CONFIGURACIONES GENERALES Y CONEXIONES ELECTICAS.

VIRDI AC-5000

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-5000RF

Descripción del dispositivo biométrico AC-5000RF

Indicador de estado LED

Pantalla LCD

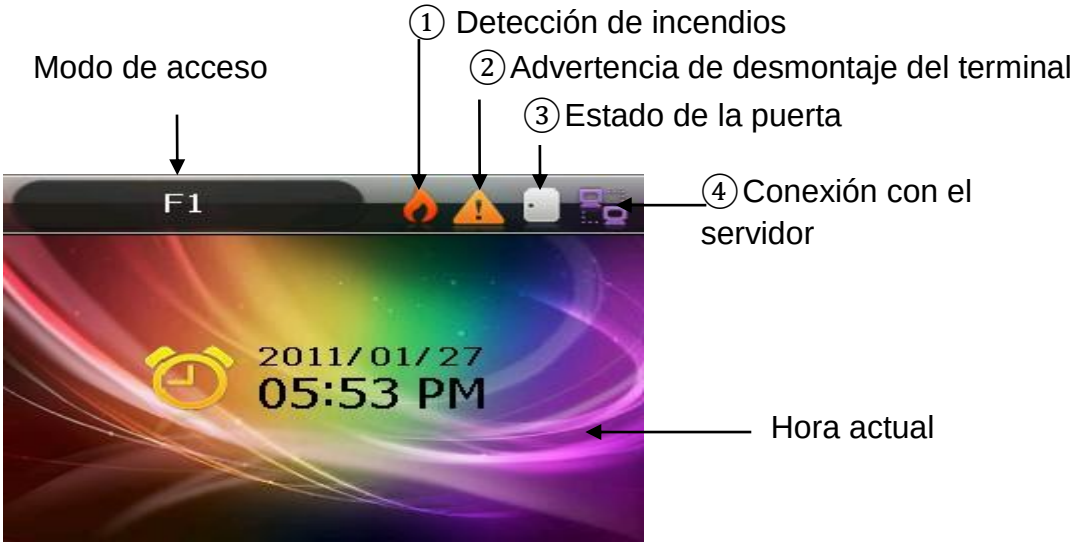
Sensor de huella dactilar

Toque de tecla

Normalmente, las cifras (números) son invisibles por que el LED se encuentra apagado. El LED se enciende y las cifras se iluminan cuando el usuario toca ligeramente esta área

Sensor de entrada a la tarjeta de proximidad

Descripción de la pantalla (durante la operación)



① Detección de incendios		Cuando se detecta fuego por el sensor de fuego (sujeto a la conexión del sensor de incendio apropiado).
② Advertencia		El estado anormal cuando el terminal es desmontado o la puerta ha encontrado un problema.
③ Estado de la puerta		:Estado de la puerta es desconocido
		:Puerta cerrada
		:Puerta abierta
④ Conexión con el servidor	Ninguno	: Cable LAN no está conectado
		: Conexión del cable LAN. Pero no al servidor
		: Conectado al servidor

Descripción del teclado

0 – 9	- Dígitos que se utilizan para la introducción de datos numéricos
F1 - F3	- Se usan para cambiar el modo de autenticación
F4 O [←]	- Se utiliza para cambiar el modo de autenticación - Utilizado como la tecla Supr. Para su corrección cuando los valores numéricos son de entrada. - Se utiliza para cancelar la entrada, y pasar al menú principal
[F4(←)]	- Significa pulsa la tecla [F4 (←)] durante dos segundos o más. - Cuando el cursor introducido está localizado en el cuadro de entrada, la entrada se cancela y sale al menú principal si mantiene pulsado durante dos segundos o más.
ENT [O MENU]	- usada para modificar el modo - Se utiliza ingresar al menú principal y poder ingresar los valores deseados.
[ENT-]	- Significa pulsa la tecla [ENT] durante dos segundos o mas - Se utiliza para acceder al menú, cuando se mantiene presionado - Cuando el digito introducido está situado en el cuadro de entrada, el usuario puede salir al menú principal con el valor actual de entrada guardando la información pulsando el botón durante 2 segundos o más. - Utilizado para aplicar la configuración en la pantalla actual en el modo menú y luego salir al menú principal.

