

CONFIGURACIONES GENERALES Y CONEXIONES ELECTICAS.

VIRDI AC-5000

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	Descripción del teclado	6
VIII	Tipos de Autenticación	7
IV	Configuraciones de su entorno	9
	Como tener acceso al menú sin la verificación del	10
Х	administrador	
XI	Configuración del idioma	11
XII	Conexión IP	13
XII	Especificaciones de la ventana Id terminal	15
XII	Extender la cadena de caracteres para el número de empleados	16
XIV	Variantes de autenticación	18
XV	Dar de alta a un usuario	19
XVI	Validación de interconexión de dispositivos biométricos	23
XVII	Descripción de conexiones eléctricas	26
XVIII	Especificaciones eléctricas	27



Manuales operacionales para usuario final	Página: 3
Configuraciones generales y conexiones electicas.	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 electromecánicos 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 electicas.	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 Virdi AC-5000RF

Descripción del dispositivo biométrico AC-5000RF



Configura	aciones gene	erales y conexiones electicas	Sentiembre 2016
Departamento de operaciones		Versión 3.0	
	Descrip	oción de la pantalla (durante la operació	n)
		 Detección de incendios 	
Modo de acceso 2 Advertencia de desmontaje de		ije del terminal	
1		3 Estado de la puerta	
\			
F1			n con el
		servidor	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	2011/0	01/27	
	05:53	3 PM	ctual
		Hora a	Cludi
1) Detección de			
ncendios	incendios Cuando se detecta fuego por el sensor de fuego (suj		sor de fuedo (suieto
		a la appavión del concer de incondic	on do laogo (bajoto
	×	a la conexión del sensor de incendio	apropiado).
	*	a la conexión del sensor de incendio	o apropiado).
2) Advertencia	×	a la conexión del sensor de incendio El estado anormal cuando el termina	al es desmontado o
2 Advertencia	× (	a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema	al es desmontado o
2 Advertencia		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema	al es desmontado o
2 Advertencia		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido	al es desmontado o a.
2) Advertencia 3) Estado de la		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido	al es desmontado o a.
<ul> <li>Advertencia</li> <li>Advertencia</li> <li>Estado de la puerta</li> </ul>		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada	al es desmontado o a.
<ul> <li>2 Advertencia</li> <li>3 Estado de la puerta</li> </ul>		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada	al es desmontado o a.
<ul> <li>Advertencia</li> <li>Advertencia</li> <li>Estado de la puerta</li> </ul>		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada :Puerta abierta	al es desmontado o a.
<ul> <li>Advertencia</li> <li>Estado de la puerta</li> </ul>		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada :Puerta abierta	al es desmontado o a.
<ul> <li>Advertencia</li> <li>Estado de la ouerta</li> </ul>	X	a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada :Puerta abierta : Cable LAN no está conectado	al es desmontado o a.
<ul> <li>Advertencia</li> <li>Estado de la puerta</li> </ul>		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada :Puerta abierta : Cable LAN no está conectado	al es desmontado o a.
<ul> <li>Advertencia</li> <li>Estado de la puerta</li> <li>Conexión con</li> <li>servidor</li> </ul>		a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada :Puerta abierta : Cable LAN no está conectado : Conexión del cable LAN. Pero no a	al es desmontado o a.
<ul> <li>2 Advertencia</li> <li>3 Estado de la ouerta</li> <li>4 Conexión con el servidor</li> </ul>	Ninguno	a la conexión del sensor de incendio El estado anormal cuando el termina la puerta ha encontrado un problema :Estado de la puerta es desconocido :Puerta cerrada :Puerta abierta : Cable LAN no está conectado : Conexión del cable LAN. Pero no a	al es desmontado o a.



Manuales operacionales para usuario final	Página: 6
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

## 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	- Se utiliza para cambiar el modo de autenticación
0 [←]	<ul> <li>Utilizado como la tecla Supr. Para su corrección cuando los valores numéricos son de entrada.</li> </ul>
	- Se utiliza para cancelar la entrada, y pasar al menú principal
	- Significa pulsa la tecla [F4 (←)] durante dos segundos o más.
[F4(←)]	<ul> <li>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.</li> </ul>
ENT	- usada para modificar el modo
[O MENU]	<ul> <li>Se utiliza ingresar al menú principal y poder ingresar los valores deseados.</li> </ul>
	- Significa pulsa la tecla [ENT] durante dos segundos o mas
	- Se utiliza para acceder al menú, cuando se mantiene presionado
[ENT-]	<ul> <li>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.</li> </ul>
	<ul> <li>Utilizado para aplicar la configuración en la pantalla actual en el modo menú y luego salir al menú principal.</li> </ul>



Manuales operacionales para usuario final	Página: 7
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

### 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



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

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



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

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.

