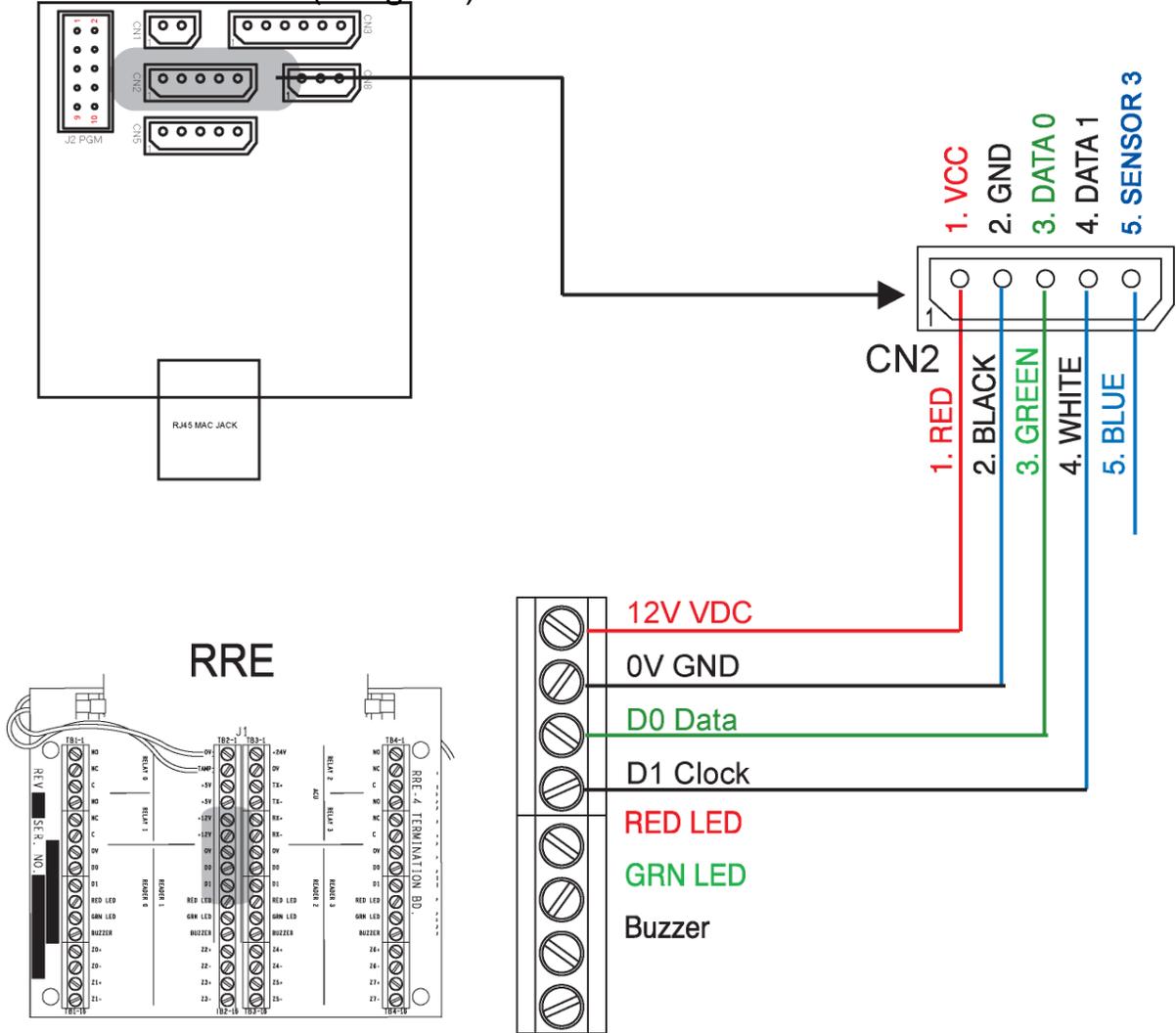
CN8: SENSOR INPUT

- 1: SENSOR 1 (EXIT)
