Manual de Programación e instalación

VW16ZGPRSIP – VW16ZIP – VW16ZGPRS - VW16Z

V5.70 – R1.8 – Octubre 2016

www.viawebsystem.com.br

Modelo: VW16ZETHGPRS

Modelo: VW16ZGPRS_V2

Modelo: VW16ZETH_V2

Modelo: VW16Z_V2

Modelo: VW10Z

El modelo VW16ZETHGPRS se refiere al producto VW16ZETHGPRS.
El modelo VW16ZETH_V2 se refiere al producto VW16ZETH.
El modelo VW16ZGPRS_V2 se refiere al producto VW16ZGPRS.
El modelo VW16Z_V2 se refiere al producto VW16Z.
El modelo VW10Z se refiere al producto VW10Z.

Este producto está homologado por la ANATEL, de acuerdo con los procedimientos reglamentados por la Resolución 242/2000, y atiende a los requisitos técnicos aplicados.

Para más informaciones, consulte el site de la ANATEL – www.anatel.gov.br

El producto en su instalación debe ser acondicionado de la siguiente forma: caja material: acero, dimensiones 33x28x8 cm; Batería modelo: UP1270E, fabricante: UNIPOWER, Capacidad nominal: 12V 7Ah.

Índice

Introducción....8
Instalación....9
Línea telefónica....10
Periféricos....10
Fijación....10
Placa Central y Módulo GPRS....11
Programando VW16ZGPRSIP....13
Programando la Central Por El Teclado....13
Programando Via Cable Serial – Software Viaweb Download....15
Programando la Central por la Página Web....16
Identificando el Dispositivo en la Red....16
Pagina Inicial....16
Botones del Menu....16
Programar para Empresas de Monitoreo....18
[020] Intervalo de Ping....18
[021 y 022] Servidores Dns 18
[023 a 025] ID ISEP....18
[026 a 028] Puerta Tcp Do Servidor....19
[029 a 031] Dirección del Servidor....19
[034 a 036] Dirección del Servidor (Para Teclado Led)....19
[066 a 073] Número de la Cuenta de la Partición....19
[032] Horario del Primero Test de Internet....19
[033] Intervalo de Test Internet....19
[440] Evento de Acceso Remoto – Código Contact ID....20
[473] Evento de Acceso Via Cable Serial – Código Contact ID....20
[363] Ajuste del Reloj y Test Periódico - Opciones (BITS) 1, 7 y 8....20
[018] Partición y Zona dos Eventos Internos....20
[086] Servidor Viaweb #3 como backup do Servidor Viaweb #1 - opción (Bit) 3....20
Informaciones de Los Leds de la Central (Conexión Con la Empresa de Monitoreo)....21
Formato de Comunicación....22
[001 a 003] Secuencias de Comunicación....22
[004 a 006] Filtro de Eventos Particiones....23
[007 a 012] Filtro de Eventos de las Secuencias....23
[013 a 015] Tentativas de Envio de las Secuencias....24
[016] Primero Periférico de Comunicación Auxiliar (Medio de Comunicación 04)....24
[017] Segundo Periférico de Comunicación Auxiliar (Medio de Comunicación 05)....24
IP (Ethernet)....25
[051] Dirección Ip Na Red....25
[052] Gateway....25
[053] Máscara de Red....25
[054] Dirección Mac (Solamente Lectura)....25
[021 y 022] Servidores DNS....25
[055] DHCP....26
[056] Servidor Ntp....26
[057] Huso Horario....26
[520] Permisión de Accesso a la Navegación Web....28
GPRS....28
[037 y 038] Selecciona Operadora Sim Card #1 y #2 (Para Teclado de Led) 28
[041 y 541] Pin Do Sim Card #1 y #2....29
[042 y 542] Apn Gprs Sim 1 y Sim 2....29

[044 y 544] Contraseña Gprs Sim 1 y Sim 2.....29
[045 y 545] Número del ICCID del Sim Card 1 y 2 (solamente lectura).....29
[502 y 503] Kbytes Trafegados Sim Card 1 y 2 (solamente lectura).....29
[046] Versión del Módulo Gprs (solamente lectura).....29
Comandos Por Sms.....29
Línea Telefônica.....31
[481 a 488] Números Telefónicos / Números SMS.....31
[060] Horario del Primero Test de Línea Telefónica.....31
[061] Intervalo del Test de Línea Telefónica.....31
[074] Detector de Línea Telefónica.....31
[058] Intervalo del Test de Línea Cuando la Partición 1 Está Armada.....32
[059] Intervalo del Test de Línea Cuando la Partición 1 Está Desarmada.....32
[081] Opiciones de la Línea.....32
[086] Opiciones de Transmisión.....33
[075] Retardo na Falla de Línea Telefónica.....33
[351] Número de Tonos Para Download.....33
[363] Habilita Callback no Download – opción (bit) 5.....33
[354] Llamada Dupla.....33
Cancelar Llamada.....33
Zonas.....34
[107] Configuración de las Zonas.....34
[108] Velocidad de las Zonas.....38
[091 a 106] Tipo de las Zonas.....38
[121 y 123] Tiempo de Entrada y Salida 1.....38
[122 y 124] Tiempo de Entrada y Salida 2.....39
[120] Particiones Que Hacen Pitidos Durante la Temporización.....39
[127] Tiempo de Zona Preventiva.....39
[187 a 202] Particiones de Control Remoto.....40
[125] Tiempo de Zona Anti-Secuestro.....40
[126] Tiempo de Zona Anti-Invasión.....41
[113] Número de Disparos Para Auto Exclusión.....41
[109 y 110] Zonas Com Chime.....41
[111 y 112] Zonas Sin Exclusión.....41
[114 y 115] Zonas Cruzadas.....42
[116] Número de Zonas Cruzadas Abiertas Para Disparo.....42
[119] Zona Olvidada Abierta (Zona 2).....42
[423] Zona Olvidada Abierta – Código Contact ID.....42
[117 y 118] Inversión del Estado de las Zonas.....42
[701 a 828] Nombre de las Zonas.....42
Contraseñas.....43
Registrando Contraseñas.....43
Registrando Contraseñas Por Teclado.....43
Registrando Contraseñas Via Página Web.....43
[220] Número de Dígitos de las Contraseñas.....44
[221] Contraseña de Programación.....44
[363] Inibir Contraseña de Programación Cuando Central Está Armada - (Bit) 2.....44
[222 a 321] Particiones que el Usuario Tiene Acceso (001 a 100).....44
[601 a 700] Nombre de los Usuarios.....44
[348] Contraseña de Coacción.....45
[352] Contraseña de Download.....45
[322 a 334] Contraseñas que Arman Forzado (Away).....45
[335 a 347] Contraseñas que no Excluyen Zonas.....46
[349 y 350] Usuários Tiemporários (Contraseñas 029 y 030).....46
[387 a 399] Contraseñas con Horario Restringido.....46
[047 a 050] Horario de Funcionamento de las Contraseñas con Horario Restringido.....47
[400] Días de la Semana de Funcionamiento de las Contraseñas con Horario Restringido.....47

Particiones.....47
[204] Sistema Particionado.....47
[171 a 186] Particiones das Zonas.....48
[591 a 598] Nombres de las Particiones.....49
[203] Partición 8 Comum.....49
Auto Activación.....49
[131 a 138] Horario de Auto Activa.....49
[206 a 209 y 358 a 361] Horario de Auto Desactiva.....49
[130] Días de la Semana con Auto Desactiva.....50
[205] Particiones Para Auto Activa (Auto Activa del Teclado).....50
[139 a 146] Activación Por Inercia de las Particiones.....50
[159 a 166] Horario en que las Particiones Activan Por Inercia.....50
[167 a 170] Días de la Semana en que las Particiones Activam Por Inercia.....51
[363] Anular Auto Activación con Zona Abierta – Opción (BIT) 4.....51
[465] Falla en el Auto Arme – Código Contact Id.....51
[147 a 154] Horario en que las Particiones Están Siempre Armadas.....51
[155 a 158] Días de la Semana en que las Particiones Están Siempe Armadas.....52
[491 a 494] Tiempo de Rearme de las Particiones Siempre Armadas.....52
Sirenes.....52
[210 y 211] Tiempo de Sirena.....52
[213 y 214] Particiones que Disparan la Sirena.....52
[216 y 217] Bip de la Sirena.....53
[219] Supervisión de la Sirena.....53
[082] Problemas que Disparam a Sirena.....53
Salidas Programables (PGMs).....53
[371 a 374] Eventos de las Pgms.....54
[375 y 376] Operación Lógica De Las Pgms.....55
[377 a 380] Complemento De Las PGM’s (Tipo Valor).....56
[381 a 384] Complemento De Las PGM’s (Tipo Función).....56
[385 y 386] Tiempo Das Pgms.....56
Viaweb Mobile(Aplicación Para Smartphones).....56
Viaweb Direct.....57
Programando la central por funciones.....58
[571] Habilita Registro Automático Viaweb Direct.....58
[570] Viaweb Direct - Llave Criptográfica.....58
[580] Habilita Dynamic Dns.....59
[581] Dirección Externa (HOSTNAME).....59
[582] Usuario Dynamic Dns.....59
[583] Contraseña Dynamic Dns.....59
[584] Resultado Dynamic Dns.....59
Página Servidor Viaweb.....60
Correo Electrónico.....61
[561] Servidor Smtp.....61
[562] Puerta Para Correo Electrónico (Servidor Smtp).....61
[564] Usuario Correo Electrónico.....61
[565] Contraseña Correo Electrónico.....61
[551] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 1.....61
[552] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 2.....61
[553] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 3.....62
[512] Horario de Envio del Informe.....62
[513] Días de la Semana Para Envio de Informe.....62
Relatórios.....63
Avanzado.....64
[000] Versión del Firmware de la Central.....64

[355 y 357] Permiso de Acceso Remoto....64
[366] Teclas Especiales 1 y 2....64
[363] Programación de Contraseñas Aleatórias - Opción (BIT) 3....65
[363] Salva la Lista de Periféricos Conectados al Innovabus - Opción (BIT) 6....65
[363] Diversos....66
[086] Ganho de transmissão e Servidor #3 como backup....66
Lacre de la Programación (Solamente Para Empresas de Monitoreo)....66
[019] Lacre de Programación....67
[471] Programación Irá Liberar Después de 4 Minutos – Código Contact ID....67
[472] Programación Lacrada – Código Contact ID....67
Agendas....68
[830 a 863] Tipo de la Agenda....68
[864 a 897] Complemento de la Agenda....69
[898 a 931] Horario de Inicio de la Agenda....69
[932 a 965] Horario Final de la Agenda....70
[966 a 999] Días de la Semana de la Agenda....70
[521 a 535] Calendário de Feriados....71
RESET....72
Reset de las Contraseñas Maestras y de Programación....72
Reset Total de la Programación....72
[362] Trava de Reset....72
Códigos de los Eventos de la Alarma (Contact – id)....73
[401 a 476] Códigos de los Eventos en Contact-ID....74

INTRODUCCIÓN

El VW16ZGPRSIP es un panel de Alarma de última generación, con comunicación via red ethernet TCP/IP, Chip GPRS y Línea telefónica.

El Panel puede ser encontrado en las siguientes versiones y características:

	Panel			
	VW16Z	VW16ZIP	VW16ZGPRS	VW16ZGPRSIP
Linha telefônica	✓	✓	✓	✓
Ethernet (cabo de rede)		✓		✓
GPRS (chip de celular)			✓	✓
Eventos por SMS			✓	✓
Aplicación / Página Web		✓		✓
Informes y eventos por correo electrónico con seguridad SSL		✓	✓	✓
Plug and Play		✓		✓
Dynamic dns próprio		✓		✓
Actualizacíon remota de versíon del firmware (por empresa de monitoreo)		✓	✓	✓
Ajuste de reloj via NTP		✓	✓	✓

Características comunes a todos los modelos:

- ✔ Puede ser monitoreada por cualquier empresa de monitoreo, enviando los eventos a través de Línea telefónica, GPRS o ETHERNET(conforme modelo de la central).
- ✔ Puede ser divida en hasta 8 ambientes (particiones).
- ✔ Posee 16 zonas de Alarma, expansible hasta 128 zonas.
- ✔ Opera con 100 usuarios (Contraseñas) distintas expansibles hasta 900 usuarios con el uso de teclados (teclados da Línea 558, 32s, Flex, Flex32, 128s, 128b e Touch).
- ✔ Salida para una Sirena de hasta 2.5A.
- ✔ Supervisión completa: Permite envío de test periódico, monitorea red eléctrica, batería, alimentación de periféricos, cableado de los sensores, Sirena.
- ✔ Fuente de alimentación con entrada full range (90V a 240V).
- ✔ Posee recursos avanzados: Contraseñas de coacción individuales, sello de programación, de las salidas programables de 100mA cada, cable de programación serial, memoria no volátil , comunicación con hasta 3 empresas de monitoreo distintas, protección contra descarga profunda de la batería.
- ✔ Acepta todos los periféricos de la Línea VIAWEB: expansor de zonas, módulo IP y GPRS (VIAWEB ip, VIAWEB gprs y VIAWEB gprs ip), teclados, controlador de acceso, receptores sin hilo iBUS y Smart1212.

INSTALACIÓN

Bateria

Es importante que sea conectada al sistema una batería de “back-up” para que en caso de falla en la energía eléctrica, el sistema continúe funcionando correctamente. Recomendamos el uso de batería sellada recarregable de 12V 7Ah de buena calidad. la central tiene disponible dos cables para la conexión de la batería 13,8V , dónde el rojo debe ser conectado al positivo (+) y el negro al negativo (-) de la batería.

Red Elétrica

Conectar el chicote eléctrico en la placa y conectarlo a la red eléctrica.

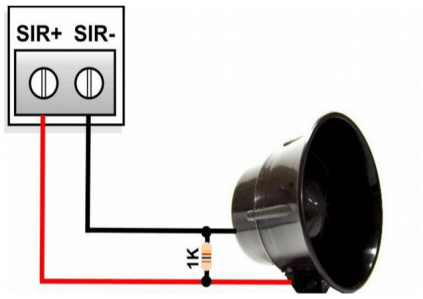
Al ser energizada el led rojo empieza a parpadear.

Conectar el cable de red en el conector RJ45 y en el rotador o switch de la red (en los modelos con ETHERNET).

Sirena

En los terminales SIR+ y SIR - la central disponibiliza al instalador una tensión de 13,8 V y 2,5 A con la batería conectada, para la instalación de la sirena. Esa salida tiene una protección contra cortocircuito o corte de sirena cuando programada.

Para que la supervisión de sirena funcione correctamente, conecte un resistor de **1K** en paralelo, el más próximo posible de la sirena.



Salida de Alimentación Auxiliar y Barramento

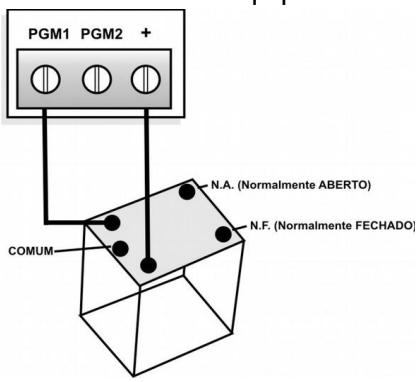
La salida auxiliar permite en el máximo 1,2A.

En los terminales (+) y (c) la central disponibiliza al instalador una tensión de 13,8V para los sensores que pueden ser conectados a la central.

Salidas Programables (PGM1 e PGM2)

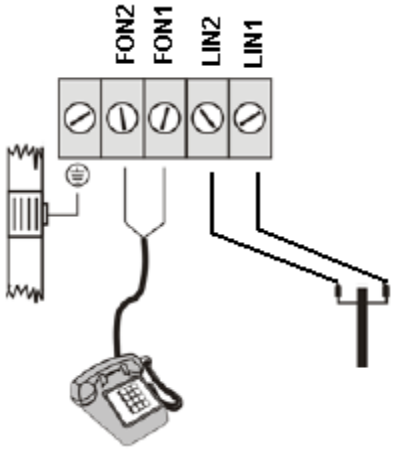
La central posee dos salidas programables. Esas salidas disponibilizan una tensión negactiva de en el máximo 100mA para la conexión de un relé que hará el accionamiento de equipamientos para automoción.

La PGM1 puede ser programada para funcionar como la segunda sirena, utilizando un relé para el accionamiento conforme el dibujo.



LÍNEA TELEFÓNICA

Conecte a linha telefônica de maneira que a central de alarme seja o primeiro equipamento que recebe a linha telefônica ou seja, a central de alarme é quem vai disponibilizar para o resto do local a linha telefônica.



LIN1 e LIN2 : Entrada da linha telefônica externa.
FON1 e FON2 : Saída da linha telefônica para os aparelhos internos.

PERIFÉRICOS

Los teclados, expansores de zonas y módulos VIAWEB son periféricos interligados a la central através del sistema de barramento. Cada periférico tiene una dirección dentro del barramento del sistema y la alimentación de los teclados precisa ser conectada al **VM** y **PR** de la central VW16Z.

FIJACIÓN

Elija un local arejado para la fijación de la caxa de la central, dónde exista energia eléctrica, red telefónica, internet, cobertura GSM para el modelo VW16ZGPRSIP, y aterramiento próximos y **NO VISIBLE A PERSONAS LEJANAS.**

Cuidados para Fijación de la Placa

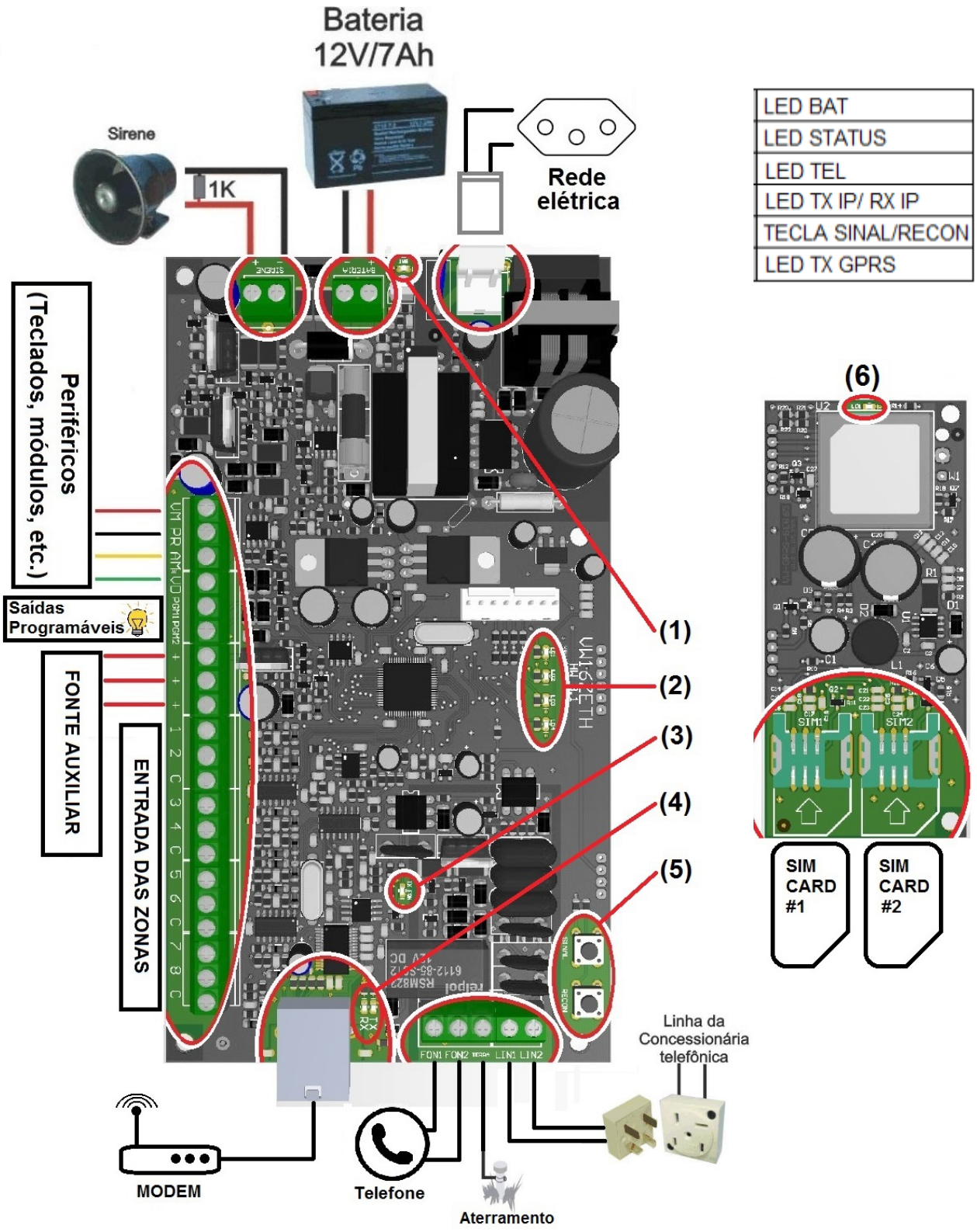
Para una buena ventilación, evite contacto de la placa con la caja metálica utilizando espaciadores plasticos. Al hacer instalación de sensores y periféricos, procure no dejar los hilos pasando sobre la placa.

Aterramiento

Para mejor protección, equipamientos electrónicos en general, necesitan de un aterramiento. la central tiene un local especial para la conexión del aterramiento. También recomendamos el aterramiento de la caja de la central.

PLACA CENTRAL Y MÓDULO GPRS

Placa VW16ZETH. Cuando la central tiene comunicación por GPRS, el módulo a la derecha va soldado junto a la placa principal.

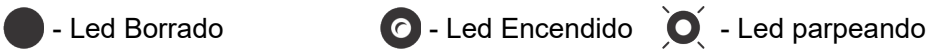


LED BAT (1):

Cuando encendido efetuando el test de bateria, el test es efectuado a cada 60 segundos. El led también queda encendido,pero con una intensidad menor cuando está carregando la bateria.

LEDS DE STATUS (2):

Normalmente muestran el status de conexión con el Servidor Viaweb 1 (pág 18). Si no hay empresa de monitoreo, los leds LD2 y LD3 quedan parpadeando. En ese manual representamos:



LED TEL (3):

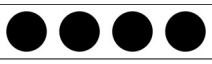
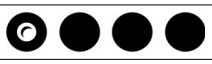
Parpadeando: monitoreo de Línea.
Encendido: discador activado enviando eventos para el receptor de monitoreo o conectado al software de download.

