



CONFIGURACIONES
GENERALES Y CONEXIONES
ELECTICAS.

VIRDI AC-7000

Manuales operacionales para usuario final	Página: 2
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

INDICE DEL MANUAL

0	introducción	3
II	configuraciones generales de red para dispositivos biométricos	4
VI	Descripción de la pantalla (Durante la operación)	5
VII	Iconos de advertencia	6
VIII	Tipos de Autenticación	7
	Configuraciones de su entorno	10
IX	Como tener acceso al menú sin la verificación del administrador	11
X	Configuración del idioma	13
XI	Conexión IP	15
XII	Extenderla cadena de caracteres para el número de empleados	17
XII	Variantes de autenticación	19
XIV	Dar de alta a un usuario	21
XV	Actualización de Firmware	25
XVI	Validación de interconexión de dispositivos biométricos	27
XVII	Descripción de conexiones eléctricas	30
XVIII	Especificaciones eléctricas	31



Manuales operacionales para usuario final	Página: 3
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.

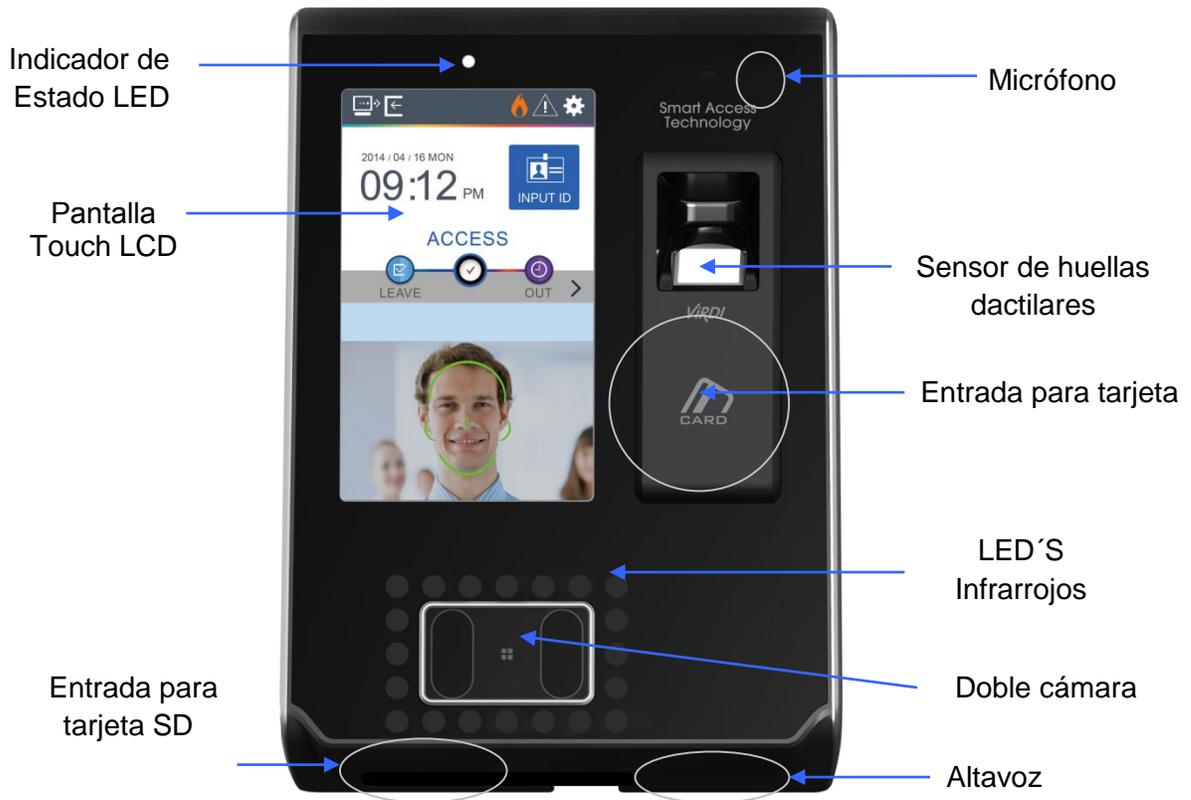


Manuales operacionales para usuario final	Página: 4
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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 Viridi AC-7000

Descripción del dispositivo biométrico AC-7000



Manuales operacionales para usuario final	Página: 5
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

Descripción de la pantalla (durante la operación)



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	 : Estado de puerta desconocido  : La puerta está cerrada  : La puerta está abierta
④ Estado de conexión del servidor	 : No está conectada la línea LAN  : No se encuentra conectado al servidor  : Conectado al servidor



