



Manual do usuário
Manual del usuario

SS 1530 MF W
SS 1540 MF W



SS 1530 MF W y SS 1540 MF W

Controlador de acceso con reconocimiento de rostro

Felicitaciones, acabas de adquirir un producto con la calidad y seguridad Intelbras.

Los dispositivos SS 1530 MF W y SS 1540 MF W son controladores de acceso con autenticación por reconocimiento facial, tarjeta RFID 13,56 MHz/código QR, contraseña y biometría digital (excepto SS 1530 MF W). Con una pantalla táctil de 4,3", es práctico para registrarse y cambiar la configuración. Se puede instalar en interiores para abrir puertas en general, mediante la activación de cerraduras eléctricas, electroimanes o solenoides.



Este equipamiento no tiene derecho a la protección contra interferencia prejudicial y no puede causar interferencia en sistemas debidamente autorizados. Este es un producto homologado por la Anatel, el número de homologación lo encuentras en la etiqueta del producto, para consultas usa el enlace: <https://www.gov.br/anatel/pt-br>.

Cuidados y seguridad

- » Debes guardar las instrucciones de seguridad y operación, para referencias futuras.
- » Usa la fuente de alimentación que acompaña el producto.
- » Debes usar el producto en ambientes internos con temperatura superior a -10 °C e inferior a 40 °C.
- » El intento de abrir el producto lo puede dañar e implica en pérdida del derecho a la garantía.
- » Cuidado al manejar los cables para no dañarlos.
- » No sobrecargues las tomas o alargues eléctricos, pues puede causar incendio o una descarga eléctrica.
- » Instalarlo en un local seguro.
- » No pongas o instales el producto en lugares expuestos a la luz del sol o fuentes de calor.
- » Mantenga el producto lejos de humedad, hollín o polvo.
- » Instala el producto de forma vertical y en local estable, garantizando la correcta fijación para que no caiga, causando daños al equipamiento.
- » Limpia el producto con paño humedecido en agua o seco. No utilice productos químicos fuertes o abrasivos.
- » Instale el producto en local ventilado y no bloquee la ventilación del controlador de acceso.
- » Usa apenas accesorios recomendados por el fabricante.
- » LGPD - Ley General de Protección de Datos Personales: la Intelbras no accede, transfiere, capta, ni realiza cualquier otro tipo de tratamiento de datos personales a partir de este producto. Este producto tiene criptografía en la transmisión y almacenamiento de los datos personales.

Atención: daños causados por el no cumplimiento de las recomendaciones de instalación o uso inadecuado del producto no son cubiertos por la garantía. Ver el certificado de garantía del producto.

1. Especificaciones técnicas

Modelo	SS 1540 MF W	SS 1530 MF W
Tensión de alimentación	12 Vdc	
Consumo	18 W	
Capacidad de conmutación	2 A / 30 Vdc	
Dimensiones (An x Al x Pr)	118 x 115 x 27,1 mm	
Temperatura de funcionamiento	-10 °C a 40 °C	
Humedad de funcionamiento	0 a 90%	
Display	Pantalla táctil de 4,3" (capacitiva)	
Cámara	CMOS RGB de 2 MP y CMOS IR de 2 MP	
Intervalo de reconocimiento facial	Distancia a la cara: 0,3 m a 1,5 m	
	Altura del usuario: 0,9 m a 2,4 m	
Tiempo de reconocimiento facial	0,2s	
Tiempo de reconocimiento digital	0,5s	-
Métodos de autenticación	Reconocimiento facial, biometría digital, contraseña y tarjeta/código QR	
Sensor biométrico digital	Si	No
Interface de comunicación	RS-485 y Wiegand (Entrada o Salida)	
Capacidad	Usuarios	3000
	Faces	3000
	Digital	5000
	Tarjetas/Códigos QR	5000
	Contraseñas	3000
	Eventos	300000
Wi-Fi	Antena	Interna
	Estándares	IEEE 802.11b, 802.11g, 802.11n
	Frecuencia de operación	2,4 GHz ~ 2,4835 GHz
	Ancho de banda	Soporta 20 MHz e 40 MHz
	Protocolo de seguridad	64/128 bit WEP, WPA/WPA2, WPA2-PSK/WPA2-PSK
	Tasa de baudios	802.11b: hasta 11 Mbps
		802.11g: hasta 54 Mbps 802.11n: hasta 300 Mbps (HT40)
RFID	Modulación	ASK
	Frecuencia	13,56 MHz
	Tasa de baudios	106 a 848 kbps
	Código de emisión	13M5K2D
	Tipo de antena	Interna

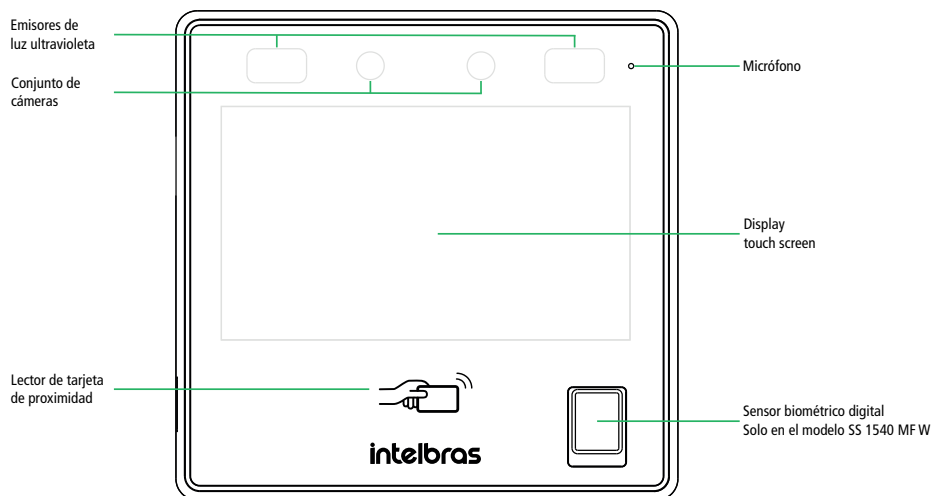
2. Características

- » Fácil instalación.
- » Visual moderno y funcional.
- » Compatible con Defense IA.
- » Integrado al sistema MIP 1000 IP.
- » Para uso en ambiente interno.
- » Función anti-falso que imposibilita la autenticación por vídeo o foto en medio físico o digital.
- » Soporta reconocimiento facial, tarjeta RFID 13,56 MHz/código QR, contraseña y biometría digital (excepto SS 1530 MF W).
- » Cámara doble grande angular de 2 MP: una de luz visible colorida (RGB) y otra de luz infrarroja (IR).
- » Precisión de verificación de rostro >99,5%.
- » Bajo índice de falso rechazo.

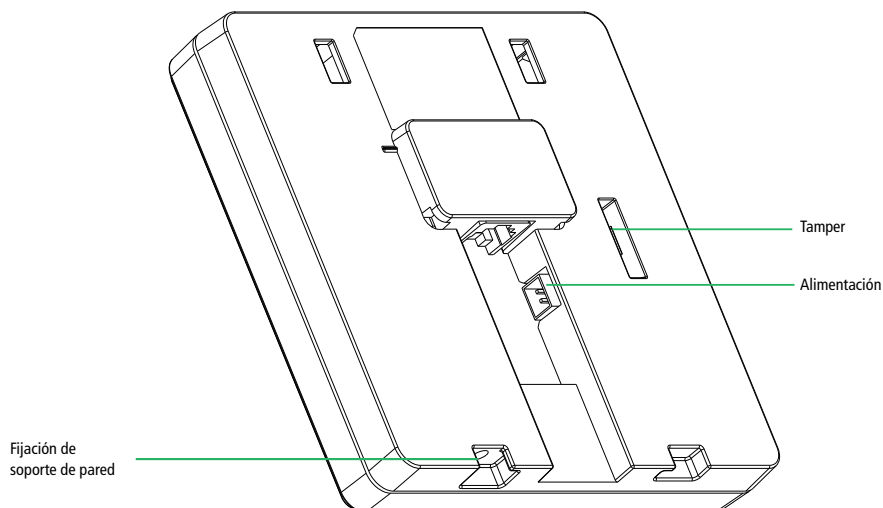
3. Contenido del embalaje

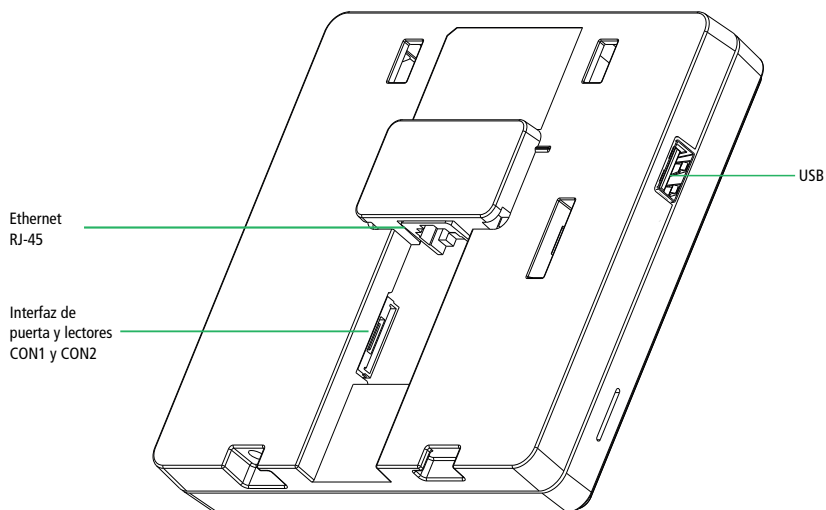
- » 1× controlador de acceso SS 1530 MF W o SS 1540 MF W
- » 1× conjunto de tarugos y tornillos
- » 1× soporte para fijación en la pared
- » 1× fuente de alimentación
- » 1× guía del usuario

