Índice de manual.

Introducción.

En este manual se describen los procedimientos para la correcta configuración inicial de las tecnologías biométricas de la marca Virdi y su integración con los sistemas de control de asistencia Ingressio en la nube y cliente servidor así como los procedimientos técnicos para la integración de los dispositivos biométricos con otros componentes electro-mecánicos compatibles para el control de accesos y otras funcionalidades.

Consideraciones:

- En este manual se describen configuraciones eléctricas las cuales son extraídas de los manuales de fabricante y estas se deben valorar y ejecutar por personal calificado para dichas actividades.
- La marca Ingressio México S.A. de C.V no se hace responsable de daños ocasionados a dispositivos biométricos por la incorrecta aplicacion de esta información.

Configuraciones generales y de red para dispositivos biométricos.

En este módulo se describen los procesos para la configuración básica de parámetros generales y de red para los dispositivos biométricos de la familia Virdi AC-2100 y AC-6000

Descripción de operación de dispositivo AC-2100:

Botón	Función
F1	- Inicialmente modo de registro "Entrada Laboral". - En modo de menú: - Funciona como opción [ESC] - Funciona como opción de movimiento [←] "Retroceso" se presiona por 2 segundos para regresar entre ventanas de configuraciones realizadas.
F2	- Inicialmente modo de registro "Salida Comida" - En modo de menú funciona como una opción de movilidad dentro del menú **[↑] "Arriba".**
F3	- Inicialmente modo de registro "Entrada Comida" - En modo de menú funciona como una opción de movilidad dentro del menú **[↓] "Abajo"** - Se presiona por 3 segundos para acceder a las opciones de menú.
F4	- Inicialmente modo de registro "Salida laboral". - En modo de menú: - Funciona como opción [ENT] - Funciona como opción de movimiento [→] "Avance" se presiona por 2 segundos para continuar entre las ventanas de configuración realizadas.

Configuraciones de sistema:

Accedemos mediante la siguiente secuencia de ventanas

(A) Menú principal ingresamos a la opción **6. Device**	(B) Menú Device ingresamos a la opción **1. System Config**	(C) Seleccionamos la longitud de la cadena de Número de Empleado utilizado en proceso de alta en lector.
1.User 2.Network 3.Option 4.Terminal Info 5.Ext Function 6.Device	1.System Config 2.Card Reader 3.FP-Sensor 4.Wiegand 5.Initialize	<UserID Length> 2 3 4 5 6 7 8
[ESC] [↑] [↓][ENT]	**[ESC][↑][↓][ENT]**	**[ESC][←][→][ENT]**

(D) Ingresamos el numero de opcion acorde a idioma a configurar		(E) Regresamos hasta la opción de guardar configuración con botón F1
<Language>:01 0=K 1=E 2=J 3=ES 4=P 5=PT 6=C 7=U 8=I 9=VT 10=TH 11=TW 12=DA 13=R 14=FR 15=FA	Default setting: '1=EN' 0=Korean, 1= English, 2=Japanese, 3=Spanish, 4=Polish, 5=Portuguese, 6=Chinese, 7=Arabic, 8=Italian, 9=Vietnamese,10=Thai,11=Taiwanes 12=Danish,13=Russian,14=French, 15=Farsi	Save? 1.Yes 2.NO
[ESC][↑][↓][ENT]		**[ESC] [↑] [↓][ENT]**

Configuraciones de red: ID Terminal

(A) Ingresamos a la opción de menú 2. Red	(B) Ingresamos a las opción ID terminal e ingresamos el dato requerido		(C) Seleccionamos el modo de validación de registros.
1.Usuario **2.Red** 3.Opciones 4.Informacion 5.Func. Extra 6.Terminal	**1. ID Terminal** 2. Dirección IP 3. IP Servidor	< ID Terminal > ID : 0000000**1**	<Modo> 0.NS **1.SN** 2.NO 3.SO
[ESC] [↑] [↓][ENT]	**[ESC] [↑] [↓][ENT]**	**[←] [↑] [↓] [→]**	**[ESC] [↑] [↓][ENT]**