LED´S TX IP/RX IP (4):

Identificación de comunicación IP: transmisión/recepción de paquetes de dados por cable. Parpadeando TX transmitiendo, parpadeando RX recebiendo.

TECLA SEÑAL (5):

Para visualizar el nível de señal GPRS del módulo, se debe mantener presionada la tecla señal. Los leds LD1 a LD4 muestran el **señal**, siendo:

	Todos borrados.	Sin señal.
	LD1 encendido.	25% de señal.
	LD1 e LD2 encendidos.	50% de señal.
	LD1, LD2 e LD3 encendidos.	75% de señal.
	LD1, LD2, LD3 e LD4 encendidos.	100% de señal.

TECLA RECON (5):

Esa tecla sirve para forzar una reinicialización en la comunicación ETHERNET y GPRS. Debe ser presionada antes de remover el SIM CARD de la bandeja.

Un toque rápido una única vez para reinicializar.

Status dos SIM CARD´s					
Cuando presionada la tecla Recon, los leds muestran el status de los SIM CARD's (GPRS).					
	SIM 1		**SIM 2**		Status
Led	**1**	**2**	**3**	**4**	
					Bandeja **inactiva.**
					SIMCARD no detectado en la bandeja.
					Conectando por la bandeja.
					Conectado (ONLINE con monitoreo) por la bandeja.

TECLA TX GPRS (6):

Transmitiendo GPRS, eventos en transmisión para el servidor VIAWEB 1.
Parpadeando indica comunicación con la antena de la operadora.

PROGRAMANDO VW16ZGPRSIP

La VW16ZGPRSIP es totalmente programable y posee inúmeras opciones y funciones. El valor predeterminado de fábrica de las funciones se ajusta para adaptarse a la mayoría de las instalaciones, lo que reduce la necesidad de hacer que la programación de todo.

La unidad de control está programada a través funciones de 3 dígitos. En este manual, las funciones se colocan entre paréntesis. Ejemplo: [204] la función que determina si el sistema tiene particiones.

Hay dos tipos de funciones:

I. Las funciones que se programan mediante la colocación de una **secuencia de dígitos.**
Em ese manual, lãs funciones se representan con el código de función seguido por el número de caracteres separados por barra.

Por ejemplo, el [121] [__/__/__]; significa que la función 121 se llena con 3 dígitos.

La función [121] es tiempo de entrada en las zonas temporizadas. En esa función colocamos “030” que equivale a 30 segundos, o a la función [131] que determina el horario de auto activación de la partición 1, podemos colocar en esa función “1500”, el correspondiente a 15:00 o tres horas de la tarde.

II. Las funciones que están programados **permitiendo bits.**
En este tipo de función, debes dejar los bits (o LED en el caso del teclado) de 1 hasta 8 activarse o desactivarse dependiendo de la configuración deseada.
En manual, estas funciones son representadas en las tablas com explicaciones de cada función. Cuando el bit no aparece en la tabla significa que no tiene ninguna función.

Ejemplo de función [091] tipo de zona 1.

Si en esa función el bit 1 esté activo, la zona 1 queda como Temporizada, sin embargo, si están activos los bits 2 y 6, la zona é deshabilitada.

Hay tres maneras de programar la central VW16ZGPRSIP, **por teclado, por el software “Viaweb Download” o por la Página Web.**

PROGRAMANDO LA CENTRAL POR EL TECLADO

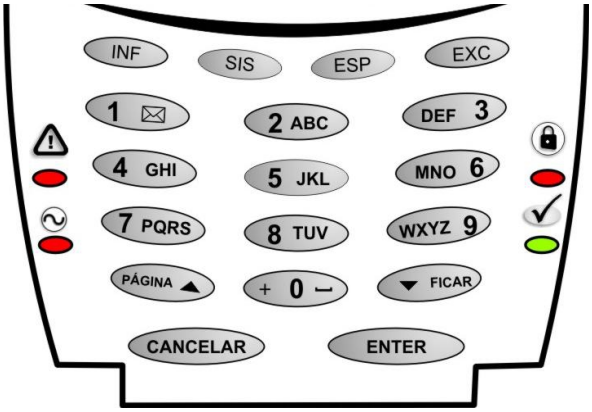
La contraseña de programación patrón de fábrica es 5353.

Para entrar en el modo de programación presione **ENTER** más la contraseña de programación, seguida de la tecla **ENTER**.

- El teclado emitirá tres pitidos que confirman que entraron en la programación (el teclado emite un pitido largo, en el caso de contraseña equivocada).
- Dentro del modo de programación, el led “  ” quedará parpadeando y los otros leds borrados.
- Digite el número de una función (**NO es necesario pulsar ENTER**), el teclado emitirá tres pitidos rápidos confirmando que entró en la función (el teclado emite un pitido largo en el caso de función equivocada).
- El led “  ” quedará encendido mostrando que el teclado está listo para recibir los valores a seren programados.

- Ponga atención en la programación pues existen funciones con valores con 3 dígitos, con 2 dígitos y elección múltiple.
- En algunas funciones, después de la entrada del valor, la central confirma automáticamente (emite tres pitidos rápidos), caso contrario presione ENT para confirmación.
- El led " ✓ " vuelve a quedar parpadeando y los otros leds borrados aguardando una nueva función.
- Para salir del modo de programación presione ENT nuevamente.

Cuando una Función contiene más do que un dígito, estos dígitos no pueden ser vistos simultáneamente. Así que una función es visitada, el primero dígito es presentado automáticamente. Dígitos adicionales (se existieren) pueden ser presentados pulsando la tecla **EXC** en los teclados de LED.



Led 🔒 y ✓ encendidos
El teclado está esperando para entrar con la contraseña de programación.

Led ✓ parpeando
El teclado está esperando el número de la funci[on que será programada.

Led 🔒 encendido y ✓ parpeando
El teclado está esperando el valor que será programado en la función.

Led ⚠ parpeando e ✓ parpeando
El teclado está esperando la dirección del periférico para programación.

ENT + 5353 + ENT + [__ __ __] (Función 3 Dígitos) + valor

Hay 5 formas de programar y visualizar la programación por el teclado:

1. **Funciones de un dígito**, en que se programa el valor deseado pulsando una única tecla (Ex: Función 091 tipo de la zona 1).

   El valor programado es representado por el led encendido, siendo que el valor zero es representado por el led 10. Para programar el nuevo valor pulsar la tecla deseada. Si quieres mantener el valor actualmente mostrado, presione la tecla EXC o CANCELAR.

   Esas funciones pueden asumir valores de 0 hasta F (hexadecimal). Para programar los valores arriba de 9, utilizar la combinación de teclas: A – INF 1, B – INF 2, C – INF 3, D – INF 4, E – INF 5, F – INF 6.

2. **Funciones de varios dígitos hexadecimales**, en que se programan vários dígitos seguidos

(Ej: Función 440 evento Contact id de 4 dígitos).

En teclados de led, la programación puede ser visualizada un dígito por vez, siendo que cada led corresponde a un número y el led 10 corresponde a cero. Para ver todos los números programados sólo tiene que ir pulsando la tecla EXC. Para visualizar valores arriba de 9 (A hasta F), primero aparecerá la tecla INF (representada por los leds 2 y 4 encendidos simultáneamente) y al pulsar EXC nuevamente, el próximo valor mostrado irá variar de 1 hasta 6, representando las letras de A hasta F.

Para programar un nuevo valor, se debe pulsar las teclas deseadas. Si quieres mantener un de los actuales valores mostrados pulse la tecla EXC.

Esas funciones pueden asumir valores de 0 hasta F (hexadecimal). Para programar los valores arriba de 9, utilizar la combinación de teclas: A – INF 1, B – INF 2, C – INF 3, D – INF 4, E – INF 5, F – INF 6.

3. **Funciones decimales**, en que se programa un número de 3 dígitos entre 000 y 255 (Ex: Función 121 Tiempo de entrada 1).

   El valor en los teclados de led es mostrado por los leds de 1 hasta 8 de forma binaría.

   El valor programado es dado por la suma de los leds encendidos:

   Ejemplo: SI los leds 1 ; 5 y 8 estén encendidos el valor será:
   1 + 16 + 128 = 145.

LED	SUMA
1	1
2	2
3	4
4	8
5	16
6	32
7	64
8	128

4. **Funciones de múltiples opciones**, en que cada led encendido de 1 hasta 8 representa una opción (Ex: Función [120] - particiones que hacen pitidos temporización).

   Al entrar en esa función los leds ya muestran el valor programado. Para alterar el valor se debe pulsar la tecla de 1 hasta 8 correspondiente a la opción. Si el led encender, la opción está habilitada, si el led borrar, deshabilitada. Se puede pulsar las teclas más de una vez até obter el valor deseado. Para programar esa función, después elegir las opciones se debe pulsar ENTER.

5. **Funciones de texto**, en que se programa un mensaje.
   (Ej: Función 029 dirección del servidor VIAWEB 1).

   Esas funciones solamente son programadas por teclados de display. Al intentar programar una de esas funciones con el teclado de leds, se oye un pitito de error. Para programar una letra presionar la tecla correspondiente hasta que la letra deseada aparezca en la pantalla.

   Para alterar entre letras mayúsculas, minúsculas y números, pulsar la tecla SIS.

   Al terminar de digitar el texto, se debe pulsar la tecla 0 hasta que el símbolo de <ENTER> aparezca, ese símbolo es que marca el fin del texto.

   Pulsar ENTER para programar.

PROGRAMANDO VIA CABLE SERIAL – SOFTWARE VIAWEB DOWNLOAD

Para programar via cable serial y para más informaciones, se debe obtener el software VIAWEB download, en el área de downloads del site www.viawebsystem.com.br.

Para acceder a VW16ZGPRSIP via cable serial es necesario contraseña de download (pág. 45).

PROGRAMANDO LA CENTRAL POR LA PÁGINA WEB

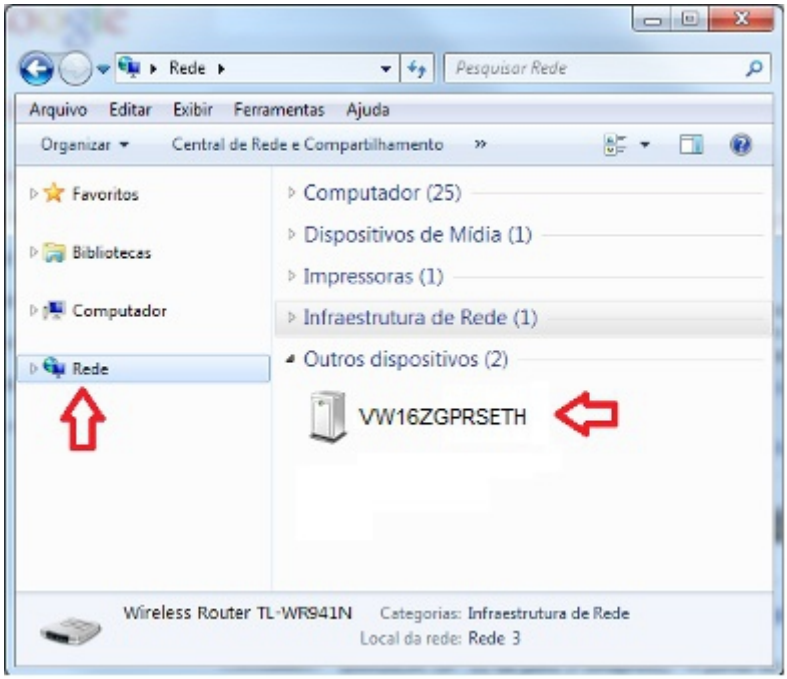
IDENTIFICANDO EL DISPOSITIVO EN LA RED

El VW16ZGPRSIP posee recurso “Universal Plug and Play” (versiones del Windows compatibles: Vista o superior). Eso significa que al ser conectada en la red local ella será automáticamente detectada por computadores compatibles con esta tecnologia.

Para identificar la central, en un computador con Windows, abra el explorador de archivos, y después haz clic en la opción “red” en el menu a la izquierda.

La central irá aparecer como “otros dispositivos de red”. Haga doble clic para abrir la página inicial.

Caso la central no esté apareciendo intente pulsar el botón actualizar algunas veces, verifique la conexión del cable de red, los leds verdes deben estar encendidos o parpadeando. Si el problema persistir, efectue la configuración manual de los parámetros de red en “Configuración manual de los parámetros de la red” (pág. 25).



PAGINA INICIAL

Clicando dos veces en la central, o digitando la dirección de red interna de él en un navegador, aparecerá un pedido de autorización. El campo de usuario debe ser dejado en blanco y en el campo contraseña se pone la **contraseña de programación (patrón:5353)** o la contraseña de usuario **maestra (patrón:1515).**

Usando la contraseña de programación podemos solamente alterar la programación, usando la contraseña maestra, podemos alterar la programación, registrar usuarios y armar/desarmar el sistema.

Página de control del sistema:

Es disponibilizado el control local a través de la página del dispositivo. Sin embargo, la conexión en ese caso posee solamente autenticación sencilla y no es segura para ser redireccionada para fuera de la red interna.

El acceso a la página web puede ser deshabilitado por programación (ver pág. 28).

BOTONES DEL MENU

Controlar PGMs	Excluir Zonas	Eventos	Relatório
Abre la página de control de las PGMS del sistema.	Habilita la selección de las zonas para la exclusión al armar*.	Abre la página con los últimos 100 eventos registrados por el sistema.	Abre la página con el relatório de status atual del sistema.

Configurar		Abre la página del assistente de configuración. En el asistente encontramos:	
	Monitoreo Acá se programa los dados de la empresa de monitoreo cuando el sistema es monitoreado.		Usuarios Permite visualización de usuarios y programación de contraseñas*.
	E-mail Acá se define el e-mail para envio de eventos, informes y los e-mails de recepción.		Red e Internet Configuraciones de red, internet y servidor de fecha e hora del módulo.
	Viaweb Direct Configuraciones para conexión del módulo con la aplicación.		Control del Sistema Vuelve para la página de control del sistema.
	**Programar** Página para programación del sistema por funciones.		

- Programando los campos de la página Monitoreo, las funciones [001], [023],[026],[029], [066] son automáticamente programadas. Al borrar los campos y salvar, todas esas funciones son desprogramadas.
- En la página Usuarios podemos modificar o registrar los usuarios y sus contraseñas. Los nombres puestos aqui programan automáticamente las funciones [601] a [700].
- Programando los campos de la página Correo electrónico, las Funciones [002], [005], [009], [010], [561], [562],[564],[565],[551],[552], [553],[512],[513] son automáticamente programadas. Al borrar los campos y salvar, todas esas funciones son desprogramadas.
- Programando los campos de la página Red e Internet, las funciones [051], [052],[053],[055], [021],[022],[056], [057] son automaticamente programadas. Al borrar los campos y salvar, todas esas funciones son desprogramadas.
- Programando los campos de la página Viaweb Direct, las funciones [003], [006],[011],[012], [570],[580], [582],[583] son automáticamente programadas. Al borrar los campos y salvar, todas esas funciones son desprogramadas.
- En la página Programar, en el campo **dirección**, dejamos 001 para programar la VW16ZETHGPRS. Ese campo es alterado cuando precisamos programar otro periférico (teclados, módulos expansores, etc.). En el campo **Función** ponemos la Función (con 3 dígitos) que deseamos programar y clicamos en cargar. En el campo **valor** aparece el que está programado en la función. Para alterar la programación solo inserte el nuevo valor y haz clic en **salvar**.

PROGRAMAR PARA EMPRESAS DE MONITOREO

Así como el envío de eventos por correo, el monitoreo se realiza también a través de las secuencias de comunicación. Es posible recibir correos electrónicos al mismo tiempo en que el sistema está controlado por una empresa de supervisión. Si VW16ZGPRSIP se instala junto con el módulo VIAWEB gprs se puede hacer con que, en caso de falla en la red IP el monitoreo pase a ser hecho via GPRS. Para más informaciones sobre las secuencias de comunicación verifique el item “Monitoreo de eventos por secuencias de comunicación” en la pág. 18.

Al contratar una empresa de monitoreo, recibirás las siguientes informaciones:

- IP del servidor de monitoreo. (VIAWEB receiver).
- Puerta TCP del servidor de monitoreo (normalmente 1733).
- ID ISEP: Identificador único de 4 dígitos, sirve para que la empresa de monitoreo identifique su equipamiento en la central de monitoreo.

DICA: En la página inicial de configuración de la VW16ZGPRSIP, hay la opción de configurar la empresa de monitoreo. Solo tiene que rellenar los 3 campos arriba y verificar en la propia página si la conexión con la empresa fue establecida. Esa página haz la configuración automática de la secuencia de comunicación 1 y atribui el ID ISEP como siendo el número de cuenta para partición 1 (Función [066]).

Pantalla de programación de la empresa de monitoreo.

Al configurar la conexión con una empresa de monitoreo, la VW16ZGPRSIP mantiene una comunicación constante con el servidor de monitoreo, enviando inmediatamente cualquier evento, falla o información generada por el sistema. También es posible para la empresa de monitoreo efectuar acceso remoto a la VW16ZGPRSIP. Toda vez que la empresa de seguridad acceder el sistema de Alarma, un evento es generado. Ese evento es configurado en la función [440].

[020] INTERVALO DE PING

[020] [__/__/__] Patrón: 010 minutos (GPRS)

Periodicamente, es enviado un paquete criptografado para el servidor VIAWEB verificando si este está respondendo correctamente. El intervalo de ping puede ser cualquier valor de 001 hasta 015.

[021 Y 022] SERVIDORES DNS

[021] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Servidor DNS Primario Patrón: 8.8.8.8
[022] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Servidor DNS Secundario Patrón: 8.8.4.4

Servidores DNS: sirven para que la central pueda encontrar el IP del servidor VIAWEB a partir de su dirección URL en la red internet (ej.: www.opendns.com). Caso el DHCP estea habilitado (opción 1 de la función 055), se puede optar por utilizar la dirección del servidor DNS fornecido por la red o progamado (opción 3 da función 055). Ese campo es automaticamente programado cuando habilitado el registro de aplicación en la página web.

[023 A 025] ID ISEP

[023] [__/__/__/__] ID ISEP Servidor VIAWEB 1 Patrón: 0000
[024] [__/__/__/__] ID ISEP Servidor VIAWEB 2 Patrón: 0000
[025] [__/__/__/__] ID ISEP Servidor VIAWEB 3 Patrón: 0000

ID_ISEP: (número identificador de la central) debe ser registrado el mismo ID_ISEP en el servidor VIAWEB RECEIVER.

[026 a 028] Puerta Tcp Do Servidor

[026] [__/__/__/__/__] Puerta TCP del Servidor VIAWEB 1 Patrón: 01733
[027] [__/__/__/__/__] Puerta TCP del Servidor VIAWEB 2 Patrón: 01733
[028] [__/__/__/__/__] Puerta TCP del Servidor VIAWEB 3 Patrón: 01733

Puerta TCP: Puerta de conexión entre la central y el servidor VIAWEB.

[029 a 031] Dirección del Servidor

Patrón: www.viawebsystem.com.br **(**Máximo 30 caracteres.)
[029] [_] IP FIJO o End URL Servidor 1
[030] [_] IP FIJO o End URL Servidor 2
[031] [_] IP FIJO o End URL Servidor 3

IP FIJO o Dirección URL del servidor VIAWEB (RECEIVER) que recebirá los eventos via internet.

[034 a 036] Dirección del Servidor (Para Teclado Led)

[034] [_ _ _ . _ _ _ . _ _ _ . _ _ _] IP FIJO Servidor 1 Patrón: 000.000.000.000
[035] [_ _ _ . _ _ _ . _ _ _ . _ _ _] IP FIJO Servidor 2 Patrón: 000.000.000.000
[036] [_ _ _ . _ _ _ . _ _ _ . _ _ _] IP FIJO Servidor 3 Patrón: 000.000.000.000

IP FIJO del servidor VIAWEB que recebirá los eventos via internet.

Ojo.: Cuando esta función es programada por teclado a cada 3 dígitos es emitida una confirmación sonora. Ejemplo: para programar el ip 192.168.1.1 se debe digitar 192 168 001 001.

[066 a 073] Número de la Cuenta de la Partición

[066] [__/__/__/__] Cuenta Partición 1 Patrón: 0000 o no particionado Patrón:0000
[067] [__/__/__/__] Cuenta Partición 2 Patrón: 0000
[068] [__/__/__/__] Cuenta Partición 3 Patrón: 0000
[069] [__/__/__/__] Cuenta Partición 4 Patrón: 0000
[070] [__/__/__/__] Cuenta Partición 5 Patrón: 0000
[071] [__/__/__/__] Cuenta Partición 6 Patrón: 0000
[072] [__/__/__/__] Cuenta Partición 7 Patrón: 0000
[073] [__/__/__/__] Cuenta Partición 8 Patrón: 0000

A	INF + 1
B	INF + 2
C	INF + 3
D	INF + 4
E	INF + 5
F	INF + 6

Se puede programar hasta 8 cuentas diferentes, siendo una para cada partición. Cuando la central no es particionada, se programa solamente el número de la cuenta de la partición 1. El número puede ser de 0000 hasta FFFF.

[032] Horario del Primero Test de Internet

[032] [__/__/__/__] Patrón: 00:00

Horario en que debe ocurrir la primera transmisión del evento de test automático en el día.

[033] Intervalo de Test Internet

[033] [__/__/__/__] Patrón: 00:00

Período de Tiempo para enviar test, en horas y minutos.
Ej.: para la transmisión de 24 testes por dia, se programa el intervalo de 1 hora (01:00).

[440] Evento de Acceso Remoto – Código Contact ID

[440] [__/__/__/__] Patrón: 1412

Código Contact ID del evento. Programar 0000 para deshabilitar el envio de ese evento. **Ojo.**: Contraseña de download se encuentra en la pág. 45 .

[473] Evento de Acceso Via Cable Serial – Código Contact ID

[473] [__/__/__/__] Patrón: 1410

Código Contact ID del evento. Programar 0000 para deshabilitar el envio de ese evento.

