CONFIGURACIONES GENERALES Y CONEXIONES ELECTICAS.

VIRDI AC-6000

INDICE DEL 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 aplicación de esta información.

Configuraciones generales de red para dispositivos biométricos.

En este módulo se describen los procesos para la configuración básica de parámetros generales y de red para el dispositivo biométrico Virdi AC-6000

Descripción del dispositivo biométrico AC-6000

1.1. Terminal description

No.	Pantalla	Descripción
1	Sensor de la cámara	Imagen tomada durante la autenticación
2	Pantalla táctil LCD	Pantalla Táctil a color LCD
3	Indicador LED	LED Alimentación(Rojo), Tarjeta(Azul), Puerta, (Verde)
4	Sensor de aproximación	Cuando enfoca a un usuario se enciende la pantalla LCD
	Sensor IRED	Cuando enfoca a un usuario la pantalla se enciende junto con los botones de función para introducir el I D de usuario
5	Teclas de función	Teclas de función (control del dispositivo)
6	USB	Entrada para USB y micro USB
7	Botón de llamada	Se utiliza para aplicaciones con un teléfono en la p uerta
8	Altavoz	Altavoz para salida de voz o audio
9	Sensor de tarjeta	Área de registro de tarjeta
10	Protección corrediza	Protección para la exposición al ambiente
11	Sensor de huella dactilar	Área de entrada para ingresar nuestra huella digital
12	Sensor UV (opcional)	Sensor UV utilizado para la limpieza de las b acterias de la ventana del sensor

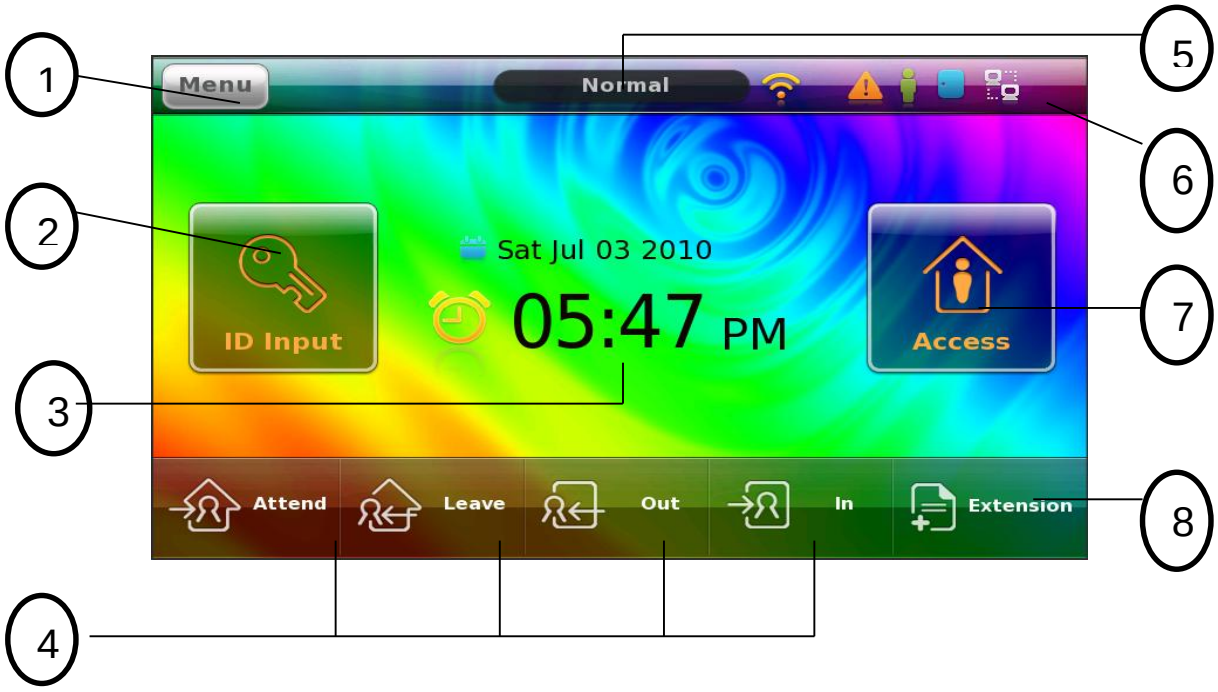
Iconos de advertencia

① Detección de Incendios		: El estado en que se reconoce el sensor de incendio (cuando se conecta el detector de fuego)
② Advertencia		: Estado anormal cuando la terminal es desmontada o la puerta ha encontrado un problema.
③ Estado de entrada		: La puerta está cerrada
		: La puerta está abierta
④Estado de conexión del servidor		: No está conectada la línea LAN
		: No se encuentra conectado al servidor
		: Conectado al servidor