4. Producto

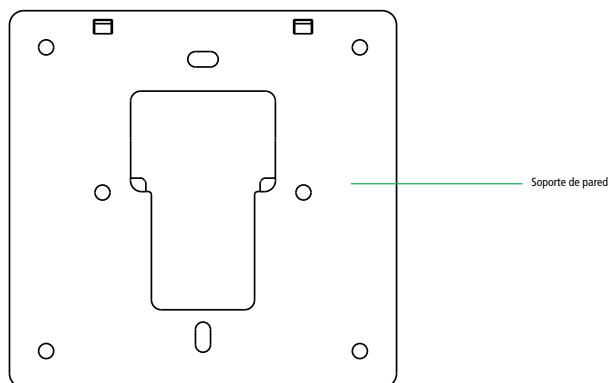


Vista frontal





Vista trasera



Soporte de fijación

4.1. Descripción de los cables

Interface de leitores (CON1)

Color	Nombre	Descripción
Amarillo	485-	Señal 485B o 485 del bus RS-485 / Salida B para integración MIP.
Púrpura	485+	Bus RS-485 485A o 485+ señal / Salida A para integración MIP.
Blanco	WD1	Entrada Wiegand D1 (para conectar un lector auxiliar) / Salida Wiegand D1 (para conectar a otro controlador de acceso).
Verde	WD0	Entrada Wiegand D0 (para conectar un lector auxiliar) / Salida Wiegand D0 (para conectar a otro controlador de acceso).
Negro	GND	Referencia al bus Wiegand.
Marrón	LED	Salida para señalización de acceso para lector auxiliar / Entrada para recepción de señalización de acceso.

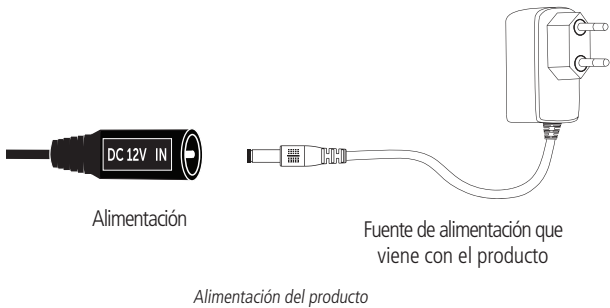
Interfaz de puerta (CON2)

Color	Nombre	Descripción
Marrón oscuro	PORTA_COM	Acceder al contacto común del relé del gatillo de liberación.
Amarillo negro	PORTA_NA	Acceda al contacto del relé del gatillo de liberación normalmente abierto.
Negro/morado	PORTA_NF	Contacto del relé del gatillo de liberación de acceso normalmente cerrado.
Negro	GND	Referencia para señal de botón de salida y sensor de puerta.
Gris negro	SEN	Conexión para sensor de puerta.
Verde negro	BOT	Conexión para botón de salida.

5. Esquemáticos de conexión

5.1. Fuente de alimentación

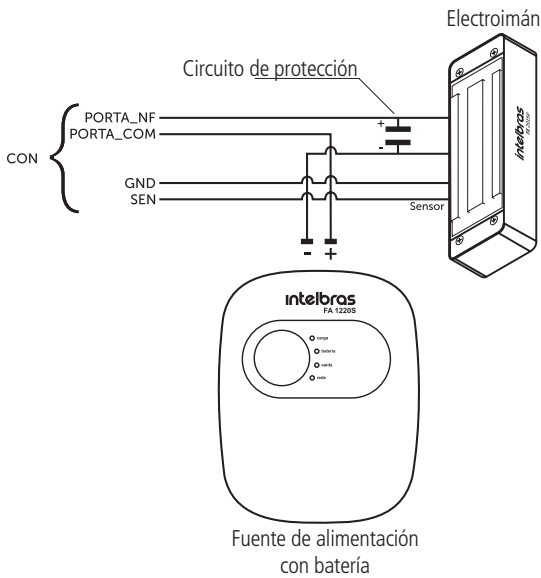
Conecte la fuente de alimentación al dispositivo y en seguida, conectarla a la toma eléctrica.



Obs.: se recomienda el uso de un nobreak para suministrar situaciones de cortes de energía eléctrica.

5.2. Cerraduras

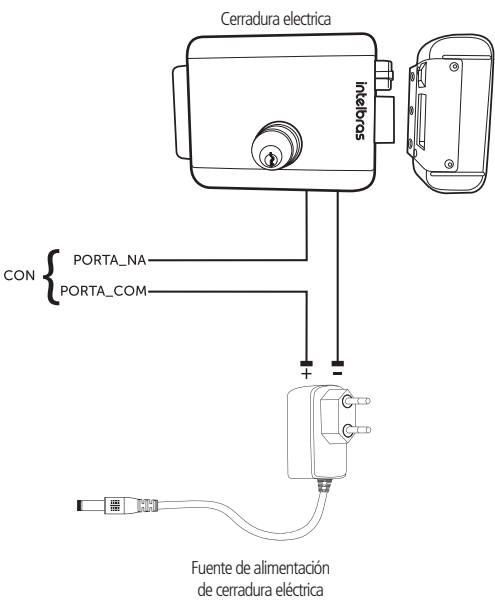
Cerradura electroimán



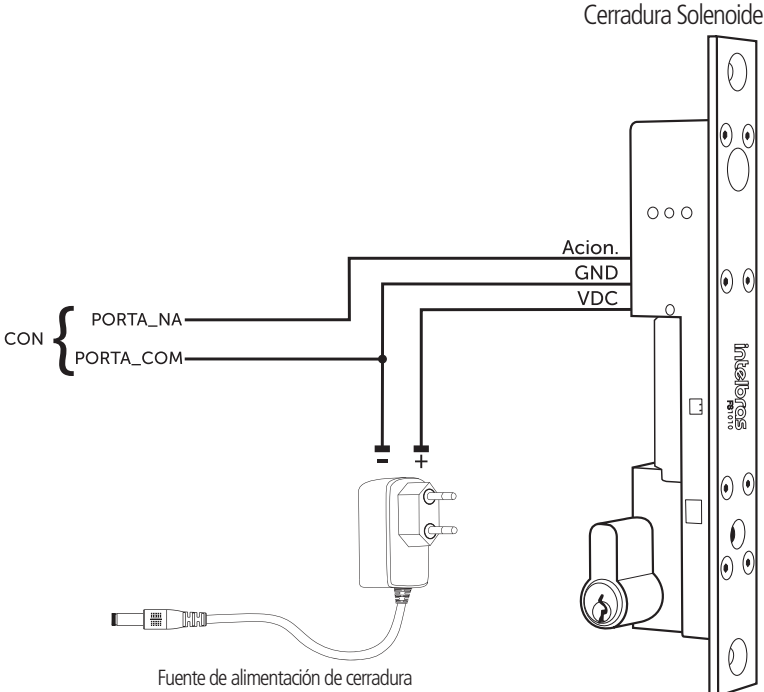
Ejemplo de conexión de cerradura electroimán

Obs.: si la cerradura no tiene sensor, ignora la conexión de este.

Cerradura eléctrica

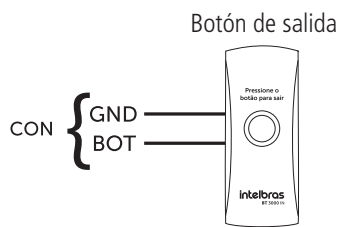


Cerradura solenoide



Ejemplo de conexión de cerradura solenoide

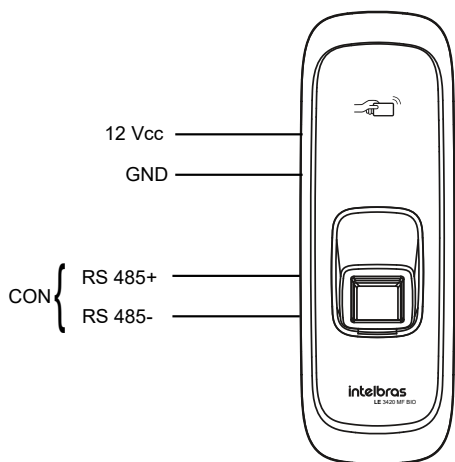
5.3. Botón de salida



Ejemplo de conexión de botón de salida

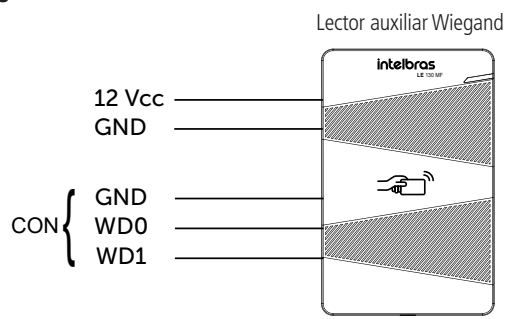
Obs.: la entrada de alarma se acciona cuando el contacto seco se cierra.