[363] Ajuste del Reloj y Test Periódico - Opciones (BITS) 1, 7 y 8

Patrón: Borrado (Deshabilitado)		**Bit/Led**
[363]	Si está activado, ajusta periódicamente el reloj interno de la hora recibida desde el servidor de Viaweb 1. Recuerde que el servidor Viaweb debe estar conectado a una de las secuencias para que pueda actualizar el reloj a través de él.	**1**
	Cuando está activado, el evento de prueba periódica (Función 439) se envía utilizando ID_ISEP (Funciones 023-025) como el número de cuenta. Si está desactivada, utiliza el número de cuenta de la partición 1 (Función 066).	**7**
	Si la opción 8 de la función está habilitada, el evento de test de GPRS irá incluir el nível de señal en el campo zona do Contact ID. El valor del nivel de la señal puede variar de 000 (0%) a 032 (100%).	**8**

[018] Partición y Zona dos Eventos Internos

[018] [P / Z / Z / Z] Patrón: 0000 [P = partición 1 dígito] [Z = zona 3 dígitos]

El sistema, conforme la programación, puede enviar diversos eventos internos: test periódico, falla de batería, falla de red eléctrica y otros.

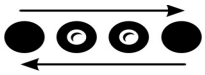
Por Patrón, cuando eses eventos son generados, la partición envía el valor cero y la zona envía el valor cero también.

Caso deseado, se puede alterar el valor de la partición y de la zona a ser enviada con eses eventos.

[086] Servidor Viaweb #3 como backup do Servidor Viaweb #1 - opción (Bit) 3

	Descrición	**Tecla/Led**
[086]	Cuando habilitado, permite que el SERVIDOR VIAWEB #3 puede ser utilizado como Backup do SERVIDOR VIAWEB #1 con lo mismo IDISEP. Ojo.: Para utilizar esta opición, poner a cero la función 025. Esta función se utiliza cuando un servidor VIAWEB tiene dos IP's distintas.	**3**

INFORMACIONES DE LOS LEDS DE LA CENTRAL (CONEXIÓN CON LA EMPRESA DE MONITOREO)

Servidor VIAWEB 1 (LD1 a LD4)		
	Leds corren de LD1 a LD4 y vuelven.	Indica funcionamiento normal de la conexción con servidor VIAWEB.
	Leds corren de LD1 a LD4 en un sentido.	Indica funcionamento normal y eventos en transmisión para el servidor VIAWEB1.
	LD2 y LD3 Parpeando	Servidor VIAWEB inactivo (el módulo no está programado para conectarse a esse servidor en ese momento).
Servidores VIAWEB 2 y 3 (LD1 a LD4)		
También es posible ver la situación de los otros servidores VIAWEB (canal 2 y 3). Presionando la tecla SEÑAL una vez los leds muestran el estado de la conexión con el VIAWEB 2 Presionando la tecla SEÑAL dos veces los leds muestran el estado de la conexión con el VIAWEB 3.		
En eses casos:		
	todos los leds borrados	esa conexión no está activa.
	todos los leds encendidos	conexión OK con el servidor.
La conexión es mostrada durante 20 segundos después de pulsar la tecla SEÑAL, después los leds vuelven a mostrar automaticamente la conexión 1.		
Status da Conexión:		
	LD1, LD2, LD3 y LD4 parpadeando	La interfaz de comunicación se enciende o se restablece. Si esta situación se mantiene durante mucho tiempo puede indicar problemas en el módulo GPRS, también puede ser ausencia o falla en SIMCARD. Problemas o falta de cable de red en VW16ZIP.
	LD1, LD2 parpadeando, LD3 y LD4 borrados	Esa conexión está en pausa. Significa que la central ya intentó conectar sin éxito en el servidor por 4 veces consecutivas, y ahora solamente irá intentar nuevamente después de 4 minutos.
	LD1, parpadeando LD2, LD3 y LD4 borrados	Conectando la red GPRS, si esa situación permanecer por mucho tiempo, las configuraciones de APN pueden estar equivocadas, sin cobertura GPRS o el SIMCARD puede no estar habilitado.
	LD1 parpadeando, LD2 y LD3 borrados, LD4 encendido	Abriendo conexión con servidor VIAWEB. Caso no salga de ese estado el servidor VIAWEB puede no estar activo o las configuraciones para conexión equivocadas.
	LD1parpadeando LD3 endendido, LD2 y LD4 borrados	Conectado al servidor VIAWEB, aguardando autorización para autenticación.
	LD1 parpadeando, LD2 borrado, LD3 y LD4 encendido,	Negociando criptografia con el servidor VIAWEB.
	LD1 parpadeando, LD2 endendido, LD3 y LD4 borrados	Enviando ID ISEP al servidor VIAWEB.
	LD1 parpadeando, LD2 y LD4 encendidos, LD3 borrado	Autenticando en el servidor VIAWEB. Caso la conexión nunca pase de ese punto la central puede no estar autorizada a conectarse en el servidor VIAWEB.
	LD1 parpadeando, LD2, LD3 y LD4 encendidos	Cerrando conexión con el servidor VIAWEB. Eso ocurre cuando no hay respuesta del servidor VIAWEB o hubo falla en la autenticación con el servidor. Verifique el ID ISEP.

FORMATO DE COMUNICACIÓN

Funciones abajo automáticamente programadas por la "Página Web"

[001 A 003] SECUENCIAS DE COMUNICACIÓN

Patrón: [0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0][0/0]
[001] [__/__/ . . . /__] Sec. de Com.1 (32 dígitos o 16 medios)
[002] [__/__/ . . . /__] Sec. de Com.2 (32 dígitos o 16 medios)
[003] [__/__/ . . . /__] Sec. de Com.3 (32 dígitos o 16 medios)

Opções	Meios de Comunicação
[00]	Fin de la Secuencia de comunicación (cuando utilizar menos que 16 medios)
[01]	Servidor VIAWEB 1 comunicación por GPRS
[02]	Servidor VIAWEB 2 comunicación por GPRS
[03]	Servidor VIAWEB 3 comunicación por GPRS
[04]	Primero periférico de comunicación auxiliar (ver Función 016)
[05]	Segundo periférico de comunicación auxiliar (ver Función 017)
[11]	Contact ID en el Número Telefónico 1
[12]	Contact ID en el Número Telefónico 2
[13]	Contact ID en el Número Telefónico 3
[14]	Contact ID en el Número Telefónico 4
[21]	4+2 pulsado en el Número Telefónico 1
[22]	4+2 pulsado en el Número Telefónico 2
[23]	4+2 pulsado en el Número Telefónico 3
[24]	4+2 pulsado en el Número Telefónico 4
[31]	Sonido de Sirena en el Número Telefónico 1
[32]	Sonido de Sirena en el Número Telefónico 2
[33]	Sonido de Sirena en el Número Telefónico 3
[34]	Sonido de Sirena en el Número Telefónico 4
[41]	SMS para el Número Telefónico 1 (disponible solamente en la versión GPRS)
[42]	SMS para el Número Telefónico 2 (disponible solamente en la versión GPRS)
[43]	SMS para el Número Telefónico 3 (disponible solamente en la versión GPRS)
[44]	SMS para el Número Telefónico 4 (disponible solamente en la versión GPRS)
[51]	Servidor VIAWEB 1 comunicación por ETH
[52]	Servidor VIAWEB 2 comunicación por ETH
[53]	Servidor VIAWEB 3 comunicación por ETH
[61]	Envío de correo electrónico (preferencialmente por ETH e GPRS cuando disponible)
[81]	Envío de notificaciones para VIAWEB direct (solamente por ETH)

En esas funciones indicamos para cual medio los eventos serán enviados y en que secuencia.

Ejemplos:

[001] [51 52 00 00 00 **…]**

En la función 001 ponemos como medio principal Servidor VIAWEB 1 (empresa de monitoreo) y Servidor VIAWEB 2 como backup. O sea, se por algún motivo el servidor principal de la empresa salir del ar, la secuencia va pasar a enviar eventos para el servidor 2. Cuando el servidor 1 volver, la secuencia vuelve a enviar eventos para el servidor 1 nuevamente.

[002] [81 00 00 00 00 **…]**

En la función 002 ponemos para enviar los eventos para el VIAWEB direct (Aplicación).

Tenga en cuenta que las funciones [001],[002] y [003] funcionan paralelamente, o sea, la central envia eventos al mismo tiempo para las tres secuencias.

Atención: Es posible programar hasta **3 servidores VIAWEB** diferentes. Cada servidor puede ser conectado usando la red Ethernet (medios 51, 52 e 53) o / y GPRS (medios 01, 02 y 03) . No es posible mantener online el mismo ID_ISEP en un servidor VIAWEB por dos Ethernet o GPRS simultáneamente.

[004 a 006] Filtro de Eventos Particiones

Patrón: Todos Encendidos (todos los eventos habilitados para todas las secuencias)

	Bit / Led / Part.							
[004] Partições da Sequência 1	1	2	3	4	5	6	7	8
[005] Partições da Sequência 2	1	2	3	4	5	6	7	8
[006] Partições da Sequência 3	1	2	3	4	5	6	7	8

Esa función determina los eventos de las particiones que cada secuencia vá enviar.

Ejemplo: la secuencia 1 puede enviar eventos solamente de las particiones 1, 2, 3 e 4 e la secuencia 2 puede enviar eventos solamente de las Particiones 5, 6, 7 e 8.

[007 a 012] Filtro de Eventos de las Secuencias

Patrón: Todos Encendidos (todos los eventos habilitados para todas las secuencias)

	Bit / Led / Part.							
[007] Eventos de la Secuencia 1	1	2	3	4	5	6	7	8
[008] Restauros da Sequência 1	1	2	3	4	5	6	7	8
[009] Eventos de la Secuencia 2	1	2	3	4	5	6	7	8
[010] Restauros de la Secuencia 2	1	2	3	4	5	6	7	8
[011] Eventos de la Secuencia 3	1	2	3	4	5	6	7	8
[012] Restauros de la Secuencia 3	1	2	3	4	5	6	7	8

CLASIFICACIÓN DE LOS CÓDIGOS DE EVENTOS:

Led
1 – Alarma (Eventos E1xx ou R1xx)
2 – _____ (Eventos E2xx ou R2xx)
3 – Fallas (Eventos E3xx ou R3xx)
4 – Desarme/Arme (Eventos E4xx ou R4xx)
5 – Exclusión (Eventos E5xx ou R5xx)
6 – Testes (Eventos E6xx ou R6xx)
7 – _____ (Eventos E7xx ou R7xx)
8 – _____ (Eventos E8xx ou R8xx)

Mas informaciones ver pág. 74 Códigos de comunicación

Los códigos de los eventos son programados en las funciones [401 a 476].

Cada led encendido corresponde al grupo de eventos y restauros que serán transmitidos en la secuencia de comunicación y quando borrados no son enviados.

Para más informaciones consulte “códigos de los eventos del Alarma” (pág. 74).

[013 a 015] Tentativas de Envio de las Secuencias

[013] [__/__/__] Tentativas Sec. de Comunicación 1 Patrón: 010
[014] [__/__/__] Tentativas Sec. de Comunicación 2 Patrón: 010
[015] [__/__/__] Tentativas Sec. de Comunicación 3 Patrón: 010

Después de intentar enviar el evento sin éxito por el número de veces programado, la central desiste de intentar enviar el evento, sin embargo, cuando for generado un nuevo evento, el módulo intentará nuevamente enviar todos los eventos que no fueran enviados.

[016] Primero Periférico de Comunicación Auxiliar (Medio de Comunicación 04)

[016] [__/__/__] Dirección del Periférico Patrón: 048

Para utilizar el medio 04 (módulo de comunicación externo 1) en alguna secuencia de comunicación (Funciones 001 a 003), se debe antes poner aqui la dirección en el barramento de este módulo.

[017] Segundo Periférico de Comunicación Auxiliar (Medio de Comunicación 05)

[017] [__/__/__] Dirección del Periférico (medio 05) Patrón: 000

Para utilizar el medio 05 módulo de comunicación externo 2) en alguna secuencia de comunicación (Funciones 001 a 003), se debe antes poner aqui la dirección en el barramento de este módulo.

Para utilizar los medios 04 o 05, debe haber en la misma instalación un de los módulos VIAWEB. Los módulos VIAWEB poseen direcciones distintas conforme el modelo:

VIAWEB Plus, VIAWEB Wireless: Dirección 048.

VIAWEB ethernet: Dirección 049 a 055 (conforme programación).

Expansor VW16ZGPRS, VW16ZETH VW16Z: Dirección 002 a 010 (conforme programación).

VIAWEB GPRS IP, GPRS, IP, IPMINI: Dirección 048 hasta 055 (conforme programación).

IP (ETHERNET)

Funciones abajo automaticamente programadas por la "Página Web"

La VW16ZGPRSIP posee recursos para configurarse automáticamente en la red ethernet en que fue instalada. Sin emabrgo, caso algun problema ocurra y no sea posible visualizar la central en la red se puede efectuar la configuración manualmente.

[051] DIRECCIÓN IP NA RED

[051] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Dirección IP de la Central Patrón: 010.001.001.009

Dirección válido dentro de la intranet dónde la central for instalada.
Caso la red utilice un servidor DHCP para atribuir os IPs, se debe programar el servidor DHCP para que no duplique el IP utilizado en la central en otro dispositivo. Para saber cual el IP se debe programar, consulte el administrador de la red.

[052] GATEWAY

[052] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Dirección IP del gateway Patrón: 010.001.001.001

Programar el IP del roteador o firewall que dá acceso a la Internet. Para saber cual el IP se debe programar, consulte el administrador de la red.

[053] MÁSCARA DE RED

[053] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Máscara de Red Patrón: 255.255.255.000

Para saber cual el valor de la máscara de red debe programar, consultar el administrador de la red.

[054] DIRECCIÓN MAC (SOLAMENTE LECTURA)

[054] [__/__/ . . . /__] Dirección MAC Patrón: C08B6FXXXXXX

MAC : XXXXXX es un número único para cada equipamiento.

[021 Y 022] SERVIDORES DNS

[021] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Servidor DNS Primario Patrón: 8.8.8.8
[022] [_ _ _ . _ _ _ . _ _ _ . _ _ _] Servidor DNS Secundario Patrón: 8.8.4.4

Servidores DNS: sirven para que la central pueda encontrar el IP del servidor VIAWEB a partir de su Dirección URL en la red internet (ex.: www.viawebservice.com.br). Caso el DHCP esté habilitado (opción 1 de la Función [055]), se puede optar por utilizar el dirección de servidor DNS fornecido por la red o programado (opción 3 de la Función [055]). Ese campo es automáticamente programado cuando habilitado el registro de aplicativo en la página web.

[055] DHCP

	Bit/Led	Descrición
[055]	1	Permite que las configuraciones de la red, (Dirección IP, gateway, máscara de red e servidores DNS) sean obtenidos automáticamente da red donde está instalado, desde que la red tenga un servidor DHCP activo como, por ejemplo, un modem roteador. Para saber se o DHCP está habilitado no modem, se debe consultar o administrador da red.
	3	El DNS via DHCP habilita la central a utilizar las configuraciones de DNS de la red dónde está instalado.
	4	Deshabilita uPNP – Al habilitar esa opción los recursos universal Plug and Play do módulo serán deshabilitados. El panel no será identificado en la red automáticamente. Esa opción es útil para reds con grande número de computadores, evitando tráfico desnecesario de datos.
	5	Deshabilita NCSI – Al habilitar esa opción el equipamiento no detecta más la presencia de Internet, asumiendo que la red IP siempre tiene acceso a la Internet. Sirve para eliminar tentactivas de comunicación del equipamiento con el servidor NCSI o para evitar que el módulo intente enviar correo electrónico por GPRS en el caso de falta de Internet via IP.
	6	Bloquea recibimiento de paquetes de Broadcast e Multicast – Disminui el tráfico de datos en caso de redes con mucha latencia. Habilitar esa opción impide el funcionamiento de la aplicación VIAWEB mobile y o PNP. Permite que el módulo opere en redes con tráfico de datos extremo, pero no es compatible con todas las redes o roteadores TCP/IP.

[056] Servidor Ntp

[056] [__/__/ . . . /__] Servidor ntp (Patrón: a.ntp.br)

Dirección de servidor de sincronismo para el reloj interno de la central. Máximo 30 caracteres. Para deshabilitar el servidor NTP solo es necesario dejar el campo em blanco.

[057] Huso Horario

[057] [__/__] Huso horario Patrón: 13 – Brasília (ETH) 37 – (GPRS)

Código de huso horario para a atualización en el servidor NTP

00	UTC – 12:00	Ilha Baker, Ilha Howland
01	UTC – 11:00	Estados Unidos, Nova Zelândia
02	UTC – 10:00	Estados unidos, Polinésia Francesa
03	UTC – 9:00	Estados unidos, Polinésia Francesa
04	UTC – 8:00	Canadá, Estados Unidos, México
05	UTC – 7:00	Canadá, Estados Unidos, México
06	UTC – 6:00	Chile, estados Unidos, Canadá, Equador
07	UTC – 5:00	**Acre**, Colômbia, Cuba, Haiti, Peru, México
08	UTC – 4:30	Venezuela
09	UTC – 4:00	**Amazonas**, **Rondônia**, **Roraima**, Bolívia e Guiana
10	UTC – 4:00	***Mato Grosso** e **Mato Grosso do Sul**

11	UTC – 3:30	Canadá
12	UTC – 3:00	**Bahia, Amapá, Pará, Alagoas, Ceará, Maranhão, Paraíba, Pernambuco, Piauí, Rio Grande do Norte, Sergipe**
13	UTC – 3:00	***Brasília, Rio Grande do Sul, Santa Catarina, Paraná, São Paulo, Rio de Janeiro, Minas Gerais, Espirito Santo, Goiás, Tocantins,** Argentina, Uruguai
14	UTC – 2:00	**Fernando de Noronha, Ilhas**
15	UTC – 1:00	Portugal, Cabo Verde
16	UTC Tiempo universal	Costa do Marfim, Gana, Libéria
17	UTC + 1:00	Europa Central, Africa Ocidental
18	UTC + 2:00	Africa do Sul, Palestina, Líbia, Ruanda
19	UTC + 3:00	Arabia Saudita, Quênia, Rússia
20	UTC + 3:30	Irão
21	UTC + 4:00	Rússia, Armênia, Geórgia, Emirados Árabes
22	UTC + 4:30	Afeganistão
23	UTC + 5:00	Cazaquistão, Maldivas, Paquistão
24	UTC + 5:30	Índia, Sri Lanka
25	UTC + 5:45	Nepal
26	UTC + 6:00	Bangladesh, Cazaquistão, Butão, Rússia
27	UTC + 6:30	Ilhas Cocos, Myanmar
28	UTC + 7:00	Camboja, Indonésia, Tailândia
29	UTC + 8:00	Austrália, Hong Kong, Indonésia
30	UTC + 9:00	Coreia do Sul, Japão
31	UTC + 9:30	Austrália
32	UTC + 10:00	Rússia, Nova Guiné
33	UTC + 11:00	Ilhas Salomão, Rússia
34	UTC + 12:00	Estados Unidos, França, Rússia
35	UTC + 13:00	Kiribati, Tonga
36	UTC + 14:00	Kiribati
37	Ajusta por red GPRS	Centrales y módulos GPRS
38	NTP deshabilitado	

*** Estados Brasileños con ajuste automático de Horario de Verano.**

[520] Permisión de Accesso a la Navegación Web

[520] [_] Patrón: 0

La VW16ZGPRSIP permite control y configuración a partir de cualquier navegador WEB. El acceso a las páginas es hecho a partir de autenticación básica HTML, sin criptografia. Esta autenticación es segura el suficiente para la mayoría de las aplicaciones en redes **domésticas**. Sin embargo, en los casos en que la red es pública, no confiable o se desea un nivel mayor de monitoreo, se puede deshabilitar o restringir el acceso al navegador WEB.

Valores:

0	Permissão total de acesso, não há restrição para acesso ao navegador WEB.
1	Solamente control. En ese caso, se puede acceder la pantalla de control, pero no es posible alterar las configuraciones.
2	Acceso restringido con llave. En ese modo, el acceso queda totalmente bloqueado. Para liberar el acceso se deve pulsar el botón multifuncional en la placa de la VW16ZGPRSIP de 3 hasta 5 segundos. El acceso es liberado por 30 minutos o hasta la llave ser presionada nuevamente.
3	Acceso bloqueado. No es posible aceder las páginas WEB de la VW16ZGRPSIP.

G P R S

[037 y 038] Selecciona Operadora Sim Card #1 y #2 (Para Teclado de Led)

[037] [ ] Operadora SIM CARD 1 (Patrón : 1)
[038] [ ] Operadora SIM CARD 2 (Patrón : 1)

Cuando la operadora es elegida automaticamente las funciones [042] [043] [044] son programadas por el módulo para el SIM Card 1 y las funciones [542] [543] [544] para el SIM Card 2.

0 – TIM APN: tim.br Usuario: tim Contraseña: tim	4 – Claro Genérica APN:generica.claro.com.br Usuario: claro Contraseña: claro	8 - TMDATA VIVO APN: tmdata.vivo.com.br Usuario: tmdata Contraseña: tmdata	C - Link Solution APN: link.claro.br Usuario: claro Contraseña: claro
1 – Claro **APN: claro.com.br** **Usuario: claro** **Contraseña: claro**	5 – VIVO APN: zap.vivo.com.br Usuario: vivo Contraseña: vivo	9 – Full Time Claro APN: ft.claro.com.br Usuario: claro Contraseña: claro	D - Link Solution APN:linksol.vivo.com.br Usuario: link Contraseña: link
2 - Datatem APN:inlog.vivo.com.br Usuario: datatem Contraseña: datatem	6 - TMDATA Claro APN:tmdata.claro.com.br Usuário: tmdata Contraseña: tmdata	A – Full Time Tim APN: telemetria.tim.br Usuario: tim Contraseña: tim	E – Datatem APN:inlog.claro.com.br Usuario: datatem Contraseña: datatem
3 - Oi APN: gprs.oi.com.br Usuario: oi Contraseña: oi	7 - TMDATA Tim APN: tmdata.tim.br Usuario: tmdata Contraseña: tmdata	B - Grupo Lógico Claro APN: logico.claro.com.br Usuario: LOGICO Contraseña: LOGICO	**A = INF+1** **B = INF+2** **C = INF+3** **D = INF+4** **E = INF+5** **F = INF+6**

[041 y 541] Pin Do Sim Card #1 y #2

[041] [__/__/__/__] PIN del SIM CARD 1 Patrón: 0000
[541] [__/__/__/__] PIN del SIM CARD 2 Patrón: 0000

Contraseña programada en el SIM CARD, para que el VIAWEB reconozca el PIN, insira el chip en un aparato móvil y active el código de seguridad PIN en las configuraciones del móvil.