Descripción de la pantalla (durante la operación)

Pantalla Principal

La apariencia de la pantalla principal es altamente configurable y puede cambiar la apariencia dependiendo de la configuración del administrador. Cuando no se ha producido ninguna actividad durante un número de minutos establecidos por el administrador la pantalla LCD se apagará estará en blanco. Cuando un usuario se acerca al terminal, la pantalla se mostrará de nuevo.



Numero	Iconos	Descripción
1	Botón de configuración	Para Entrar al modo configuración de la terminal
2	Botón de entrada ID	Introducir la identificación de numero de usuario para su autenticación
3	Hora y fecha	Hora/fecha Diferentes opciones para su visualización disponibles en el modo de configuración
4	Teclas de función	Estas teclas se utilizan para cambiar los modos de autenticación. La misma función que los botones F1-F4 en la terminal.
5	Estado	Texto de estado que indica el modo actual de autenticación (Acceso, Permiso, Asistir, Entrada y salida)
6	Iconos de estado	Iconos de estado (Alerta de incendio, Problemas, Proximidad, Puerta, Red y UV)
7	Botón de acceso	Para cambiar el modo de autenticación actual a ‘modo normal’
8	Botón de extensión	En caso de que se necesiten más de cuatro teclas de función, Este botón se utiliza para extender el número de teclas de función

Tipos de autenticación	
Huella dactilar	Registro de huella digital Autenticación de huella digital
ID y Contraseña	Registro de contraseña Autenticación de contraseña y después entrada de ID
Huella digital o contraseña	Registro de contraseña y huella digital Autenticación de contraseña o huella digital
Huella digital y contraseña	Registro de contraseña y huella digital Autenticación de contraseña
Tarjeta	Registro de tarjeta Autenticación de tarjeta
Tarjeta o huella digital	Autenticación de tarjeta o huella digital
Tarjeta y huella digital	Registro de huella digital y de tarjeta Autenticación de tarjeta después autenticación de tarjeta
Tarjeta o contraseña	Registro de contraseña y tarjeta Autenticación de contraseña o tarjeta
Tarjeta y contraseña	Registro de contraseña y tarjeta Autenticación de tarjeta después autenticación de contraseña
ID de usuario y huella digital o tarjeta y huella digital	Registro de huella digital y tarjeta Autenticación de huella digital después ID de entrada o autenticación de huella digital después autenticación de tarjeta

ID de usuario y contraseña o tarjeta y contraseña	Registro de contraseña y tarjeta Autenticación de contraseña después entrada de ID o autenticación de contraseña y después autenticación de tarjeta
Tarjeta, contraseña y huella digital	Tarjeta, contraseña y huella digital, Es necesaria una tarjeta después de la contraseña y huella digital
Usuario deshabilitado	Sin función para el usuario

Configuraciones de su entorno

Aspectos a considerar antes de configurar su entorno

Entrar al menú

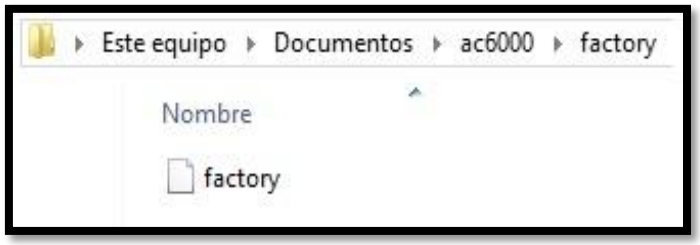
1.-Pulse la tecla [Menú] en la parte superior izquierda de nuestra pantalla principal. El usuario ahora puede acceder a la pantalla de menú principal.

El usuario tendrá acceso a cada opción del menú principal, si el usuario administrador ya está registrado, aparecerá la pantalla de administrador verificar que se muestre la siguiente pantalla.