5.4. Lector auxiliar biométrico digital



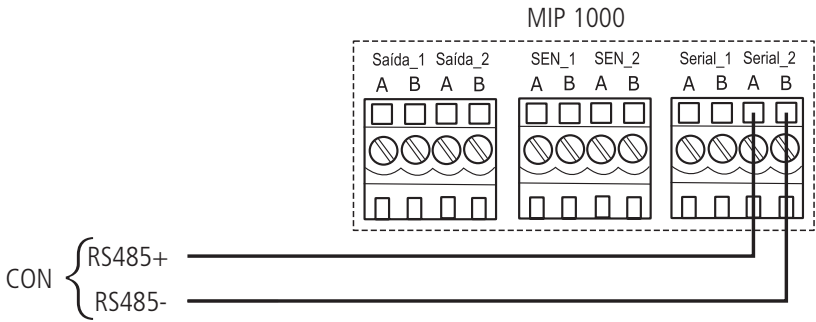
Ejemplo de conexión de lector biométrico digital

5.5. Lector auxiliar Wiegand



Ejemplo de conexión de lector Wiegand

5.6. Módulo inteligente de portería (MIP 1000 IP)



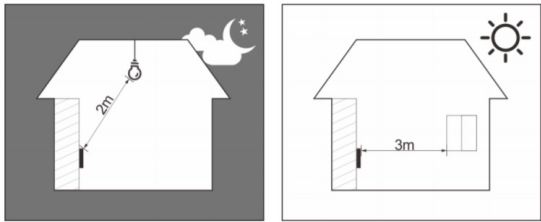
Ejemplo de conexión con MIP 1000 IP

Obs.: para activar el funcionamiento con el dispositivo MIP 1000 IP, accede al menú Utilidades > MIP.

6. Instalación

6.1. Locales recomendados

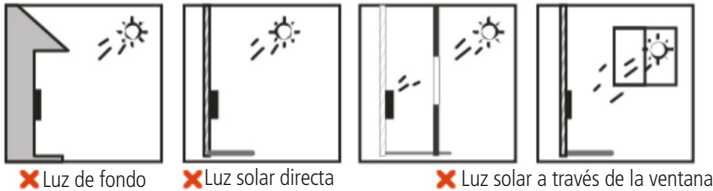
El dispositivo debe instalarse por lo menos a 2 m de una lámpara y por lo menos a 3 metros de un local donde pueda entrar claridad, proveniente de rayos solares.



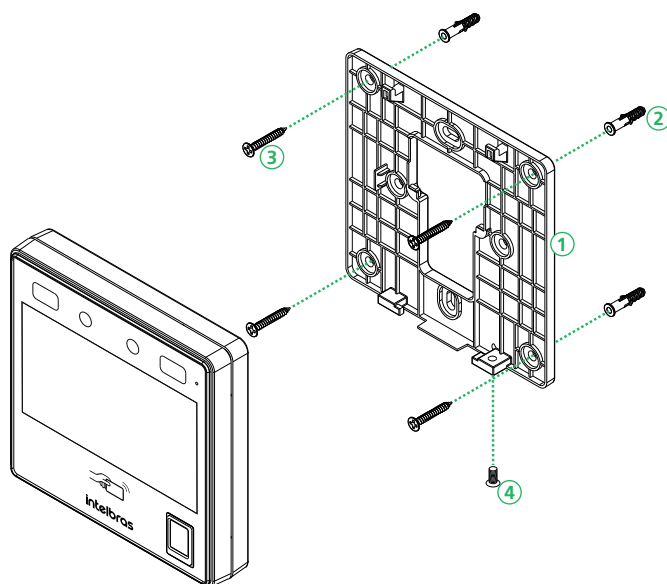
6.2. Locales no recomendados

Certifcate de que el dispositivo esté instalado en un local con poca claridad detrás del rostro a ser identificado y la luz del sol no sea directamente sobre el dispositivo mismo que pasando a través de una ventana.

Escenarios como los ilustrados en la figura abajo pueden afectar el funcionamiento del dispositivo.



6.3. Diagrama de instalación



Modelo de fijación

1. Retira el soporte (1) del equipamiento;
2. Haz cinco agujeros (cuatro agujeros de instalación del soporte y una entrada de cable) en la pared de acuerdo con los agujeros en el soporte y fija el soporte en la pared usando los tarugos (2) y tornillos (3) que acompañan el producto;
3. Efectúa la conexión de los cables (ver ítem 5. *Esquemáticos de conexión*);
4. Encaja el controlador de acceso en el soporte y coloque el tornillo de fijación (4).

Obs.: para garantizar la lectura del usuario de acuerdo con las especificaciones técnicas del ítem 1, se recomienda instalar el dispositivo a una altura de 1,4 m.

7. Operaciones del dispositivo

7.1. Inicio del dispositivo

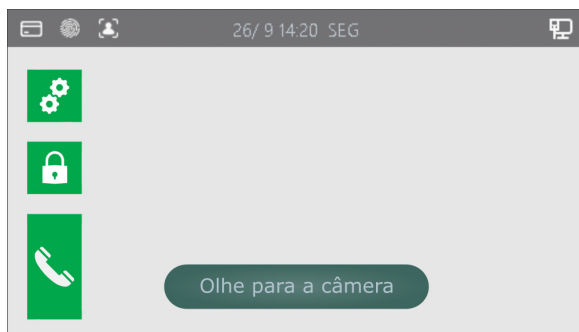
Al iniciar el dispositivo por primera vez, elija el idioma deseado (inglés, portugués o español (Latinoamérica)) y luego de ser seleccionado, es necesario crear un usuario administrador. Una contraseña y un correo electrónico son de registro obligatorio y deben definirse la primera vez que se activa el controlador de acceso. El nombre de usuario del administrador es admin por defecto. El controlador de acceso no se puede utilizar sin este registro.

La imagen muestra la interfaz de usuario de la pantalla de inicialización. El título es 'Inicialização'. Hay cuatro campos de entrada: 'Admin' (con el valor predeterminado 'Admin'), 'Senha', 'Repetir senha' y 'E-mail'. En la parte inferior hay dos botones: 'Ok' y 'Limpar'.

Importante:

- » Se puede rehacer la contraseña del administrador a través del correo electrónico tecleado, usa un correo electrónico válido y activo.
- » La contraseña debe tener de 8 a 32 caracteres, no puede tener espacios y debe tener por lo menos dos tipos de caracteres entre mayúsculas, minúsculas, número y caracteres especiales (excluyendo ' " ; : &).

7.2. Pantalla inicial



Pantalla inicial

En esta pantalla inicial el usuario es capaz de autenticar su acceso a través del rostro (), tarjeta () y/o contraseña () como indicado en la esquina superior izquierda. En la derecha se exhiben los íconos de conexión como Ethernet, Wifi y USB.

En la lateral izquierda el ícono para acceso al menú principal (), disponible apenas para el administrador y usuarios con ese nivel de acceso, y el ícono para acceso por contraseña ().

Obs.: el ícono de contraseña deja de aparecer en la esquina superior izquierda caso estén activos los cuatro métodos de verificación.

7.3. Autenticación

El usuario puede desbloquear la puerta por reconocimiento facial, contraseña y/o tarjeta.

Facial

Para autenticarse por reconocimiento facial basta posicionarse al frente del equipamiento de manera que el rostro sea exhibido y encuadrado en la pantalla. Una señal visual es exhibida en la pantalla y, de forma opcional, puede haber una señalización sonora.

Contraseña

Para autenticar por contraseña es necesario acceder el menú *Contraseña* ().

En el menú *Contraseña* dos opciones se presentarán al usuario: *Contraseña* y *contraseña maestra*.

En la opción *Contraseña* el usuario podrá autenticarse usando su ID de usuario y contraseña registrados.

La opción *Contraseña Maestra* no está relacionada a un usuario específico y necesita estar habilitada por el administrador del sistema. La contraseña maestra destrabará la puerta, independiente de los modos de autenticación activos, zona de tiempo, vacaciones y reglas de anti-passback.

Tarjeta

La verificación ocurre al pasar la tarjeta en el área indicada, en el centro.

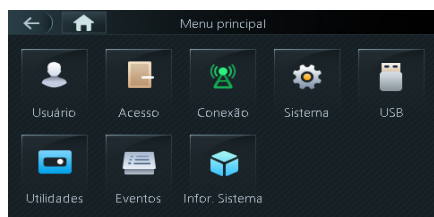
7.4. Menú principal

En el menú principal se pueden registrar usuarios, cambiar configuraciones de acceso, conexión y sistema, verificar la capacidad del dispositivo etc.

Para acceder el menú principal es necesario estar autenticado como administrador. Esa autenticación puede ser a través del rostro, tarjeta, contraseña de usuario o a través de la contraseña registrada en el inicio del equipamiento.

En la pantalla inicial, abre el menú principal a través del ícono ().

Si es el primer acceso al menú principal, selecciona la opción Admin y teclea la contraseña registrada en el inicio del dispositivo.



Métodos de autenticação do menu principal



Menu principal

7.5. Gerencia de usuarios

El menú *Usuario* ofrece opción para registro de un nuevo usuario, ver y modificar lista de usuarios y lista de administradores, además de habilitar/deshabilitar o cambiar la contraseña maestra.

Nuevo usuario

Al acceder *Nuevo usuario*, se exhibe la pantalla de registro.