[042 y 542] Apn Gprs Sim 1 y Sim 2

[042] [_] APN GPRS SIM CARD 1 Patrón: claro.com.br
[542] [_] APN GPRS SIM CARD 2 Patrón: claro.com.br

APN: Nombre del punto de acceso GPRS de la operadora móvil GSM. (máx. 30 caracteres)

[043 y 543] Usuario Gprs Sim 1 y Sim 2
[043] [_] Usuario GPRS SIM CARD 1 Patrón: claro
[543] [_] Usuario GPRS SIM CARD 2 Patrón: claro

Usuario: Fornecido por la operadora móvil GSM para conexión GPRS. (máx. 30 caracteres)

[044 y 544] Contraseña Gprs Sim 1 y Sim 2

[044] [_] Contraseña GPRS SIM CARD 1 Patrón: claro
[544] [_] Contraseña GPRS SIM CARD 2 Patrón: claro

Contraseña: Fornecida por la operadora móvil GSM para autenticación GPRS. (máx. 30 caracteres)

[045 y 545] Número del ICCID del Sim Card 1 y 2 (solamente lectura)

[045] [_] Número del ICCID SIM CARD 1
[545] [_] Número del ICCID SIM CARD 2

Número de identificación del SIM CARD (solamente lectura).

[502 y 503] Kbytes Trafegados Sim Card 1 y 2 (solamente lectura)

[502] [_ _ _ _] KBytes Traficados SIM CARD #1
[503] [_ _ _ _] KBytes Traficados SIM CARD #2

Muestra la cantidad de Kilo Bytes traficados en el SIM CARD.
Programando "0000" o descolgando el equipamiento, se pone a cero el Cuentador.

[046] Versión del Módulo Gprs (solamente lectura)

[046] [_ _ _] versión del módulo

Utilizado solamente para lectura de la versión del módulo.

Comandos Por Sms

- Los 8 números de control pueden ser usados para efectuar y recibir comandos via SMS;
- Para comandos SMS **no** es necesario configurar los parámetros de GPRS;
- Estea seguro que el SIMCARD utilizado está con el servicio de SMS activo;
- Un SMS enviado por un de los 8 teléfonos de control será tratado como comando;
- Más de un comando en el mismo SMS debe ser separado por espacio;

- No es posible enviar comandos de Arme y Desarme en el mismo SMS;
- Se comandos de Armar y Armar Forzado son enviados en el mismo SMS, el arme será hecho en el modo Forzado;
- Si el reloj no está ajustado, los comandos SMS no serán ejecutados;
- Comandos con más de 15 minutos de diferencia en el horario de recibimiento son desconsiderados, sin respuesta;

Ojo.: El monitoreo por SMS permite el envio de más de un evento en el mismo SMS hasta el límite de 140 caracteres.

Ejemplo de retorno de información del SMS:

Sistema VIAWEB:
PART ARMADAS: 1,2,3,4,5,6,7,8 – ARMADO – DESARMADO
Sem AC, prob BAT, falha COM
Zonas disparadas: 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
ZONAS ABERTAS.
ZONAS ABERTAS: .. ..
SISTEMA PRONTO

Comandos que pueden ser enviados por SMS:

I / i	**(Informaciones del sistema)**
E<z> / **e**<z>	**(Excluir <nºzona>)**
A / a	**(Armar no particionado o Particiones default)**
D / d	**(Desarmar no particionado o Partición default)**
A<p> / **a**<p>	**(Armar Partición<NºPartición>)**
D<p> / **d**<p>	**(Desarmar Partición<NºPartición>)**
L<o> / **l**<o>	**(Conectar PGM <NºPGM>)**
L<o><t> / **l**<o><t>	**(Conectar PGM <NºPGM> por el tiempo<t>)**
O<o> / **o**<o>	**(Desconectar PGM<NºPGM>)**
F<p> / **f**<p>	**(Armar Partición <NºPartición> forzado)**
F / f	**(Armar no particionado o Particiones default)**

Obs:. la exclusión de varias zonas en el mismo SMS, es necesario un comando E <z> para cada área excluida, recordando que cada comando debe estar separado por un espacio.

Ex: Eliminar las zonas 1,3,5,8 en el mismo SMS: E1 E3 E5 E8 o e1 e2 e5 e8.

LÍNEA TELEFÔNICA

[481 A 488] NÚMEROS TELEFÓNICOS / NÚMEROS SMS

Son 8 números de control con 12 dígitos cada, se fue menor que 12 dígitos, debe terminar con INF+6(F).

[481] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 1
[482] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 2
[483] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 3
[484] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 4
[485] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 5
[486] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 6
[487] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 7
[488] [__/__/__/__/__/__/__/__/__/__/__/__] Número Telefónico 8

Para mayor seguridad, inicie el número sempre con el DDD.

Ej: **99876543**

ponga:

4199876543, si es de Curitiba y

1199876543 si es de São Paulo

Los cuatro primero números telefónicos de uso general, pueden ser usados para llamar para monitoreo (protocolos Contact-ID e 4+2), para el envio de SMS o sonido de sirena, dependiendo de que esté programado en las secuencias de comunicación. (mirar función [001] a [003] pág.22).

Ojo.: (INF + 6 = F) fin de número, debe ser programado al final de cada número de telefóno.
INF + 1 = “A” Para una pausa de 3 segundos en la llamada (captura de tronco en PABX).
INF + 2 = dígito * (asterisco)
INF + 3 = dígito # (picadillo)
INF + 4 = “D” Para una pausa de 2 segundos en la llamada (captura de tronco en PABX).

El número telefónico 4 [484]

1) Si el callback está habilitado (Función[363], opción 5), entonces el número telefónico que el panel irá llamar para efectuar download será el número 4.

2) SI una de las secuencias de comunicación esté configurada para enviar solamente testes (Funciones [007], [009] ou [011]) y el medio de comunicación es el 34 (sonido de sirena en el número telefónico 4) entonces, el painel de Alarma irá discar en el horario programado para test, pero así que detectar el tono de discar, irá desconectar inmediatamente. Esta facilidad permite que se haga la supervisión de la línea telefónica sin costos de llamada para el cliente.

Ojo: Ver en las cunciones 187 a 194 quales particiones el número irá activar (SMS).

[060] HORARIO DEL PRIMERO TEST DE LÍNEA TELEFÓNICA

[060] [__/__/__/__] Patrón: 00:00

Horario del primero test del dia, en ese momento es reiniciada la contaje de tiempo de intervalo de test. Siempre en este horario la central vá enviar un test.

Para funcionar correctamente el reloj de la central deberá ser ajustado con la hora cierta.

[061] INTERVALO DEL TEST DE LÍNEA TELEFÓNICA

[061] [__/__/__/__] Patrón: 00:00

Define cual será el intervalo entre los testes automáticos de comunicación por la Línea que el panel irá hacer con la central de monitoreo. Ese tiempo puede variar de 1 minuto hasta 99 horas y 59 minutos.

[074] DETECTOR DE LÍNEA TELEFÓNICA

[074] [__/__] Patrón: 01 (Retornovisual en el teclado “LED 8”)

Tecla	Acción
00	Deshabilitado
01	**Retorno visual en el teclado “LED 8” (PATRÓN)**
02	Dispara la sirena cuando la central esté armada
03	Hace con que las zonas silenciosas disparen la sirena si violadas
04	Dispara la Sirena cuando ocurre la falla, independiente del estado de la central

Quando habilitado a central VW16ZGPRSIP verifica a cada 4 segundos a existência da Línea telefónica. A falta da Línea ocorre quando a tensão na Línea for inferior a 4 volts, quando a central detectar um toque de chamada na Línea, o test é suspenso por um minuto.

[058] Intervalo del Test de Línea Cuando la Partición 1 Está Armada

[058] [__/__/__/__] Patrón: 00:00

Se programado con valor diferente de 0000, irá contar el tiempo periodicamente a partir de la hora programada en la función [060]. Se al fin del contaje la partición 1 esté armada, el evento de test de línea será enviado.

[059] Intervalo del Test de Línea Cuando la Partición 1 Está Desarmada

[059] [__/__/__/__] Patrón: 00:00

Se programado con valor diferente de 0000, irá contar el Tiempo periodicamente a partir de la hora programada en la función [060]. Si al fin del contaje la partición 1 esté desarmada, el evento d test de línea será enviado.

Se deseado, el evento de test puede ser enviado también por las otras vias de la placa (GPRS/ETHERNET) habilitando la opción 4 de la función [081] (pág.32).

[081] Opciones de la Línea

Patrón: 1 y 2 (Habilitados)

	Bit/Led	Descrição	Selecionado	Apagado
[081]	**1**	**Tipo de Llamada**	**Tono (DTMF)**	**Pulso**
	2	**Tono de Lamada**	**Habilitado**	**Deshabilitado**
	3	Testes solamente con central armada	Habilitado	Deshabilitado
	4	Envio de Testes	Testes por la Internet	Deshabilitado
	5	Deshabilita envío de Test de línea	No envia test de línea pela sequência 1	Envia test de línea por la secuencia 1
	6	Deshabilita envío de Test de línea	No envia teste de línea pela sequência 2	Envia teste de línea por la secuencia 2
	7	Deshabilita envío de Test de línea	No envia teste de línea pela sequência 3	Envia teste de línea por la secuencia 3

- **Tono – digital:**

En una línea telefónica por tono (multifrecuencia), la marcación de un se número traduce en el envío de señales en distintas frecuencias (sonidos diferentes). la llamada de un número en este tipo de línea es más rápida que en una línea por pulso.

- **Pulso – analógica:**

Los señales de digitación son enviados por una série de pequeños impulsos, separados por espacios. la llamada de los números en este tipo de línea es más lenta.

Tono de llamada: Si habilitado, el sistema espera por lo señal de línea, si no for detectado señal de línea, la central efectua una nueva tentactiva, hasta detectar el tono de línea.

Se deshabilitado la central empieza la llamada mismo sin el tono de línea.

Testes solamente con central armada: Si habilitado el envío del test de línea será hecho solamente si una o más particiones están armadas, caso contrario, el test siempre será enviado. (En la VW10Z a partir de la versión 1.30).

Envío de Testes: En esta función es definido si la central irá enviar test de comunicación [602] por la internet. En los ítems 5, 6 y 7 se define cuales secuencias de comunicación enviarán test de línea.

[086] Opciones de Transmisión

	Descricpción	Tecla/Led
[086]	Benefício de transmisión. Se habilitado aumenta el benefício de la transmisión en los eventos contact-id por la línea telefônica.	1

[075] Retardo na Falla de Línea Telefónica

[075] [__/__/__] Patrón: 000 (minutos)

Si se estabelece el valor 000 el envío de Falla de Línea telefónica o restauración se hará inmediatamente. De lo contrario el detector esperará que la condición de Falla ou restauración de Línea permanece constante los minutos programados antes de enviar el evento. Puede ser programado desde 000 até 255 minutos.

[351] Número de Tonos Para Download

[351] [__/__/__] Patrón: 014

Define cuantos tonos en el teléfono la central aguarda para capturar la conexión del software VIAWEB DOWNLOAD. Es posible ejecutar la programación via software con una secretaria electrónica en la misma línea. Si la secretaria electrónica atiende en el 5º tono de teléfono y la central está programada para atender después de 8 tonos del teléfono será necesário hacer dos llamadas consecutivas para la central atender. La central memoriza el número de tonos por 45 segundos, después del último tono.

[363] Habilita Callback no Download – opción (bit) 5

Patrón: Borrado (Deshabilitado)		Bit/Led
[363]	Cuando efectuar download por Línea telefónica, esa opción hace con que o panel de alarme, después de comprobar la contraseña, desconectar y marcar el número de teléfono da la memória 4 (función[484]) para descargar.	5

[354] Llamada Dupla

[354] [__/__/__] Patrón: 000 (Deshabilitado)

Cuando diferente de zero a central atiende en el primero toque de la segunda llamada, facilitando la conexión. El valor programado es el tiempo máximo en segundos entre una llamada y otra.

Cancelar Llamada

ENT + Contraseña de Programación o Contraseña Master 001/002 + CANC

ZONAS

La VW16ZGPRSIP posee 8 entradas de zona, permitiendo la instalación de hasta 16 zonas distintas. Caso la instalación tenga más que 16 sensores, estes pueden ser agrupados. Si mismo así fue necesario un número mayor de zonas, se puede instalar expansores de zonas, ampliando la capacidad de la central hasta 128 zonas.

OJO: Se recomienda agrupar en el máximo tres (3) sensores en la misma zona. También se recomienda no agrupar sensores con tecnologías de detección diferentes en la misma zona, separando magnéticos, IVPs, Microondas, sensores de barrera, etc...

Instalación de los sensores en las zonas:

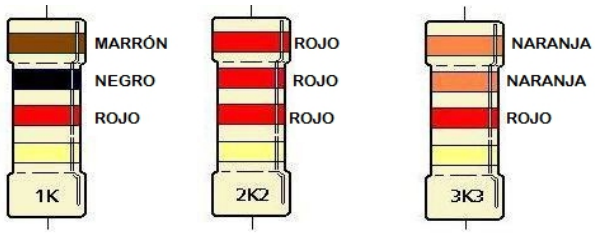
Existem 8 formas diferentes de instalar los sensores en las zonas. La forma de instalación debe estar de acuerdo con el valor de la función 107.

[107] CONFIGURACIÓN DE LAS ZONAS

[107] [__/__] Patrón: 04 (16 zonas normalmente cerradas sin resistor de fin de línea y sin tamper)

El resistor de fin de Línea, cuando instalado, permite que la central detecte falla de tamper (cuando hay rompimiento en el cable del sensor o abertura de la cajaa del sensor) y corto circuito (cuando hay sabotaje en el hilo del sensor).

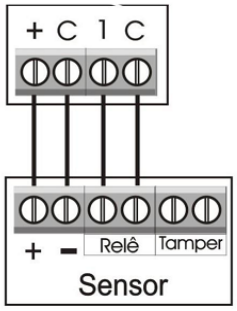
La central posibilita el funcionamiento de 8 o 16 zonas con o sin resistor de fin de línea (RFL).



Esas posibilidades están divididas en 10 diferentes modos:

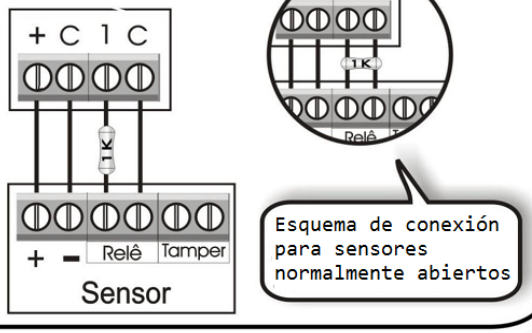
Modo 00 - 8 zonas sin RFL y sin tamper

Esta programación no detecta corto en el cableado y ni tamper, permite que la central de alarma reconosca la abertura y el cerramiento de la zona sin resistor de fin de línea y sin reconocimiento de tamper. No utilize esta programación con sensores normalmente abiertos, pues así la central estará siempre en



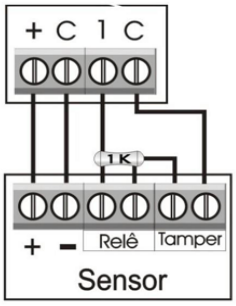
Modo 01 - 8 zonas con RFL y sin tamper

Cuando la instalación no necesita de reconocimiento de támper, pero con detección de corto en el cableado (resistor fin de línea RFL). Los sensores pueden ser normalmente abiertos con un resistor de 1k en paralelo con el relé del sensor.



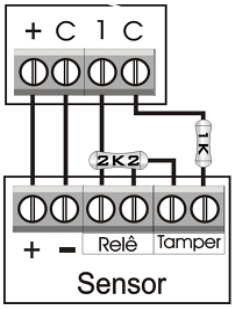
Modo 02 - 8 zonas sin RFL y con tamper

Cuando la instalación necesita de reconocimiento de tamper y sin resistor de fin de línea, eso es posible utilizando un resistor de 1K en paralelo con o rele del sensor. La central irá reconocer la abertura o el corte de línea.



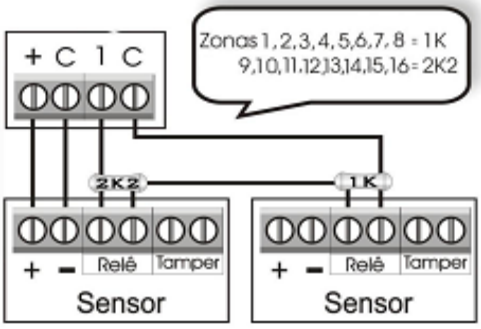
Modo 03 - 8 zonas con RFL y con tamper

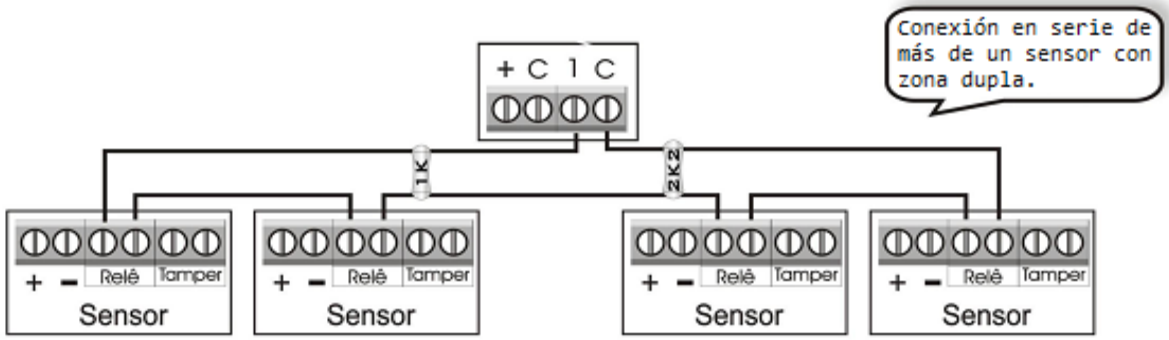
Si la instalación necesita el reconocimiento de tamper y fallas de línea (corto en el cableado) y alarmes, es necesario la utilización de sensores normalmente cerrados, colocando un resistor de 1KΩ en serie con el cableado del alarme y un resistor de 2k2Ω en paralelo con el rele del sensor.



Modo 04-16 zonas sin RFL y sin tamper

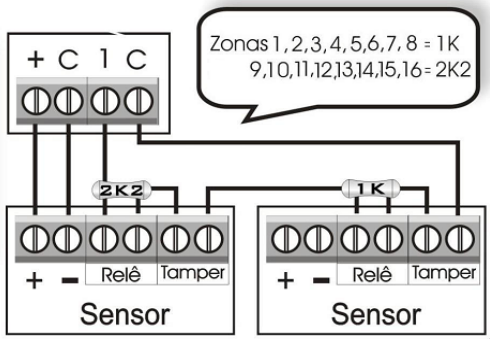
(PATRÓN)
Para la instalación que no necesita el reconocimiento de tamper o falla de línea. Es necesario utilizar sensores normalmente cerrados, para las zonas de 1 a 8 usar resistor de 1k y las zonas de 9 a 16 usar resistor de 2k2. La central va reconocer la abertura y cerramiento de cada una de las 16 zonas.





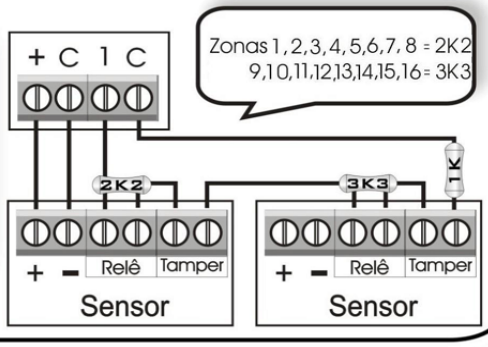
Modo 05 - 16 zonas sin RFL y con tamper

Para utilizar 16 zona con el reconocimiento de tamper: Es necesario utilizar sensores normalmente cerrados. Para las zonas de 1 a 8 usar resistor de 1 k en paralelo con el relé del sensor y las zonas de 9 a 16 usar resistor DE 2k2 en paralelo con el relé del sensor. La central va reconocer la abertura y cerramiento de cada una de las 16 zonas y cortes en el cableado.



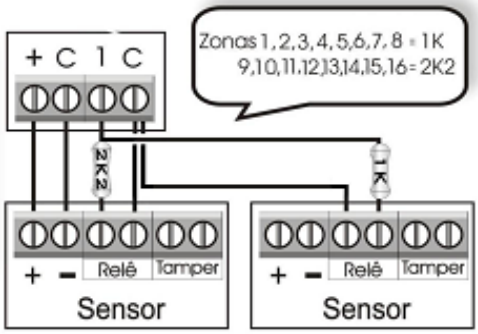
Modo 06 - 16 zonas con RFL y con tamper

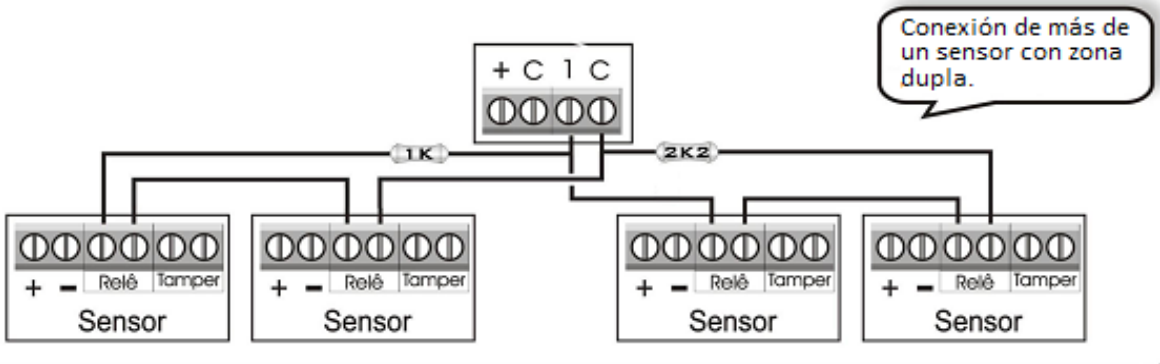
Para que la central reconozca el tamper y falla de línea (corto en el cableado) necesita ser puesto un resistor de 1K en serie con la entrada de la zona y utilizar un resistor de 2k2 en paralelo para las zonas de 1 a 8 y para las zonas 9 a 16 o resistor de 3k3 en paralelo no relé de los sensores.