Como tener acceso al menú sin la verificación del administrador

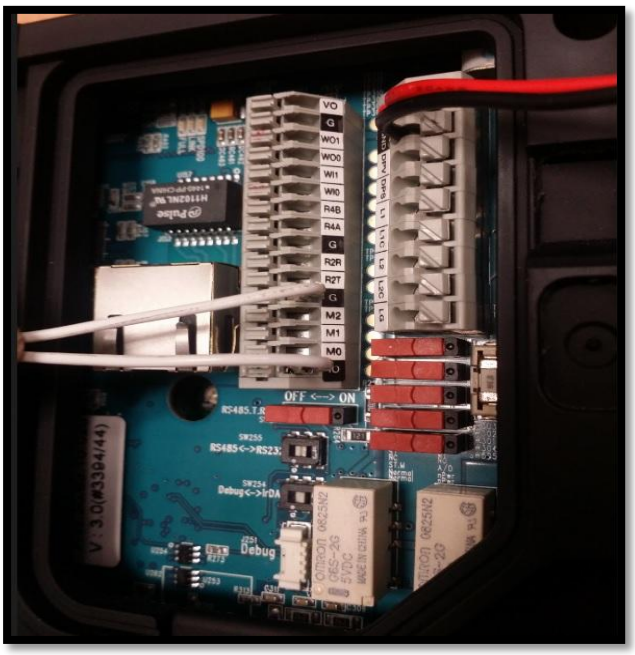
Esta es la forma para poder acceder al menú, en caso de que el usuario olvide la contraseña del administrador, o pérdida de la tarjeta registrada en el terminal, o no cuente con un administrador.

1.- En una Memoria USB crear una carpeta con el nombre (ac6000), dentro de ella crear otra con el nombre (Factory) y copiamos el archivo Factory como se muestra a continuación (solicitar el archivo Factory con el área de soporte técnico)



2.- Enseguida Procedemos a insertar la memoria USB a nuestro dispositivo, lo encendemos y esperamos un momento en lo que carga el archivo, y enciende correctamente el dispositivo.

3.- A continuación retiramos la tapa trasera de nuestro dispositivo y realizamos la siguiente conexión (cableamos la salida [IO con G] del puerto J304) como se muestra en la imagen.

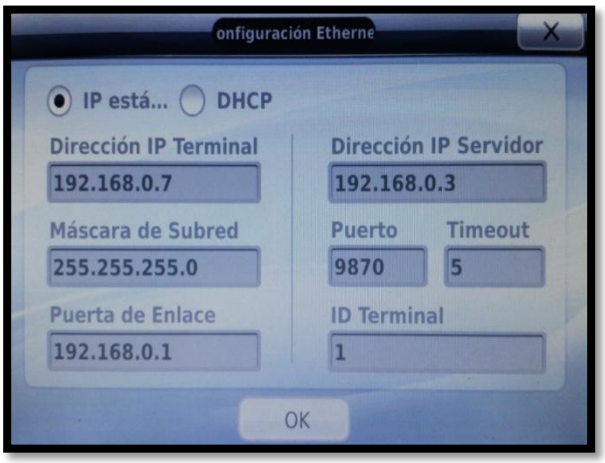


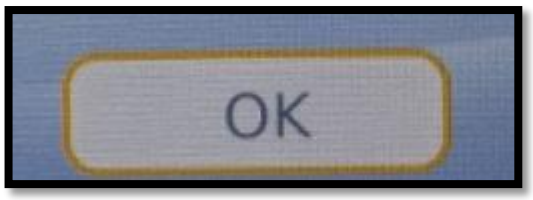
4.- Final mente entramos al menú de nuestra pantalla principal y tendremos acceso a la opciones de configuración.

Configuración del idioma

Configuraciones del sistema: Para el cambio de idioma Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos el icono menú de la pantalla principal y seleccionamos la opción [Display].	
2.- En el siguiente submenú presionamos la opción language y en la barra de idiomas seleccionamos Spanish para cambiar nuestro idioma a español.	
3.- Final mente presionamos [Ok] y listo.	