Tipos de autenticación

Rostro	Registro de rostro Autenticación de rostro
Huella Dactilar	Registro de huella dactilar Autenticación de huella dactilar
Tarjeta	Registro de tarjeta Autenticación de tarjeta
Contraseña	Registro de contraseña Autenticación de contraseña
Tarjeta o huella digital	Registro de tarjeta o huella digital Autenticación de tarjeta o huella digital
Tarjeta y huella digital	Registro de tarjeta y huella digital Autenticación de tarjeta y huella digital
Tarjeta o contraseña	Registro de tarjeta o contraseña Autenticación de tarjeta o contraseña
Tarjeta y contraseña	Registro de tarjeta y contraseña Autenticación de tarjeta y contraseña
Huella digital o contraseña	Registro de huella digital o contraseña Autenticación de contraseña cuando la autenticación de huella digital ha fallado



Manuales operacionales para usuario final	Página: 8
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

Huella digital y contraseña	Registro de huella digital y contraseña Autenticación de contraseña después autenticación de huella digital
Tarjeta o rostro	Registro de rostro o tarjeta Autenticación de rostro o tarjeta
Tarjeta y rostro	Registro de rostro y tarjeta Autenticación de rostro después autenticación de tarjeta
Rostro o contraseña	Registro de contraseña o rostro Autenticación de rostro o autenticación de contraseña cuando la autenticación de rostro ha fallado después de introducir el ID
Rostro y contraseña	Registro de contraseña y rostro Autenticación de contraseña después autenticación de rostro
Huella digital o rostro	Registro de huella digital o rostro Autenticación de huella digital o autenticación de rostro cuando la autenticación de huella digital ha fallado después de introducir el ID
Huella digital y rostro	Registro de huella digital y rostro Autenticación de rostro después autenticación de huella digital
Tarjeta, Huella digital o rostro	Registro de huella digital, rostro y tarjeta Autenticación de rostro cuando la autenticación de huella digital ha fallado después de alguna otra autenticación.
(ID o tarjeta) y Huella digital	Registro de huella digital y tarjeta Autenticación de huella digital y autenticación de tarjeta



Manuales operacionales para usuario final	Página: 9
Configuraciones generales y conexiones eléctricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

(ID o tarjeta) y contraseña	Registro de contraseña y tarjeta Autenticación de contraseña después ID de entrada o autenticación de contraseña y tarjeta
(ID o tarjeta) y Rostro	Registro de rostro y tarjeta Autenticación de rostro después ID de entrada o autenticación de rostro después autenticación de tarjeta
Tarjeta, huella digital y contraseña	Registro de contraseña, huella digital y tarjeta Autenticación de huella digital y contraseña después de la autenticación de la tarjeta
Tarjeta, rostro y contraseña	Registro de contraseña, tarjeta y rostro Autenticación de tarjeta después autenticación de contraseña y rostro
Tarjeta, huella digital y rostro	Registro de rostro, huella digital y tarjeta Autenticación de huella digital, rostro y después autenticación de la tarjeta
Huella digital, rostro y contraseña	Registro de contraseña, huella digital y rostro Autenticación de rostro y contraseña después de la autenticación de huella digital
Tarjeta, huella digital, rostro y contraseña	Registro de contraseña, rostro, huella digital y tarjeta Autenticación de huella digital, rostro y contraseña después de la autenticación de la tarjeta.



Manuales operacionales para usuario final	Página: 10
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

Configuraciones de su entorno

Comprobaciones antes de configurar el entorno

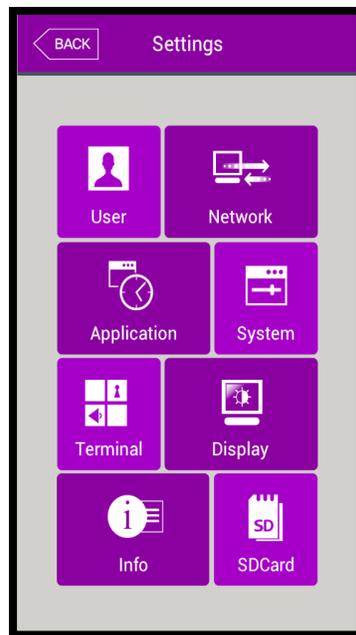
Entrar al menú:

Dar click en el icono [🔧] en la ventana básica, puede entrar a la ventana del menú principal de la siguiente manera.

Para ingresar a la ventana principal dar click en [BACK]

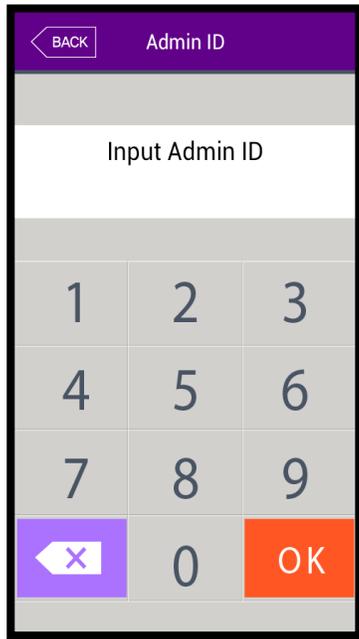
*Autorización del administrador

Si se ha registrado un administrador, la siguiente ventana pide la autorización del administrador por primera vez.