Configuration	
1.User	
2.Network	
3.Application	
4.System	
5.Terminal	
6.Information	

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.

Ve	rify Admin
SR o	Input Admin ID

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.



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

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 ( $\leftarrow$ )] 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.



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

Configuración del idioma

Configuraciones del sistema: Para el cambio de idioma Accedemos mediante la siguiente secuencia de ventanas 1.- Presionamos la tecla [ENT] de Configuration nuestro dispositivo durante un periodo de 4 segundos, a continuación nos 1.User desplegara la siguiente ventana. 2.Network **3.**Application 4.System 5.Terminal 6.Information 2.- Seleccionamos la opción 4. System, System nos mostrara el siguiente menú. 1.System Setting 2.Authentication 3.Fingerprint 4.Language **5.Date Time** 6.Database 3.- Seleccionamos la opción 4. Language Language y nos desplegara la siguiente menú. 01 ▶ Language 1.English 2.Korean 4.Spanish 3.Japanese 5.Portuguese 6.Polish 7.Danish 8.Russian 9.Chinese 10.Arabic 12.French 11.Srpski 14.Turkish 13.Dutch



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

<ul> <li>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.</li> </ul>	Language 1.English 2.Korean 3.Japanese 4.Spanish 5.Portuguese 6.Polish 7.Danish 8.Russian 9.Chinese 10.Arabic 11.Srpski 12.French 13.Dutch 14.Turkish
5 A continuación mantenemos presionada la tecla [ENT] para salir de la ventana actual y regresamos a la pantalla anterior.	System 1.System Setting 2.Authentication 3.Fingerprint 4.Language 5.Date Time 6.Database
<ul> <li>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.</li> </ul>	Configuration Save? 1.Yes 2.No



Manuales operacionales para usuario final	Página: 13
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

CONEXION IF
-------------

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.	Configuración 1.Usuario 2.Red 3.Aplicación 4.Sistema 5.Terminal 6.Info.	
<ul> <li>2 A continuación Seleccionamos la opción</li> <li>[2. Red] y nos mostrara el siguiente menú.</li> </ul>	Red 1.IP 2.IP del Servidor 3.ID Terminal	
<ul> <li>3 Seleccionamos (1.IP), por default nos aparece marcada la opción (1.IP Estática).</li> <li>Eliminamos los valores existentes con la tecla [F4 (←)] Para comenzar a ingresar los datos de red.</li> <li>IP, Mascara de subred y Entrada correspondientes al equipo que vallamos a utilizar como servidor.</li> </ul>	IP • 1.IP Estática • 2.DHCP IP 192.168.000.209 Máscara de Subred 255.255.255.000 Entrada 192.168.000.001	



Manuales operacionales para usuario final	Página: 14
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.	IP del Servidor IP del Servidor 184.072.217.188 Puerta del servidor 9879
5 Salimos del menú presionando la tecla [ENT] e ingresamos a la opción [3. ID Terminal] del menú de Red.	ID Terminal
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	<ul> <li>Autenticación</li> <li>1.Servidor/Terminal</li> <li>2.Terminal/Servidor</li> <li>3.Sólo Servidor</li> <li>4.Sólo Terminal</li> </ul>
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.	
<ul> <li>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.</li> </ul>	Configuration Save? 1.Yes 2.No



Manuales operacionales para usuario final	Página: 15
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.

Manuales operacionales para usuario final	Página: 16
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.	Configuración 1.Usuario 2.Red 3.Aplicación 4.Sistema 5.Terminal 6.Info.	
2 Seleccionamos la opción [4.Sistema] para acceder al siguiente menú y elegimos la opción [1.Config. Del sistema].	Sistema 1.Config. Del Sistema 2.Autenticación 3.Huella [FP] 4.Idioma 5.Fecha & Hora 6.Base de Datos	
<ul> <li>3A continuación con la tecla [F4←] editamos el número de usuarios a considerar dentro de un rango de 0-9 dígitos.</li> <li>En [Opciones del Display]: Es recomendable seleccionar la opción [3.Nombre de usuario].</li> </ul>	Config. Del Sistema Longitud ID Usuario 08 Opciones del Display 1.Nada 2.ID Usuario 3.Nombre Ust 4.Clave de Usu 5.Mensaje	