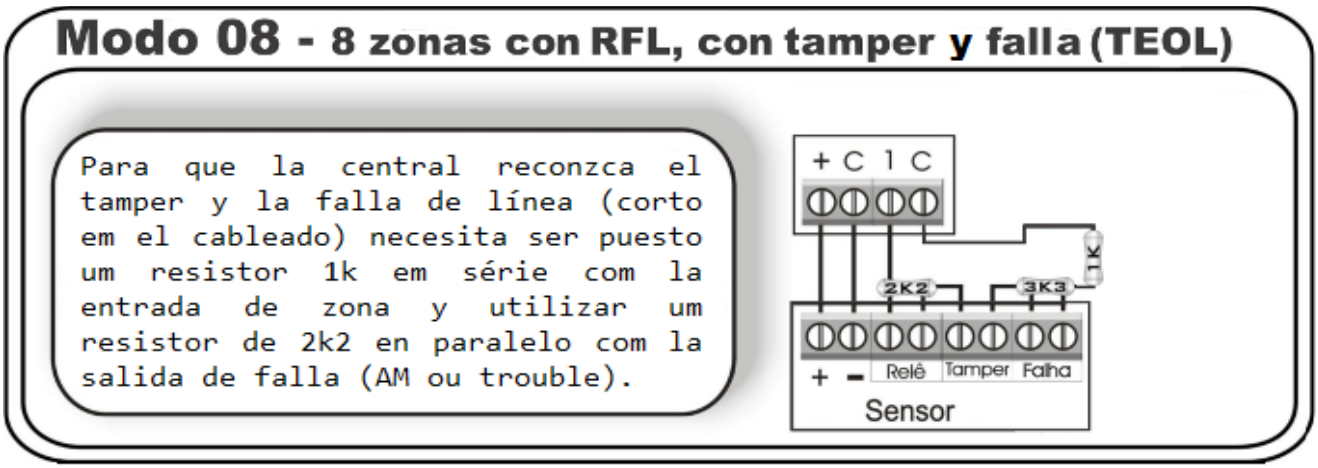


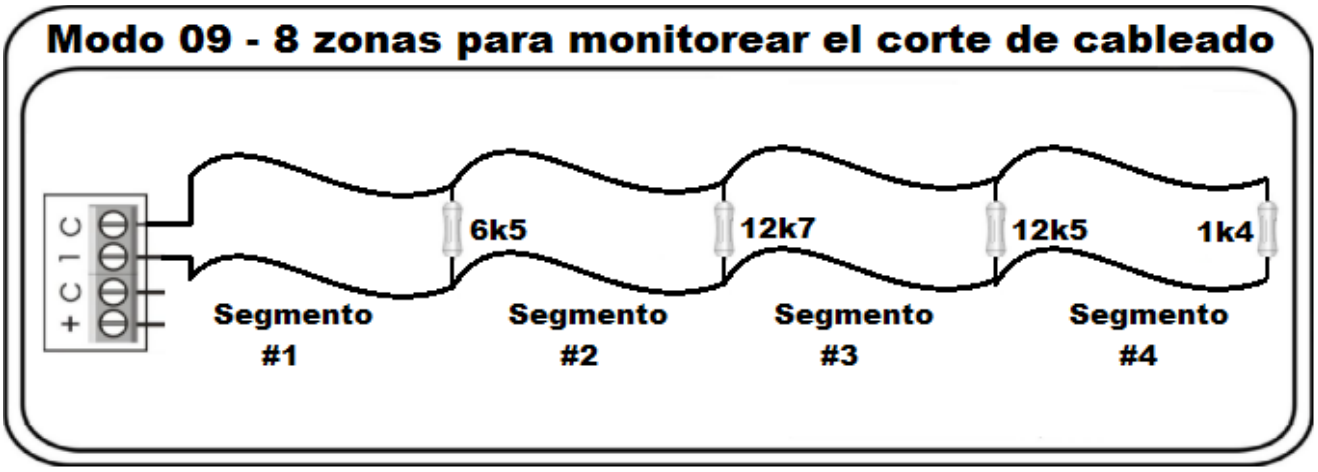
Modo 07 - 16 zonas con RFL y sin tamper

Para instalación que no necesita el reconocimiento de tamper: es necesario utilizar sensores normalmente cerrados, para las zonas de 9 a 16 usar un resistor de 2k2. La central va reconocer la abertura y cerramiento de cada una de las 16 zonas.









MODO 9

El modo 9 es una forma especial de uso de las áreas. Desarrollado específicamente para supervisar corte de cables, permite detectar en cuál de los 4 segmentos se cortó el cable.

Debe configurar las zonas para trabajaren 24 horas con restaurauro (opciones 4 e 7 de las funciones 091-098). Si lo desea, puede inhibir la activación de la sirena, configurando la zona silenciosa (Opción 5).

Posee supervisión de corto, generando evento de falla de corto caso el cable monitoreado estea en circuito.

Para cada segmento cortado un evento es generado:

Segmento #4: Disparo de la zona
Código programado en las funciones 402 hasta 409. Restauro programado en las funciones 442 a 449.

Segmento #3: Disparo de la zona alta (equivalente al TROUBLE del modo 8)
Código programado en las Funciones 410 a 417. Restauro programado en las funciones 450 hasta 457.

Segmento #2: Evento de falla de loop
Código programado en la función 477. Restauro programado en la función 478.

Segmento #1: Falla de Tamper
Código programado en la función 418. Restauro programado en la función 458.

Corto-circuito:
Código programado en las funciones 432. Restauro programado en las funciones 467.

[108] Velocidad de las Zonas

[108] [__/__/__] Patrón: 005 (0,5 segundos)

Tiempo en décimos de segundo, para que la central reconozca la abertura o cerramiento de las zonas, el tiempo puede variar de 001 hasta 020.

[091 a 106] Tipo de las Zonas

Para facilitar la instalação, la zona 1 ya viene programada como temporizada. Todas las zonas tienen la opción “Auto Exclusión” habilitada por Patrón.

Patrón: 8 - Auto Exclusión	Bits/Leds							
[091] Tipo de la Zona 1	**1**	2	3	4	5	6	7	**8**
[092] Tipo de la Zona 2	1	2	3	4	5	6	7	**8**
[093] Tipo de la Zona 3	1	2	3	4	5	6	7	**8**
[094] Tipo de la Zona 4	1	2	3	4	5	6	7	**8**
[095] Tipo de la Zona 5	1	2	3	4	5	6	7	**8**
[096] Tipo de la Zona 6	1	2	3	4	5	6	7	**8**
[097] Tipo de la Zona 7	1	2	3	4	5	6	7	**8**
[098] Tipo de la Zona 8	1	2	3	4	5	6	7	**8**
[099] Tipo de la Zona 9	1	2	3	4	5	6	7	**8**
[100] Tipo de la Zona 10	1	2	3	4	5	6	7	**8**
[101] Tipo de la Zona 11	1	2	3	4	5	6	7	**8**
[102] Tipo de la Zona 12	1	2	3	4	5	6	7	**8**
[103] Tipo de la Zona 13	1	2	3	4	5	6	7	**8**
[104] Tipo de la Zona 14	1	2	3	4	5	6	7	**8**
[105] Tipo de la Zona 15	1	2	3	4	5	6	7	**8**
[106] Tipo de la Zona 16	1	2	3	4	5	6	7	**8**

[1] – Temporizada 1
[2] – Temporizada 2
[3] – Preventiva
[4] – 24 Horas
[5] – Silenciosa
[6] – Control Remoto
[7] – Restauro
[8] – Auto Exclusión

[1 e 2] – Seguidora

[2 e 6] – Zona deshabilitada

[5 e 6] - Entrada “Anti-Secuestro”

[4, 5 e 6] – Anti-Invasión

[4, 5 e 7] – Pánico

Dentro de cada función seleccione el tipo de la zona con las teclas de 1 hasta 8 (led aceso: tipo seleccionado).

A seguir, una descripción con detallada de cada opción:

INSTANTANEA – TODAS LAS OPCIONES BORRADAS

Cuando ningún led este encendido, la zona dispara inmediatamente después de la abertura, si la central esté armada.

TEMPORIZADA 1 – OPCIÓN 1

La zona posee dos temporizaciones, entrada 1 y salida 1.

Tiempo de Entrada: Tiempo que el usuario tiene para desarmar el sistema vía teclado antes que el mismo genere el disparo de la zona.

Tiempo de Salida: Tiempo que el usuario tiene para salir del sitio después de armar el sistema.

[121 y 123] Tiempo de Entrada y Salida 1

[121] [__/__/__] Tiempo de Entrada 1 Patrón: 010 segundos
[123] [__/__/__] Tiempo de Salida 1 Patrón: 030 segundos

El tiempo puede variar de 001 hasta 255 segundos.

TEMPORIZADA 2 – OPCIÓN 2

La zona posee dos Temporizaciones, entrada 2 y salida 2.

Tiempo de Entrada: Tiempo que el usuario tiene para desarmar el sistema via teclado antes que el mismo genere el disparo de la zona.

Tiempo de Salida: Tiempo que el usuario tiene para salir del sitio después de armar el sistema.

[122 y 124] Tiempo de Entrada y Salida 2

[122] [__/__/__] Tiempo de Entrada 2 Patrón: 020 segundos
[124] [__/__/__] Tiempo de Salida 2 Patrón: 040 segundos

El Tiempo puede variar de 001 hasta 255 segundos.

[120] Particiones Que Hacen Pitidos Durante la Temporización

Patrón: Todos encendidos (Habilitados)	Bit / Led / Part.							
[120] Particiones que hacen pitidos	1	2	3	4	5	6	7	8

Si la instalación cuenta con los teclados, estos pueden señalizar a través de pitidos cuando una zona este temporizando. Los teclados hacen pitidos que indican la hora de salida sólo si hay una o más zonas de VW16ZGPRSIP temporizando y hacen pitidos el tiempo de entrada cuando se viola cualquier zona temporizada.

SEGUIDORA – OPCIÓN 1 y 2

Si una zona seguidora abrir sin que ninguna otra zona esté temporizando, su disparo es inmediato, caso contrario irá temporizar juntamente con la otra zona. Al armar el sistema las zonas seguidoras siguen el tiempo de salida #1.

PREVENTIVA – OPCIÓN 3

Previne alarmas falsas. Las zonas programadas como preventivas operan en conjunto, ellas solamente disparan si durante un determinado período de tiempo:

Abrieren más de una vez; Permanecieren abiertas; dos o más zonas abrieren.

El tiempo es programado en la función [127]. No se debe programar la zona como preventiva si el sensor es del tipo magnético o sensor de barrera.

[127] Tiempo de Zona Preventiva

[127] [__/__/__] Patrón: 045 segundos

El tiempo puede variar de 001 hasta 255 segundos.

24 HORAS – OPCIÓN 4

Al ser abierta, siempre genera disparo, independiente si la central o partición está armada. Esta característica permite programar botones de pánico o proteger áreas dónde nunca debe haber violación (como sensores de barrera en muros, por ejemplo).

SILENCIOSA – OPCIÓN 5

Al disparar, no toca la sirena, solamente genera disparo en el teclado y envia evento. Esta característica habilitada en conjunto con la opción “24 horas” y el “Restauro” permite programar botones de pánico silencioso.

CONTROL REMOTO – OPCIÓN 6

La zona funciona como llave para armar y desarmar el sistema. Se puede instalar una llave o receptor de control remoto, desde que los contatos sean del tipo NF (normalmente cerrado). La llave o receptor debe ser instalado de la misma forma que un sensor de alarma. Cualquier una de las zonas de la VW16ZGPRSIP puede ser configurada como control remoto.

En ese caso el número de la zona se torna el usuario del sistema. Por ejemplo, si la zona 8 es programada para control remoto, tendremos la información de que el usuario 8 fue quién armó o desarmó el sistema. Caso el sistema sea particionado, entonces debe configurar Cuales particiones el control remoto puede armar o desarmar.

[187 a 202] Particiones de Control Remoto

Patrón: Partición 1	Bit / Led / Part.							
[187] Particiones del Control Remoto Zona 1	**1**	2	3	4	5	6	7	8
[188] Particiones del Control Remoto Zona 2	**1**	2	3	4	5	6	7	8
[189] Particiones del Control Remoto Zona 3	**1**	2	3	4	5	6	7	8
[190] Particiones del Control Remoto Zona 4	**1**	2	3	4	5	6	7	8
[191] Particiones del Control Remoto Zona 5	**1**	2	3	4	5	6	7	8
[192] Particiones del Control Remoto Zona 6	**1**	2	3	4	5	6	7	8
[193] Particiones del Control Remoto Zona 7	**1**	2	3	4	5	6	7	8
[194] Particiones del Control Remoto Zona 8	**1**	2	3	4	5	6	7	8
[195] Particiones del Control Remoto Zona 9	**1**	2	3	4	5	6	7	8
[196] Particiones del Control Remoto Zona 10	**1**	2	3	4	5	6	7	8
[197] Particiones del Control Remoto Zona 11	**1**	2	3	4	5	6	7	8
[198] Particiones del Control Remoto Zona 12	**1**	2	3	4	5	6	7	8
[199] Particiones del Control Remoto Zona 13	**1**	2	3	4	5	6	7	8
[200] Particiones del Control Remoto Zona 14	**1**	2	3	4	5	6	7	8
[201] Particiones del Control Remoto Zona 15	**1**	2	3	4	5	6	7	8
[202] Particiones del Control Remoto Zona 16	**1**	2	3	4	5	6	7	8

Cuando una zona es programada para control remoto, Se programa cual de las particiones el control va operar.

Entre en la función correspondiente a la zona em que está conectado el receptor.

Para seleccionar una o más particiones pulse la tecla correspondiente a la partición.

El led encendido indica partición seleccionada, pulse ENT para confirmar.

Se puede usar teléfonos como control remoto (pág. 31).

En ese caso las funciones **[187 a 194]** serán usadas para seleccionar cuales particiones cada número telefónico irá accionar.

RESTAURO – OPCIÓN 7

Restaura la zona y envia el evento de restauro luego después del cerramiento. Si no for habilitado, el restauro es enviado solamente cuando la sirena parar de tocar.

ANTI-SECUESTRO – OPCIÓN 5 E 6

Cuando una zona es abierta con la característica “anti-Secuestro”, una contraseña precisa ser digitada en el teclado o un control remoto accionado durante el tiempo de “anti- Secuestro” Función [125]. Caso eso no ocurra, la central irá reportar el evento de COACCIÓN. Función [422].

[125] Tiempo de Zona Anti-Secuestro

[125] [__/__/__] Patrón: 000 segundos (Anti-Secuestro deshabilitada)

Tiempo (de 000 à 255 segundos) antes de enviar disparo de la zona caso una zona anti-Secuestro tenga sido abierta.

ANTI-INVASIÓN – OPCIÓN 4, 5 E 6

La zona anti-Invasión funciona en conjunto con la zona anti-secuestro. Después de abrir la zona anti-secuestro, es posible violar la zona anti-Invasión una vez, sin que genere disparo. Si hay una nueva abertura o la zona permanecer abierta por el tiempo de zona anti-Invasión, dispara eç sistema.

[126] Tiempo de Zona Anti-Invasión

[126] [__/__/__] Patrón: 000 segundos

Tiempo en segundos que la zona anti-Invasión puede quedar abierta sin generar disparo.

Las zonas anti-secuestro e anti-invasión permiten que se monte un sistema de seguridad para llegada de coches en una caseta de vigilancia de condominio. Al se aproximar del local, el morador acciona el control remoto abriendo la zona anti-secuestro. Una barrera instalada en la zona anti-invasión, irá permitir el pasaje del vehículo, sin generar disparo. Caso alguien aproveche la abertura de la puerta principal para entrar, antes o después del vehículo, hará con que la zona anti-invasión dispare.

De la misma forma, si el usuario accionó la zona anti-secuestro, pero no desarmó el sistema en el tiempo programado, un evento de coacción es generado, indicando que el usuario no consiguió llegar en seguridad.

La zona anti-Invasión también puede ser instalada en la puerta principal, para evitar que se olvide abierta.

AUTO EXCLUSIÓN – OPCIÓN 8

La zona que disparar, consecutivamente, en el mismo período de armado, el número de veces de la función [113], será automáticamente anulada. El evento de auto exclusión de zona es enviado.

[113] Número de Disparos Para Auto Exclusión

[113] [__/__/__] Patrón: 005

Número de veces consecutivas que una zona, configurada con auto Exclusión, debe disparar dentro del tiempo de armado para ser automáticamente anulada. Si alguna otra zona disparar, reinicia el contaje de disparos.

El número de disparos puede variar de 001 hasta 255.

[109 y 110] Zonas Com Chime

Patrón:Todos Borrados (Deshabilitados)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Bit / Led**
[109] Chime en las Zonas (1 – 8)	1	2	3	4	5	6	7	8	**Zona**
[110] Chime en las Zonas (9 – 16)	9	10	11	12	13	14	15	16	

Define cuales as zonas que podrán funcionar también como anunciador de presencia. Todas las zonas que son programadas con el anunciador de presencia habilitado podrán emitir un señal sonoro en los teclados toda vez que son abiertas. En los teclados de LED para que emita un señal de una determinada zona, fuera del modo de programación, mantenga presionada la tecla correspondiente a zona hasta oír un bip de OK, repita el proceso para desconectar el señal.

[111 y 112] Zonas Sin Exclusión

Patrón:Todos Borrados (Deshabilitados)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Bit / Led**
[111] Zonas sin exclusión (1 – 8)	1	2	3	4	5	6	7	8	**Zona**
[112] Zonas sin exclusión (9 – 16)	9	10	11	12	13	14	15	16	

Impide que esas zonas sean excluidas al armar el sistema.

[114 y 115] Zonas Cruzadas

Patrón:Todos Borrados (Deshabilitados)	1	2	3	4	5	6	7	8	Bit / Led
[114] Zonas cruzadas (1 – 8)	1	2	3	4	5	6	7	8	Zona
[115] Zonas cruzadas (9 – 16)	9	10	11	12	13	14	15	16	

Una zona cruzada, solamente genera disparo si es violada en conjunto con una o más zonas cruzadas del mismo equipamiento. O sea, si la zona for programada como “cruzada” solamente genera disparo si en el momento de la violación, otras zonas “cruzadas” están violadas. Caso el número de zonas cruzadas violadas es inferior al mínimo necesario (Función 116), la zona abre sin generar disparo. Caso alguna otra zona cruzada ya tenga disparado, entonces las otras zonas cruzadas irán disparar independiente del número de zonas abiertas.

[116] Número de Zonas Cruzadas Abiertas Para Disparo

[116] [__/__/__] Patrón: 000

Indica cuantas zonas cruzadas (Funciones [114] e [115]) necesitan abrir al mismo tiempo para disparar.

[119] Zona Olvidada Abierta (Zona 2)

[119] [__/__/__ /__] Patrón: 0000 (MM:SS - Recurso deshabilitado)

En esa función se programa el tiempo (en minutos y segundos) en que la zona 2 puede permanecer abierta. Si la zona 2 permanecer abierta allá del tiempo programado, el evento programado en el campo [423] es enviado. El campo partición del evento será la partición de la zona 2 y el campo zona será 002.

[423] Zona Olvidada Abierta – Código Contact ID

[423] [__/__ /__/__] Patrón: 0000 (evento deshabilitado)

Quatro dígitos com o código Contact ID do evento.

[117 y 118] Inversión del Estado de las Zonas

Patrón:Todos Borrados (Deshabilitados)	1	2	3	4	5	6	7	8	Bit / Led
[117] Invierte zonas (1 – 8)	1	2	3	4	5	6	7	8	Zona
[118] Invierte zonas (9 – 16)	9	10	11	12	13	14	15	16	

Si la opción esté habilitada, ocurre la inversión del estado de la zona. La zona abierta será considerada cerrada y la zona cerrada será considerada abierta. No hay alteración en el modo de conexión de las zonas o en los estados de tamper, corte y corto.

[701 a 828] Nombre de las Zonas

[701 a 828] [__/__/ . . . /__] 16 caracteres Patrón: Setor xxx (donde xxx es el número del setor)

Ese es el nombre dado a las zonas que componen la VW16ZGPRSIP. Es enviado cuando el usuario recibe un correo electrónico, o cuando accede la central por el Navegador de Internet.

CONTRASEÑAS

La VW16ZGPRSIP posee 100 contraseñas de usuario, cada contraseña de usuario puede ter acceso a cualquier una de las ocho particiones del sistema. Eso significa que es posible tener contraseñas que arman una partición, contraseñas que arman todas las particiones o mismo contraseñas que no arman partición alguna.

Las contraseñas representan los usuarios del sistema, siendo la contraseña 1 para el usuario 001, Contraseña 2 para el usuario 002 y así sucesivamente.

Algunos periféricos como teclados pueden incluir más usuarios al sistema, que puede ser expandido para hasta 999 usuarios. Eses usuarios pueden ter contraseñas adicionales, controles remotos o tarjetas de acceso.

Las contraseñas son usadas en los teclados, software VIAWEB mobile o navegador WEB, para armar, desarmar o inhibir zonas do sistema.

REGISTRANDO CONTRASEÑAS

El registro de nuevos usuarios puede ser hecho vía teclado o vía navegador **WEB**. Los usuarios 1 y 2 son considerados usuarios “maestros”, solamente eses usuarios pueden registrar nuevos usuarios. En el patrón de fábrica, el usuario 1 viene con la Contraseña “1515” (o “151515” si configurado para 6 dígitos) y el usuario 2 no posee contraseña.