- » **ID:** número que identifica el usuario. Ese número debe ser único y se incrementa automáticamente, entretanto puede ser personalizado por el administrador como, por ejemplo, la matrícula o alguna referencia al apartamento, sala etc.
- » **Nombre:** nombre que se exhibirá para este usuario.
- » **Face:** foto del usuario que se usará para identificarlo a través del método de autenticación de reconocimiento facial (ver sección 10. *Buenas prácticas para el Reconocimiento Facial*).
- » **Tarjeta:** permite el registro de hasta 5 tarjetas o tags RFID por usuarios. En esa opción es permitido habilitar uno de esos registros como coacción (emite una alerta para el software de monitoreo y/o acciona una salida de alarma).
- » **Contraseña:** permite crear una contraseña de acceso individual de hasta 8 dígitos numéricos. Para acceder por este método de autenticación es necesario que el usuario también inserte la ID del usuario.
- » **Permiso:** este campo define si este registro será de un Usuario común o un Admin. Este último con acceso al menú principal y todas las configuraciones del dispositivo.
- » **Zona de tiempo:** ID de la zona de tiempo atribuida al usuario.
- » **Plano vacación:** ID del plano de vacación atribuida al usuario.
- » **Validad:** fecha límite que este usuario tendrá de acceso. A partir de esta fecha el usuario continuará registrado en el dispositivo, mas su acceso se negará.
- » **Perfil:** define el perfil que se atribuirá al usuario. De los cuales:
 - » **General:** usuarios con el perfil General pueden acceder normalmente.
 - » **Lista negra:** el usuario insertado de este perfil genera un evento de alarma al efectuar el acceso.
 - » **Visitante:** el usuario tiene un número limitado de accesos a este dispositivo.
 - » **Ronda:** apenas registra evento, no hace ningún accionamiento.
 - » **VIP:** libera el acceso independiente de las configuraciones de zona de tiempo o regla de anti-passback.
 - » **PcD:** extiende el tiempo de accionamiento en 5 segundos para persona con deficiencia.
 - » **Usuario 1:** reservado para personalización. Usuarios pueden acceder normalmente.
 - » **Usuario 2:** reservado para personalización. Usuarios pueden acceder normalmente.
- » **Nº de usos:** campo permite seleccionar cuantos accesos el usuario Visitante (del campo anterior) puede realizar en el dispositivo.

Informaciones de usuario

Es posible acceder la lista de usuarios, lista de usuarios administradores y modificar sus informaciones dentro del menú *Usuarios*.

Lista de usuarios

Presenta la lista de usuarios por orden de registro. No lista los usuarios definidos como administradores, ver siguiente subsección. Al seleccionar un usuario es posible editar informaciones de acceso, excepto el número de la ID del usuario.

Lista de administradores

Presenta apenas la lista de usuarios definidos con permiso de administradores (Admin). Al seleccionar un usuario es posible modificar informaciones de acceso, excepto el número de la ID del usuario.

Contraseña maestra

En esta opción del menú es posible activar y desactivar la función *Contraseña maestra*, bien como crear y cambiar esa contraseña.

La opción *Contraseña maestra* no está relacionada a un usuario específico y destrabará la puerta independiente de los modos de autenticación activos, zona de tiempo, feriados y reglas de anti-passback.

7.6. Gerencia de acceso

Zona de tiempo/Vacaciones

Las zonas de tiempo sirven para restringir o liberar grupos específicos de usuarios en días y horarios de la semana. El mismo puede ocurrir al registrar una vacación.

Período NA

Al atribuir una zona de tiempo en este campo, la puerta permanecerá abierta durante los períodos especificados en la zona horaria configurada a través de la web.

Período NC

Al atribuir una zona de tiempo en este campo, la puerta permanecerá cerrada durante los períodos especificados y no podrá desbloquearse en la zona horaria configurada a través de la web.

Verificación remota¹

En la verificación remota, siendo presentada una credencial válida, se envía un mensaje al software de gerencia, solicitando la liberación del acceso. Si confirmado, la puerta abre, de lo contrario nada se exhibe al usuario. Después de definir la zona de tiempo que funcionará en ese modo es necesario activarla .

¹ Función no disponible en el software Incontrol Web. Verifica junto al manual del software que usas, si hay soporte para esta función.

Métodos de autenticación

Al seleccionar la opción *Acceso > Método de autenticación* son presentadas tres opciones:

- » **Autenticación por usuario:** al seleccionar ese método se puede optar por hacer la autenticación por Tarjeta, huella digital (si hay lector auxiliar), Rostro (reconocimiento facial) y contraseña. En este menú también es posible combinar el acceso. Para abrir la opción presiona sobre el nombre Autenticación por usuario. El botón *On/Off* sirve para habilitar el método.
- » **En la opción /O:** el usuario usa de cualquier uno de los métodos para realizar el acceso, o sea, considerando las opciones *Tarjeta* y *Rostro* seleccionadas, el usuario tendrá su acceso liberado si verifica apenas por el Rostro y también tendrá su acceso liberado si hace la liberación apenas a través de la tarjeta/tag RFID.
- » **Al usar la opción +E:** el usuario tendrá que utilizar todos los métodos seleccionados para que su acceso se libere, o sea, caso las opciones *Tarjeta* y *Rostro* estén seleccionadas, el usuario tendrá que pasar su Tarjeta/tag RFID y en la secuencia verificar por Rostro. El acceso es liberado al verificar ambas las credenciales.

Alarma

El administrador del sistema a través del menú *Acceso > Alarma* puede habilitar o deshabilitar alarmas.

- » **Anti-passback:** después de autenticarse en el dispositivo en la dirección de entrada, es necesario autenticarse para salir antes de una nueva autenticación de entrada y viceversa. Para eso, es necesario un lector auxiliar.
- » **Coacción:** tarjetas y tag RFID se pueden registrar como credencial de coacción. Caso esta opción esté activada, además de un evento de coacción, también se accionará la salida de alarma si hay un acceso utilizando una credencial de coacción.
- » **Intrusión:** abertura indebida de la puerta (requiere uso del sensor de puerta).
- » **Tiempo limite del sensor:** define después de cuanto tiempo suena la alarma sonora en el propio dispositivo. Puede configurar de 1-9999 segundos.
- » **Sensor de puerta:** necesario estar activado para que el dispositivo detecte abertura indebida de la puerta o que la misma permaneció abierta.

Obs.: la integración de alarma del dispositivo y su configuración (relé de accionamiento, evento o alarma sonora) requiere uso de software.

Estado de la puerta

Son tres opciones para el estado de la puerta: *NA*, *NC* y *Normal*.

- » **NA:** define que la puerta estará siempre abierta, o sea, relé de accionamiento siempre activo.
- » **NC:** define que la puerta estará siempre cerrada, o sea, no hay accionamiento, mismo que verifiques en la credencial válida.
- » **Normal:** puerta será liberada con una credencial válida.

Tiempo de abertura de puerta

Define el tiempo de accionamiento del relé de abertura, por estándar 3 segundos.

7.7. Configuración de conexión

A través del menú *Conexión* es posible hacer la gerencia de conexión de red y de la puerta serial.

Red

- » **Red cableada:** configuraciones de dirección de IP, máscara de red y gateway estándar. Si hay un servicio DHCP en la red es posible activar esta opción para que una configuración de IP se atribuya automáticamente.
- » **Registro activo:** permite conectar el controlador de acceso a la plataforma de gerencia compatible y de esa forma hacer la gerencia del dispositivo. Es necesario configurar la dirección IP y puerta de comunicación del servidor, además de atribuir una ID al dispositivo.
- » **Wifi:** al activar la red Wifi, busca por las redes disponibles usando el ícono de la lupa en la esquina superior derecha. Elige la SSID deseada e inserte la contraseña. La opción DHCP por estándar viene habilitada.

Obs.: » Para uso del software InControl Web es necesario un IP fijo. Antes de usar la opción DHCP, certifique que tu red atribuirá siempre el mismo IP para ese equipamiento.

- » Para evitar conflictos de IP, certifique de configurar la red cableada para un rango no usado, en casos que se opte por usar la red inalámbrica.

Puerta serial

- » **Paso 1:** en el menú principal, seleccione *Conexión > Puerto serie*.
- » **Paso 2:** seleccione el tipo de puerta, según el uso previsto:
 - » **Lector:** la conexión RS485 del dispositivo recibirá datos de un lector auxiliar. Actúa como entrada de datos y el dispositivo procesa los datos para abrir y cerrar la puerta.
 - » **Controlador:** actúa como lector auxiliar. La conexión RS485 del dispositivo enviará la información de la credencial a un controlador de acceso. Esta información puede ser de dos tipos:
 - » **User ID:** envía el ID de usuario de acuerdo con la credencial leída.
 - » **Nº de tarjeta:** envía el número de tarjeta como credencial cuando el usuario acerca una tarjeta al dispositivo. Si se utiliza otro método de autenticación que no sea una tarjeta/etiqueta/QRCode, envía datos como una credencial en función del primer número de la tarjeta del usuario al que pertenece esa credencial.
 - » **Lector OSDP:** permite que el dispositivo se comunique con un lector de tarjetas basado en el protocolo OSDP.
 - » **Módulo de seguridad:** permite el uso de un relé externo para activar la puerta. Cuando esta opción está habilitada, las conexiones de entrada y bloqueo del botón pulsador del controlador están desactivadas, y se deben usar las conexiones de entrada y bloqueo del botón pulsador del relé externo.
Si esta opción está habilitada y el relé externo no está conectado o no responde, el dispositivo devolverá acceso denegado incluso si se presentan credenciales válidas.