Tipos de autenticación

FP	Registro de huella digital Autenticación de huella digital
PW	Registro de tarjeta Autenticación de tarjetas
FP or PW	Huella digital o contraseña de registro Autenticación de contraseña cuando falla la autenticación de huella digital
FP & PW	Huella digital y contraseña de registro Autenticación de huella digital y luego autenticación de contraseña
Card	Registro de tarjeta Autenticación de tarjeta
Card or FP	Registro de huella digital y tarjeta Autenticación de huella digital o tarjeta
Card & FP	Registro de huella digital y tarjeta Autenticación de tarjeta y autenticación de huella digital
Card or PW	Tarjeta y contraseña de registro Tarjeta o autenticación de contraseña de registro
Card and PW	Tarjeta y contraseña de registro Autenticación de tarjeta y autenticación de contraseña
(ID or Card) &	Registro de huella digital y tarjeta

FP	ID de entrada y luego autenticación de huellas dactilares, o autenticación de tarjeta y después autenticación de huella digital
(ID or Card) & PW	Contraseña de registro y tarjeta Entrada de ID y luego autenticación de contraseña, o autenticación de tarjeta y luego autenticación de contraseña
Card & PW & FP	Tarjeta, contraseña, y registro de huella digital Autenticación de tarjeta, huella digital y autenticación de contraseña

Configuraciones de su entorno

Aspectos a considerar antes de configurar su entorno

Entrar al menú

1.-Pulse la tecla [ENT] durante 4 segundos o más. El usuario ahora puede acceder a la pantalla de menú principal.

El usuario tendrá acceso a cada submenú presionando la tecla numérica correspondiente, si el usuario administrador ya está registrado, aparecerá la pantalla de administrador verificar que se muestre la siguiente pantalla.

En cumplimiento con el método de autenticación, como tarjeta, huella digital o contraseña, los usuarios pueden acceder a cada menú, sujeto a la identificación exitosa, después de que la verificación del administrador haya terminado.

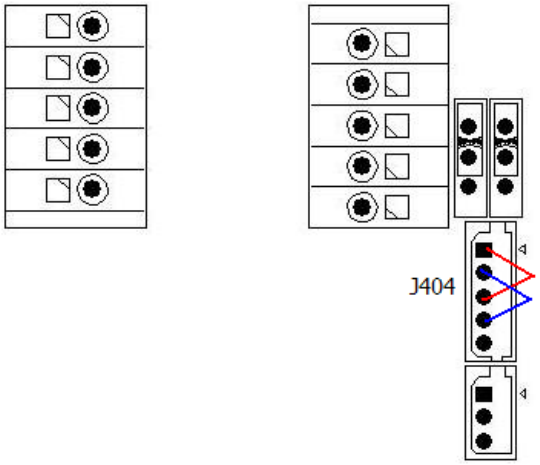
- Verificar que el administrador sólo aparezca si hay un usuario registrado de administración. Cuando acceda al modo menú, después de ser identificado, el usuario puede acceder a todos los menús hasta salir completamente del menú principal.

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.- Quitar el soporte en la parte superior del terminar para abrir la tapa.

2.- con la tapa abierta, como se muestra en la figura a continuación conectar el pin 1 con el 3 y el pin 2 al 4 del conector J404.

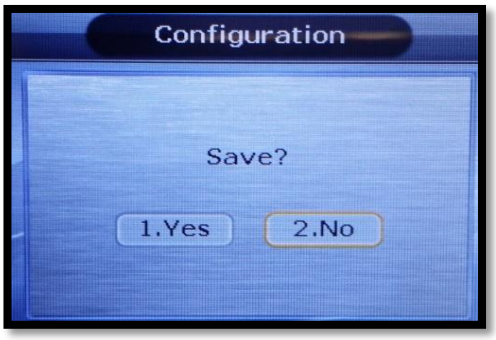


3.-Acceda al menú manteniendo pulsada la tecla [F4 (←)] durante 2 segundos o un poco más. Ingrese el ID Admin “0000” después pulsar la tecla [ENT]. Ahora el usuario puede tener acceso al menú seleccionado.

4.- Después de realizar la configuración retirar los cables de conexión del conector J404.