- 2: SENSOR 2 (DOOR CONTACT)
- 3: GND

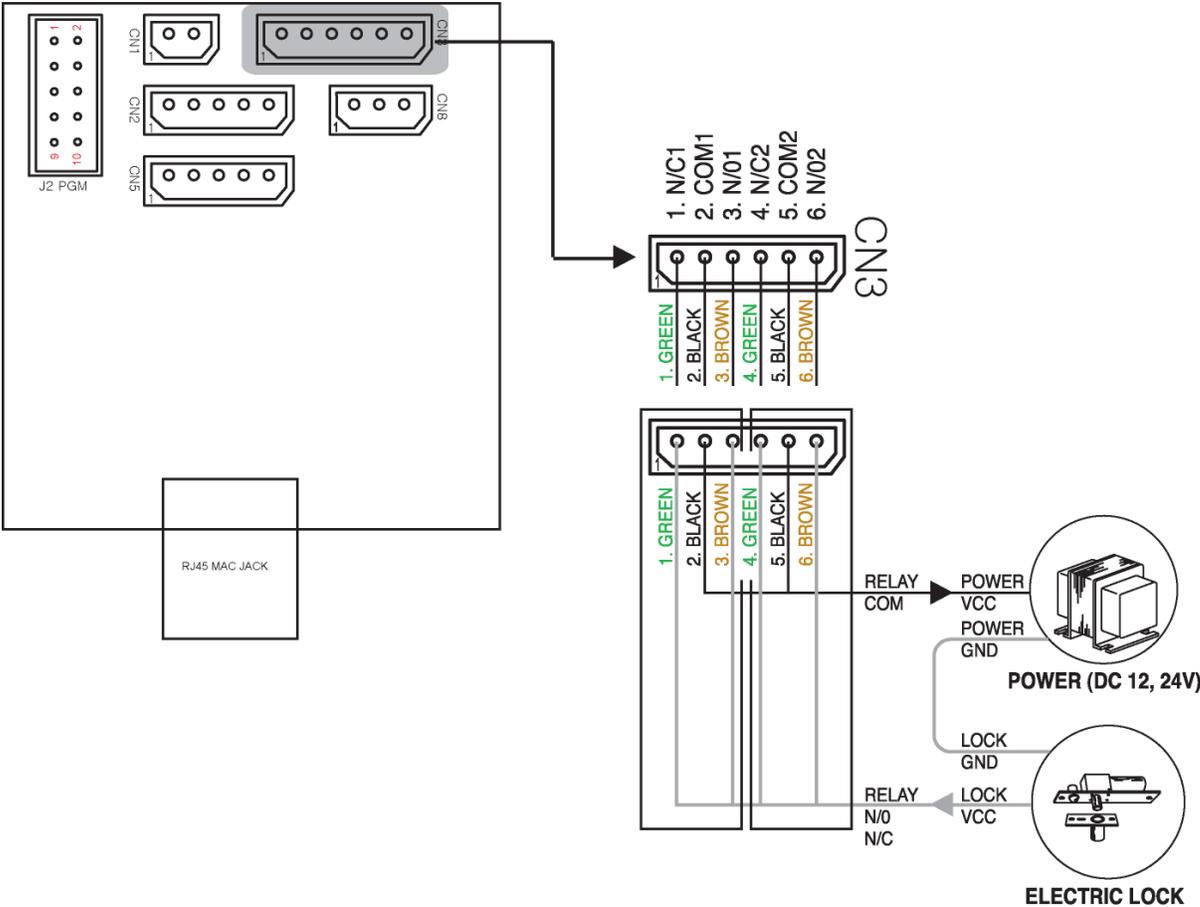
11.2 CN1: Conector de