Para verificar el diagrama de conexión, consulte el manual del producto XR 2201 en nuestro sitio web: <https://www.intelbras.com.br>.

7.8. Sistema

Fecha y hora

Para cambiar informaciones de fecha y hora como ajustar fecha, formato de fecha, ajustar hora, horario de verano, servicio NTP y huso horario, accede *Sistema > Fecha y hora*.

Parámetros de rostro

Presiona sobre la(s) opción(es) que deseas cambiar, haz el debido ajuste y presiona salvar .

- » **Umbral de detección facial:** ajusta la precisión del reconocimiento facial. Cuanto mayor el valor, mayor será la semejanza de la captura del dispositivo con la foto usada para el registro, o sea, menor será la tolerancia a variaciones de apariencia como expresiones faciales, barba, accesorios y edad del registro. Valor estándar es de 85.
- » **Máx. ángulo de reconocimiento facial:** ajusta el ángulo del perfil acepto por el dispositivo para iniciar el reconocimiento facial. Valor estándar es 90°.
- » **Distancia pupilar:** representa la cantidad de píxeles en la imagen, entre los centros de las pupilas. El valor muda de acuerdo con el tamaño del rostro y la distancia entre el rostro y la lente. Cuanto más próximo el rostro de la cámara, mayor será ese valor. La distancia pupilar para un adulto posicionado a 1,5 metros del dispositivo está entre 50 y 70. Valor estándar es 60.
- » **Tiempo limite de reconocimiento (s):** tiempo limite entre la presentación para el reconocimiento facial y el mensaje de acceso liberado.
- » **Tiempo limite para acceso facial negado:** tiempo limite entre el momento que se presenta el rostro que no tiene acceso en el dispositivo y el mensaje de acceso negado.
- » **Umbral anti-falso:** previene el uso de fotos, imágenes o videos en medio impreso o digital de acceder al dispositivo.
- » **Modo máscara:** permite cambiar y hasta bloquear usuarios sin máscara. Selecciona la opción No detectar para que el dispositivo no cambie o bloquee usuarios que no estén de máscara. Selecciona cambiar cuando deseas identificar los usuarios a través de reconocimiento facial y modificar los usuarios que no estén de máscara. Caso desees usar el reconocimiento facial y también bloquear usuarios que no estén de máscara, selecciona la opción bloquear.

Obs: para usar la opción bloquear usuarios sin máscara, será acepto apenas el método de autenticación facial. En la opción cambiar, se dará la alerta a todos los usuarios que usen métodos alternativos al reconocimiento facial.

Volumen

Usa las teclas + y – para ajustar el volumen del equipamiento.

Idioma

Los idiomas inglés, español y portugués están disponibles.

Obs.: es necesario reiniciar el dispositivo.

Intensidad de luz infrarroja

Usa las teclas + y – para ajustar la intensidad de la luz infrarroja. Cuanto mayor el valor atribuido, más intensa será la emisión de la luz infrarroja.

Configuraciones de pantalla

- » **Protección de pantalla:** configura cuanto tiempo después de ninguna acción el dispositivo exhibirá la protección de pantalla. Por estándar ese tiempo está en 30 segundos.
- » **Tiempo limite de pantalla prendida:** configura cuanto tiempo después de ninguna acción la pantalla se apagará. Ese tiempo por estándar en la configuración es de 60 segundos.

Obs.: al detectar movimiento el dispositivo vuelve a la pantalla de verificación automáticamente.

Restaurar estándares de fábrica

Datos se perderán al seleccionar restaurar estándares de fábrica.

Las configuraciones de IP no se modificarán al restaurar los estándares de fábrica.

Hay dos opciones para restaurar los estándares de fábrica:

- » **Restaurar estándares de fábrica:** restaura las configuraciones para el **estándar** y borrar todos los datos del dispositivo.
- » **Restaurar estándares de fábrica (mantener usuarios y eventos):** restaura las configuraciones para el **estándar** y mantiene los datos de usuario.

Después de seleccionar la opción deseada, confirma tu elección.

Reiniciar

Selecciona *Sistema > Reiniciar* y confirma para que el dispositivo se reinicie.

7.9. USB

Atención: verifica si el dispositivo de almacenamiento USB está correctamente insertado antes de exportar/importar datos de usuario o actualizar el producto. Nunca remuevas el dispositivo de almacenamiento USB mientras hace la exportación/importación o actualización del producto. De lo contrario la operación fallará.

Es necesario exportar las informaciones de un controlador de acceso antes de importar esas configuraciones a otro producto.

La entrada USB también puede ser usada para actualización de firmware.

Obs.: el dispositivo de almacenamiento debe estar formateado en FAT32.

Exportar

Para exportar datos del dispositivo selecciona *USB > Exportar*.

Selecciona los datos que deseas exportar y confirma. El administrador puede optar por exportar los usuarios, los datos faciales, tarjetas, huellas digitales (cuando hay), eventos o todas las opciones anteriormente seleccionando la opción *Todos*.

Importar

Para importar datos para el dispositivo selecciona *USB > Importar*.

Selecciona los datos que deseas importar y confirma. Es posible importar usuarios, datos del rostro, tarjeta y huella digital que hayan sido exportados de otro dispositivo. También es posible importar fotos en formato JPG, donde el nombre del archivo debe ser la ID del usuario. Caso la ID del usuario no exista, una se creará con la foto disponible. Consulta la sección 10 para mas informaciones sobre los requisitos de las fotos.

Actualizar

Para actualizar a través de un dispositivo de almacenamiento USB rebautiza el archivo de actualización para *update.bin* y salva ese archivo en la raíz del dispositivo USB.

Para actualizar selecciona *USB > Actualizar y confirma*.

O, con el controlador de acceso apagado, conecte el dispositivo de almacenamiento al puerto USB y encienda el dispositivo. La actualización comenzará automáticamente.

7.10. Utilidades

En ese menú están las configuraciones de seguridad, opción para invertir el código recibido en la entrada Wiegand, configurar tipo de sensor de puerta y el resultado del feedback.

Configuraciones de seguridad

- » **Habilitar restablecer la contraseña:** si habilitado, se permite **restablecer la contraseña** a través de la interfaz web.
- » **HTTPS:** cuando habilitado, se usará el protocolo HTTPS para el acceso a los comandos CGI, de lo contrario se usará HTTP. El dispositivo reiniciará al habilitar o deshabilitar el protocolo HTTPS.
- » **CGI:** ofrece un protocolo para que los softwares configuren el dispositivo. Habilita el uso del protocolo CGI.
- » **SSH:** habilita el protocolo de seguridad SSH.
- » **Capturar foto:** el dispositivo tomará una foto del usuario cuando hay una tentativa de acceso.
- » **Limpiar todas las fotos capturadas:** promueve la remoción de todas las capturas.

Sensor de puerta

El sensor de puerta se configurará como NA o NC.

- » **NA:** cuando la puerta está abierta, el estado del sensor es normalmente abierto o NA.
- » **NC:** cuando la puerta está abierta, el estado del sensor es normalmente cerrado o NC.

Resultado del feedback

- » **Éxito o falla:** muestra el mensaje *¡Éxito!* acceso liberado y el mensaje *No autorizado* para acceso negado.
- » **Solo nombre:** presenta ID del usuario, nombre y horario para el acceso liberado y el mensaje *No autorizado* y horario para el acceso negado.
- » **Foto y nombre:** presenta ID del usuario, nombre y horario acompañado de la foto registrada para el acceso liberado y el mensaje *No autorizado* y horario para el acceso negado.
- » **Foto, imagen y nombre:** presenta ID del usuario, nombre y horario acompañado de la foto registrada y de la foto actual para el acceso liberado y el mensaje *No autorizado* y horario acompañado de la foto actual para el acceso negado.
- » **Personalizado:** muestra un mensaje *Liberado o Denegado* en pantalla completa con color e icono indicativo.

MIP

Al habilitar esta opción el dispositivo usará la entrada 485 para comunicarse con el dispositivo MIP 1000.

Verifica en la sección 5.5. *Módulo inteligente de portería (MIP 1000)* como es la conexión de los dispositivos. Para informaciones de operación y registro consulta el manual de usuario del MIP 1000.

7.11. Eventos

En el menú Eventos es posible visualizar todos los eventos de acceso. Es posible hacer la busca por ID de usuario al acceder el ícono de lupa en el lado superior derecho.

7.12. Info. Sistema

En informaciones del sistema es posible consultar la capacidad de almacenamiento del dispositivo, número de serie, versión de software, versión de firmware y dirección MAC.

8. Interfaz web

El controlador de acceso puede configurar y operar en la web. A través de la web, es posible definir parámetros de red y de vídeo de acceso.

La interfaz web se puede usar para la actualización del sistema.

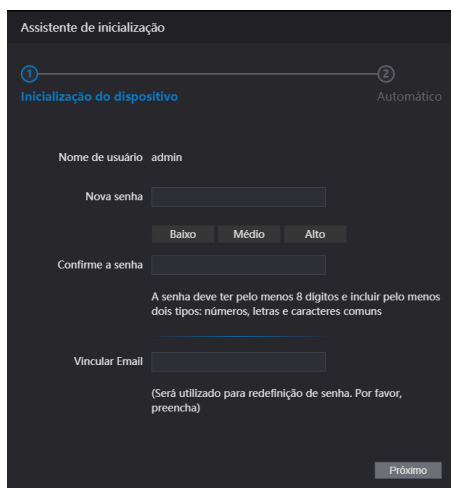
Importante: la gerencia de usuarios solo se puede hacer directamente en el dispositivo o con la ayuda de software, no se puede realizar registros de usuario o exportar/importar datos de usuarios a través de la interfaz web.