Configuración del idioma

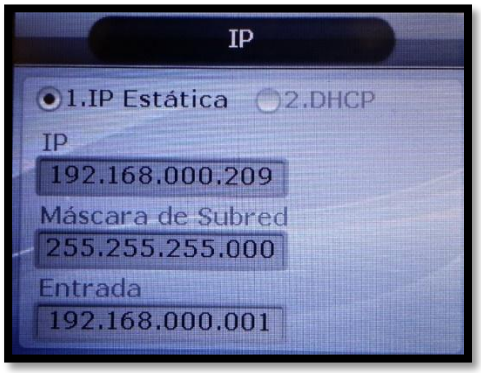
Configuraciones del sistema: Para el cambio de idioma Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos la tecla [ENT] de nuestro dispositivo durante un periodo de 4 segundos, a continuación nos desplegara la siguiente ventana.	
2.- Seleccionamos la opción 4. System, nos mostrara el siguiente menú.	
3.- Seleccionamos la opción 4. Language y nos desplegara la siguiente menú.	

4.- por default nos aparecerá el lenguaje en ingles [01] procedemos a cambiarlo con la tecla [F4←] borramos [01] e ingresamos los dígitos 04 para cambiar el lenguaje a español.	
5.- A continuación mantenemos presionada la tecla [ENT] para salir de la ventana actual y regresamos a la pantalla anterior.	
6.- Presionamos la tecla [F4←] y nos aparecerá el siguiente mensaje, seleccionamos la opción [1.Yes] después [ENT] para guardar los cambios. A continuación se actualizara el lenguaje a español.	

Conexión IP

Configuraciones del sistema: Conexión IP

Accedemos mediante la siguiente secuencia de ventanas

1.- Presionamos la tecla [ENT] de nuestro dispositivo durante un periodo de 4 segundos, a continuación nos desplegara la siguiente ventana.	
2.- A continuación Seleccionamos la opción [2. Red] y nos mostrara el siguiente menú.	
3.- Seleccionamos (1.IP), por default nos aparece marcada la opción (1.IP Estática). Eliminamos los valores existentes con la tecla [F4 (←)] Para comenzar a ingresar los datos de red. IP, Mascara de subred y Entrada correspondientes al equipo que vallamos a utilizar como servidor.	

4.- A continuación presionamos la tecla [ENT] para salir de la ventana [IP], Regresamos al menú anterior y seleccionamos la opción [2.IP del servidor], modificamos acorde a su escenario de red.	
5.- Salimos del menú presionando la tecla [ENT] e ingresamos a la opción [3. ID Terminal] del menú de Red. ID Terminal: corresponde al ID de la puerta de entrada del servidor. Autenticación: Esto determina la prioridad para la autenticación entre el terminal y el servidor de red. Para validar la comunicación seleccionamos la opción. [2.Terminal/servidor] de preferencia. Por ultimo presionamos la tecla [ENT] para salir de la ventana.	
6.- Regresamos a la ventana de red presionando la tecla [ENT] después [F4←] para regresar a la pantalla principal, finalmente para guardar los cambios seleccionamos la opción [1.Yes] después [ENT] para guardar los cambios. Y los datos de red serán actualizados.	

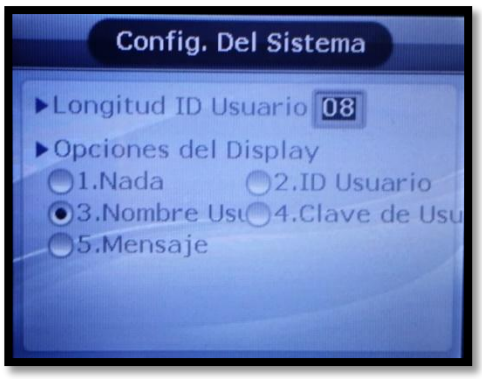
Especificaciones de la ventada id terminal