Manuales operacionales para usuario final	Página: 11
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

Como entrar al menú sin la autorización del administrador



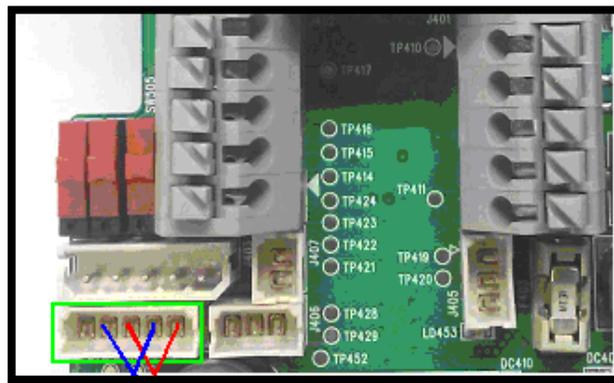
-Autorización del administrador

Si introduce el ID de administrador, la autorización del administrador se cumple junto con el método de autorización del administrador como la tarjeta, huella digital, la cara o la contraseña.

La autorización de administrador sólo aparece cuando existe el administrador registrado. La autorización sólo se cumple una vez al entrar en el modo de menú y se puede acceder a todo el menú hasta que salga el menú principal.

Para acceder al menú sin la autenticación de huellas dactilares o del rostro, o cuando no es posible debido a que la tarjeta de administrador registrada en el terminal se pierde o no hay administrador.

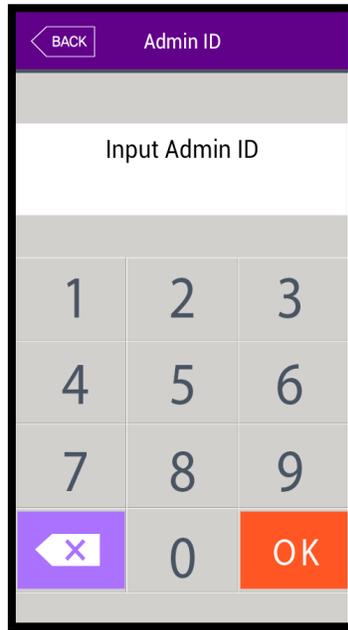
- ① Abrir la tapa quitando el soporte en la parte trasera del terminal del dispositivo biométrico.
- ② con la tapa abierta, como se muestra en la figura a continuación conectar el pin 1 con el 3 y el pin 2 al 4 del conector J404, Como se muestra en la siguiente imagen.



Manuales operacionales para usuario final	Página: 12
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

③ Haga clic en el icono  en la ventana principal, para entrar en la autorización del administrador.

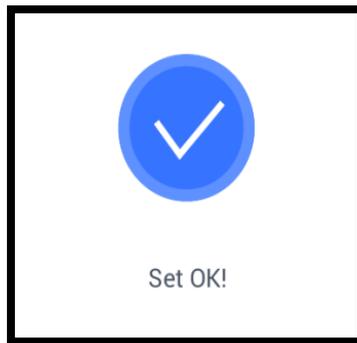
En la siguiente ventana introducimos como ID del administrador un '0' y dar click en el botón [] y a continuación podremos acceder a la ventana menú.



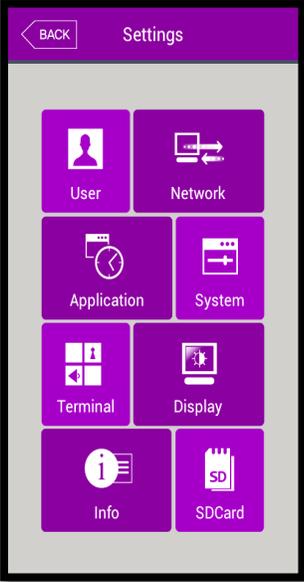
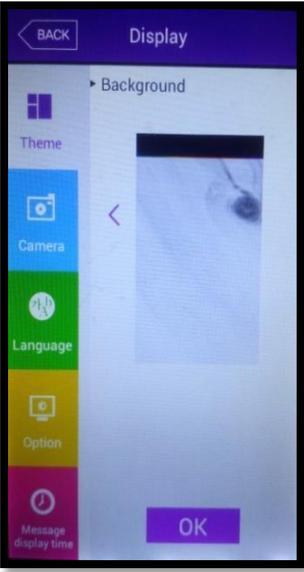
A continuación procedemos a retirar los cables de conexión en la parte trasera del dispositivo biométrico.

Como guardar los valores ingresados

Al realizar un registro en el dispositivo procedemos a guardarlo, nos tiene que mostrar la siguiente ventana. Para confirmar que el registro haya sido guardado.