REGISTRANDO CONTRASEÑAS POR TECLADO

Para registrar nuevos usuarios por teclado, ejecute la secuencia:

ENT (Contraseña maestra 1 o 2) ENT

Si la contraseña es correcta, se oye un pitido de OK y el teclado entra en el modo de registro.

Digita el número del usuario con 3 dígitos (001 hasta 100). En seguida, digita la contraseña que este usuario irá utilizar, o pulsa CANCELAR para borrar la contraseña de este usuario.

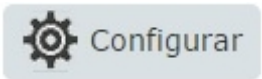
(número del usuario) (contraseña de 4, 5 o 6 dígitos)

Si el código del usuario fue registrado correctamente, se oye un pitido de OK. Se puede repetir la secuencia: “número del usuario”, “código del usuario” hasta que todos los usuarios sean registrados. Al fin del proceso de registro se debe pulsar **ENTER** para salir del modo de registro.

Ejemplos:

1) Registrar usuario maestro 2: **ENTER 1515 ENTER 002 1234 ENTER**
2) Alterar usuario maestro 1: **ENTER 1515 ENTER 001 4321 ENTER**
3) Cancelar usuario 3: **ENTER 4321 ENTER 003 CANCELAR**
4) Registrar 2 usuarios: **ENTER 4321 ENTER 004 4444 005 5555 ENTER**

REGISTRANDO CONTRASEÑAS VIA PÁGINA WEB

Abra o navegador WEB, clique em “ 

“ e em seguida “  “;

[220] Número de Dígitos de las Contraseñas

[220] [_] Patrón: 4 dígitos

Define cuantos dígitos tendrán las contraseñas, si 4, 5 o 6 dígitos. Esa función afecta todas las contraseñas, (Programación, Maestra y de Usuarios).
Ojo.: La contraseña de download siempre tendrá 6 dígitos.

[221] Contraseña de Programación

[221] [__/__/__/__/__/__] Patrón: 535353

La contraseña de programación permite alterar todas las funciones de la central. (zonas, particiones, Sirena, llamada, download), pudiendo ser de 4, 5 o 6 dígitos, de acuerdo con la función [220].

[363] Inibir Contraseña de Programación Cuando Central Está Armada - (Bit) 2

Patrón: Borrado (Deshabilitado)		**Bit/Led**
[363]	Si habilitado, la contraseña de programador solamente irá funcionar si todas las particiones estén desarmadas. De esa forma se puede impedir que el usuario altere la programación vía teclado si la central esté armada.	**2**

[222 a 321] Particiones que el Usuario Tiene Acceso (001 a 100)

Patrón: Partición 1	**Led \ Bit \ Partión**							
[222 a 231] Usuarios de 001 hasta 010	**1**	2	3	4	5	6	7	8
[232 a 241] Usuarios de 011 hasta 020	**1**	2	3	4	5	6	7	8
[242 a 251] Usuarios de 021 hasta 030	**1**	2	3	4	5	6	7	8
[252 a 261] Usuarios de 031 hasta 040	**1**	2	3	4	5	6	7	8
[262 a 271] Usuarios de 041 hasta 050	**1**	2	3	4	5	6	7	8
[272 a 281] Usuarios de 051 hasta 060	**1**	2	3	4	5	6	7	8
[282 a 291] Usuarios de 061 hasta 070	**1**	2	3	4	5	6	7	8
[292 a 301] Usuarios de 071 hasta 080	**1**	2	3	4	5	6	7	8
[302 a 311] Usuarios de 081 hasta 090	**1**	2	3	4	5	6	7	8
[312 a 321] Usuarios de 091 hasta 100	**1**	2	3	4	5	6	7	8

Se programa para cada contraseña, cuales las particiones ella tendrá acceso para armar o desarmar. Para sistema no particionado la partición 1 deberá ser utilizada para permitir acceso

[601 a 700] Nombre de los Usuarios

[601 a 700] [__/__/ . . .] (16 caracteres) Patrón: Usuario xxx (dónde xxx Es el número del usuario).

El nombre registrado aquí es enviado cuando el usuario recibe un correo electrónico, o cuando accede a la central por lo Navegador de Internet.

[348] Contraseña de Coacción

Patrón: Borrado (Deshabilitado)		Led / Bit
[348]	Habilita contraseña 100 del **panel de Alarma** como contraseña de coacción. La contraseña 100 pasa a operar como contraseña de coacción, arma y desarma el sistema, todas las particiones, y envía evento de coacción. **(E121)**	**1**
	Habilita **todas** las contraseñas del **panel de Alarma** para coacción. Cualquier contraseña que, al ser digitada, tenga los dos últimos dígitos invertidos, genera coacción. La contraseña continua armando y desarmando. Ej : Contraseña **1 2 3 4**, al ser digitado **1 2 4 3** será generado evento de coacción. **Ojo.:** Para evitar conflictos de contraseñas iguales se debe habilitar ese modo antes de registrar los códigos de las contraseñas.	**2**

Coacción es cuando el usuario es “forzado” a desarmar la central. En ese momento el usuario puede digitar la contraseña de coacción para que el sistema desarme y al mismo tiempo envíe un evento de coacción. El evento de coacción es programado en la función [422], evento 1121 es el patrón de fábrica para esa función.

[352] Contraseña de Download

[352] [__/__/__/__/__/__] Patrón: 363636 (6 dígitos)

La Contraseña de download es la contraseña que permite la programación de la central via cable serial o por línea telefónica utilizando el software VIAWEB download. La contraseña que está en la central debe ser la misma del computador.

[322 a 334] Contraseñas que Arman Forzado (Away)

El arme forzado solamente es posible usando los teclados Graph, 128s, 128b o Touch.

Patrón: Deshabilitado todos os leds borrados	1	2	3	4	5	6	7	8	Bit
[322] Contraseñas que Arman Forzado (AWAY)	001	002	003	004	005	006	007	008	Usuario
[323] Contraseñas que Arman Forzado (AWAY)	009	010	011	012	013	014	015	016	
[324] Contraseñas que Arman Forzado (AWAY)	017	018	019	020	021	022	023	024	
[325] Contraseñas que Arman Forzado (AWAY)	025	026	027	028	029	030	031	032	
[326] Contraseñas que Arman Forzado (AWAY)	033	034	035	036	037	038	039	040	
[327] Contraseñas que Arman Forzado (AWAY)	041	042	043	044	045	046	047	048	
[328] Contraseñas que Arman Forzado (AWAY)	049	050	051	052	053	054	055	056	
[329] Contraseñas que Arman Forzado (AWAY)	057	058	059	060	061	062	063	064	
[330] Contraseñas que Arman Forzado (AWAY)	065	066	067	068	069	070	071	072	
[331] Contraseñas que Arman Forzado (AWAY)	073	074	075	076	077	078	079	080	
[332] Contraseñas que Arman Forzado (AWAY)	081	082	083	084	085	086	087	088	
[333] Contraseñas que Arman Forzado (AWAY)	089	090	091	092	093	094	095	096	
[334] Contraseñas que Arman Forzado (AWAY)	097	098	099	100	-	-	-		

Los usuarios que han permitido que las contraseñas (led on) aquí puedan armarlas ignorando las áreas abiertas del panel de control. Estas zonas sólo se activarán si restaura y vuelve a abrir después de la activación. El evento de disparo forzado (función [474], por patrón: 3456) se envía junto con el evento de activación. La activación forzada sólo puede realizarse en los teclados con LCD (opción en el menú LCD).

[335 a 347] Contraseñas que no Excluyen Zonas

Patrón: Deshabilitado todos os leds borrados	1	2	3	4	5	6	7	8	Bit
[335] Contraseñas que no Excluyen Zonas	001	002	003	004	005	006	007	008	Usuario
[336] Contraseñas que no Excluyen Zonas	009	010	011	012	013	014	015	016	
[337] Contraseñas que no Excluyen Zonas	017	018	019	020	021	022	023	024	
[338] Contraseñas que no Excluyen Zonas	025	026	027	028	029	030	031	032	
[339] Contraseñas que no Excluyen Zonas	033	034	035	036	037	038	039	040	
[340] Contraseñas que no Excluyen Zonas	041	042	043	044	045	046	047	048	
[341] Contraseñas que no Excluyen Zonas	049	050	051	052	053	054	055	056	
[342] Contraseñas que no Excluyen Zonas	057	058	059	060	061	062	063	064	
[343] Contraseñas que no Excluyen Zonas	065	066	067	068	069	070	071	072	
[344] Contraseñas que no Excluyen Zonas	073	074	075	076	077	078	079	080	
[345] Contraseñas que no Excluyen Zonas	081	082	083	084	085	086	087	088	
[346] Contraseñas que no Excluyen Zonas	089	090	091	092	093	094	095	096	
[347] Contraseñas que no Excluyen Zonas	097	098	099	100	-	-	-		

Estas contraseñas no pueden excluir zonas cuando habilitadas.

[349 y 350] Usuários Tiemporários (Contraseñas 029 y 030)

[349] [__/__/__] Tiempo de duración del usuario 29 Patrón:000 (deshabilitado)
[350] [__/__/__] Tiempo de duración del usuario 30 Patrón:000 (deshabilitado)

Duración (desde 000 hasta 255 horas) de las contraseñas para usuarios temporales (29 y 30).
El valor 000 indica que la contraseña no es una contraseña temporal.
Configure estos campos con la duración (en horas) de la contraseña.
El tiempo empieza a contar inmediatamente después de configurar la función.

[387 a 399] Contraseñas con Horario Restringido

Patrón: Deshabilitado todos os leds borrados	1	2	3	4	5	6	7	8
[387] Contraseñas con Horario restringido 1 a 8	001	002	003	004	005	006	007	008
[388] Contraseñas con Horario restringido 9 a 16	009	010	011	012	013	014	015	016
[389] Contraseñas con Horario restringido 17 a 24	017	018	019	020	021	022	023	024
[390] Contraseñas con Horario restringido 25 a 32	025	026	027	028	029	030	031	032
[391] Contraseñas con Horario restringido 33 a 40	033	034	035	036	037	038	039	040
[392] Contraseñas con Horario restringido 41 a 48	041	042	043	044	045	046	047	048
[393] Contraseñas con Horario restringido 49 a 56	049	050	051	052	053	054	055	056
[394] Contraseñas con Horario restringido 57 a 64	057	058	059	060	061	062	063	064
[395] Contraseñas con Horario restringido 65 a 72	065	066	067	068	069	070	071	072
[396] Contraseñas con Horario restringido 73 a 80	073	074	075	076	077	078	079	080
[397] Contraseñas con Horario restringido 81 a 88	081	082	083	084	085	086	087	088

[398] Contraseñas con Horario restringido 89 a 96	089	090	091	092	093	094	095	096
[399] Contraseñas con Horario restringido 97 a 100	097	098	099	100	-	-	-	

Las contraseñas que tengan esa opción habilitada solamente irán funcionar en los días y horarios determinados en las Funciones 047, 048, 049, 050 e 400.

[047 a 050] Horario de Funcionamento de las Contraseñas con Horario Restringido

Patrón: 00:00

[047] [__/__ : __/__] Inicio del Primero Horario de Funcionamiento de las Contraseñas

[048] [__/__ : __/__] Fin del Primero Horario de Funcionamiento de las Contraseñas

[049] [__/__ : __/__] Inicio del Segundo Horario de Funcionamiento de las Contraseñas

[050] [__/__ : __/__] Fin del Segundo Horario de Funcionamento de las Contraseñas

Las contraseñas habilitadas en las funciones 387 a 399 solamente irán operar durante un de los dos intervalos de horario programados en esas funciones.

[400] Días de la Semana de Funcionamiento de las Contraseñas con Horario Restringido

[400] Días de la Semana de las Contraseñas (Deshabilitado)								
	Dom	Lun	Mar	Miér	Jue	Vier	Sáb	
Tecla/Led	1	2	3	4	5	6	7	8

Contraseñas habilitadas en las funciones 387 hasta 399 pueden tener días de la semana definidos para funcionar, siendo tecla 1 para domingo, 2 para lunes, 3 para martes hasta 7 para el sábado.

En los días habilitados en esa función, las contraseñas solamente irán funcionar durante un de los intervalos programados en las funciones 047 a 050.

Para los otros días de la semana, las Contraseñas pueden no funcionar o funcionar el día todo, dependiendo del valor habilitado en la opción 8. Siendo:

Opción 8 habilitada – En los otros días, las contraseñas funcionan el día todo.

Opción 8 deshabilitada – En los otros días, las contraseñas no funcionan.

PARTICIONES

[204] Sistema Particionado

Patrón: **Borrado (Deshabilitado)**		**Bit/Led**
[204]	Sistema particionado	**1**
	Partición 2 como partición interna	**2**

Sistema particionado (opción 1):

Cuando está habilitado, permite la partición del sistema. Es posible definir qué contraseñas operarán cada partición, y qué áreas van a ser parte de esas particiones. El panel tiene 8 particiones con funcionamiento independiente. Si el sistema no está particionado, todas las zonas se asignan automáticamente a la partición 1.

Partición 2 como partición interna (opción 2):

Al armar la partición 1, la partición 2 espera movimiento en las zonas de partición 1 durante el tiempo de salida 1 (función 123). Si una o más zonas de la partición 1 se abren durante ese tiempo, la partición 2 se armará automáticamente. Si no hay movimiento en ninguna zona de la partición 1, la partición 2 no se armará.

Si al final del tiempo de espera, la partición 1 está alarmada, la partición 2 no se armará.

Al desarmar la partición 1, la partición 2 se desarmará también.

La partición 2 todavía puede ser armada o desarmada por otros medios (contraseñas, control remoto,
Etc ...)

Utilización:

Cuando el usuario arma la partición 1 y sale de la ubicación (violando las zonas temporizadas de la partición 1), la partición 2 entiende que no hay personas en el área interna y la activa automáticamente.

Cuando el usuario arma la partición 1, pero permanece en su lugar (no se mueve a áreas externas y no viola ninguna zona de partición 1), la partición 2 permanece desarmada.

Si el usuario configura la partición 1 y se produce un disparo (violación de una zona no temporizada por ejemplo), la partición 2 permanecerá desarmada para evitar más disparos no deseados.

Si alguna zona de la partición 2 se olvida abierta, se producirá un disparo después del armado de la partición 2.

Ajustes:

Esta opción debe activarse junto con la opción 1 (sistema particionado).

Los usuarios y los controles sólo deben tener acceso a la partición 1, dejando la partición 2 para armar y desarmar automáticamente.

Todas las zonas externas deben configurarse para la partición 1.

Todas las zonas internas deben configurarse para la partición 2.

La partición 1 debe tener al menos una zona temporizada de modo que sea posible que el usuario abandone el sitio después de armar la partición 1 sin activarla.

[171 A 186] PARTICIONES DAS ZONAS

Patrón: 1 (partición 1)

[171] [__] Partición de la Zona 1
[172] [__] Partición de la Zona 2
[173] [__] Partición de la Zona 3
[174] [__] Partición de la Zona 4
[175] [__] Partición de la Zona 5
[176] [__] Partición de la Zona 6
[177] [__] Partición de la Zona 7
[178] [__] Partición de la Zona 8
[179] [__] Partición de la Zona 9
[180] [__] Partición de la Zona 10
[181] [__] Partición de la Zona 11
[182] [__] Partición de la Zona 12
[183] [__] Partición de la Zona 13
[184] [__] Partición de la Zona 14
[185] [__] Partición de la Zona 15
[186] [__] Partición de la Zona 16

Cuando particionado el sistema, definimos aqui cual partición la zona pertenece.

1 - Zona para la Partición 1 (Patrón)
2 - Zona para la Partición 2
3 - Zona para la Partición 3
4 - Zona para la Partición 4
5 - Zona para la Partición 5
6 - Zona para la Partición 6
7 - Zona para la Partición 7
8 - Zona para la Partición 8.

Cuando utilizada la partición común, (función [203]), las zonas programadas para la partición 8 solamente serán activadas cuando las particiones programadas en la Función [203] estén activadas.

[591 a 598] Nombres de las Particiones

[591] [__/__ / . . . /__/__] (16 caracteres) Patrón: Partição x (donde x es el número de la partición)

Nombres de las Particiones que aparecerán en los informes y mensajes enviados por correo electrónico.

[203] Partición 8 Comum

Patrón: Deshabilitado todos los leds borrados	Led \ Bit \ Partición						
[203] Particiones en común con la Partición 8	**1**	**2**	**3**	**4**	**5**	**6**	**7**

Cuando es habilitado el sistema particionado, existe la posibilidad de la partición de número 8 armar solamente cuando las otras particiones en conjunto con ella estén también armadas. Cuando alguna de las particiones es desarmada, la partición 8 desarma junto hasta que todas las otras sean armadas nuevamente.

Para programar cual o cuales particiones deben funcionar en conjunto, deje los leds referentes à las particiones encendidos.

Para que la partición 8 funcione independiente, los leds deben estar todos borrados.

Auto Activación

[131 a 138] Horario de Auto Activa

Patrón: FF:FF (hh : mm) deshabilitado

[131] [__/__/__/__] Horario de Auto activa de la Partición 1
[132] [__/__/__/__] Horario de Auto activa de la Partición 2
[133] [__/__/__/__] Horario de Auto activa de la Partición 3
[134] [__/__/__/__] Horario de Auto activa de la Partición 4
[135] [__/__/__/__] Horario de Auto activa de la Partición 5
[136] [__/__/__/__] Horario de Auto activa de la Partición 6
[137] [__/__/__/__] Horario de Auto activa de la Partición 7
[138] [__/__/__/__] Horario de Auto activa de la Partición 8

Programando un horario válido em eses campos (0000 hasta 2359), el sistema arma independiente del estado de las zonas. Si alguna zona inmediata está abierta, inmediatamente, después de armar, un disparo será generado. Para desprogramar rellene con FFFF (INF+6).

[206 a 209 y 358 a 361] Horario de Auto Desactiva

Patrón: FF:FF (hh : mm) deshabilitado

[206] [__/__/__/__] Horario de Auto Desactiva de la Partición 1
[207] [__/__/__/__] Horario de Auto Desactiva de la Partición 2
[208] [__/__/__/__] Horario de Auto Desactiva de la Partición 3
[209] [__/__/__/__] Horario de Auto Desactiva de la Partición 4
[358] [__/__/__/__] Horario de Auto Desactiva de la Partición 5
[359] [__/__/__/__] Horario de Auto Desactiva de la Partición 6
[360] [__/__/__/__] Horario de Auto Desactiva de la Partición 7
[361] [__/__/__/__] Horario de Auto Desactiva de la Partición 8

Programando un horario válido en eses campos (0000 hasta 2359), la partición correspondiente a la función irá desarmar en ese Horario. Los días de la semana en que las particiones serán desarmadas automáticamente deben ser programados en la función [130].

[130] Días de la Semana con Auto Desactiva

Patrón: Deshabilitado todos los leds borrados	Dom	Lun	Mar	Mier	Jue	Vier	Sáb	Dia
[130] Días de la Semana con Auto Desactiva	1	2	3	4	5	6	7	**Led\Bit**

Determina cuales días de la semana el auto desactiva (Funciones [206 hasta 209 y 358 a 361]) irá funcionar. Los días que no estén marcados de 1 hasta 7 no desactivan.

[205] Particiones Para Auto Activa (Auto Activa del Teclado)

Patrón: Borrado (Deshabilitado)	Bit / Led / Part.							
[205] Particiones para Auto Activa	1	2	3	4	5	6	7	8

Define las particiones que serán activadas por las Funciones de auto activa de los teclados.

Para habilitar o auto activa por hora en el teclado programe:
ENT + Contraseña de programación o maestra + INF + HH + MM

[139 a 146] Activación Por Inercia de las Particiones

Patrón: 000 Minutos (Deshabilitado)

[139] [__/__/__] Tiempo para Armar por Inercia de la Partición 1 **O NO Particionado**
[140] [__/__/__] Tiempo para Armar por Inercia de la Partición 2
[141] [__/__/__] Tiempo para Armar por Inercia de la Partición 3
[142] [__/__/__] Tiempo para Armar por Inercia de la Partición 4
[143] [__/__/__] Tiempo para Armar por Inercia de la Partición 5
[144] [__/__/__] Tiempo para Armar por Inercia de la Partición 6
[145] [__/__/__] Tiempo para Armar por Inercia de la Partición 7
[146] [__/__/__] Tiempo para Armar por Inercia de la Partición 8

Ese es el tiempo, en minutos (000 hasta 255 minutos), para que la partición active si no hay movimiento en las zonas de esa partición. Programar 000 para deshabilitar.

[159 a 166] Horario en que las Particiones Activan Por Inercia

[159] [__/__/__/__] Inicio de la activación por Inercia de la Partición 1 Patrón: 00:00
[160] [__/__/__/__] Inicio de la activación por Inercia de la Partición 2 Patrón: 00:00
[161] [__/__/__/__] Inicio de la activación por Inercia de la Partición 3 Patrón: 00:00
[162] [__/__/__/__] Inicio de la activación por Inercia de la Partición 4 Patrón: 00:00

[163] [__/__/__/__] Fin de la activación por Inercia de la Partición 1 Patrón: 23:59
[164] [__/__/__/__] Fin de la activación por Inercia de la Partición 2 Patrón: 23:59
[165] [__/__/__/__] Fin de la activación por Inercia de la Partición 3 Patrón: 23:59
[166] [__/__/__/__] Fin de la activación por Inercia de la Partición 4 Patrón: 23:59

Las particiones de 1 hasta 4 pueden ser programadas para que el auto activa por inercia funcione solamente en un determinado período del día. Las particiones de 5 hasta 8 si son programadas para auto activar por inercia, funcionan 24 horas.

En el Horario de inicio, el tiempo sin movimiento empieza a ser contado. En el horario final, si el sistema esté armado, permanece armado.

[167 a 170] Días de la Semana en que las Particiones Activam Por Inercia

Patrón: Deshabilitado todos los leds borrados	Dom	Lun	Mar	Mier	Jue	Vie	Sáb		Bit / Led
[167] Días da Semana da Partición 1	1	2	3	4	5	6	7	8	
[168] Días da Semana da Partición 2	1	2	3	4	5	6	7	8	
[169] Días da Semana da Partición 3	1	2	3	4	5	6	7	8	
[170] Días da Semana da Partición 4	1	2	3	4	5	6	7	8	

Las particiones de 1 hasta 4 con Horario de activación por inercia, pueden tener días de la semana definidos para funcionar, siendo tecla 1 para domingo, 2 para lunes, 3 para martes, hasta 7 para el sábado.