1.Servidor/Terminal	La autenticación es echa por el servidor cuando se conecta a la red del terminal, y por la terminal cuando es desconectado por el servidor debido a perturbaciones por la red, etc.
2.Terminal/Servidor	La autenticación se realiza mediante el terminal, incluso si el servidor está conectado, y el resultado de la autenticación se transfiere al servidor en tiempo real. Sin embargo, la autenticación se realiza mediante el servidor cuando la entrada ID de usuario o la tarjeta no está registrada en la terminal (no intentar la autenticación del servidor en caso de 1: N la autenticación de huella dactilar).
3. Solo servidor	Aunque el usuario está registrado en el terminal, la autenticación se realiza a través del servidor. Por lo tanto, la autenticación no puede realizarse a menos que el servidor esté conectado.
4. Solo Terminal	Sólo los usuarios registrados en la terminal están autenticados. Cuando está conectado al servidor, la autenticación de los resultados se transmite al servidor en tiempo real.

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 la tecla [ENT] durante un periodo de 4 segundos, a continuación nos desplegara la siguiente ventana.	
2.- Seleccionamos la opción [4.Sistema] para acceder al siguiente menú y elegimos la opción [1.Config. Del sistema].	
3.-A continuación con la tecla [F4←] editamos el número de usuarios a considerar dentro de un rango de 0-9 dígitos. En [Opciones del Display]: Es recomendable seleccionar la opción [3.Nombre de usuario].	

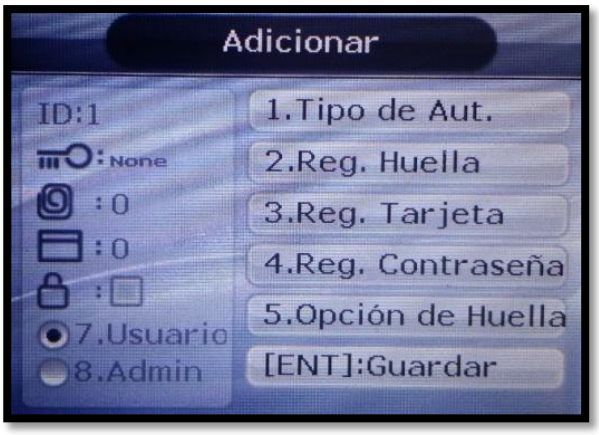
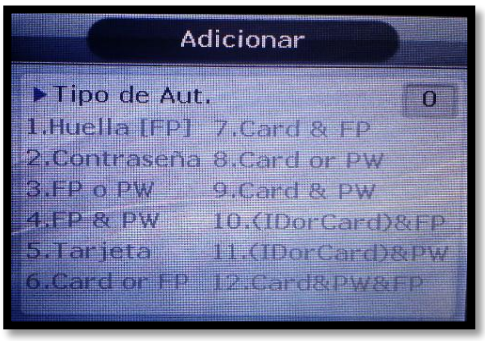
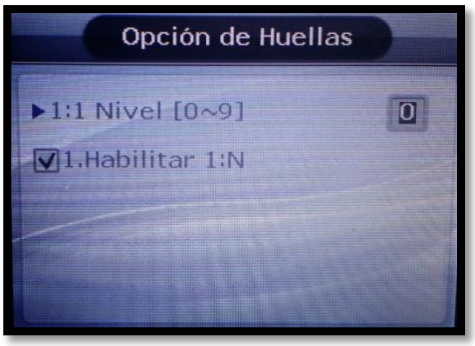
3.- Seleccionamos la tecla [ENT] para regresar a la ventana anterior [4.Sistema], y [F4←] para volver al menú de configuración.	
4.- En la siguiente ventana seleccionamos la opción [1.Si] y con la tecla [ENT] guardamos la configuración realizada.	

Variantes de autenticación

Configuraciones del sistema: Autenticación Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos la tecla [ENT] durante un periodo de 4 segundos, a continuación nos desplegara la siguiente ventana.	
2.-Seleccionamos la opción [4.Sistema] para acceder al siguiente menú y elegimos la opción [2.Autenticación].	
3.- En la ventana de autenticación nos muestra las distintas formas de ingresar usuarios al dispositivo.	

Dar de alta a un usuario

Configuraciones del sistema: Alta a usuario Accedemos mediante la siguiente secuencia de ventanas	
1.- Presionamos la tecla [ENT] de nuestro dispositivo durante un periodo de 4 segundos, a continuación nos desplegara la siguiente ventana.	
2.- A continuación seleccionamos la opción [1.Usuario], para añadir un nuevo usuario pulsamos [1.Adicionar].	
3.- En la ventana Adicionar borramos el registro con la tecla [F4 (←)] y colocamos el [ID Usuario] a registrar y finalmente presionamos [ENT]. Para acceder al siguiente menú.	