Conexión IP

Configuraciones del sistema: Conexión IP Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos el icono menú de la pantalla principal y seleccionamos la opción [Red].	
2.- A continuación nos muestra la siguiente ventana [configuración Ethernet] por default nos aparece marcada la opción [IP estática] En Dirección IP, Mascara de subred y Puerta de enlace son correspondientes al equipo que vallamos a utilizar como servidor.	

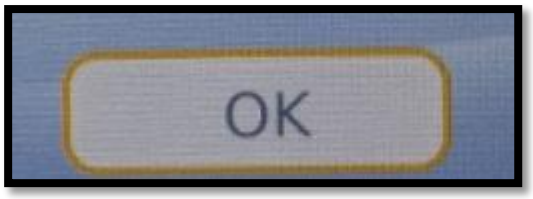
2.-En la siguiente opción [DHCP] modificamos según nuestro escenario de red.	
3.- Por ultimo seleccionamos [Ok] para guardar los cambios.	

Extender la cadena de caracteres para el número de empleados

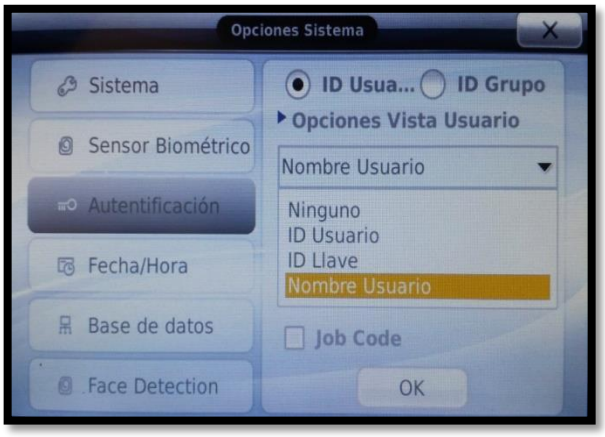
Configuraciones del sistema: Cadena de caracteres

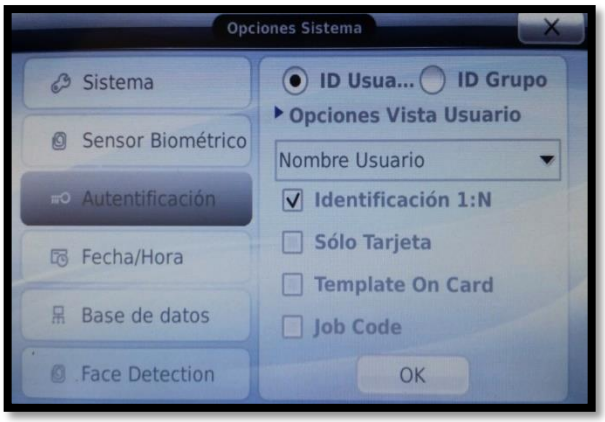
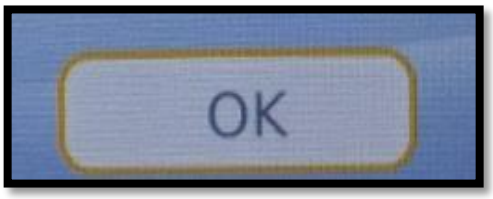
Accedemos mediante la siguiente secuencia de ventanas

1.- Presionamos el icono menú de la pantalla principal y seleccionamos la opción [Sistema].	
2.- A continuación nos envía directamente a la primer opción [Sistema] ►Longitud ID usuario: Seleccionamos esta opción para extender el número de caracteres del usuario [2-8]. ►Autentificación: En esta opción seleccionamos el tipo de autenticación del dispositivo, de preferencia [Terminal/Servidor].	

3.- Al terminar de ingresar la configuración correctamente seleccionamos [ok] para guardar nuestra información.	