Los días que no estén marcados en los leds de 1 hasta 7 podrán tener el auto activa funcionando 24 horas o deshabilitado, dependiendo de la tecla/led 8. Siendo:

Led 8 Encendido: En los otros días opera 24horas.

Led 8 Borrado: En los otros días deshabilitado.

[363] Anular Auto Activación con Zona Abierta – Opción (BIT) 4

Patrón: Borrado (Deshabilitado)		Bit/Led
[363]	Si habilitado, el auto arme por inercia de cualquier partición no irá armar si alguna zona de la central disparar. En ese caso el sistema reinicia el contaje de tiempo y envía el evento programado en la función [465], "Falla en el auto arme" Informando la partición que no armó.	**4**

[465] Falla en el Auto Arme – Código Contact Id

[465] [__/__ /__/__] Patrón: 0000 (deshabilitado)

Cuatro dígitos con el código Contact ID del evento.

[147 a 154] Horario en que las Particiones Están Siempre Armadas

Las particiones 1 a 4 se pueden programar para que siempre estén armadas durante un cierto período del día y durante ciertos días de la semana. Es posible desarmarlo momentáneamente, sin embargo, después del tiempo programado la partición se arma automáticamente, independientemente del estado de las zonas, que si se deja abierta, generará un disparo.

Patrón: FF:FF

[147] [__/__ : __/__] Inicio del tiempo siempre armado de la partición 1
[148] [__/__ : __/__] Inicio del tiempo siempre armado de la partición 2
[149] [__/__ : __/__] Inicio del tiempo siempre armado de la partición 3
[150] [__/__ : __/__] Inicio del tiempo siempre armado de la partición 4

Al comienzo de las horas de funcionamiento, si la partición está desarmada, se armará automáticamente. En este caso, el sistema mantiene en la memoria que el sistema estaba armado automáticamente y al final de las horas de funcionamiento, la partición se desarmaría automáticamente.

[151] [__/__ : __/__] Fin del tiempo siempre armado de la partición 1
[152] [__/__ : __/__] Fin del tiempo siempre armado de la partición 2
[153] [__/__ : __/__] Fin del tiempo siempre armado de la partición 3
[154] [__/__ : __/__] Fin del tiempo siempre armado de la partición 4

Después de este tiempo, la partición ya no se armará automáticamente.

[155 a 158] Días de la Semana en que las Particiones Están Siempre Armadas

Patrón: Deshabilitado todos los leds borrados	Dom	Lun	Mar	Mier	Jue	Vie	Sáb		Bit / Led
[155] Días da Semana da Partición 1	1	2	3	4	5	6	7	8	
[156] Días da Semana da Partición 2	1	2	3	4	5	6	7	8	
[157] Días da Semana da Partición 3	1	2	3	4	5	6	7	8	
[158] Días da Semana da Partición 4	1	2	3	4	5	6	7	8	

Determina cuales días de la semana a partición será siempre armada, siendo tecla 1 para domingo, 2 para lunes, 3 para martes, hasta 7 para el sábado.

Los días que no estén marcados en los leds de 1 hasta 7 podrán tener el auto activa funcionando 24 horas o deshabilitado, dependiendo de la tecla/led 8. Siendo:

Led 8 Encendido: En los otros días opera 24 horas.

Led 8 Borrado: En los otros días deshabilitado.

[491 a 494] Tiempo de Rearme de las Particiones Siempre Armadas

Patrón: 000 minutos

[491] [__/__/__] Tiempo de Rearme de la Partición 1
[492] [__/__/__] Tiempo de Rearme de la Partición 2
[493] [__/__/__] Tiempo de Rearme de la Partición 3
[494] [__/__/__] Tiempo de Rearme de la Partición 4

Se o valor programado es cero, es imposible desarmar a la partición durante el período de siempre armado. Caso contrario, la partición podrá ser desarmada y permanecerá desarmada por el período programado en minutos en estas funciones. Pasado ese tiempo, la partición irá armar nuevamente, independiente de haber movimiento en las zonas o zonas abiertas. Caso alguna zona esté violada en el momento del auto arme, el sistema irá disparar.

SIRENES

[210 y 211] Tiempo de Sirena

[210] [__/__ : __/__] Tiempo de la Sirena 1 Patrón: 05:00 (mm:ss)
[211] [__/__ : __/__] Tiempo de la Sirena 2 Patrón: 00:00

Definir cuanto tiempo en minutos y segundos que la sirena permanecerá activa después del disparo de una alarma. (00:00 sin sirena) el tiempo puede variar de 00:01 hasta 99:99 minutos.

OJO.: La sirena 2 es la pgm1 con programación para Sirena 2 (pág. 54)

[213 y 214] Particiones que Disparan la Sirena

Patrón: **Todos Encendidos (Habilitado)**	**Bit / Led / Part.**							
[213] Particiones que disparan la Sirena 1	1	2	3	4	5	6	7	8
[214] Particiones que disparan la Sirena 2	1	2	3	4	5	6	7	8

Se puede particionar la Sirena haciendo con que ela dispare apenas se zonas de algunas parciciones dispare.

Así que podemos tener particiones que disparan una sirena y particiones que desencadenan otra. **Recuerde:** los periféricos antiguos como los expansores o las zonas de teclado pueden no ser compatibles con el particionamiento de la sirena. En este caso, la Sirena 1 siempre se activará, independientemente de la partición.

[216 y 217] Bip de la Sirena

Patrón: Todos Encendidos (Habilitado)	Bit / Led / Part.
[216] Particiones con Bip en la Sirena 1	1 2 3 4 5 6 7 8
[217] Particiones con Bip en la Sirena 2	1 2 3 4 5 6 7 8

Un bip : Sistema Armado
Dos bips : Sistema Desarmado

[219] Supervisión de la Sirena

Patrón: Aceso (Habilitado)	Bit / Led
[219] Supervisión	1

Cuando está deshabilitado, no envía un mensaje de error al centro de supervisión. Sólo en el panel de control principal será posible comprobar cuando la sirena tiene un problema.

La supervisión siempre funciona debido a la protección del cortocircuito del sistema. La resistencia 1K debe colocarse en paralelo con la sirena

[082] Problemas que Disparam a Sirena

Padrão: Todos (desabilitados)

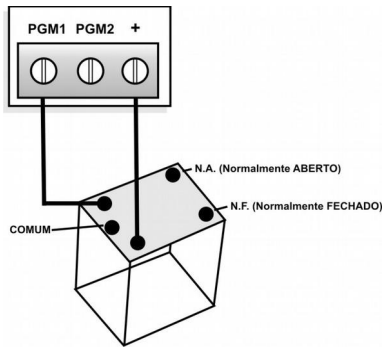
	Bit/Led	Descrición
[082]	1	Falla de bateria
	2	Falla de red elétrica
	3	Falla de sirena
	4	Sobrecarga no barramento
	5	Falla de comunicación
	6	Falla de hilado/tamper
	7	Falla de periférico

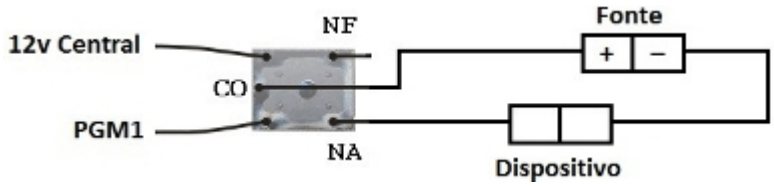
Se a partición 1 estiver armada no momento em que a Falla selecionada ocorrer, as Sirenas programadas para disparar a partición 1 se dispararán.

Salidas Programables (PGMs)

La VW16ZGPRSIP posee dos salidas programables. Son conectadas al negativo de la alimentación y cuando accionadas pueden fornecer hasta 100mA cada.

Pueden ser usadas para accionar leds de confirmación, reles de portón. A PGM 1 (salida programable 1) aún puede funcionar como una segunda sirena para el sistema.





[371 a 374] Eventos de las Pgms

Evento: Cuando los dos eventos programados ocurrieren la PGM será accionada.(ver tabla)

[371] [__/__] 1º Evento da PGM 1 Patrón: 00 **[373]** [__/__] 1º Evento da PGM 2 Patrón: 00

[372] [__/__] 2º Evento da PGM 1 Patrón: 00 **[374]** [__/__] 2º Evento da PGM 2 Patrón: 00

Valor	1º Evento	Pgm1	Pgm2	Para programar el complemento
00	Nada			
01	Evento	**[377]**	**[379]**	Código CID del evento QCCC
02	Zona disparada	**[377]**	**[379]**	Cual zona, de 0001 a 0016
03	Zona inhibida	**[377]**	**[379]**	Cual zona, de 0001 a 0016
04	Hora pasada	**[377]**	**[379]**	Horario HH:MM
05	Hora exacta	**[377]**	**[379]**	Horario HH:MM
06	Algún problema	**[381]**	**[383]**	Teclas referentes a los problemas* ENT
07	Eses problemas	**[381]**	**[383]**	Teclas referentes a los problemas* ENT
08	Alguna partición armada	**[381]**	**[383]**	Teclas 1 a 8 referentes a las particiones ENT
09	Esas Particiones armadas	**[381]**	**[383]**	Teclas 1 a 8 referentes a las particiones ENT
0A	Algunas Particiones Disparadas	**[381]**	**[383]**	Teclas 1 a 8 referentes a las particiones ENT
0B	Siempre verdadero	**-**	**-**	-
0C	Sirenas disparadas	**[381]**	**[383]**	Teclas 1 e 2 referentes às Sirenas ENT
0D	Temporizando zonas	**[377]**	**[379]**	Cual zona, de 0001 a 0016
0E	Zona de periférico disparó	**[377]**	**[379]**	Cual zona, de 0001 a 9999
0F	Zona de periférico abrió	**[377]**	**[379]**	Cual zona, de 0001 a 9999
10	Contraseña digitada mayor o igual	**[377]**	**[379]**	Cual Contraseña
11	Sirena 2 (solamente para pgm 1)***	**-**	**-**	-
12	Falla en el medio de comunicación	**[377]**	**[379]**	Cual medio de comunicación**. 4 dígitos
13	Memoria de disparo***	**[381]**	**[383]**	Teclas 1 a 8 referentes as Particiones **ENT**

Valor	2º Evento	Pgm1	Pgm2	Para programar el complemento
00	Nada			
01	Evento	**[378]**	**[380]**	Código CID del evento QCCC
02	Zona disparada	**[378]**	**[380]**	Cual zona, de 0001 a 0016
03	Zona inhibida	**[378]**	**[380]**	Cual zona, de 0001 a 0016
04	Hora pasada	**[378]**	**[380]**	Horario HH:MM
05	Hora exacta	**[378]**	**[380]**	Horario HH:MM
06	Algún problema	**[382]**	**[384]**	Teclas referentes a los problemas* ENT
07	Eses problemas	**[382]**	**[384]**	Teclas referentes a los problemas* ENT
08	Alguna partición armada	**[382]**	**[384]**	Teclas 1 a 8 referentes a las particiones ENT
09	Esas Particiones armadas	**[382]**	**[384]**	Teclas 1 a 8 referentes a las particiones ENT
0A	Algunas Particiones Disparadas	**[382]**	**[384]**	Teclas 1 a 8 referentes a las particiones ENT
0B	Siempre verdadero	**-**	**-**	-

Valor	2º Evento	Pgm1	Pgm2	Para programar el complemento
0C	Sirenas disparadas	[382]	[384]	Teclas 1 e 2 referentes às Sirenas ENT
0D	Temporizando zonas	[378]	[380]	Cual zona, de 0001 a 0016
0E	Zona de periférico disparó	[378]	[380]	Cual zona, de 0001 a 9999
0F	Zona de periférico abrió	[378]	[380]	Cual zona, de 0001 a 9999
10	Contraseña digitada mayor o igual	[378]	[380]	Cual Contraseña
11	Sirena 2 (solamente para pgm 1)***	-	-	-
12	Falla en el medio de comunicación	[378]	[380]	Cual medio de comunicación**. 4 dígitos
13	Memoria de disparo***	[382]	[384]	Teclas 1 a 8 referentes as Particiones **ENT**

A = INF 1	B = INF 2	C = INF 3	D = INF 4	E = INF 5	F = INF 6

*** Los problemas son:**

1 - Falla de la batería 2 - Falla de red eléctrica 3 - Falla de sirena 4 - Falla de barramento
5 - falla en la comunicación 6 – Falla de támper 8 – Falla de LíneaTelefónica

** "Falla en medio de comunicación".

Caso un medio de comunicación programado en el complemento falle, la condición es verdadera (para programar o complemento, siempre los dos primeros dígitos serán "00", ejemplo: 0001, 0011, 0041, etc).

***Programando 11 en la función [371], la PGM1 se comporta como otra sirena las configuraciones de la Sirena 2 están en la pág. 54.

[375 y 376] Operación Lógica De Las Pgms

[375] [__] Operación lógica PGM 1 Patrón: 0
[376] [__] Operación lógica PGM 2 Patrón: 0

La operación lógica para determinar cómo se pueden combinar los dos eventos de PGM para decidir si el PGM se activará o no.

0	**Evento 1º Y Evento 2º**	La PGM se activa cuando ambos eventos se llevan a cabo, por ejemplo, si el evento 1 es Zona 1 abierta y el evento 2 es Zona 2 abierta, el PGM se activará solamente si las duas zonas están abiertas.
1	**Evento 1º O Evento 2º**	La PGM es activada cuando cualquer uno de los dos eventos están ocurriendo. En el ejemplo anterior, cualquer de las zonas (1 o 2) que fue abierta accionaria a PGM, que sólo **no** sería activado si ambos fueran cerrados.
2	**Não Evento 1º Y Evento 2º**	La PGM es activa cuando el Evento 1 no esta sucediendo y el Evento 2 está. En el ejemplo anterior, el PGM sólo se activa si la zona 1 fue cerrada y la Zona 2 abierta.
3	**Não Evento 1º O Evento 2º**	La PGM es activa cuando el Evento 1 no esta sucediendo o cuando el Evento 2 está. En el ejemplo anterior, seria suficiente para ser activado la PGM, que la zona 1 se cierre, y la Zona 2 se mantenga abierta. Para no accionar la PGM es necesario que la zona 1 permanezca abierta, junto com el área 2 cerrada.
4	**Não Evento 1º Y Não Evento 2º**	Para activar la PGM, ninguno de los dos eventos pueden ocurrir. En el caso de los ejemplos anteriores, para activar la PGM requeriría tanto zona (1 y 2) cerradas.
5	**Não Evento 1º O Não Evento 2º**	Para activar la PGM, uno de los dos eventos no pueden ocurrir. En el caso de los ejemplos anteriores, para activar la PGM seria necesario mantener las áreas cerradas de los dos (o ambos). Para no activar el PGM, ambas áreas deben estar abiertas.

[377 a 380] Complemento De Las PGM's (Tipo Valor)

[377] [__/__/__/__] Complemento del 1o. Evento de la PGM 1 Patrón: 0000
[378] [__/__/__/__] Complemento del 2o. Evento de la PGM 1 Patrón: 0000
[379] [__/__/__/__] Complemento del 1o. Evento de la PGM 2 Patrón: 0000
[380] [__/__/__/__] Complemento del 2o. Evento de la PGM 2 Patrón: 0000

Para el accionamiento de la PGM un complemento debe ser programado conforme el evento programado. Algunos eventos no tiene complementos.

[381 a 384] Complemento De Las PGM's (Tipo Función)

[381] [1-2-3-4-5-6-7-8] Complemento do 1º. Evento de la PGM 1
[382] [1-2-3-4-5-6-7-8] Complemento do 2º. Evento de la PGM 1
[383] [1-2-3-4-5-6-7-8] Complemento do 1º. Evento de la PGM 2
[384] [1-2-3-4-5-6-7-8] Complemento do 2º. Evento de la PGM 2

[385 y 386] Tiempo Das Pgms

[385] [__/__:__/__] Tiempo de Accionamiento da PGM 1 Patrón: 00:00 (mm:ss)
[386] [__/__:__/__] Tiempo de Accionamiento da PGM 2 Patrón: 00:00

Definido cuanto tiempo en minutos y segundos que la PGM quedará accionada cuando ocurriir algun evento programado. Si el tiempo for 0000 sigue el estado de las condiciones que la activó.

VIAWEB MOBILE(APLICACIÓN PARA SMARTPHONES)

Disponible para Smartphones iOS ou Android.

https://itunes.apple.com/br/app/viaweb-mobile/id633559815?mt=8	https://play.google.com/store/apps/developer?id=VIAWEB+system

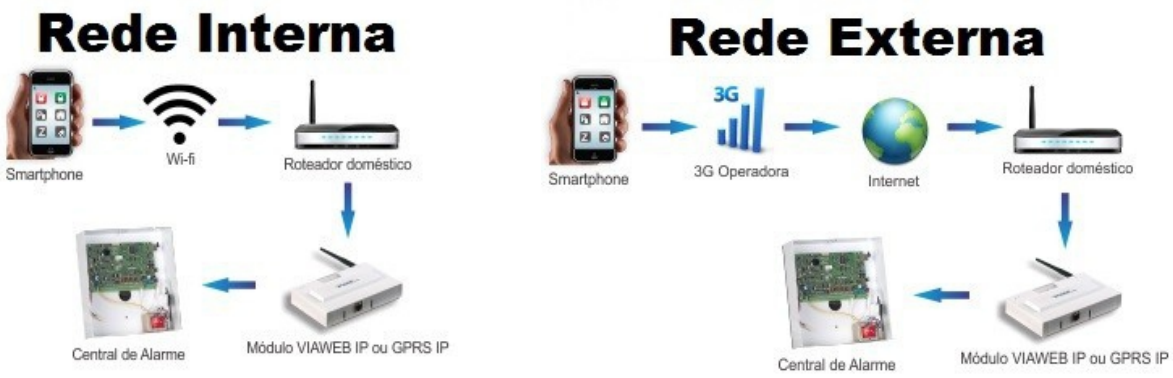
Es possible controlar una central VIAWEB conectada al módulo a través de la aplicación VIAWEB mobile, disponible para Android y iOS (iPhone). El control puede ser hecho adónde esteas, de cualquier lugar con acceso a la Internet.

Baje la aplicación directamente del Smartphone, a través de la tienda de aplicaciones correspondiente.

La aplicación VIAWEB mobile permite utilizar dos tecnologias distintas para acceder y controlar el sistema, el "VIAWEB direct" y el "VIAWEB service".

VIAWEB DIRECT

Esa tecnologia permite la conexión directa entre el sistema de alarma VIAWEB y el aplicativo móvil. El smartphone se comunica directamente con la VW16ZGPRSIP.



Vantajas:

- Comunicación instantánea, rápida e directa.
- Protocolo criptografado AES CBC 128 bits, de alta seguridad.
- No depiende de terceros, servidores externos.

Registro en la aplicación:

- Abra el navegador WEB, clic en " 

" y después " 

";
- En la página Viaweb Direct clic em la opción" 

";
- En el smartphone, estea seguro de que el aparato está conectado en la misma red que el módulo. Abra la APP y siga los pasos:

1°	2°	3º
Pantalla inicial: Tú encuentras el símbolo de wifi en gris con el modelo del equipamiento y el número de série. Haz clic en él.	Tela de registro: El registro principal* es hecho con login en el google o facebook. Para registrar otros móviles use la contraseña del VIAWEB DDNS (contraseña puede ser visualizada en la página web "Viaweb Direct").	Pantalla principal alarma: Cuando aparece esa pantalla, clic en "Zonas", espere la pantalla cargar, y listo! El móvil ya está conectado.
		

Íconos en la parte inferior de la pantalla inicial		Íconos en la parte inferior de la pantalla principal	
	Entra en modo de edición (funciona solamente con centrales registradas).		Configuraciones
	Entra en modo de exclusión (funciona solamente con centrales registradas).		Habilita \ Deshabilita recebimiento de notificaciones
	Sale de los modos de exclusión y edición		Vuelve para pantalla inicial (cambia de alarma)
	Procura dispositivos en la red		Informaciones sobre utilización
	Informaciones sobre permisos		Informaciones sobre permisos

*Cadastro principal é o login social (usuário) que tem acesso à página do servidor. Somente um usuário pode ter acesso à Página do servidor.

PROGRAMANDO LA CENTRAL POR FUNCIONES

Funciones abajo automaticamente programadas por la "Página Web"

Para envío de eventos para la aplicación, se programa el valor "81" en una de las secuencias de comunicación

Se preferir, en vez de programar el acceso al Viaweb direct por la página web, podemos programar por teclado o por software de programación (Viaweb Download).

[571] HABILITA REGISTRO AUTOMÁTICO VIAWEB DIRECT

[571] [__] Patrón: 0 Deshabilitado.

Se debe programar el valor 1 para habilitar el registro automático.

A partir del momento en que el modo es habilitado, el usuario tiene hasta 4 minutos para efetuar el registro automático de un nuevo VIAWEB mobile.

Cuando una nueva aplicación es registrada, la función sale del modo de registro automaticamente.

Solo permite el registro de un aparato por vez.

[570] VIAWEB DIRECT - LLAVE CRIPTOGRÁFICA

[570] [__/__/ . . . /__] Patrón: FFFFFFF... (VIAWEB direct deshabilitado) (32 caracteres)

Caso el registro automático no esté habilitado, al abrir la app (conectado en el Wifi de la misma red del módulo), un ícono gris irá aparecer, al clicar en ese ícono una llave criptográfica será generada. Esa llave deberá ser programada en esta función.

Caso el módulo ya tenga una llave, al ser registrado un nuevo dispositivo esa misma llave debe ser inserida en la app.

Estando programada correctamente la app irá abrir y estará lista para acceder el módulo.

[580] Habilita Dynamic Dns

[580] [__/__/__] Patrón: 000 Deshabilitado.

Se define cual servicio de DNS será utilizado para el módulo. La vantaja del servicio VIAWEB DNS es que en él pueden ser hechas personalizaciones en eventos y el envio de notificación del módulo offline.