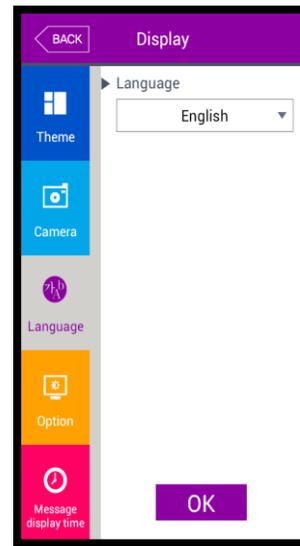
Configuración del idioma

Configuraciones del sistema: Para el cambio de idioma	
Accedemos mediante la siguiente secuencia de ventanas	
<p>1.- Presionamos el icono  en la pantalla del dispositivo, para acceder al menú principal, a continuación seleccionamos la opción [Display].</p>	
<p>2.- En el siguiente menú de la izquierda seleccionamos la opción [Language] para proceder a cambiar el idioma.</p>	



3.- Por default nos aparece el lenguaje en ingles procedemos a cambiarlo en la barra [English ▼]

Seleccionamos español.



4.- Para finalizar seleccionamos [ok] para guardar los datos nos mostrara el siguiente mensaje y listo.



Conexión IP

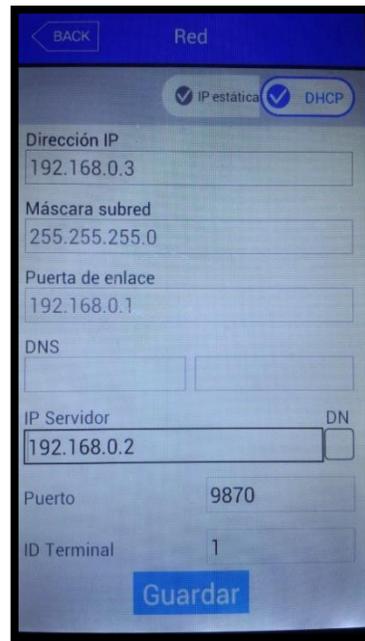
Configuraciones del sistema: Conexión IP

Accedemos mediante la siguiente secuencia de ventanas

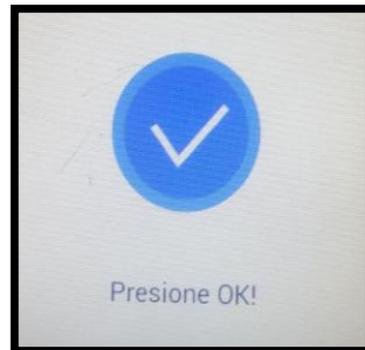
<p>1.- Presionamos el icono  en la pantalla del dispositivo, para acceder al menú, y seleccionamos la opción [Red].</p>	
<p>2.- En la siguiente ventana seleccionamos la opción [IP estática] para comenzar a editar.</p> <p>En Dirección IP, Mascara de subred y Puerta de enlace son correspondientes al equipo que vallamos a utilizar como servidor.</p>	



3.- En la siguiente opción [DHCP] modificamos según nuestro escenario de red.



4.- Por ultimo damos click en guardar, nos mostrara el siguiente mensaje y listo.



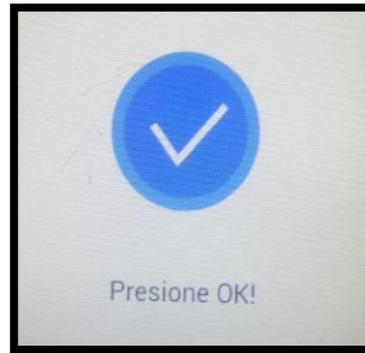
Extender la cadena de caracteres para el número de empleados

Configuraciones del sistema: Cadena de caracteres Accedemos mediante la siguiente secuencia de ventanas	
<p>1.- Presionamos el icono  en la pantalla del dispositivo, para acceder al menú principal, a continuación seleccionamos la opción [Sistema].</p>	
<p>2.- Nos envía directamente a la primera opción [Sistema]:</p> <ul style="list-style-type: none"> ▶ Longitud ID usuario: Seleccionamos esta opción para extender el número de caracteres del usuario [2-9]. ▶ Autenticación: En esta opción seleccionamos el tipo de autenticación del dispositivo, de preferencia [Terminal/Servidor]. ▶ Registro obligatorio: Escogemos el tipo de registro a considerar por usuario. <p>Número de dedos: seleccionamos el número de dedos a registrar de preferencia seleccionamos 2 por usuario</p>	



Manuales operacionales para usuario final	Página: 18
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

3.- Al ingresar nuestros registros correctamente seleccionamos [OK] para guardar nuestra información. Y seleccionamos de nuevo para regresar al menú principal.