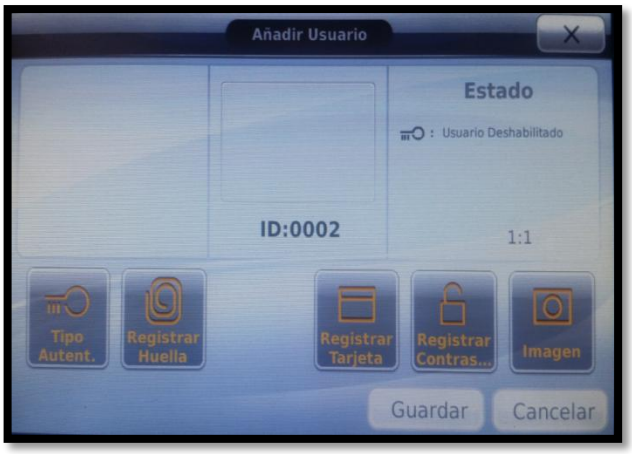
Variantes de autenticación

Configuraciones del sistema: Autenticación Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos el icono menú de la pantalla principal y seleccionamos la opción [Sistema].	
2.- A continuación seleccionamos en el menú de la izquierda la opción autenticación, por default nos aparece marcada [ID Usuario] en: ►Opciones Vista Usuario: nos aparecen cuatro opciones de mensaje al ingresar una autenticación.	

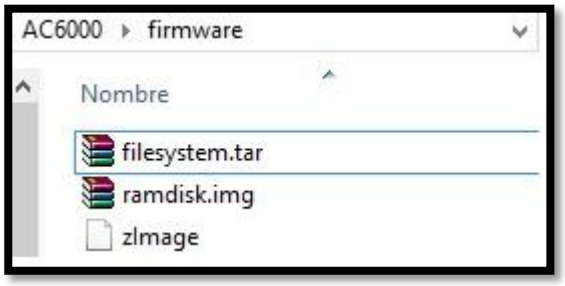
3.- A continuación hay cuatro opciones para el tipo de autenticación a elegir por [ID Usuario] o [ID Grupo].	
4.- Finalmente presionamos [Ok] para guardar los cambios.	

Dar de alta a un usuario

Configuraciones del sistema: Alta a usuario Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos el icono menú de la pantalla principal y seleccionamos la opción [Usuario].	
2.- En el siguiente menú elegimos la primer opción [Añadir]. Y nos mostrara una ventana con el ID a ingresar. Para borrar los dígitos presionamos la tecla [←], e ingresamos el ID correspondiente, presionamos [ok] para que nos muestre la siguiente ventana.	

3.- A continuación nos mostrara una ventana con las distintas formas de autenticar a un usuario (Registro de huella, Tarjeta, Contraseña), ya que tengamos por lo menos dos registros guardados podemos elegir entre cinco combinaciones de registros para nuestra autenticación.	
4.- Por ultimo seleccionamos guardar y listo.	

Actualización de Firmware

Configuraciones del sistema: Firmware Accedemos mediante la siguiente secuencia de ventanas	
1.- En una memoria USB Creamos una carpeta con el nombre [AC6000] y dentro de ella otra con el nombre firmware y copiamos todos los archivos necesarios para la actualización del Firmware como se muestra a continuación. (Recomendable solicitar la actualización más actual del dispositivo, con el área de soporte técnico).	
2.- Procedemos a insertar la tarjeta SD a nuestro dispositivo, enseguida seleccionamos el icono menu para acceder a la configuración principal.	

2.- A continuación presionamos el icono [USB] para acceder al siguiente menú y pulsamos el botón [Actualizar Firmware].	
3.- Esperamos unos segundos en los que se lleva a cabo la actualización y listo.	

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.