8.1. Inicio

Alternativamente el inicio del dispositivo en pantalla (ítem 7.1. *Inicio del dispositivo*), puede registrar la contraseña del administrador del sistema a través de la interfaz WEB.

Para eso, abre el navegador y accede el IP del dispositivo (el IP estándar de la interfaz de red cableada es 192.168.1.201).

Obs.: usa la última versión del Microsoft Edge® o Chrome®.



Pantalla de inicio a través de la Interfaz web

Entra con la nueva contraseña, confirma y agrega un correo electrónico válido y sigue para la próxima etapa.

Importante:

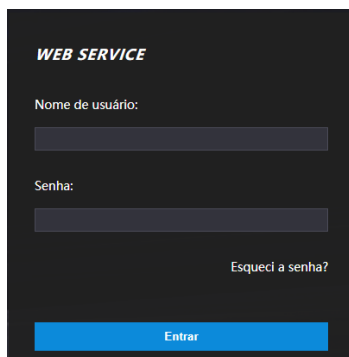
- » La contraseña del administrador se puede restablecer a través del correo electrónico tecleado, usa un correo electrónico válido y activo.
- » La contraseña debe tener de 8 a 32 caracteres, no puede tener espacios y debe tener por lo menos dos tipos de caracteres entre mayúsculas, minúsculas, número y caracteres especiales (excluyendo ' " ; &).

En la siguiente pantalla el administrador puede optar por estar informado de una nueva versión cuando disponible (exige que el dispositivo esté conectado a la internet).

8.2. Login

Abre el navegador y accede el IP del dispositivo (el IP estándar de la interfaz de red cableada es 192.168.1.201).

Entra con el *Nombre de usuario* y *Contraseña* y presione *Entrar*.



Pantalla de login

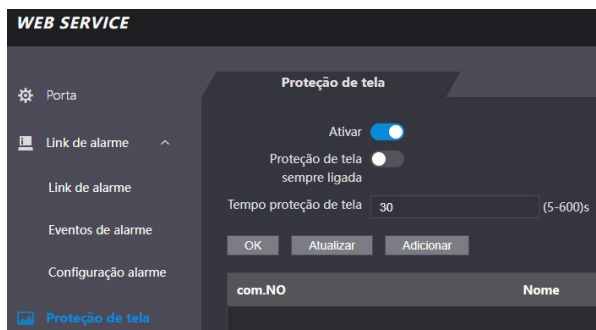
Importante:

- » El nombre de usuario estándar del administrador es admin y la contraseña es creada en el inicio del dispositivo (ver ítem 7.1. Inicio del dispositivo o 8.1. Inicio)
- » Si te olvidas la contraseña de administrador, presiona *¿Olvidé la contraseña?* en la pantalla de login de la interfaz web y sigue las instrucciones en la pantalla (ver ítem *Olvidé la contraseña*).

Olvidé la contraseña

Caso hayas olvidado la contraseña, usa la opción *¿Olvidé la contraseña?* en la interfaz WEB. Usa la cámara de tu celular para escanear el código QR presentado y sigue las instrucciones. Se enviará una contraseña en el correo electrónico registrado en el inicio del dispositivo. Inserta esa contraseña y una ventana para registrar una nueva contraseña se exhibirá.

8.3. Protección de pantalla



Proteccion de pantalla

- » Formato: retrato;
- » Tipo de archivo: .JPG o .JPEG;
- » Resolución recomendada: 272 × 480;
- » Tamaño máximo de archivo: 512 KB.

Obs.: es posible añadir sólo una imagen. El protector de pantalla se mostrará después del tiempo de pantalla activa (el tiempo predeterminado del dispositivo es de 30 segundos).

8.4. Enlace de alarma

Configuración de enlace de alarma

Dispositivos de alarma se pueden conectar al controlador de acceso y se puede configurar la acción del controlador de acceso, cuando recibir una entrada de alarma.

En *Enlace de alarma* > *Enlace de alarma* es presentado el canal de entrada. Para modificar presiona el ícono  en la columna modificar.

- » **Entrada:** no puede ser modificado. La entrada 1 se refiere a la entrada de alarma ALM_IN.
- » **Nombre:** inserta un nombre para la zona de alarma.
- » **Tipo de alarma:** selecciona de acuerdo con el sistema de alarma. Al seleccionar NA, la alarma se disparará caso se detecte el cierre de un circuito entre GND y la entrada de alarma. Al seleccionar NC, se disparará una alarma cuando es detectado que la entrada de alarma no está conectada al GND.
- » **Activar enlace de incendio:** si el enlace de incendio está activo, el controlador de acceso destrabará la puerta si hay un accionamiento en la entrada de alarma. Al activar el enlace de incendio la puerta es configurada para siempre abierta. Verifica las demás configuraciones para la acción deseada.
- » **Activar enlace de acceso:** cuando activo permite forzar el estado de la puerta en el campo *Tipo de canal*.
- » **Tipo de canal:** si NA, abrirá y mantendrá la puerta abierta. En la opción NC mantendrá la puerta cerrada y negará cualquier intento de acceso.

Eventos de alarma

En la opción *Eventos de alarma* es posible hacer una búsqueda por período y por tipo de alarma.

8.5. Capacidad

Al acceder la pestaña capacidad se presentan las cantidades de usuarios y credenciales registradas en el dispositivo.

8.6. Config. de vídeo

Están disponibles configuraciones de vídeo, detección de movimiento y modo de imagen.

Configuraciones de vídeo

Permite ajustes en el streaming de vídeo y en la imagen presentada en la pantalla del dispositivo.

Detección de movimiento

El área en rojo representa el área utilizada para detectar objetos en movimiento. El gráfico al lado permite visualizar la interacción entre movimiento y detección. Por estándar, todo frame es utilizado para detección de movimiento y los parámetros Sensibilidad y Umbral con el valor de 50. Para salvar tu modificación presiona *Ok*. Después de presionar *Estándar* para restaurar los estándares de fábrica, también es necesario presionar *Ok*.

Modo de imagen

En *Config. De vídeo > Modo de imagen* selecciona la opción que se adecua a tu escenario. Es posible ajustar la pantalla para el modo: *Interno, Externo u Otro*.

8.7. Detección de rostro

En esa ventana es posible establecer una región para el control de acceso facial y el tamaño del rostro (que definirá la distancia de reconocimiento).

A través del botón *Detectar región* es posible ajustar el área de la pantalla en que el dispositivo efectuará el reconocimiento facial. Afuera de ese área el dispositivo no efectuará el reconocimiento facial.

El botón *Dibujar objetivo* permite especificar a partir de cual tamaño el dispositivo efectuará la verificación del rostro. Cuanto mayor el área, más próximo tiene que estar el usuario a ser identificado. Cuanto menor ese valor, mayor la distancia que el dispositivo efectuará la lectura del rostro.

- » **Umbral de reconocimiento facial:** ajusta la precisión del reconocimiento facial. Cuanto mayor el valor, mayor será la semejanza de la captura del dispositivo con la foto usada para realizar el registro, o sea, menor será la tolerancia a variaciones de apariencia como expresiones faciales, barba, accesorios y edad del registro. Valor estándar es de 85.
- » **Máx. ángulo de reconocimiento facial:** ajusta el ángulo del perfil acepto por el dispositivo para iniciar el reconocimiento facial. Valor estándar es 90°.
- » **Umbral anti-fake:** previene el uso de fotos, imágenes o vídeos en medio impreso o digital de acceder al dispositivo.
- » **Luz infrarroja:** ajusta la intensidad de la luz **infrarroja**. Cuanto mayor el valor atribuido, más intensa será la emisión de luz **infrarroja**.
- » **Tiempo limite de reconocimiento (s):** tiempo limite entre la presentación para el reconocimiento facial y el mensaje de acceso liberado.
- » **Tiempo limite para acceso facial negado:** tiempo limite entre el momento que se presenta el rostro que no tiene acceso en el dispositivo y el mensaje de acceso negado.
- » **Distancia pupilar:** representa la cantidad de píxeles en la imagen entre los centros de las pupilas. El valor muda de acuerdo con el tamaño del rostro y la distancia entre el rostro y la lente. Cuanto más próximo el rostro de la cámara, mayor debe ser ese valor. La distancia pupilar para un adulto posicionado a 1,5 metros del dispositivo está entre 50 y 70. Valor estándar es 60.
- » **ID canal:** son dos opciones: 1 para la cámara de luz visible y 2 para la cámara de luz infrarroja.
- » **Activar Exp. Facial:** al activar esa opción, prepara el dispositivo para funcionar mejor en ambientes más iluminados como recepciones y áreas de acceso a visitantes.
Para salvar tus cambios presiona *Ok*. Después de presionar *Estándar* para restaurar los estándares de fábrica, también es necesario presionar *Ok*.
- » **Brillo objeto Rostro:** ajusta el brillo de la imagen capturada. El valor estándar es 50.
- » **Intervalo de detección de exposición facial:** después que un rostro es detectado, el controlador de acceso emitirá luz para iluminar el rostro. El controlador de acceso no emitirá luz otra vez hasta que el intervalo definido haya pasado.