4.- A continuación Seleccionamos [1.Tipo de Aut.] para acceder al siguiente sub menú según el tipo de autenticación que se requiera para el registro de usuario.	
5.- En tipo de Aut. Escogemos el tipo de combinación de autenticación que se requiera eje. (Huella o Tarjeta y contraseña etc.), después presionamos [ENT] para regresar al menú anterior.	
6.- A continuación seleccionamos el tipo de Registro a ingresar [2.Reg Huella, 3.Reg Tarjeta o 4.Reg contraseña]. Según lo requiera el administrador. De haber seleccionado la opción [2.Reg. Huella] procedemos a pulsar [5.opcion de Huella].	
7.- La opción [5.Opción de Huella] nos mostrara la siguiente ventana: [>1:1 Nivel [0~9] de Preferencia lo dejamos en [0] y palomeamos la opción [1.Habilitar 1:N) con la tecla de función [1] para salir mantenemos presionada la tecla [ENT] durante 4 segundos para regresar a la ventana [modificar].	

8.- A continuación presionamos [F4 (←)] dos veces para regresar al menú configuraciones y posteriormente para regresar a la pantalla principal, nos mostrara el siguiente mensaje presionamos la tecla 1 [1.Sí] para guardar el registro y listo.	

Variantes de autenticación

1.Usar ID grupo	Cuando se marca este método, se realiza la autenticación de huella dactilar de los usuarios cuyo identificador comienza con la misma letra de entrada Si no se comprueba este método, se considera el registro de entrada como el ID de usuario y los intentos 1: 1 de autenticación contra la huella digital del usuario.
2.Habilitar 1:N	Esta opción permite sólo autenticación de huellas dactilares sin introducir tarjeta o identificador de usuario. Incluso si el usuario está registrado con autenticación 1: N, autenticación 1:1 sólo se permite en la terminal donde esta opción no está activada.
3. Solo tarjeta	Esta opción permite sólo la autenticación con tarjetas sin ingresar la huella digital. Incluso si el usuario está registrado con (tarjeta y FP) o se permite la autenticación única (tarjeta y PW), con tarjeta en el terminal donde esta opción es comprobada.
4. plantilla en tarjeta	Esta opción permite la autenticación con información del usuario y huellas dactilares registradas en la tarjeta sin necesidad de descargar el usuario en el terminal del usuario.
5. Verify Multi-FP	Esta función tiene todas las huellas registradas para autenticar el usuario entradas ID (o tarjeta). Cuando esta opción es marcada, el usuario debe, sin falta, Checar la entrada con entrada con tarjeta o identificador el ID de usuario.

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.