Variantes de autenticación

Configuraciones del sistema: Autenticación

Accedemos mediante la siguiente secuencia de ventanas

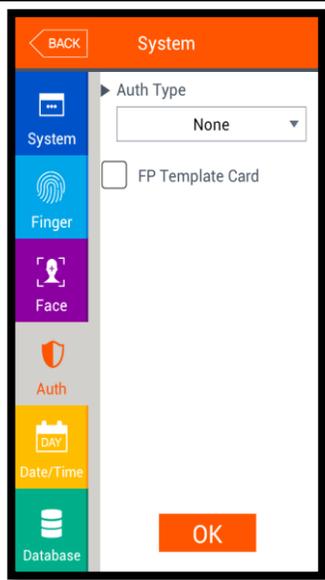
1.- Presionamos el icono  en la pantalla del dispositivo, para acceder al menú principal, a continuación seleccionamos la opción [Sistema].



2.-Enseguida en la barra de lado izquierdo seleccionamos la opción [Auth]:

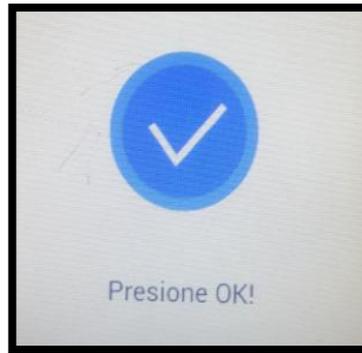
► Tipo de autenticación (Auth Type): seleccionamos el método de autorización de la terminal.

Huella en tarjeta (FP Template Card): Esta opción permite la autorización solo con la información del usuario en la tarjeta sin necesidad de descargar la información del usuario en la terminal.



Manuales operacionales para usuario final	Página: 20
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

3.- Al terminar de ingresar nuestros registros correctamente seleccionamos [ok] para guardar nuestra información. Y seleccionamos de nuevo para regresar al menú principal.

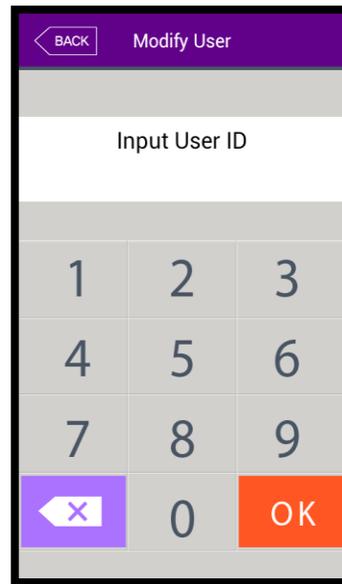


Dar de alta a un usuario

Configuraciones del sistema: Alta a usuario	
Accedemos mediante la siguiente secuencia de ventanas	
<p>1.- Presionamos el icono  en la pantalla principal del dispositivo, para acceder al menú, a continuación seleccionamos la opción [Usuario].</p>	
<p>2.- En la ventana usuario presionamos la opción [añadir] para ingresar un nuevo usuario.</p>	



3.- A continuación introducimos el número de ID del usuario a registrar y le damos click en [OK].

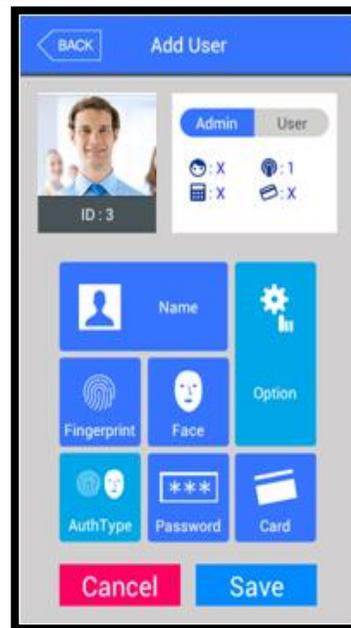


4.- En el siguiente menú nos muestra las diferentes opciones para registrar a un usuario:

-  : Numero de rostros registrados
-  : Numero de huellas dactilares registradas
-  : Registro de contraseña
-  : Numero de tarjetas registradas
- ID : 4** : Registro de ID

Admin **User** : Registro de usuario

Admin **User** : Registro del administrador



Nombre: Nombre de usuario

Identificación única: ID de usuario

Opción: En esta ventana nos muestra el nivel de autorización del usuario, puede tener distintos niveles de autorización con esta opción.

Huella: Registro de huella

Cara: Registro de rostro

Duress Huella : Registro de huella desgastada

Clave: Registro de cable y confirmación de la misma.