Manuales operacionales para usuario final		Página: 17
Configuraciones generales y conexiones electicas.		Septiembre 2016
Departamento de operacione	S	Versión 3.0
<ul> <li>3 Seleccionamos la tecla [ENT] para regresar a la ventana anterior [4.Sistema], y [F4←] para volver al menú de configuración.</li> </ul>	Configur 1.Usuario 2.Red 3.Aplicació 4.Sistema 5.Terminal 6.Info.	n
4 En la siguiente ventana seleccionamos la opción [1.Si] y con la tecla [ENT] guardamos la configuración realizada.	Configur Salva 1.Si	ación ar? 2.No



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

Variantes de autenticación

Configuraciones del sistema: Autenticación Accedemos mediante la siguiente secuencia de ventanas 1.- Presionamos la tecla [ENT] durante un Configuración periodo de 4 segundos, a continuación 1.Usuario nos desplegara la siguiente ventana. 2.Red 3.Aplicación 4.Sistema 5.Terminal 6.Info. 2.-Seleccionamos la opción [4.Sistema] Sistema para acceder al siguiente menú y elegimos la opción [2.Autenticación]. 1.Config. Del Sistema 2.Autenticación 3.Huella [FP] 4.Idioma 5.Fecha & Hora 6.Base de Datos 3.- En la ventana de autenticación nos Autenticación muestra las distintas formas de ingresar 1.Usar ID del Grupo usuarios al dispositivo. **√**2.Habilitar 1:N 3.Sólo tarjeta **4.**Plantilla en tarjeta 5.Verif. Multi-FP ▶ Tiempo de Bloqueo 0 NetErrTime(sec) 5

Manuales operacionales para usuario final	Página: 19
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.	Configuración 1.Usuario 2.Red 3.Aplicación 4.Sistema 5.Terminal 6.Info.	
2 A continuación seleccionamos la opción [1.Usuario], para añadir un nuevo usuario pulsamos [1.Adicionar].	Usuario 1.Adicionar 2.Borrar 3.Modificar 4.Borrar Todos	
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.	Adicionar ID Usuario 0001	

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

4 A continuación Seleccionamos [1.Tipo de Aut.] para acceder al	Adicionar
siguiente sub menú según el tipo de autenticación que se requiera para el registro de usuario.	ID:11.Tipo de Aut.ID:12.Reg. HuellaID:13.Reg. TarjetaID:13.Reg. ContraseñaID:14.Reg. ContraseñaID:15.Opción de HuellaID:1ENT]:Guardar
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.	Adicionar Tipo de Aut. 1.Huella [FP] 7.Card & FP 2.Contraseña 8.Card or PW 3.FP o PW 9.Card & PW 4.FP & PW 10.(IDorCard)&FP 5.Tarjeta 11.(IDorCard)&PW 6.Card or FP 12.Card&PW&FP
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].	Adicionar ID:1 ID:1 I.Tipo de Aut. 2.Reg. Huella 3.Reg. Tarjeta 4.Reg. Contraseña 5.Opción de Huella IENT]:Guardar
<ul> <li>7 La opción [5.Opción de Huella] nos mostrara la siguiente ventana:</li> <li>[&gt;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].</li> </ul>	Opción de Huellas ▶ 1:1 Nivel [0~9] ☑ 1.Habilitar 1:N



Manuales operacionales para usuario final	Página: 21
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.





Manuales operacionales para usuario final	Página: 22
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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.



Manuales operacionales para usuario final	Página: 23
Configuraciones generales y conexiones electicas.	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 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.



Manuales operacionales para usuario final	Página: 24
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

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

C:\Windows\system32\cmd.exe	- 🗆 🗙
Microsoft Windows [Versión 6.3.9600] (c) 2013 Microsoft Corporation. Todos los derechos rese	rvados.
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= Respuesta desde 192.168.0.202: bytes=32 tiempo<1m TTL=1 Respuesta desde 192.168.0.202: bytes=32 tiempo=1ms TTL= Respuesta desde 192.168.0.202: bytes=32 tiempo=1ms TTL=	128 28 28 128
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:



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.



Manuales operacionales para usuario final	Página: 25
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

#### 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.

1 ei	THE	lates	AC		iea

universities and the sec

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
♡	♥		~ 🕈	♥	✓ ♥	2

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 1	0:56:10 a.m.	caehg37743 - Virdi 2100 caehg37743	AC-2100 AC-	Lector Biométrico	635	Entradas/Salidas

#### Imagen 1 – Reporte Accesos



Manuales operacionales para usuario final	Página: 26
Configuraciones generales y conexiones electicas.	Septiembre 2016
Departamento de operaciones	Versión 3.0

#### Descripción de conexiones eléctricas.

Especificaciones eléctricas para dispositivo biométrico Virdi AC-2100.



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

## Especificaciones eléctricas botón liberador EB-030.