Niveles de seguridad para autentificación de usuarios.	
NS	Si está conectado el servidor, la autenticación se procesa en el servidor. Si el servidor se desconecta debido a un fallo de red, la autenticación se procesa en la terminal.
SN	Incluso si está conectado el servidor, la autenticación se procesa en el terminal y el resultado de la autenticación se envía al servidor en tiempo real. Sin embargo, si un usuario que no estuviese registrada en el terminal, la autenticación se procesa en el servidor. (En caso de 1: N autenticación de huellas digitales, autenticación de servidor no se intenta.)
NO	Incluso si un usuario se ha registrado en el terminal, la autenticación siempre se procesa en el servidor.
SO	Sólo un usuario registrado en el terminal está autenticado. Si está conectado el servidor, el resultado de la autenticación se envía en tiempo real.

Configuraciones de red: Dirección IP

(A) Ingresamos a la opción 2.Direccion de red	(B) Ingresamos a la opción acorde a su escenario de red Se recomienda asignar una IP Estática	(C) Ingresamos la dirección IP, Mascara de Red y Puerta de Enlace
1. ID Terminal 2. Dirección IP 3. IP Servidor	<Tipo de Red> 0: Estatica 1:DHCP	<Dirección IP> 192.168.000.010 <Mascara de Red> 255.255.255.000 < Puerta Enlace > 192.168.000.001
[ESC] [↑] [↓][ENT]	**[ESC] [↑] [↓][ENT]**	**[←] [↑] [↓] [→]**

Configuraciones de red: IP Servidor

(A) Ingresamos a la opción 2.Direccion de red	(B) Ingresamos a la opción acorde a su escenario de red Se recomienda asignar una IP Estática	(C) Ingresamos la dirección IP, Mascara de Red y Puerta de Enlace	(D) Regresamos hasta la opción de guardar configuración con botón F1
1. ID Terminal 2. Dirección IP 3. IP Servidor	< Server IP > 184.72.217.188	< Server Port > Num : 9870	Save? 1.Yes 2.NO
[ESC] [↑] [↓][ENT]	**[←] [↑] [↓] [→]**	**[←] [↑] [↓] [→]**	**[ESC] [↑] [↓][ENT]**

Registro de usuarios en dispositivo biométrico.

En este módulo se describen los procesos para el alta o registro de empleados o usuarios en dispositivo biométrico sean estos usuarios estándar o del tipo administrador.

Ejemplo para dispositivos biométricos de la familia Virdi AC-2100:

(A) Ingresamos a la opción de menú 1. Usuario	(B) Seleccionamos la opción adecuada ya sea Anadir o Añadir Admin	(C) Ingresamos el ID de usaurio	(D) Seleccionamos el tipo de autentificación deseado
1.Usuario 2.Red 3.Opciones 4.Informacion 5.Func. Extra 6.Terminal	1. Anadir 2. Eliminar 3. Modificar 4. Añadir Admin 5. Eliminar Todo	< ID Usuario > ID : 00001	<Auth Type> 1. FP 2. Card 3. Cardo or FP 4. Card and FP
[ESC] [↑] [↓][ENT]	**[ESC] [↑] [↓][ENT]**	**[←] [↑] [↓] [→]**	**[ESC] [↑] [↓][ENT]**

(D) Seleccionamos de la escala el nivel de rapidez para validar dato biometrico	(E) Ingresamos nuestro registro biométrico o de tarjeta	Tipos de autentificación
0 1 2 3 4 5 6 7 8	**<Add FP>** Input your Fingerprint **<Add FP>** Please try again **<Registro completado>**	**FP** -> Solo Huella Dactilar **Card** -> Solo Tarjeta de Proximidad **Card or FP** -> Huella Dactilar o Tarjeta de Proximidad **Card and FP** -> Tarjeta de Proximidad y Huella Dactilar
[ESC] [↑] [↓][ENT]		

Validación de interconexión de dispositivos biométricos.