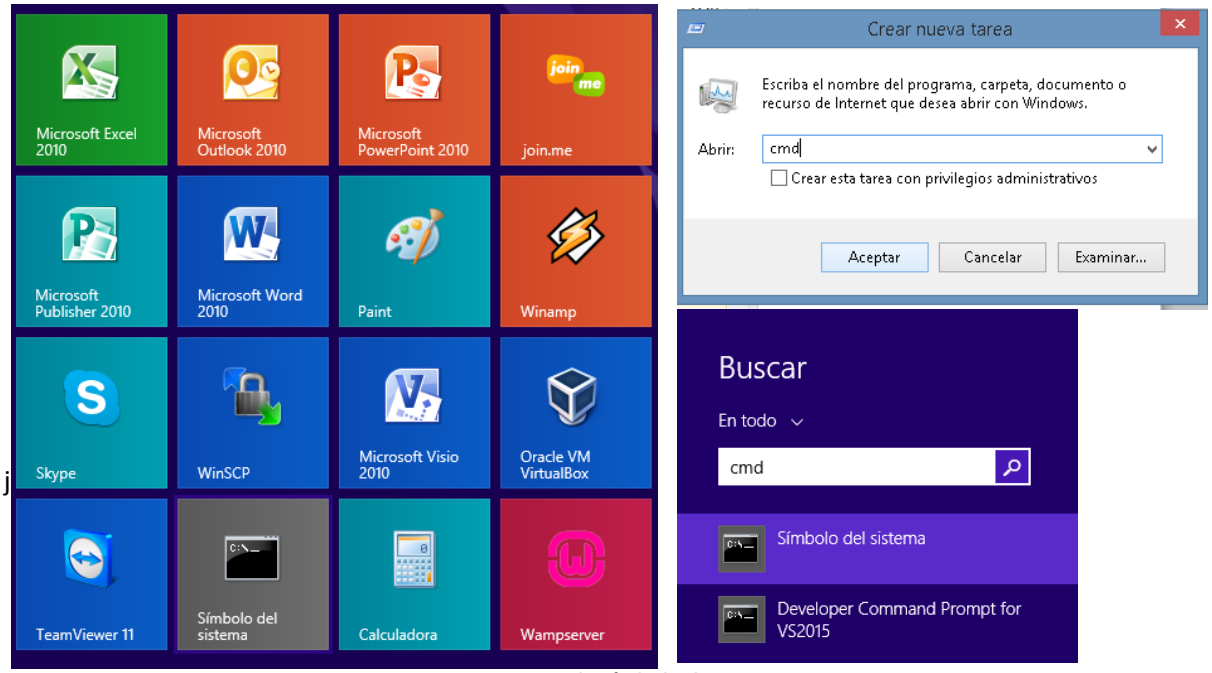


Imagen 1 – Icono de Símbolo de Sistema

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:

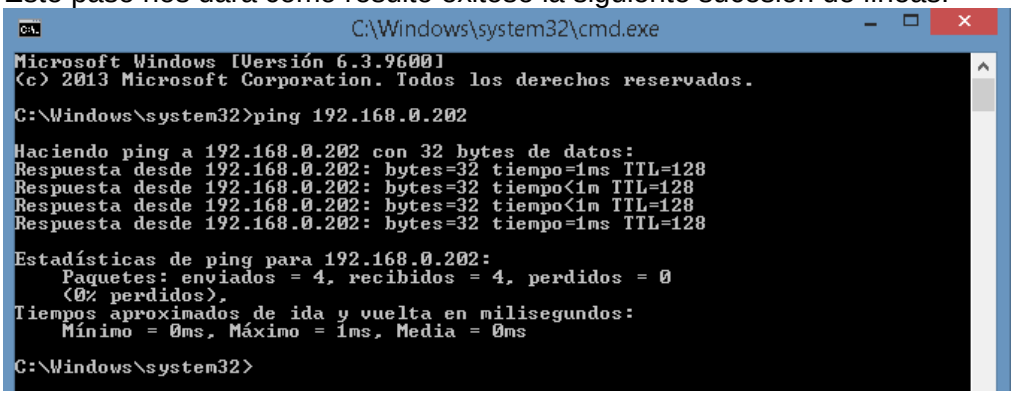


Imagen 1 – Ventana de sistema ping exitoso

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

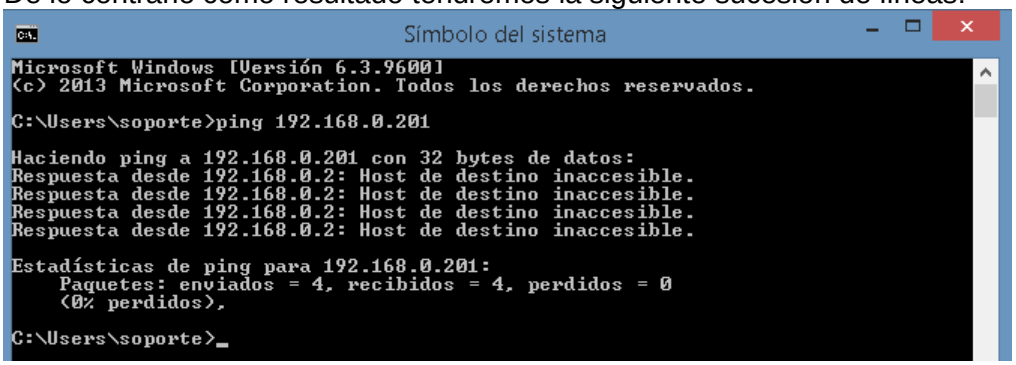


Imagen 1 – Ventana de sistema ping fallido

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.