8.8. Red

Las configuraciones de dirección de IP, máscara de red y gateway estándar pueden ser consultadas o cambiadas en *Red > TCP/IP*. En *Red > Puertas* es posible establecer el número máximo de conexiones, puertas TCP, HTTP y HTTPS. La opción *Red>Registro*, cuando activa permite conectar el controlador de acceso a plataformas de gerencia compatibles y de esa forma hacer gerencia del dispositivo. Es necesario configurar la dirección IP y puerta de comunicación del servidor, además de atribuir una ID al dispositivo.

8.9. Seguridad

En la opción *Seguridad>Seguridad IP* es posible limitar el acceso al dispositivo liberando o bloqueando IPs o segmentos de IP o por MAC. Usa la lista blanca para liberar o la lista negra para bloquear. Es posible configurar para ignorar comandos de PING e impedir semijoin.

En *Seguridad > Servicios* el administrador del dispositivo puede habilitar/deshabilitar los protocolos SSH, CGI, HTTPS, bien como habilitar el reinicio de contraseña a través de la opción *¿Olvidé la contraseña?* de la pantalla de login en la interfaz web.

8.10. Configuración de voz

En el menú *Config. de voz* se puede cambiar el volumen del dispositivo.

8.11. Usuarios de red

Permite registrar otros usuarios administradores y modificar el usuario admin.

Importante: el usuario admin no puede ser excluido.

8.12. Manutención

Define horario para que el dispositivo se reinicie automáticamente. De esta forma el sistema operacional se puede ajustar para mejorar la actuación y el desempeño. El dispositivo tiene por estándar la configuración definida para reiniciar todo martes a las dos de la mañana (de acuerdo con el reloj del dispositivo).

8.13. Gest. config.

Permite que el usuario administrador salve una copia de las configuraciones del dispositivo o restaurar una configuración previamente creada. Se puede usar cuando varios dispositivos necesitan utilizar la misma configuración.

Gest. config.

Para guardar la configuración de su dispositivo presione *Exportar configuraciones* y un archivo se salvará en tu dispositivo. La importación puede ser realizada iniciando por *Buscar* el archivo deseado y entonces *Importar configuraciones*.

Servicio eventos

Al activar el servicio de eventos, el dispositivo enviará activamente los eventos a la dirección IP, puerto y Path configurados en esta página. Para obtener más información, consulte nuestro Soporte técnico para la documentación API/CGI.

8.14. Actualizar

Importante: usa apenas archivos proporcionados por la Intelbras.

Mantiene el dispositivo y el controlador de acceso energizados durante todo el proceso de actualización.

La actualización inicia por el botón *Buscar* para indicar la localización del archivo. Usa archivos locales, archivos en red pueden causar fallas en el proceso de actualización.

8.15. Informaciones de la versión

Presenta informaciones del sistema como versión de firmware, de la interfaz web, número de serie y MAC.

8.16. Usuario online

Al acceder Usuario online será exhibido una lista con el ID del usuario, nombre del usuario, dirección de IP y hora del login.

8.17. Eventos

Exhibe una lista con los eventos de administradores y eventos de sistema.

8.18. SIP

Es posible configurar el dispositivo como un terminal SIP conectado a una central SIP. Para habilitar esta función, consulte el manual web disponible en: <https://manuais.intelbras.com.br/manual-interface-web-linha-bio-t/>

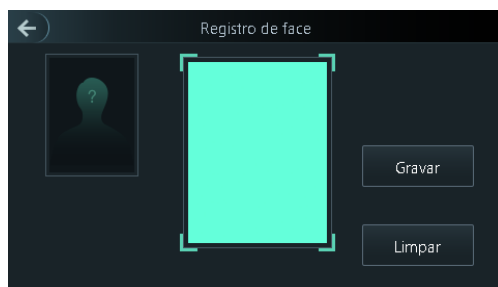
9. Buenas prácticas para el Reconocimiento Facial

9.1. Antes del registro

- » Lentes, gorros y barbas pueden influenciar el desempeño del reconocimiento de rostro. No cubra las cejas al usar gorros.
- » Actualiza el registro caso haya un cambio muy grande en el visual, como la retirada de la barba, si hay dificultad en el acceso.
- » Mantenga el rostro visible.
- » Mantenga el dispositivo por lo menos a dos metros de distancia de la fuente de luz y por lo menos a tres metros de ventanas o puertas; de lo contrario, la luz solar directa puede influenciar en el desempeño del reconocimiento de rostro del dispositivo.

9.2. Durante el registro

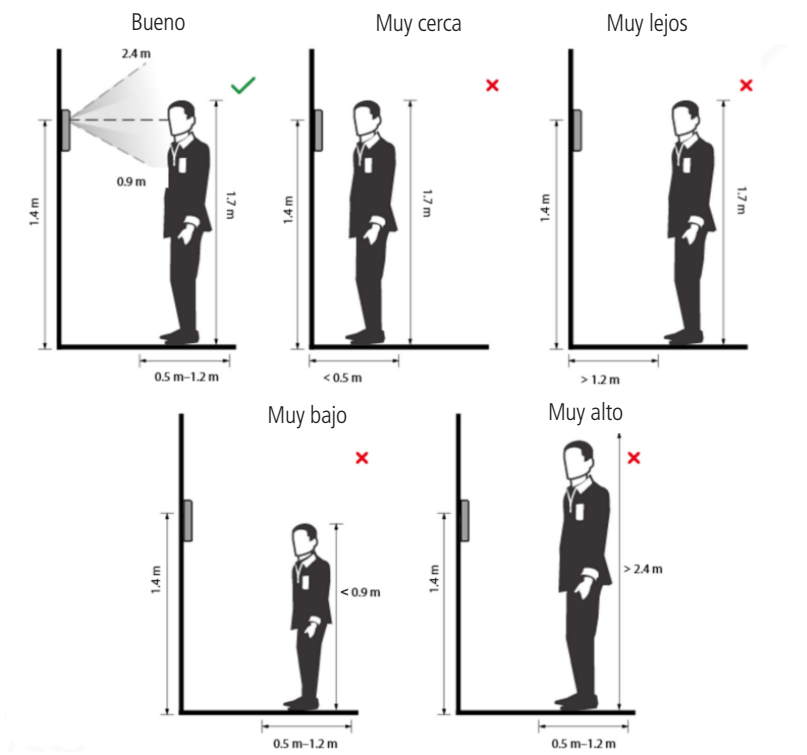
Puedes registrar rostros a través del controlador de acceso o a través del software. Para registro a través del software, consulta el manual del usuario del software. Posiciona la cabeza en la moldura de captura de fotos. Se capturará una foto de tu rostro automáticamente.



- » Permanezca inmóvil, no muevas la cabeza o el cuerpo, pues el registro puede fallar.
- » Encuadra todo el rostro, visión frontal y de ojos abiertos;
- » Encuadra de la cabeza a los hombros;
- » Haz preferencia por un fondo neutro;
- » Apenas un rostro debe aparecer en la foto;
- » El rostro debe estar completamente visible, libre de cualquier objeto que lo pueda cubrir (ej.: máscara);
- » Evita sombras en el rostro o al fondo;
- » Haz una expresión neutra y natural.

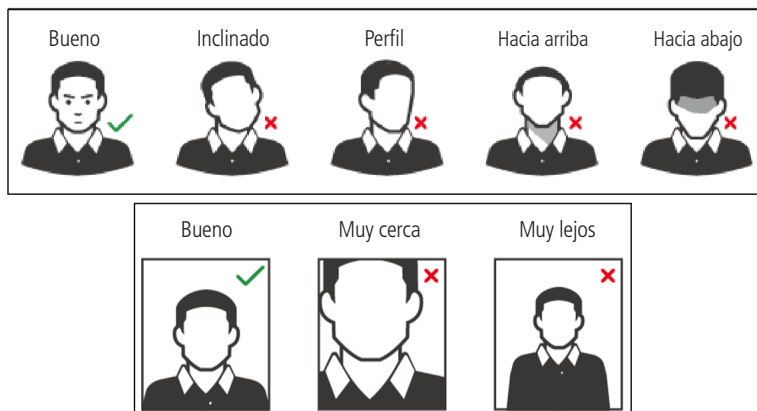
Posición del rostro

Siga las pautas a continuación para obtener el mejor rendimiento del reconocimiento facial.



Requisitos de rostros

- » Verifica si el rostro está visible y si la frente no está cubierta por cabellos.
- » Encuadra todo el rostro, mirando hacia la cámara o luego abajo de ella en el tope de la pantalla y abre los ojos durante el registro.
- » Evita usar lentes y no uses gorros u otros adornos para el rostro que influyan la grabación de la imagen del rostro, o que incluya máscaras faciales.
- » Encuadra de la cabeza a los hombros y haz preferencia por un fondo neutro o blanco.
- » Evita sombras en tu rostro o en el fondo.
- » Haz una expresión neutra y natural y mantenga los brazos a lo largo del cuerpo.
- » Al grabar tu rostro o durante el reconocimiento de rostro, no lo mantengas muy próximo o muy lejos de la cámara.



Requisitos para importación de fotos

Cuando importes las fotos de usuarios - a través de la entrada USB o usando un software de gerencia de control de acceso compatible - se recomienda usar imágenes con resolución superior a 500×500 píxeles ($L \times A$)¹, donde el rostro no debe ocupar más que 2/3 del área total de la imagen. En caso de bases de datos preexistente, atenta para las resoluciones mínima y máxima:

- » **Resolución mínima:** 150×300 píxeles ($L \times A$)¹
- » **Resolución Máxima:** 600×1200 píxeles ($L \times A$)¹

Para todos los casos, el tamaño máximo del archivo debe ser inferior a 100 KB y estar en el formato JPG.