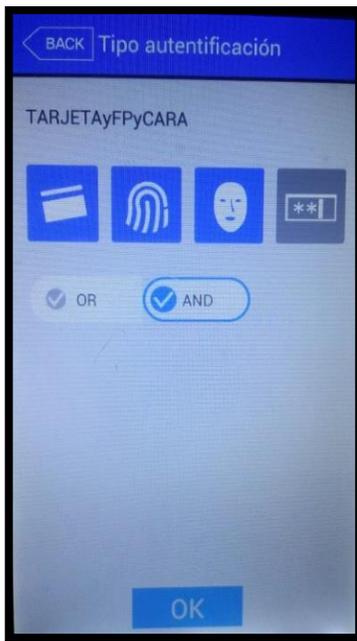
Tarjeta: Registro de tarjeta



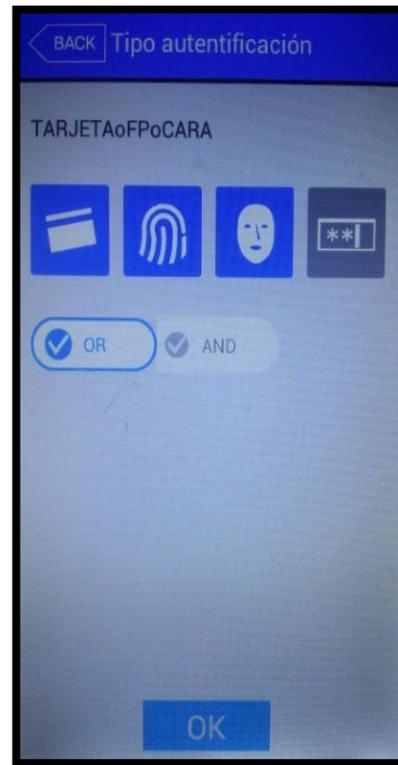
En la opción:

Tipo de autenticación: Teniendo los registros de rostro, huella digital, contraseña e identificación de tarjeta podemos seleccionar entre uno o máximo tres tipos de registro para nuestra autenticación, como se muestra a continuación.

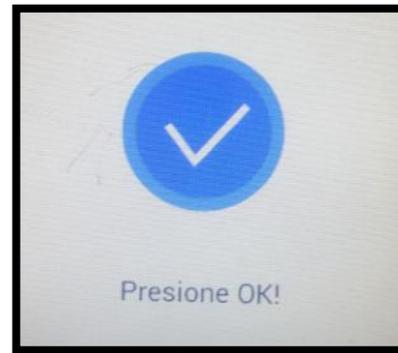
En la opción: [AND] Tenemos seleccionados tres tipos de registros, los cuales tenemos que ingresar para poder autorizar nuestra autenticación en el dispositivo.



5.- En la opción [OR]: podemos elegir un solo registro de las cuatro opciones para nuestra autenticación en el dispositivo.



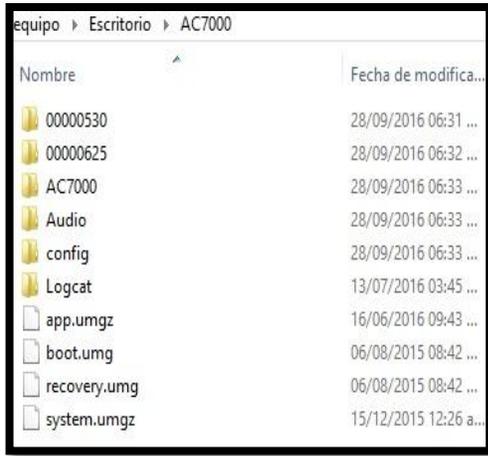
5.- Al terminar de ingresar nuestros datos correctamente seleccionamos [OK] y listo.



Actualización de Firmware

Configuraciones del sistema: Firmware

Accedemos mediante la siguiente secuencia de ventanas

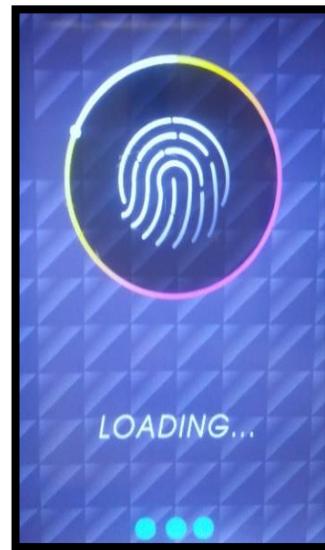
<p>1.- Creamos una carpeta con el nombre [AC7000] en la tarjeta SD y copiamos todos los archivos necesarios para la actualización del Firmware como se muestra a continuación.</p> <p>(Recomendable solicitar la actualización más actual del dispositivo, con el área de soporte técnico).</p>	
<p>2.- Procedemos a insertar la tarjeta SD a nuestro dispositivo, enseguida seleccionamos el icono  para acceder al menú principal.</p>	



3.- A continuación seleccionamos el icono [TarjetaSD] para acceder al siguiente menú y pulsamos el botón [Actualizar Firmware].



4.- Enseguida el Firmware comenzara a actualizarse, No apagar el dispositivo hasta que la actualización se haya completado, se reiniciara automáticamente y listo.