alimentación



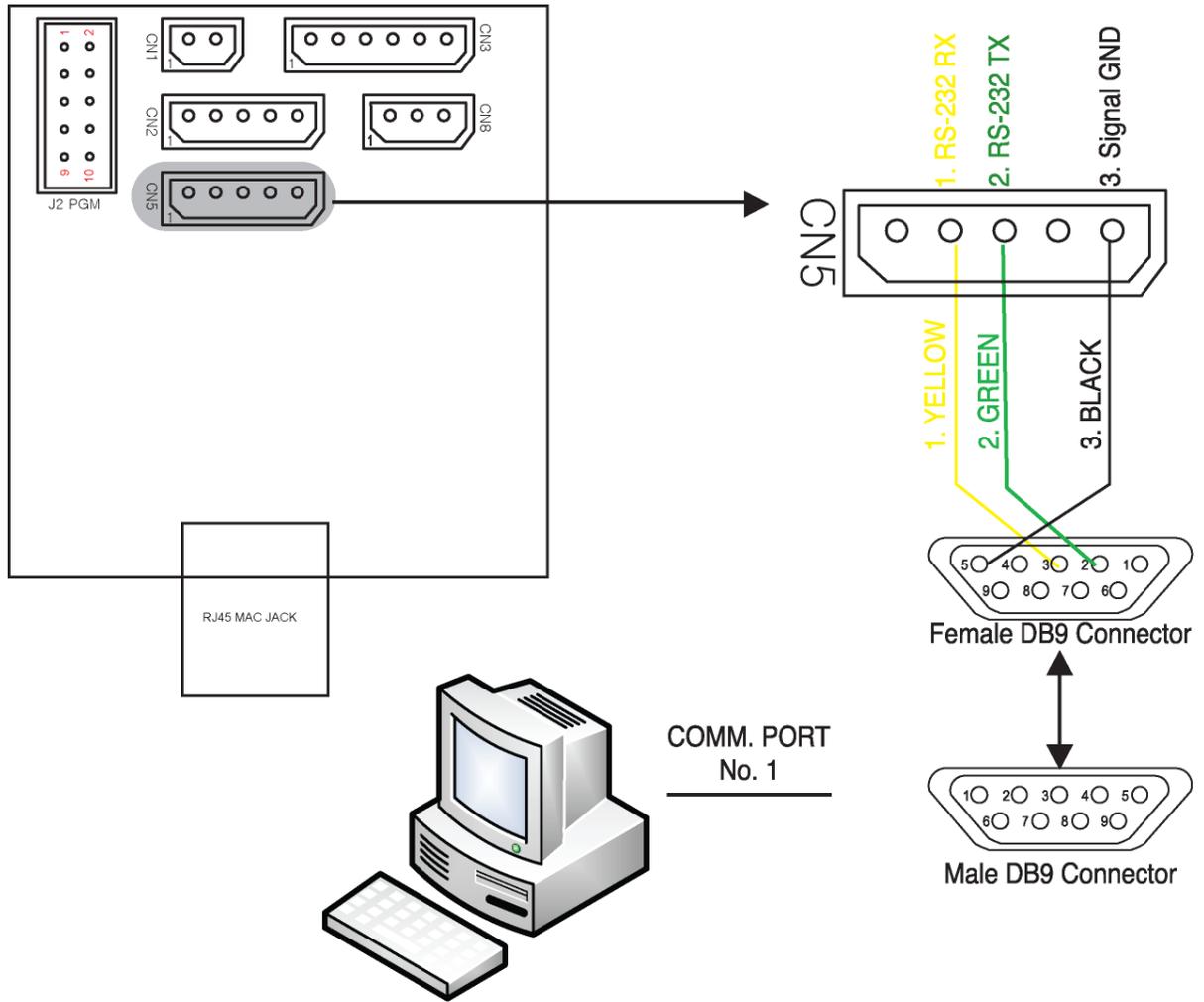
11.3 CN2: Conector RRE (Wiegand)