En este módulo se describen una serie de procesos básicos recomendados para la validación de la correcta conexión de nuestros dispositivos biométricos a la red local de usuario final, así como la confirmación exitosa de interconexión del dispositivo biométrico con su base de datos en la nube.

Prerrequisitos:

- Correcta configuración de parámetros generales y de red en dispositivos biométricos.
- Alta de usuario “solo se requiere el alta de un empleado” tanto en sistema como en dispositivo biométrico para una actividad de validación efectiva.

Consideraciones:

- Al ser este un tema de carácter técnico se recomienda realizar actividad por parte de personal especializado.

Prueba (A) Conexión de dispositivo biométrico a red local:

Paso uno: abrimos una venta de línea de comandos “Símbolo de sistema” en un equipo de cómputo conectado en el mismo segmento de red al que está conectado nuestro dispositivo biométrico, Inicio-> Ejecutar-> “CMD” o “Símbolo de Sistema”, igualmente podemos ubicar la herramienta en nuestra lista de programas en PC.

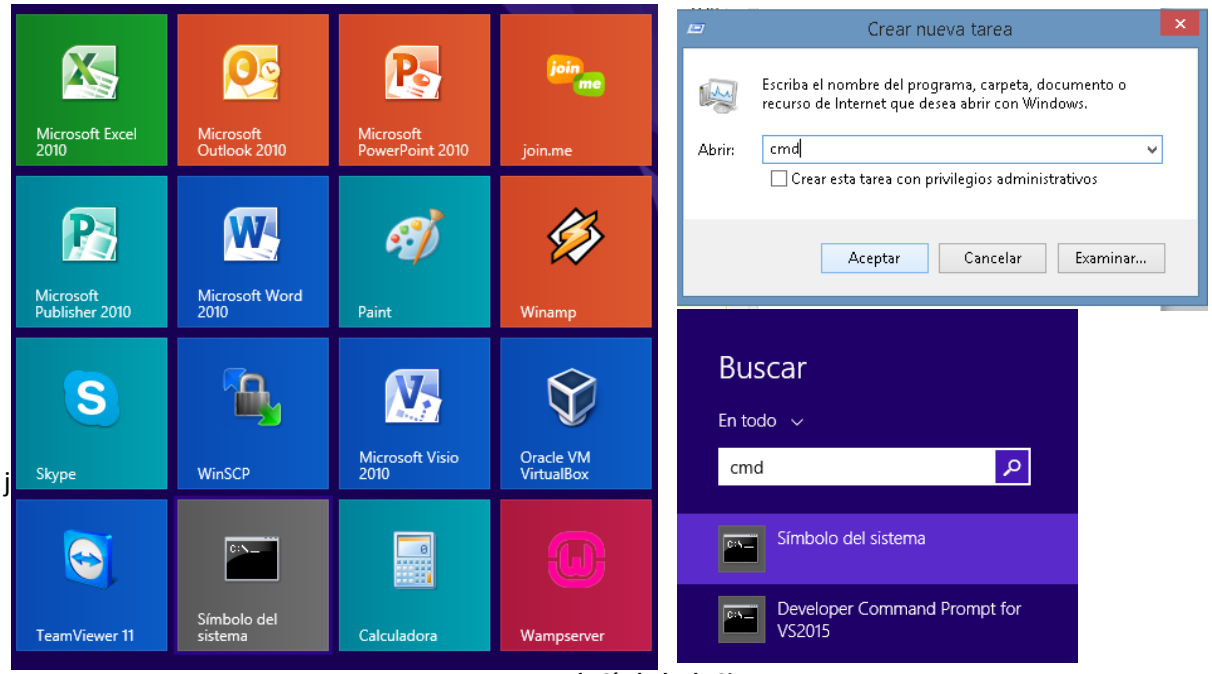


Imagen 1 – Icono de Símbolo de Sistema

Paso dos: en línea de comandos tecleamos el siguiente comando: **C:\>ping X.X.X.X**, donde las X son el parámetro de IP local asignado a lector, ejemplo: **C:\>ping 192.168.0.200** y finalmente ejecutamos el comando preciando la tecla **Enter**.