Manuales operacionales para usuario final	Página: 27
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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 ventana 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.

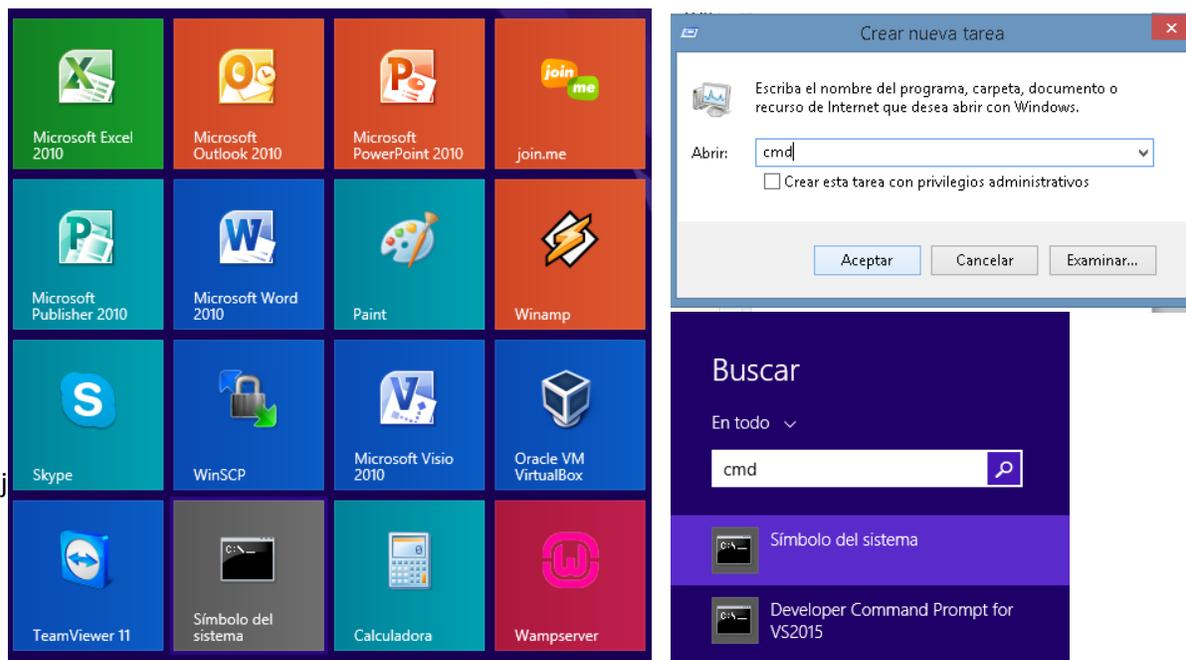


Imagen 1 – Icono de Símbolo de Sistema

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 presionando la tecla **Enter**.



Manuales operacionales para usuario final	Página: 28
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>ping 192.168.0.202

Haciendo ping a 192.168.0.202 con 32 bytes de datos:
Respuesta desde 192.168.0.202: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.0.202: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.202: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.202: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 192.168.0.202:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Windows\system32>

```

Imagen 1 – Ventana de sistema ping exitoso

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

```

C:\Users\soporte
Símbolo del sistema
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Users\soporte>ping 192.168.0.201

Haciendo ping a 192.168.0.201 con 32 bytes de datos:
Respuesta desde 192.168.0.2: Host de destino inaccesible.