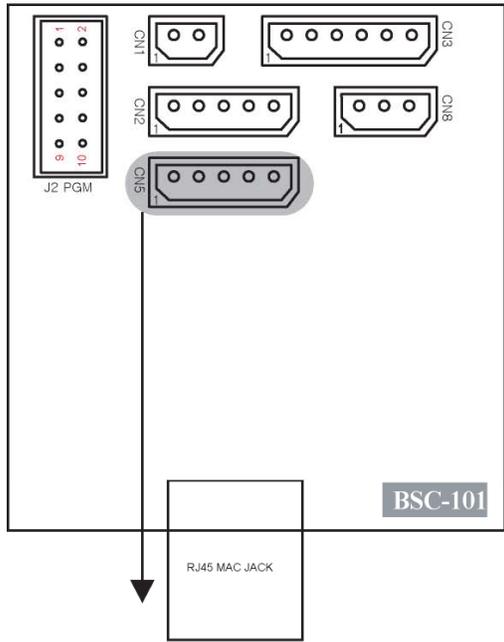
11.4 CN3: Conector de relé



11.5 CN5: Conector RS232



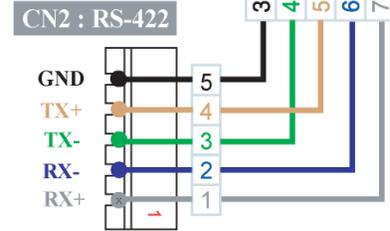
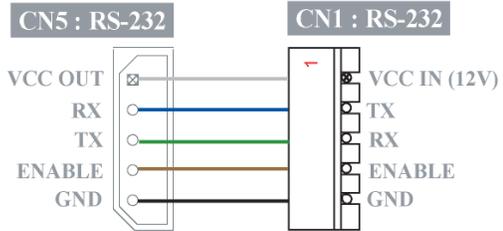
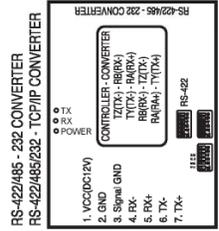
11.6 CN5: Conexión Convertidor RS422