Este paso nos dará como resultado exitoso la siguiente sucesión de líneas:

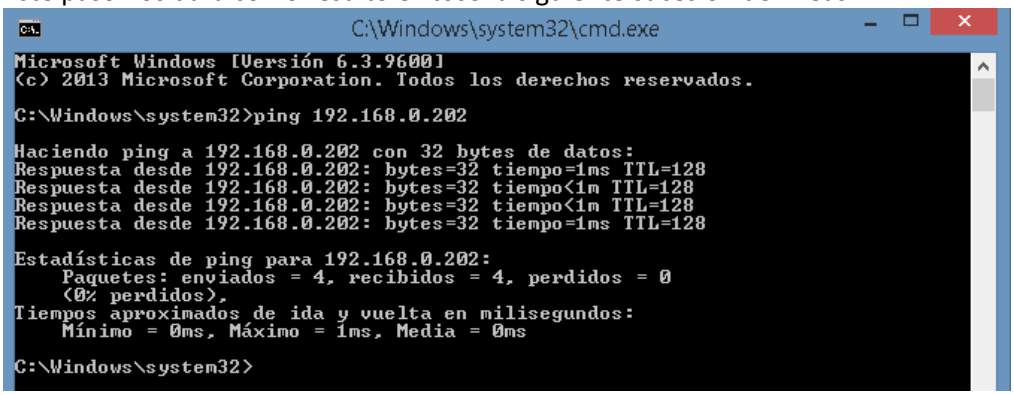


Imagen 1 – Ventana de sistema ping exitoso

De lo contrario como resultado tendremos la siguiente sucesión de líneas:

Imagen 1 – Ventana de sistema ping fallido

Si es el caso de **validación fallida** se deben valorar aspectos de comunicación interna en su red local como cableado de red se recomienda usar un cable plano con la configuración tipo B, confirmar apertura de puerto asignado a dispositivo de entrada y salida tanto en firewall como con el proveedor de servicio de internet, finalmente confirmar la correcta configuración de parámetros de red en dispositivos biométricos.