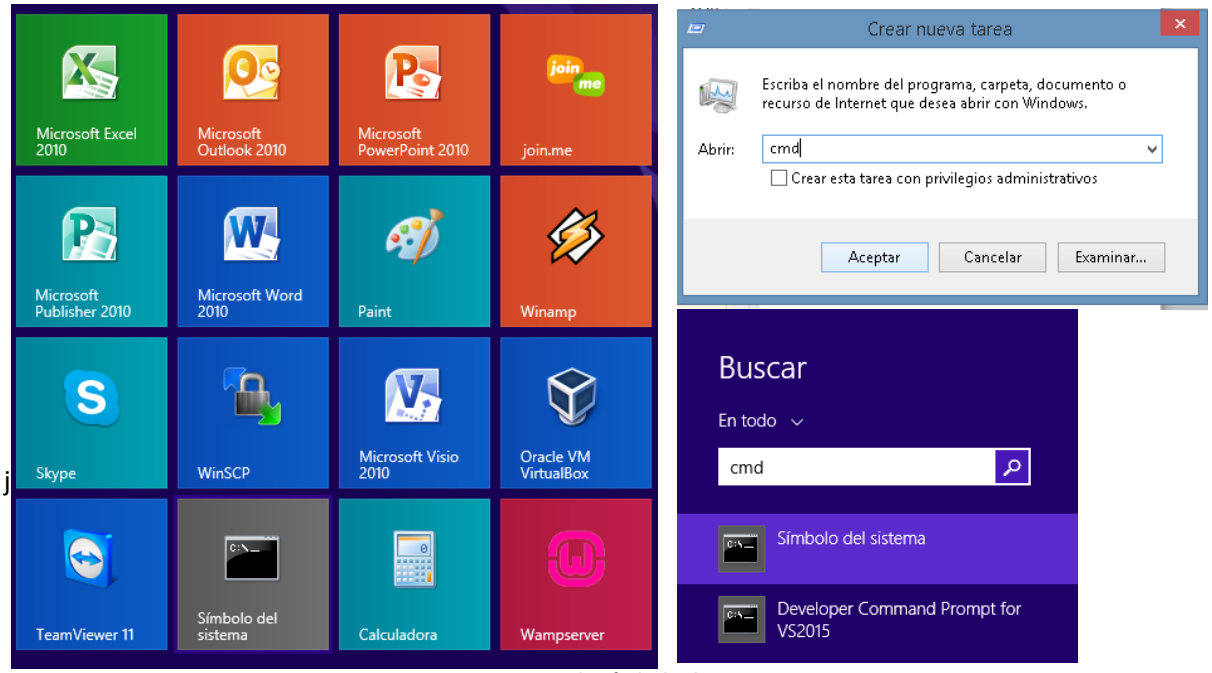


Imagen 1 – Icono de Símbolo de Sistema

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 resulto exitoso la siguiente sucesión de líneas:

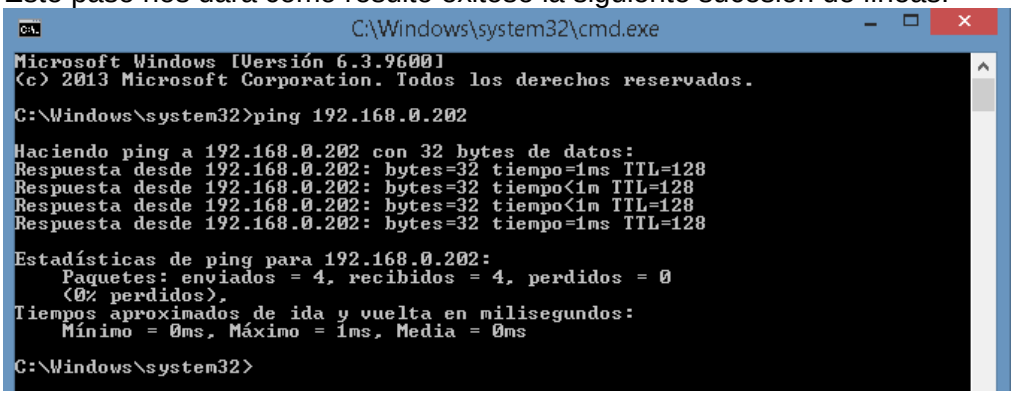


Imagen 1 – Ventana de sistema ping exitoso

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

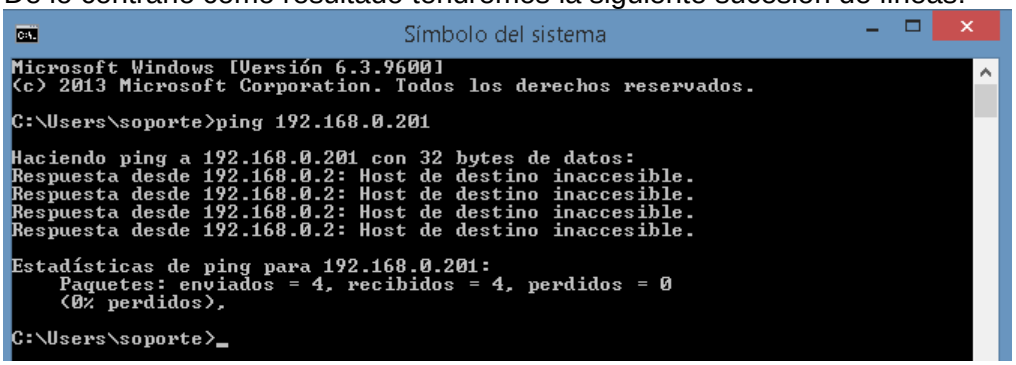


Imagen 1 – Ventana de sistema ping fallido

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.