Estadísticas de ping para 192.168.0.201:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
C:\Users\soporte>_

```

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.

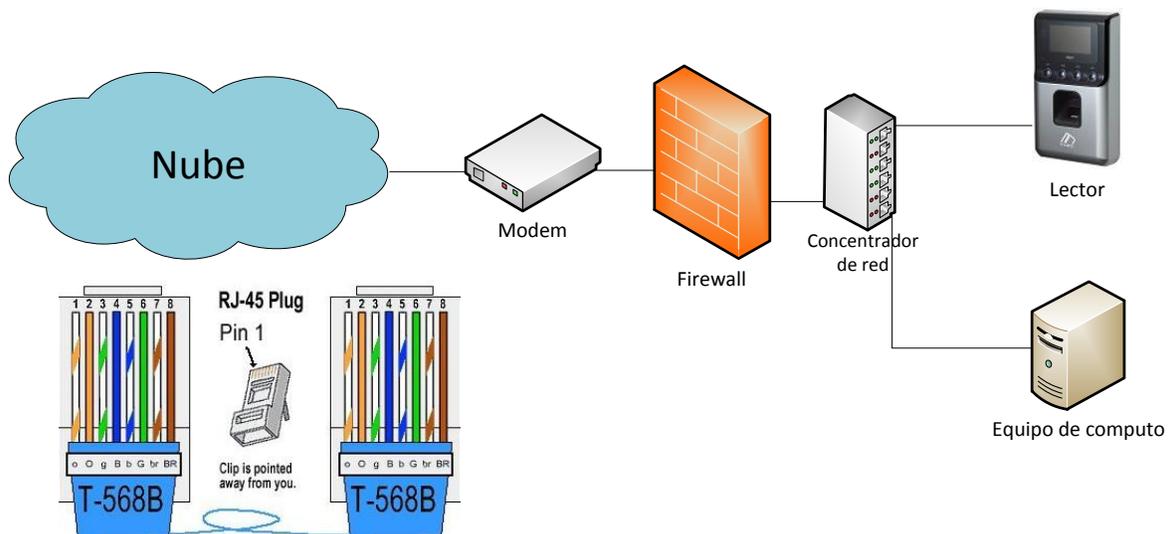


Imagen 1 – Esquema de red local estándar.



Prueba (B) Interconexión de dispositivo biométrico a base de datos en la nube:

En esta prueba lo que pretendemos valorar es el hecho de envío 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 envío 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.

Terminales AC En Línea

Arrastre una columna aquí para agrupar por dicha columna						
ID Terminal	Puerto	Conexión Activa Desde	Último Poleo	Minutos Sin Polear	Registro Tiempo Real	Empleado Tiempo Real

Sin datos para mostrar

Imagen 1 – Ventana de sistema Poleo inexistente

Terminales AC En Línea

Arrastre una columna aquí para agrupar por dicha columna						
ID Terminal	Puerto	Conexión Activa Desde	Último Poleo	Minutos Sin Polear	Registro Tiempo Real	Empleado Tiempo Real
402	9870	23/02/2016 13:31:02	23/02/2016 09:38:13	106809	23/02/2016 08:32:22	612661
403	9870	07/05/2016 13:46:14	07/05/2016 01:43:07	724	06/05/2016 17:29:08	601110
404	9870	22/04/2016 11:48:50	22/04/2016 11:47:05	21720	22/04/2016 11:48:47	40006192
405	9870	07/05/2016 13:46:14	07/05/2016 01:44:13	723	06/05/2016 13:41:00	40005201
631	9870	07/05/2016 13:46:14	07/05/2016 11:04:15	163	07/05/2016 11:03:41	613570

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.

Número de Empleado	Nombre	Apellido Paterno	Apellido Materno
25072011	ALEJANDRO	GUITIERREZ	SOSA

Fecha	Lector	Origen Checada	Terminal	Tipo Checada
18/04/2016 10:56:10 a.m.	caehg37743 - Virdi AC-2100 AC-2100 caehg37743	Lector Biométrico	635	Entradas/Salidas

Imagen 1 – Reporte Accesos

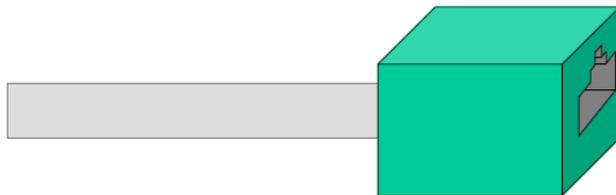


Descripción de conexiones eléctricas.

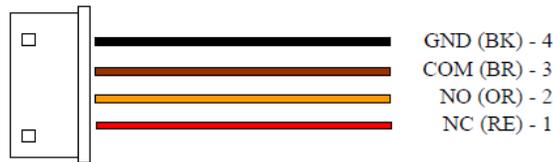
Especificaciones eléctricas para dispositivo biométrico Viridi AC-2100.



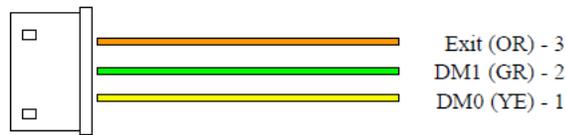
Cable adaptador de voltaje (101)



Cable de red RJ45 (102)



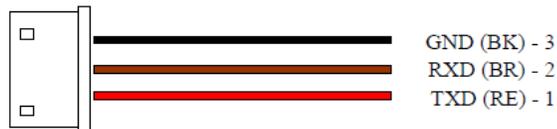
Lock Cable (4P) "Cable de control para aperturas" (103)



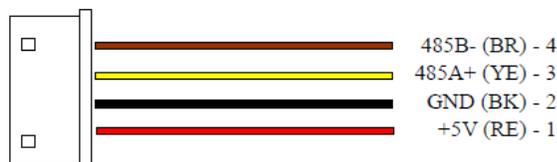
Lock Monitor & Exit Cable (3P) "Cable de control para pulsos de bandera" (104)



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)



INGRESIO

☎ +52 (55) 9000 07 34 a 36

✉ info@ingressio.com

🌐 www.ingressio.com

Manuales operacionales para usuario final	Página: 31
Configuraciones generales y conexiones electricas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

Especificaciones eléctricas botón liberador EB-030.

Cable externo (5P)