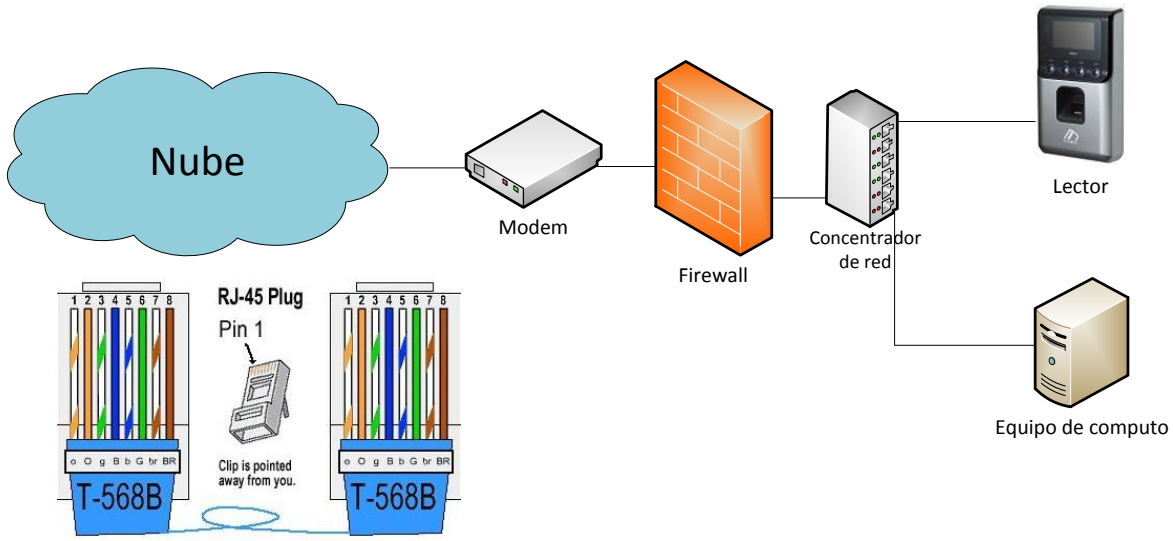


Imagen 1 – Esquema de red local estándar.

Prueba (B) Interconexión de dispositivo biométrico a base de datos en la nube:
En esta prueba lo que pretendemos valorar es el hecho de envió de datos del tipo registros o checadas desde un dispositivo biométrico a su correspondiente base de datos en la nube por lo cual debemos tener todas las partes antes descritas en manual cubiertas y validadas exitosamente.

Paso uno: realizar una serie de checadas o registros físicos en lector validando que el registro del empleado en cuestión sea exitoso.

Paso dos: ingresar a nuestra cuenta de sistema en la nube a la opción de menú Lectores->Monitor de Terminales AC, esta ventana lo que nos despliega y muestra es la relación de Poleos entendiéndose con esto la actividad de envió de datos de dispositivo biométrico a base de datos y registrándose así las últimas fechas de interconexión de los biométrico y los minutos sin actividad.

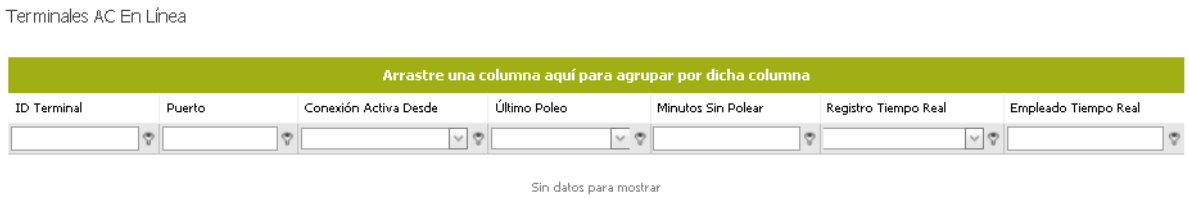


Imagen 1 – Ventana de sistema Poleo inexistente

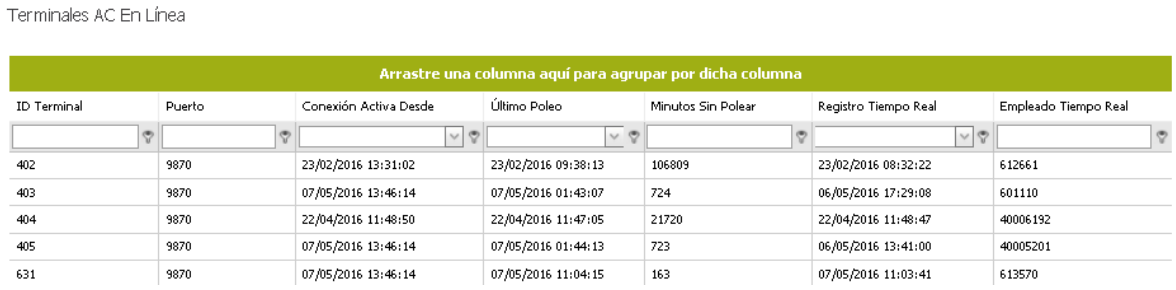


Imagen 1 – Ventana de sistema Poleo exitoso

Pasó tres: finalmente y para cerrar por completo el ciclo de interconexión de dispositivos biométricos con sistema ingresamos a nuestra cuenta de sistema en la nube y generamos un reporte del tipo Accesos en la siguiente ruta de menú Reportes->Reporteados->Accesos para el día en que se realizó la actividad.
El reporte del tipo Accesos genera una lista de registros o checadas físicas en lector obtenidas de un proceso de Poleo exitoso por tanto este reporte nos debe confirmar la fecha, hora, ID de Terminal y empleado registrado correctamente.