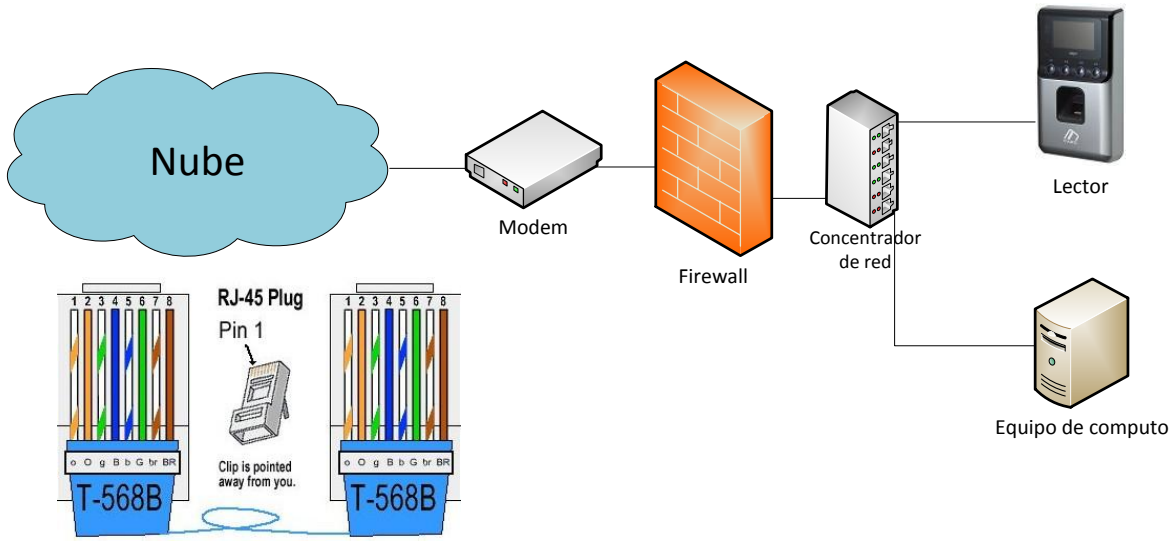


Imagen 1 – Esquema de red local estándar.

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.

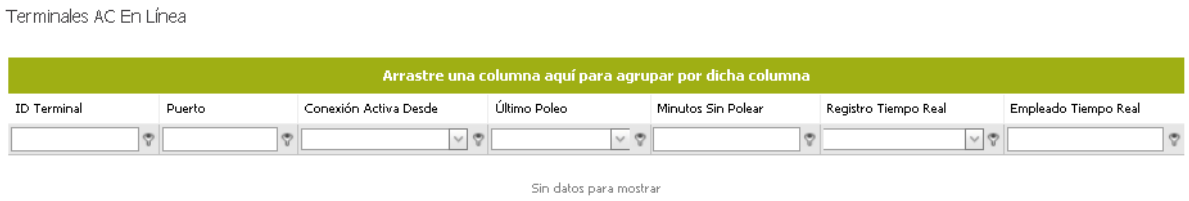


Imagen 1 – Ventana de sistema Poleo inexistente

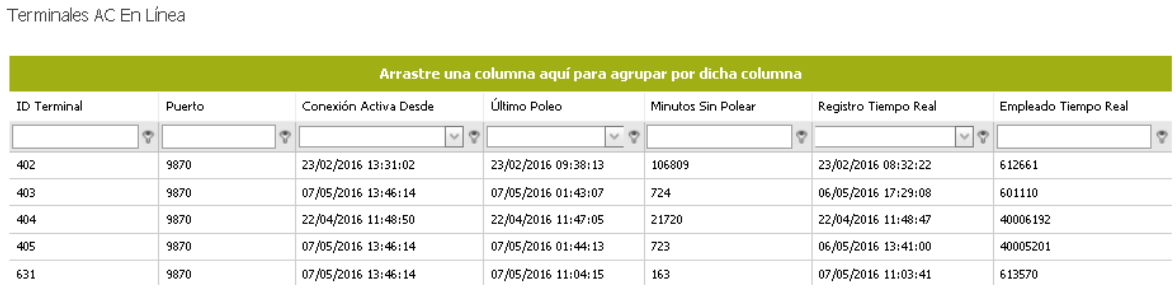


Imagen 1 – Ventana de sistema Poleo exitoso

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.