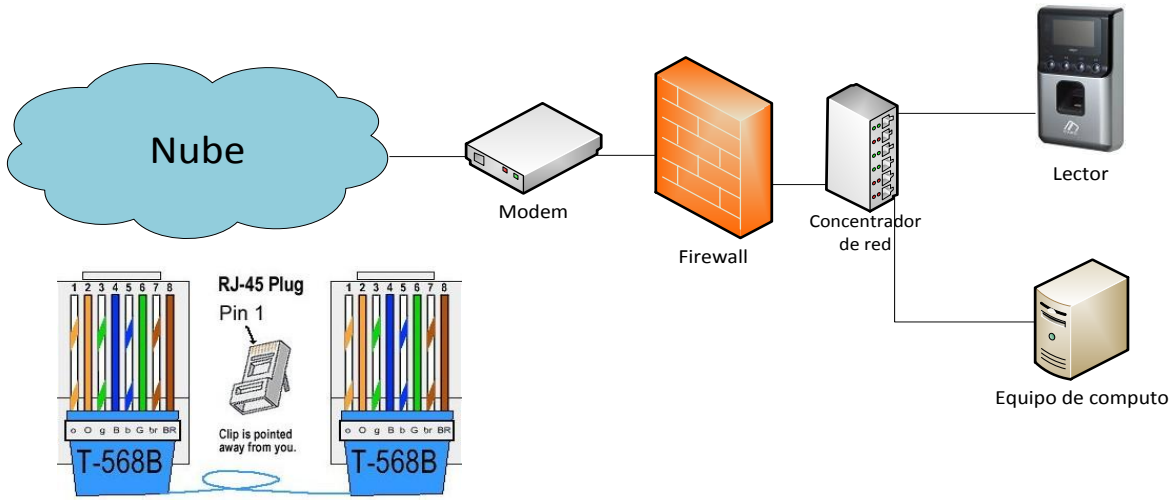


Imagen 1 – Esquema de red local estándar.

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.

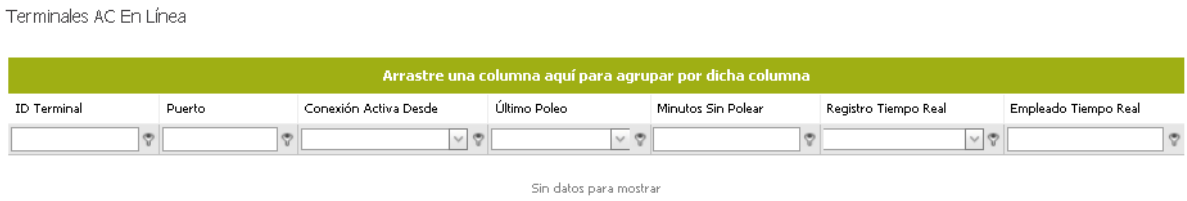


Imagen 1 – Ventana de sistema Poleo inexistente

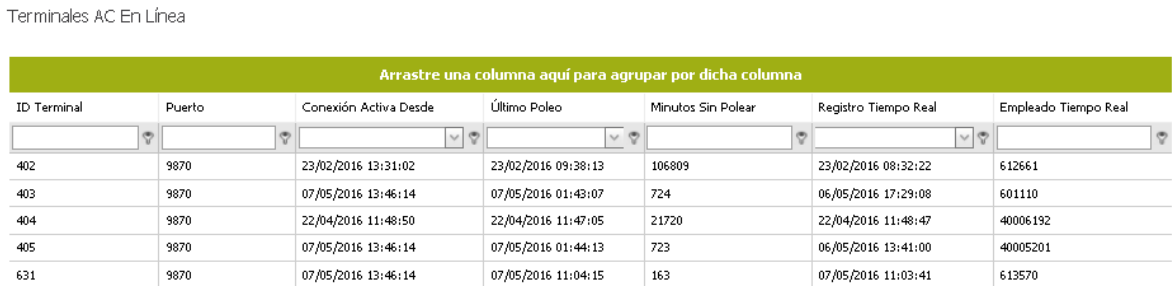


Imagen 1 – Ventana de sistema Poleo exitoso

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.