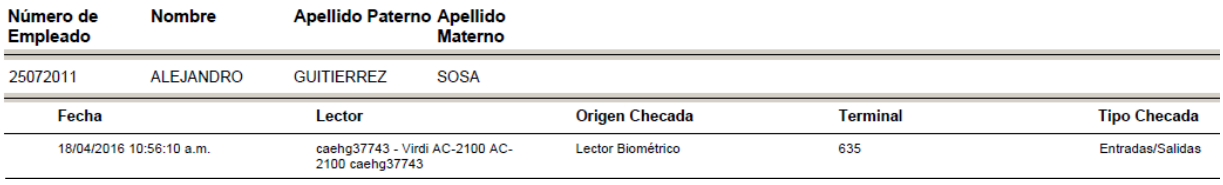
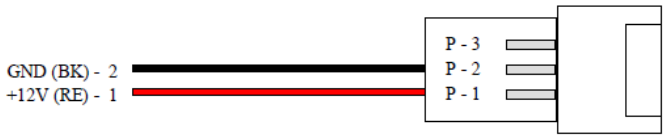


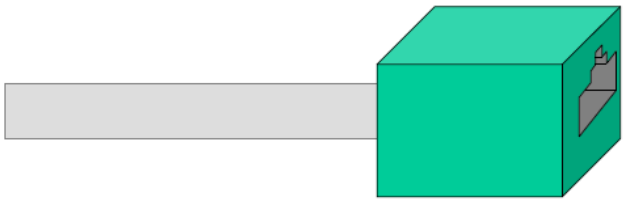
Imagen 1 – Reporte Accesos

Descripción de conexiones eléctricas.

Especificaciones eléctricas para dispositivo biométrico Virdi AC-2100.

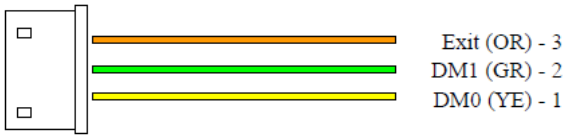


Cable adaptador de voltaje (101)



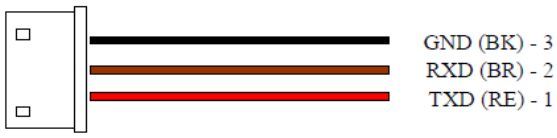
Cable de red RJ45 (102)

Lock Cable (4P) "Cable de control para aperturas" (103)

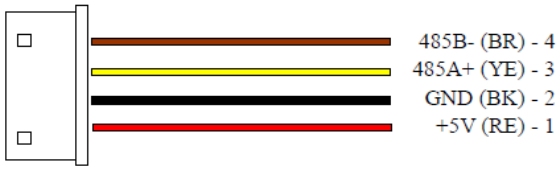


Lock Monitor & Exit Cable (3P) "Cable de control para pulsos de bandera" (104)