HOST COMPUTER



CONVERTER

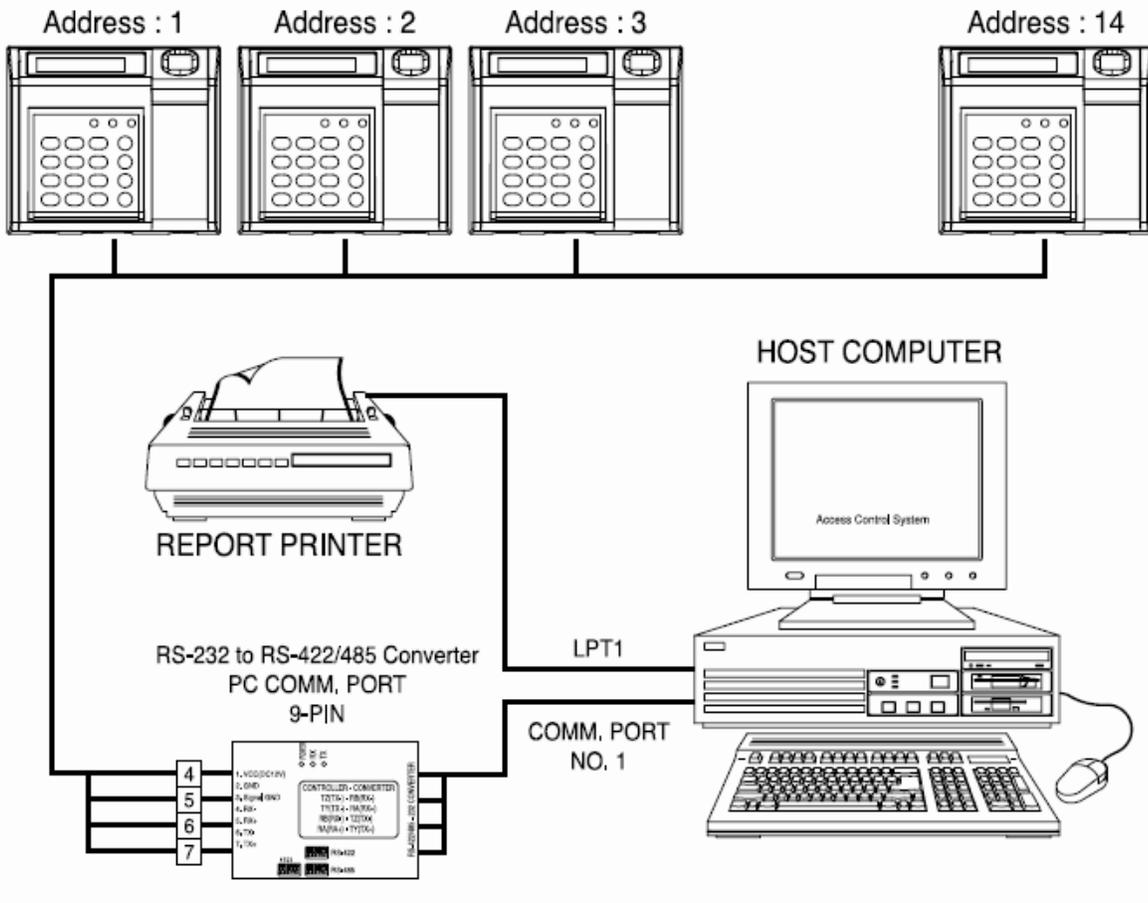


TYPICAL BSC-101 / RS-422 CONFIGURATION #1

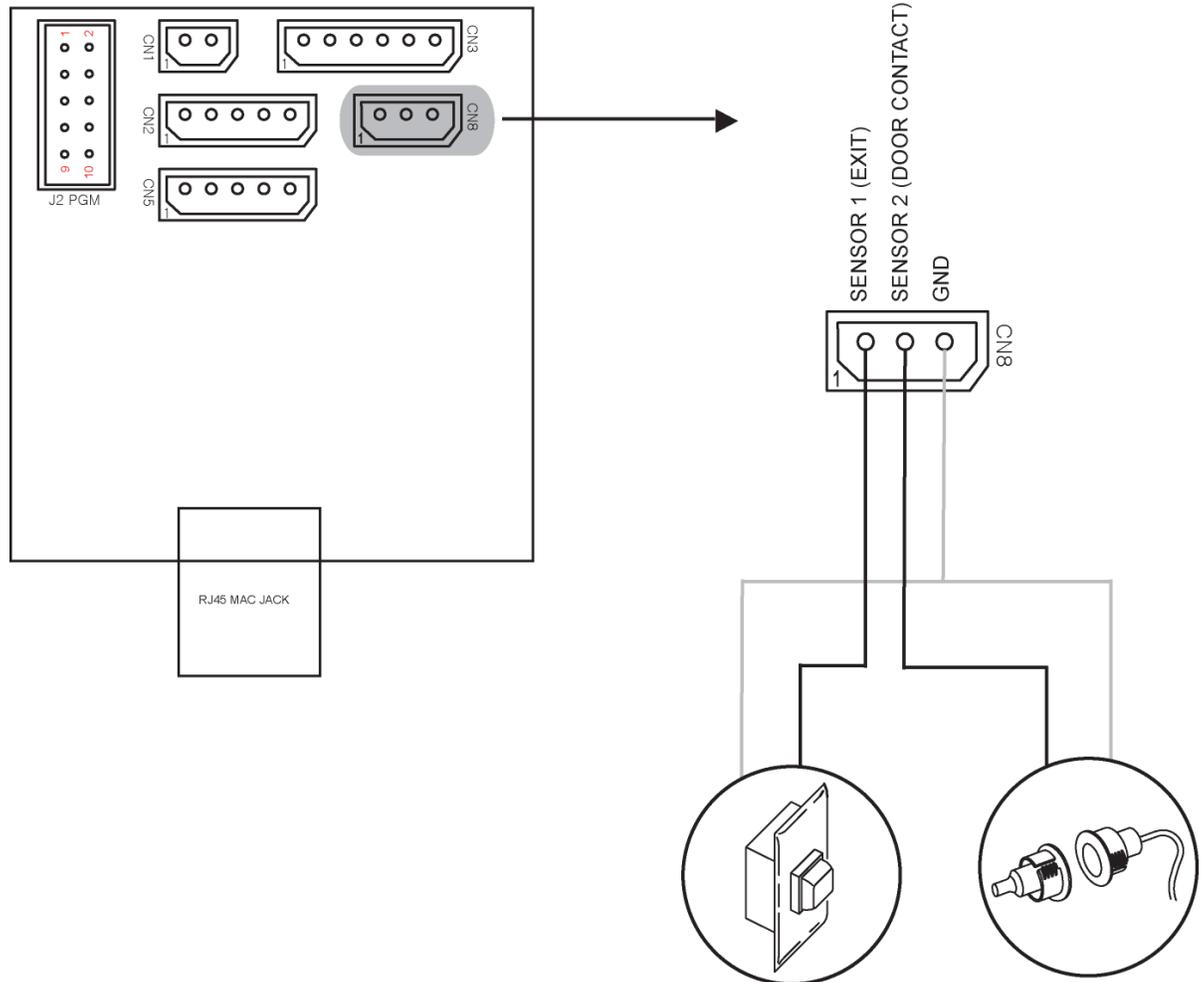
NOTE :