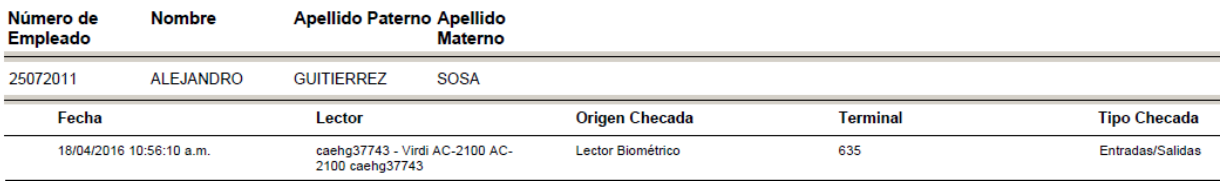
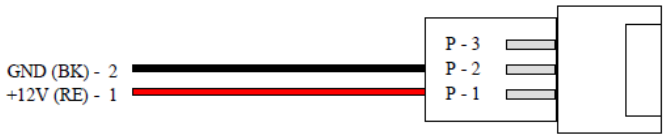


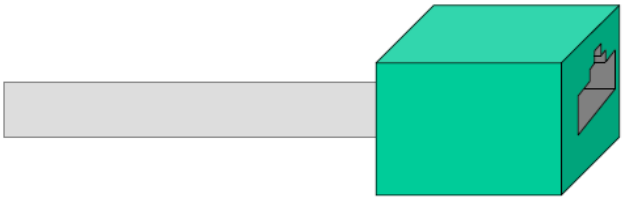
Imagen 1 – Reporte Accesos

Descripción de conexiones eléctricas.

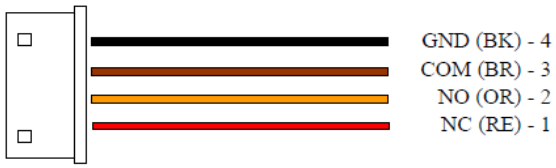
Especificaciones eléctricas para dispositivo biométrico Virdi AC-2100.



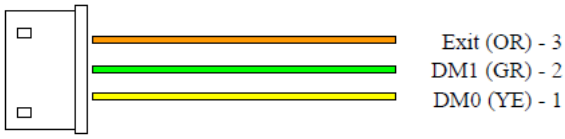
Cable adaptador de voltaje (101)



Cable de red RJ45 (102)

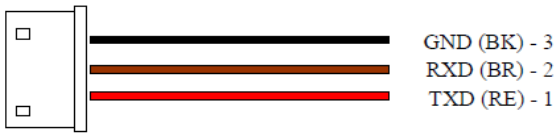


Lock Cable (4P) "Cable de control para aperturas" (103)

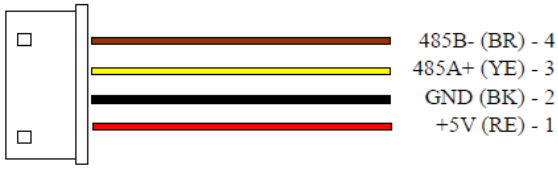


Lock Monitor & Exit Cable (3P) "Cable de control para pulsos de bandera" (104)

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



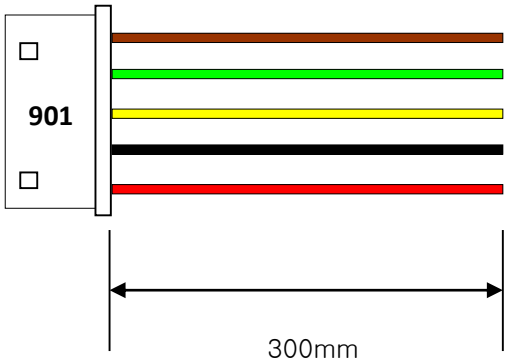
RS232 Cable (3P) "Cable de control para comunicaciones estándar Serial RS232" (106)



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)