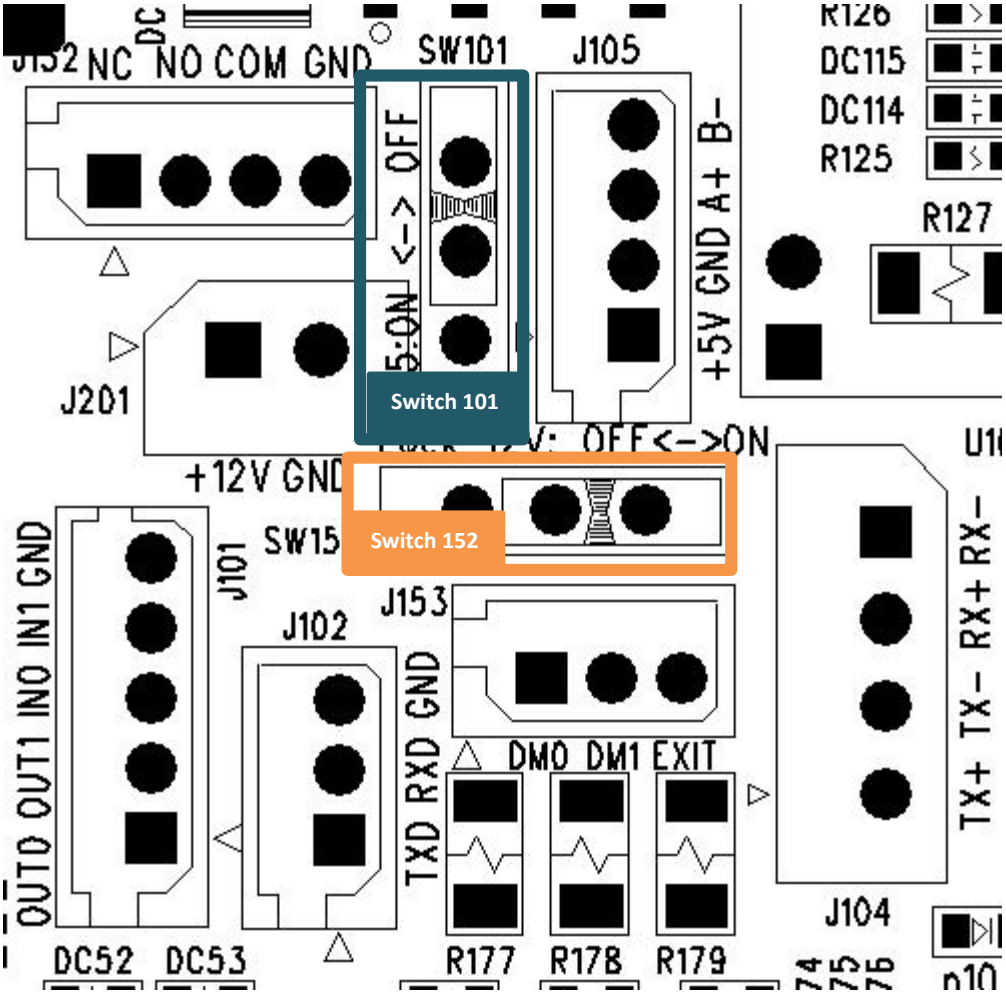
Wiegand Cable (5P) "Cable de control para tecnologías de tarjetas de proximidad" (105)

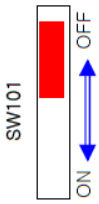


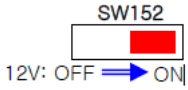
RS232 Cable (3P) "Cable de control para comunicaciones estándar Serial RS232" (106)



RS485 Cable (4P) "Cable de control para comunicaciones estándar Serial RS485" (107)





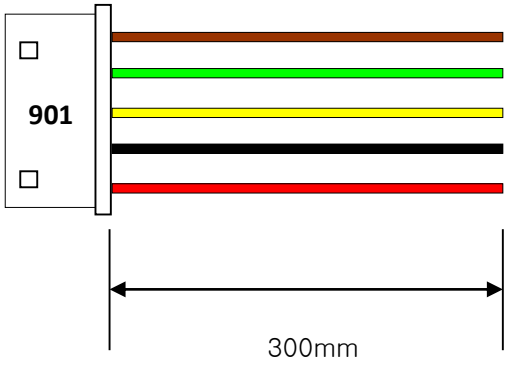


Switch 101 OFF-> Comunicación RS485 deshabilitada
ON -> 120 Ohm resistencia conectada entre 485A and 485B

Switch 152 OFF-> Voltaje deshabilitado
ON-> Voltaje 12 V. habilitado para controles de apertura

Especificaciones eléctricas botón liberador EB-030.