RX & TX deben cruzarse para que funcionen con un convertidor. Por favor, asegúrese de que cruza el cable como se indica anteriormente.

11.6.1 Red RS422



11.7 CN8: Conector de sensor



NOTE :

Todos los sensores están deshabilitados excepto Sensor (conmutador de salida). Por favor, si se van a utilizar, habilite los sensores desde el menú del sistema.

11.8 Diagrama de instalación

Índice

- A -

Dirección 49
Configuración de alarma 76
Retropase 53
Asia 54
Asistencia 60
Relés auxiliares 73

- B -

Velocidad de comunicación 51
Timbre 76

- C -

Velocidad Com. 51
Contraseña de comunicaciones 49
Ocultar PIN 58
Visualización personalizada 55

- D -

Formato de fecha 54
Borrar Todos los Usuarios 43
Borrar Usuario Individual 43
Visualizar ENTRADA o SALIDA 60
Relé de Puerta 52
Coacción 53

- E -

Modificar Tarjeta de Usuario 32
Modificar la Huella Dactilar del Usuario 31
Modificar ID de Usuario 31

Modificar el Nivel de Usuario 32

Modificar el Nombre de Usuario 33

Registrar Bloque de Tarjetas 27

Registrar tarjeta 25

Registrar Tarjeta & Huella Dactilar 26

Registrar huella dactilar 24

Europa 54
Reinicialización de Eventos

51
Eventos 39
sistema de alarmas externo 58

- F -

Código de instalación

50
Versión Escáner Huella 40
firmware 40
Función 73
Teclas de función 60

- I -

Opción ID 35
INTERIOR 70
Tipo de entrada 7
3

- L -

Luz de LCD 57
Condiciones de iluminación 70
Fallo de línea 74
Hora cierre 48
Cierre 58

- N -

ID Red 4
9
Normalmente Abierto 52

- O -

| | |
|---|----|
| Funcionamiento del BioScan | 17 |
| Funcionamiento de la Tecla de Funciones | 19 |
| Modo de funcionamiento | 45 |
| EXTERIOR | 70 |

- P -

| | |
|----------|----|
| Posición | 11 |
| Presión | 11 |

- R -

Tiempo bloqueo Re 48
Re-Escaneado 69
Rotación 11

- S -

Niveles de seguridad 69
Establecer el Modo de Funcionamiento 47
Código de Instalación 50
Reinicialización del sistema 50

- T -

Hora 45
Dos Personas 35, 52

- U -

código de identificación único 49
EE.UU.54
Retropase de usuario 34
Lista de usuarios 38

Endnotes 2... (after index)

Back Cover