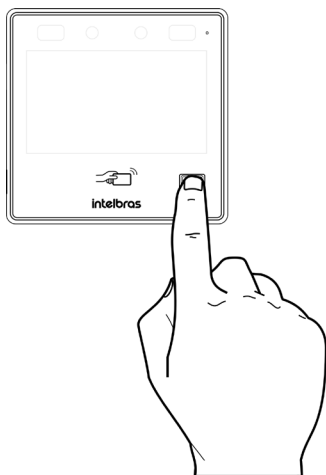
¹ La altura no debe exceder dos veces el ancho. Por ejemplo, si el ancho es 300 píxeles, entonces la altura podrá ser igual o inferior a 600 píxeles.

10. Mejores prácticas para el reconocimiento biométrico digital

Esta sección es solo para el modelo SS 1540 MF W.

10.1. Postura recomendada al registrarse

- » Colóquese frente al equipo, coloque su dedo directamente sobre el lector biométrico y espere la confirmación de la captura de la plantilla.



- » No presione el dedo con demasiada fuerza sobre el sensor biométrico, ya que esto distorsiona la imagen de la huella dactilar y no permite que el dispositivo identifique los puntos formados por las intersecciones de las líneas (crestas y valles) que forman la huella dactilar.
- » No coloque el dedo torcido o solo la punta del dedo sobre el sensor biométrico. El uso inadecuado del sensor biométrico en el momento de la lectura de la huella dactilar impide que el sistema transmita una imagen susceptible de ser transformada en una plantilla.



- » Siga las instrucciones visuales y audibles para capturar datos biométricos digitales.

Póliza de garantía

Importado por:

Intelbras S/A - Industria de Telecomunicación Electrónica Brasileña

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – Brasil – 88122-001

CNPJ 82.901.000/0014-41 – www.intelbras.com.br

soporte@intelbras.com | www.intelbras.com

Industria de Telecomunicación Electrónica Brasileña de México S.A. de C.V. se compromete a reparar o cambiar las piezas y componentes defectuosos del producto, incluyendo la mano de obra, o bien, el producto entero por un período de 1 año (3 meses por norma y 9 meses adicionales otorgados por el fabricante) a partir de la fecha de compra. Para hacer efectiva esta garantía, solamente deberá presentarse el producto en el Centro de Servicio, acompañado por: esta póliza debidamente sellada por el establecimiento en donde fue adquirido, o la factura, o el recibo, o el comprobante de compra, en donde consten los datos específicos del producto. Para las ciudades en donde no hay un centro de servicio, deberá solicitarse una recolección mediante el servicio de paquetería asignado por Intelbras, sin ningún costo adicional para el consumidor. El aparato defectuoso debe ser revisado en nuestro Centro de Servicio para evaluación y eventual cambio o reparación. Para instrucciones del envío o recolección favor comunicarse al Centro de Servicio:

El tiempo de reparación en ningún caso será mayor de 30 días naturales contados a partir de la fecha de recepción del producto en el Centro de Servicio.

ESTA GARANTÍA NO ES VÁLIDA EN LOS SIGUIENTES CASOS:

- a. Cuando el producto ha sido utilizado en condiciones distintas a las normales.
- b. Cuando el producto no ha sido instalado o utilizado de acuerdo con el Manual de Usuario proporcionado junto con el mismo.
- c. Cuando el producto ha sido alterado o reparado por personas no autorizadas por Industria de Telecomunicación Electrónica Brasileña.
- d. Cuando el producto ha sufrido algún daño causado por: accidentes, siniestros, fenómenos naturales (rayos, inundaciones, derrumbes, etc.), humedad, variaciones de voltaje en la red eléctrica, influencia de naturaleza química, electromagnética, eléctrica o animal (insectos, etc.).
- e. Cuando el número de serie ha sido alterado.

Con cualquier Distribuidor Autorizado, o en el Centro de Servicio podrá adquirir las partes, componentes, consumibles y accesorios.

Datos del producto y distribuidor.

Producto:	Colonia:
Marca:	C.P.:
Modelo:	Estado:
Número de serie:	Tipo y número de comprobante de compra:
Distribuidor:	Fecha de compra:
Calle y número:	Sello:

Término de garantía

Queda expreso que esta garantía contractual es conferida mediante las siguientes condiciones:

Nombre del cliente:

Firma del cliente:

Nº de la nota fiscal:

Fecha de la compra:

Modelo:

Nº de serie:

Revendedor:

1. Todas las partes, piezas y componentes del producto son garantizados contra eventuales vicios de fabricación, que por ventura vengan a presentar, por el plazo de 1 (un) año — siendo este de 90 (noventa) días de garantía legal y 9 (nueve) meses de garantía contractual —, contado a partir de la fecha de la compra del producto por el Señor Consumidor, conforme consta en la nota fiscal de compra del producto, que es parte integrante de este Término en todo el territorio nacional. Esta garantía contractual comprende el cambio gratuito de partes, piezas y componentes que presentaren vicio de fabricación, incluyendo los gastos con la mano de obra utilizada en ese reparo. Caso no sea constatado vicio de fabricación, y si vicio(s) proveniente(s) de uso inadecuado, el Señor Consumidor arcará con esos gastos.
2. La instalación del producto debe ser hecha de acuerdo con el Manual del Producto y/o Guía de Instalación. Caso tu producto necesite la instalación y configuración por un técnico capacitado, busca un profesional idóneo y especializado, siendo que los gastos de esos servicios no están incluidos en el valor del producto.
3. Constatado el vicio, el Señor Consumidor deberá inmediatamente comunicarse con el Servicio Autorizado más próximo que conste en la relación ofrecida por el fabricante — solo estos están autorizados a examinar y sanar el defecto durante el plazo de garantía aquí previsto. Si eso no es respetado, esta garantía perderá su validez, pues estará caracterizada la violación del producto.
4. En la eventualidad del Señor Consumidor solicitar atendimento domiciliar, deberá encaminarse al Servicio Autorizado más próximo para consulta de la tasa de visita técnica. Caso sea constatada la necesidad de la retirada del producto, los gastos corrientes, como los de transporte y seguridad de ida y vuelta del producto, quedan bajo la responsabilidad del Señor Consumidor.
5. La garantía perderá totalmente su validez en ocurrencia de cualesquiera de las siguientes hipótesis: a) si el vicio no es de fabricación, mas si causado por el Señor Consumidor o por terceros extraños al fabricante; b) si los daños al producto son oriundos de accidentes, siniestros, agentes de la naturaleza (rayos, inundaciones, deslizamientos, etc.), humedad, tensión en la red eléctrica (sobretensión provocada por accidentes o fluctuaciones excesivas en la red), instalación/uso en desacuerdo con el manual del usuario o debido al desgaste natural de las partes, piezas y componentes; c) si el producto haya sufrido influencia de naturaleza química, electromagnética, eléctrica o animal (insectos, etc.); d) si el número de serie del producto fue adulterado o tachado; e) si el aparato fue violado.
6. Esta garantía no cubre pérdida de datos, por lo tanto, se recomienda, si es el caso del producto, que el Consumidor haga una copia de seguridad regularmente de los datos que constan en el producto.
7. La Intelbras no se responsabiliza por la instalación de este producto, y también por eventuales tentativas de fraudes y/o sabotajes en tus productos. Mantenga las actualizaciones del software y aplicaciones utilizados al día, si es el caso, así como las protecciones de red necesarias para protección contra invasiones (hackers). El equipamiento es garantizado contra vicios dentro de sus condiciones normales de uso, siendo importante que se tenga ciencia de que, por ser un equipamiento electrónico, no está libre de fraudes y burlas que puedan interferir en su correcto funcionamiento.
8. Después de su vida útil, el producto debe ser entregado a una asistencia técnica autorizada de la Intelbras o realizar directamente la destinación final ambientalmente adecuada evitando impactos ambientales y a la salud. Caso prefieras, la pila/batería así como demás electrónicos de la marca Intelbras sin uso, puede ser descartado en cualquier punto de colecta de la Green Eletron (gestor de residuos electroelectrónicos a lo cual somos asociados). En caso de duda sobre el proceso de logística reversa, entra en contacto con nosotros por los teléfonos (48) 2106-0006 o 0800 704 2767 (de lunes a viernes, de las 08 a las 20h y a los sábados de las 08 a las 18h) o a través del correo electrónico suporte@intelbras.com.br.

Siendo estas las condiciones de este Término de Garantía complementar, la Intelbras S/A se reserva el derecho de alterar las características generales, técnicas y estéticas de sus productos sin previo aviso.

Todas las imágenes de este manual son ilustrativas.

intelbras



fale com a gente / hable con nosotros

Brasil

Suporte a clientes:  (48) 2106 0006

Fórum: forum.intelbras.com.br

Suporte via chat: chat.intelbras.com.br

Suporte via e-mail: suporte@intelbras.com.br

SAC / Onde comprar? / Quem instala? : 0800 7042767

Otros países

soporte@intelbras.com

Importado no Brasil por: / Importado en Brasil por:

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001

CNPJ 82.901.000/0014-41 – www.intelbras.com.br | www.intelbras.com

01.24

Origem: China

Fabricado en China