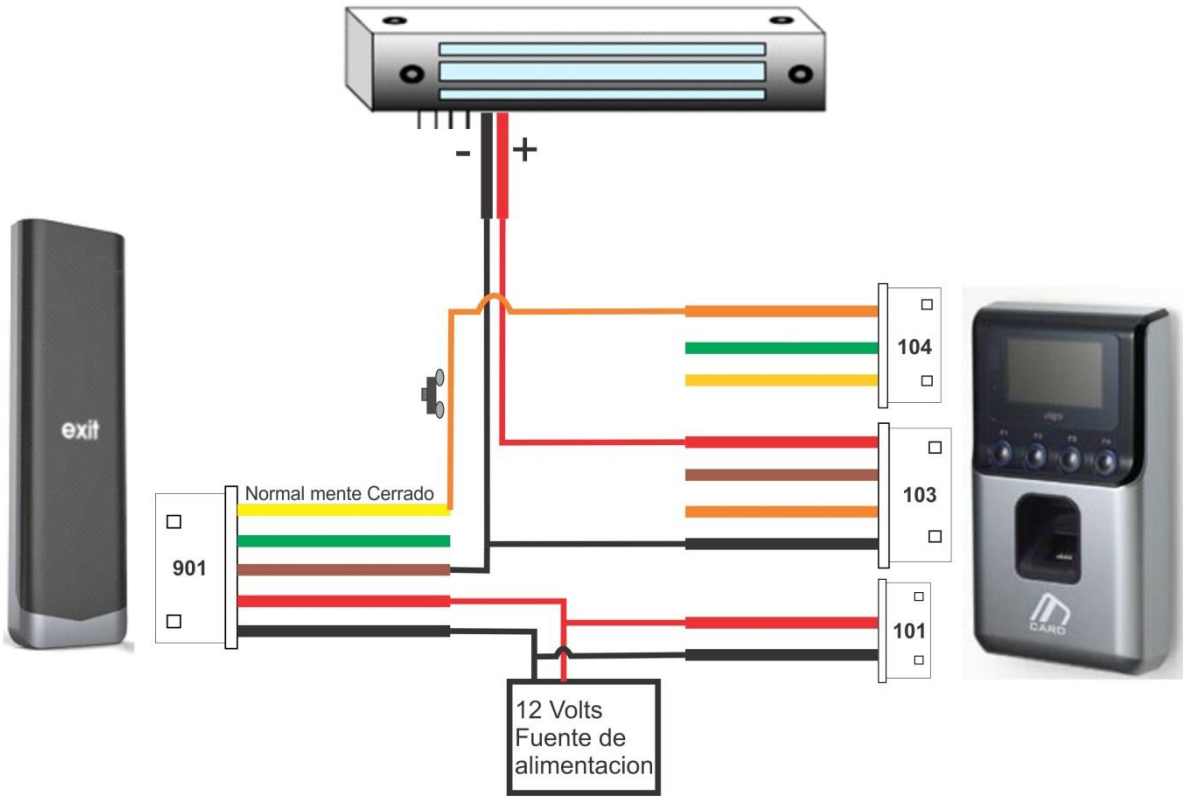
Cable externo (5P)



5: COM (Cafe)
4: NO (Verde)
3: NC (Amarillo)
2: GND (Negro)
1: +12VDC (Rojo)

Ejemplo práctico de integración de dispositivo biométrico y botón liberador.

Configuración para dispositivos de la familia Virdi AC-2100 con botón liberador EB-030 y electroimán estándar:



Circuito para interconexión de dispositivo biométrico modelo Virdi AC-2100 con botón liberador modelo EB-030 y control de acceso del tipo electroimán estándar normalmente cerrado.