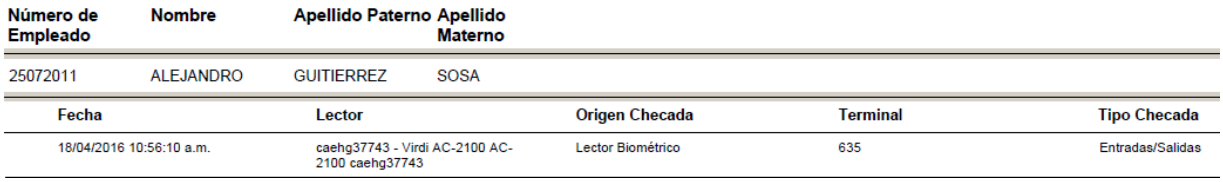
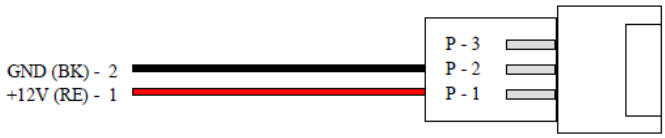


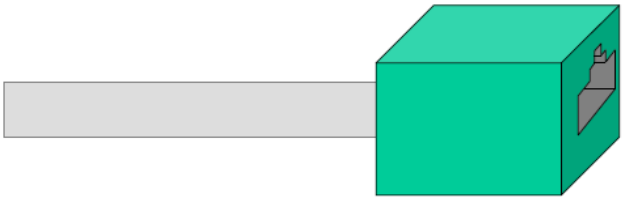
Imagen 1 – Reporte Accesos

Descripción de conexiones eléctricas.

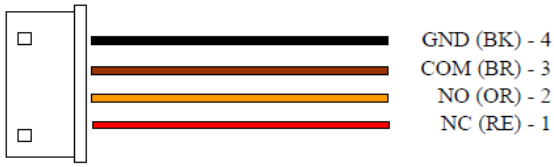
Especificaciones eléctricas para dispositivo biométrico Virdi AC-2100.



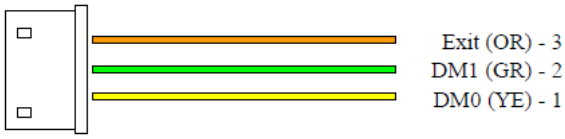
Cable adaptador de voltaje (101)



Cable de red RJ45 (102)

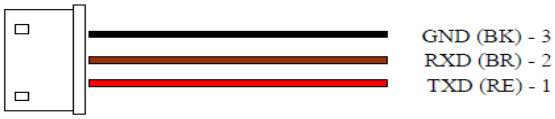


Lock Cable (4P) "Cable de control para aperturas" (103)

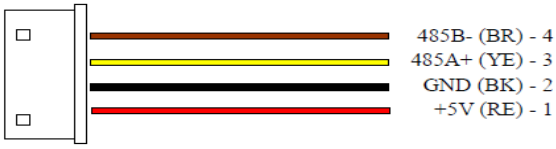


Lock Monitor & Exit Cable (3P) "Cable de control para pulsos de bandera" (104)

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



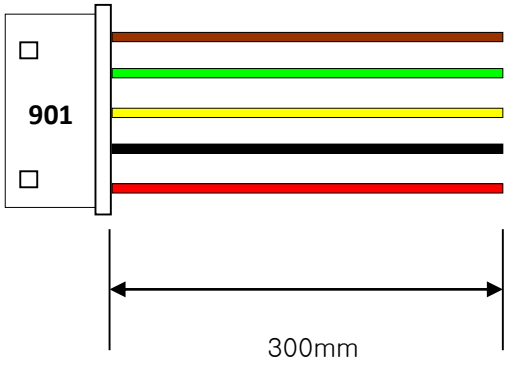
RS232 Cable (3P) "Cable de control para comunicaciones estándar Serial RS232" (106)



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

Especificaciones eléctricas botón liberador EB-030.

Cable externo (5P)



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