OPCIONES: 000 – Deshabilitado; **001 - VIAWEB DDNS**; 002 – NO-IP.ORG

[581] Dirección Externa (HOSTNAME)

[581] [__/__/ . . . /__] (30 caracteres) Patrón: n<<número de serie >>.viawebservice.com.br

Domínio con hasta 30 caracteres especificando la dirección registrada en el servicio de

Dynamic DNS. De fábrica esta función viene con dirección propia en el VIAWEB DNS. Ejemplos: meumodulo.no-ip.org; meumodulo.noip.me.

Ojo:. Si utiliza DDNS Viaweb, no es necesario cambiar esta función

[582] Usuario Dynamic Dns

[582] [__/__/ . . . /__] Patrón: Número de série del equipamiento

Usuario o correo electrónico registrado en el servicio de Dynamic DNS (hasta 30 caracteres).

Ojo:. Si utiliza DDNS Viaweb, no es necesario cambiar esta función

[583] Contraseña Dynamic Dns

[583] [__/__ / . . . /__] Patrón: Ajustado de fábrica, único para cada equipamiento.

Contraseña registrada en el servicio de Dynamic DNS (hasta 30 caracteres).

Ojo:. Si utiliza DDNS Viaweb, no es necesario cambiar esta función

[584] Resultado Dynamic Dns

[584] [__/__/ . . . /__] (30 caracteres) Función solamente de lectura.

Es posible verificar el resultado de la actualización del servicio Dynamic DNS, leyendo el valor de esa función.

Posibles valores:

Valor Programado en la función	Interpretación
DDNS deshabilitado	Programado el valor 000 en la función 580.
Servicio inválido	Programado valor distinto de 000, 001, y 002 en la función
URL Inválida	Provedor de servicio no disponíble (ej. no-ip fuera del aire).
Timeout conexión	No fue posible abrir conexión con el servidor.
Timeout memória	No fue posible leer los parámetros de la memória (dirección, usuario, contraseña).
Timeout envio de dados	No fue posible enviar dados para atualización del IP.
good	Atualización del IP concluída con éxito.
nochg	Revalidación del IP concluída, sin alteración.
nohost	Valor programado en la función 581 es inválido.

Valor Programado en la función	Interpretación
badauth	Valor programado en la función 582 o 583 es inválido.
badagent	Falla general en la utilización del servicio (programar 000 en la función 580 y entrar en Contato con el suporte inmediatamente).
!donator	Atualización indisponible - limitaciones en el registro de esta Cuenta junto al no-ip.
abuse	Muchas atualizaciones en un corto espacio de tiempo, programar 000 en la función 580, por lo mínimo 1 hora antes de reactivar el servicio.
911	Falla no servidor no-ip, a próxima tentativa de atualización será em 30 minutos.
401 Unauthorized	Valor programado en la función 582 o 583 es inválido.

PÁGINA SERVIDOR VIAWEB

En el servidor puedes:

- Personalizar notificaciones de cada móvil habilitado;
- Restringir notificaciones para cada celular habilitado;
- Habilitar notificaciones de Módulo offline;
- Visualizar los últimos 30 eventos transmitidos por el módulo.
- Para sincronizar la cuenta google o facebook en el servidor Viaweb:
- Habilite el recibimiento de notificaciones en la APP. **Link para la licencia de uso:** https://www.viawebservice.com.br/site/viawebservice/licenca_uso_viaweb_mobile.php ;
- Siga los pasos:

1°	2°	3°
Tela principal alarme: Clique no ícone do VIAWEB service (ícone com o planeta)	**Selecione rede social:** Nessa tela selecione a rede social que deseja sincronizar.	**Status da sincronização:** Aguarde todos os itens ficarem em verde. Pronto! A conta está sincronizada*.
		

*Caso algun íten de la pantalla de status de la sincronización quede en rojo, verifique la conexión del celular con la internet o outra cuenta está sincronizada.

Solamente una cuenta puede ser sincronizada con el servidor, si otra cuenta intentar sincronizar, es impedida.

Una vez hecho el registro con login social del Gmail o Facebook, el usuario puede acceder la página del servidor dónde los eventos generados por el sistema llegan y son editados antes de ser enviados para la APP.

- Accese el site www.viawebservice.com.br;
- Entre con el login del Google o Facebook registrado;

CORREO ELECTRÓNICO

- Funciones abajo automáticamente programadas por la “Página Web”
- Para envio de eventos por correo electrónico se programa el valor “61” en una de las secuencias de comunicación
- Los correos son enviados prioritariamente por ETHERNET si la conexión fallar o no existir, la central envia por GPRS. El envio de correo electrónicos por GPRS consonidoe datos del chip, llevar eso en consideración al hacer el plan del chip que será usado.
- Para que el módulo pueda enviar un correo electrónico, él debe poseer una cuenta de correo electrónico. Elija un provedor de correo electrónico, después rellene las funciones a seguir.

[561] SERVIDOR SMTP

[561] [__/__/ . . . /__] (30 caracteres) Patrón: FFFFFFFF. . .

SMTP es el protocolo patrón para envio de correo electrónicos a través de la Internet. Necesitas tener el nombre del Servidor SMTP de su provedor de correo electrónico para enviar y reciber sus mensajes. Ejemplos : smtp.live.com; smtp.mail.yahoo.com.br, smtp.terra.com.br

[562] PUERTA PARA CORREO ELECTRÓNICO (SERVIDOR SMTP)

[562] [__/__/__/__/__] Patrón: 00025

Para el envío de correos electrónicos debes registrar una puerta TCP, por lo general definido por el proveedor de correo electrónico.
Ejemplos:smtp.live.com – porta 25; smtp.mail.yahoo.com.br – porta 465; smtp.terra.com.br – porta 587

[564] USUARIO CORREO ELECTRÓNICO

[564] [__/__/ . . . /__] (30 caracteres) Patrón: FFFFFFFF. . .

Acá insieres el usuario de correo electrónico que has registrado para su módulo. Ejemplos : meumodulo@hotmail.com; meumodulo@yahoo.com.br; meumodulo@gmail.com

[565] CONTRASEÑA CORREO ELECTRÓNICO

[565] [__/__/ . . . /__] (20 caracteres) Patrón: FFFFFFFF. . .

Corresponde a la contraseña que haz registrado en el correo electrónico de su módulo.

[551] DIRECCIONES DE CORREO ELECTRÓNICO PARA RECEPCIÓN DE EVENTOS Y INFORMES 1

[551] [__/__/ . . . /__] (30 caracteres) Patrón: FFFFFFFF. . .

[552] DIRECCIONES DE CORREO ELECTRÓNICO PARA RECEPCIÓN DE EVENTOS Y INFORMES 2

[552] [__/__/ . . . /__] (30 caracteres) Patrón: FFFFFFFF. . .

[553] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 3

[553] [__/__/ . . . /__] (30 caracteres) Patrón: FFFFFFFF. . .

Las funciones 551, 552 y 553 permiten cada una hasta 30 caracteres para inserir correos electrónicos que irán recibir eventos o informes.
Para acrecentar más de un correo electrónico, se debe separar los correos electrónicos por un espacio.
Ejemplo: “email@gmail.com email@outlook.com”

Se puede también iniciar la dirección de correo electrónico en la función 551 y terminarlo en la función 552.

Ejemplo:
Función 551: “email@gmail.com viaweb@viawebsystem”
Función 552: “.com.br test@viawebsystem.com.br”

Además de los eventos enviados en el mismo momento en que ocurren, es posible configurar el módulo para generar informes periódicos sobre la situación del sistema. En eses informes tenemos informaciones de fallas o problemas, hora del sistema y una lista com los últimos eventos ocurridos.

DICA: En la página inicial de configuración del módulo, al configurar la cuenta de correo electrónico, ya estarán disponibles las opciones de configuración necesarias al envio de eventos y generación de informes. Esta página ya irá atribuir el envío de eventos paral os correo electrónicos configurados y cuales eventos deben ser enviados. Al finalizar esta configuración, la secuencia de comunicación 1 será automáticamente programada, juntamente com las funciones 512 e 513.

[512] Horario de Envio del Informe

[512] [__/__/__/__] Patrón: 12:00

Corresponde a la hora del día en que un informe del sistema será enviado por correo electrónico.

[513] Días de la Semana Para Envio de Informe

Patrón: Bit 2 habilitado (todo LUNES)	Dom	Lun	Mar	Miér	Jue	Vier	Sab	*	**Dia**
[513] Días de la semana para envio de informe	1	2	3	4	5	6	7	8	**Led/Bit**

* La opción 8 hace con que un informe sea enviado todo dia 1°, permitiendo el envío de informe una vez al mes.

Indica cuales días de la semana el informe será enviado.

Ojo.: Por programación, podemos editar los nombres de los usuarios, particiones y zonas que aparecen en el informe y en los eventos enviados por correo electrónico:
Nombre de las zonas (pág. 44)
Nombre de las Particiones (pág. 49)

RELATÓRIOS

Los informes del sistema son enviados por correo electrónico. Además, se puede obtener a cualquier momento un informe del sistema vía navegador WEB.

Formato del informe

No informe es posible verificar:

- Si hay alguna Falla (Sirena, alimentación, comunicación, tamper, periférico).
- Si la Sirena esté tocando.
- Cual el estado de la red eléctrica y tensión de la batería.
- Cual el estado del VIAWEB direct (si habilitado).
- Cual el estado del correo electrónico (si habilitado).
- Cual el estado del monitoreo (si habilitado).
- Cual el estado de la Internet.
- Si el sistema está armado o desarmado, o se fue particionado, cuales particiones están armadas.
- Zonas abiertas, falladas, inhibidas.
- Últimos eventos del sistema.

Ejemplo:

Informe VIAWEB system – Estado del Sistema

********** SUPERVISIÓN **********
Falla en la supervisión da Sirena.
Red eléctrica OK, batería en 12,51V.
Último acceso VIAWEB direct: 07/08/2013 12:02.
Correo electrónico OK.
Monitoreo OK. Internet OK.

********** ALARMA **********
Sistema Desarmado
Cocina (001) abierto
Sala (009) excluido
Zona 011 Falla de cableado
Zona 020 disparado

********** EVENTOS **********
05/08 08:22 R402 Partición 2 armada por Derossi (001)
05/08 08:22 E130 Disparo Zona 020
05/08 08:27 R130 Restauro Zona 020
05/08 12:33 E602 Test periódico
05/08 21:20 E401 Desarmado por Usuario 100
06/08 00:00 E602 Test periódico
06/08 07:44 4768 EVENTO: 4768 P01 Z055
07/08 11:34 R401 Armado por Nelson (009)
07/08 11:34 E570 Excluido Sala (009)
07/08 12:13 E121 Coacción Usuario 099

Informe generado en 12:14 07/08/2013.

AVANZADO

[000] VERSIÓN DEL FIRMWARE DE LA CENTRAL

[000] [_ _ _ _] Versión do firmware (Función solamente de lectura)

[355 Y 357] PERMISO DE ACCESO REMOTO

Restringe el acceso remoto a la VW16ZGPRSIP, siendo:

[355] Permiso de acceso remoto por VIAWEB DOWNLOAD, SMS o servidor VIAWEB
[357] Permiso de acceso remoto por la Página WEB o VIAWEB DIRECT

Patrón: Todos Habilitados

	Níveis	Descripción	Tecla/Led
[355] [357]	**Monitoreamento, PGM, Status**	Si borrado, no es posible visualizar el status usando el VIAWEB download.	**1**
	Armar y Desarmar (Inibir)	Se Borrado, no es posible armar, desarmar o inhibir zonas usando el VIWEB download.	**2**
	Programar y Leer programación	Se Borrado, no es posible alterar o leer la programación usando el VIWEB download.	**3**
	Leer Eventos	Se Borrado, no es posible leer los eventos usando el VIWEB download.	**4**
	Registrar y Leer Contraseñas	Si borrado, no es posible registrar o leer contraseñas usando el VIAWEB download.	**5**
	Llamada Telefónica ATV-DTV*	Si borrado, no es acepto llamadas para armar para o desarmar la central.	**6**
	Comandos por SMS*	Si borrado, no son aceptos comandos por SMS	**7**
	Retornar status a cada comando SMS OK*	Habilita el retorno de un SMS para cada comando ejecutado por los números de telefóno de control (481 hasta 488). Cuando deshabilitado el retorno solamente será efectuado si el usuario enviar en el SMS el comando de información “I”.	**8**

*Disponible solamente en la Función [355]

[366] TECLAS ESPECIALES 1 Y 2

[366] [__/__] Patrón: 00 (Deshabilitado)

Función	Característica
0	Deshabilitado
1	Emergencia silenciosa
2	Alarma de furto
3	Incendio
4	Emergencia médica
5	Activar pgm 1
6	Desactivar pgm 1
7	Activar pgm 2
8	Desactivar pgm 2
9	Auto activar Particiones da Función [205]

Esta Función es programada a través de dos dígitos. El primero dígito para la tecla especial 1 (ESP + 1) y el segundo para la tecla especial 2 (ESP + 2).

Ejemplo:

Para enviar emergencia silenciosa pela tecla especial 1 y auto armar pela especial 2 en esa Función programe “19”.

[363] Programación de Contraseñas Aleatórias - Opción (BIT) 3

Patrón: Apagado (Deshabilitado)		Bit/Led
[363]	Modo de operación con Contraseñas aleatorias. Si habilitado, las contraseñas de usuario 3, 4 y 5 son generadas aleatoriamente y cambiadas automáticamente cuando utilizadas. Al deshabilitar ese modo, las contraseñas de usuario 3, 4 y 5 son borradas. Más detalles de ese modo de operación son descriptos abajo.	3

Modo de operación con contraseñas aleatorias:

En determinadas soluciones de seguridad, algunas veces es necesario que empresas o personas que prestan servicios tercerizados, tengan acceso al local protegido. Por ejemplo, servicios de limpieza y conservación, manutención periódica, reabastecimiento de cajas y suporte. En eses casos, personas lejanas al área protegida necesitan desarmar el sistema y pasan a tener conocimiento de una o más contraseñas de acceso.

Eso normalmente genera la inseguridad de que una o más personas desconocidas retengan contraseñas y puedan desarmar la alarma en momentos indeseados. La solución común para ese problema es el desarme remoto de la Alarma por la empresa de monitoreo o el acceso via Download y cambio manual de la contraseña utilizada. Esas soluciones requieren intervención manual del operador y están sujetas a fallas humanas.

Con ese modo de operación, el sistema pasa a tener 3 contraseñas que solamente son conocidas por el panel de alarma y por la empresa de monitoreo. Toda vez que una de las contraseñas es digitada, ella es cambiada por otra, generada aleatoriamente.

Las contraseñas aleatorias son de los usuarios 003, 004 y 005. En el momento en que la opción 3 de la función 363 es habilitada, esas 3 Contraseñas son generadas aleatoriamente. Cuando esta opción é deshabilitada, esas contraseñas son borradas automáticamente.

Para que el monitoreo reciba la información de nueva contraseña, un evento en Contact ID con formato especial es enviado a monitoreo. Los eventos en Contact ID posee el siguiente formato: CCCC QEEE PP ZZZ, dónde CCCC es la cuenta del cliente, Q o Qualifier del evento, EEE y el código del evento, PP la partición y ZZZ la zona correspondiente del evento.

Al generar una nueva contraseña aleatoria, el evento será enviado en el formato abajo:

CCCC 2[D1][D2][D3] 01 [D4][D5][D6] para informar a nova senha do usuário 003.
CCCC 4[D1][D2][D3] 01 [D4][D5][D6] para informar a nova senha do usuário 004.
CCCC 6[D1][D2][D3] 01 [D4][D5][D6] para informar a nova senha do usuário 005.

Dónde [D1][D2][D3][D4][D5][D6] son los 6 dígitos de la nueva contraseña. Caso la contraseña posee menos de 6 dígitos, los últimos deben ser ignorados.

Como no existen eventos en Contact ID cuyo Qualifier (Q) sea diferente de 1 o 3, entonces no monitoreo es posible saber cual es el evento que contiene la nueva contraseña observando el valor del Qualifier. 2 para la contraseña del usuario 003, 4 para la Contraseña del usuario 004 y 6 para la contraseña del usuario 005.

De esa manera, para que el monitoreo sepa cual es la contraseña actual, basta mirar cuales fueron los últimos eventos Contact ID recibidos con qualifier 2, 4 o 6.

[363] Salva la Lista de Periféricos Conectados al Innovabus - Opción (BIT) 6

Padrão: Apagado (Desabilitado)		Bit/Led
[363]	Ao habilitar essa função a central irá memorizar de forma permanente quais periféricos estão conectados ao barramento. Mesmo que a energia elétrica seja removida essa lista é mantida. Isso evita que em caso de falha de algum periférico a ordem das zonas, senhas e pgms seja alterada na inicialização do sistema.	6

[363] Diversos

Patrón: Borrado (Deshabilitado)		Bit/Led
[363]	Si está activado, ajusta periódicamente el reloj interno de la hora recibida desde el servidor de Viaweb 1. Recuerde que el servidor Viaweb debe estar conectado a una de las secuencias para que pueda actualizar el reloj a través de él.	**1**
	Si habilitado, la contraseña de programador solamente irá funcionar si todas las particiones estén desarmadas. De esa forma se puede impedir que el usuario altere la programación vía teclado si la central esté armada.	**2**
	Modo de operación con Contraseñas aleatorias. Si habilitado, las contraseñas de usuario 3, 4 y 5 son generadas aleatoriamente y cambiadas automáticamente cuando utilizadas. Al deshabilitar ese modo, las contraseñas de usuario 3, 4 y 5 son borradas. Más detalles de ese modo de operación son descriptos abajo.	3
	Si habilitado, el auto arme por inercia de cualquier partición no irá armar si [363] alguna zona de la central disparar. En ese caso el sistema reinicia el contaje de tiempo y envía el evento programado en la función [465], “Falla en el auto arme” Informando la partición que no armó.	**4**
	Cuando efectuar download por Línea telefónica, esa opción hace con que o panel de alarme, después de comprobar la contraseña, desconectar y marcar el número de teléfono da la memória 4 (función[484]) para descargar.	**5**
	Ao habilitar essa função a central irá memorizar de forma permanente quais periféricos estão conectados ao barramento. Mesmo que a energia elétrica seja removida essa lista é mantida. Isso evita que em caso de falha de algum periférico a ordem das zonas, senhas e pgms seja alterada na inicialização do sistema.	6
	Cuando está activado, el evento de prueba periódica (Función 439) se envía utilizando ID_ISEP (Funciones 023-025) como el número de cuenta. Si está desactivada, utiliza el número de cuenta de la partición 1 (Función 066).	**7**
	Si la opción 8 de la función está habilitada, el evento de test de GPRS irá incluir el nível de señal en el campo zona do Contact ID. El valor del nivel de la señal puede variar de 000 (0%) a 032 (100%).	**8**

[086] Ganho de transmissão e Servidor #3 como backup

	Descrición	Tecla/Led
[086]	Ganancia de transmisión. Si está habilitado, aumenta la ganancia de transmisión en eventos de identificación de contacto enviados por línea telefónica.	**1**
	Cuando está activada, se puede utilizar VIAWEB SERVER # 3 como copia de seguridad VIAWEB SERVER # 1 con el mismo IDISEP. NOTA: Para utilizar esta opción, la función 025 se debe programar con cero.	**3**

Lacre de la Programación (Solamente Para Empresas de Monitoreo)

En instalaciones de alta seguridad, una vez que el sistema tenga sido configurado, programado y su funcionamiento garantido, se puede desear evitar que si haga cualquier tipo de alteración en él. Con la función de lacre, si puede garantir que la programación no fue alterada, mismo por alguién con

conocimiento de las contraseñas de programación y download o acceso al servidor VIAWEB.

Para aumentar la seguridad y evitar programaciones indeseadas, el lacre solo puede ser alterado a través del software de programación VIAWEB download.

Una vez lacrado, el acceso del software de programación VIAWEB download queda restringido a la conexión VIAWEB. Luego, solamente se debe lacrar la central después de ella tener sido programada y se encontrar ONLINE con el VIAWEB receiver. Caso contrario, existe la posibilidad de no más ser posible entrar en programación.

Todos los periféricos compatibles con esta nueva tecnología de lacre irán se lacrar también de la misma forma que la central. Los periféricos sin suporte a lacre no sufrirán alteraciones en el funcionamiento.

Atención: Una vez activado el lacre (programado con los valores 1, 5 o 9), solo será posible deshabilitar el lacre definitivamente haciendo un reset en la programación de la central. Caso la central esté con traba de reset, se debe liberar el lacre (programando la función 019 con 1) y después destrabar el reset. Note que si el equipamiento no está online, y fue lacrado con la traba de reset, no será más posible acceder su programación, ni resetarlo, y este deberá ser encaminado para manutención.

[019] Lacre de Programación

Patrón: 0 deshabilitado		**Tecla Led**
[019]	Valor Patrón de fábrica, o **lacre está desactivado** y la programación de la central puede ser alterada normalmente.	0
	Abertura de lacre: Programar 1 hará con que el evento de "Programación irá liberar" (Función 471) sea enviado. Caso ninguna programación sea hecha en esa Función, después de 4 (cuatro) minutos el lacre será liberado, y será posible alterar la configuración de la central normalmente. Después de 30 minutos el lacre vuelva automáticamente para el valor 5.	1
	Lacre total: Programar ese valor hará con que el evento de "Programación Lacrada" (Función 472) sea enviado. Cuando el lacre en ese nivel esté activado: **a)** No acepta la contraseña de programación. **b)** No atiende al download via Línea telefónica o vía cable serial. **c)** Solamente acepta liberación del lacre si esta fue hecha a través del VIAWEB receiver (VIAWEB download conectado por VIAWEB). **d)** No es posible cancelar la llamada o limpiar el buffer de comunicación.	5
	Lacre parcial: Tiene el mismo efecto del lacre total, con excepción de que aún es posible alterar la programación a través del VIAWEB download. Para garantir la eficiencia del lacre no se debe dejar el lacre parcial programado indefinidamente. Así que posible se debe lacrar totalmente la central grabando 5 en la función 019. Se puede alterar el lacre de 5 (total) para 9 (parcial), mas se debe aguardar 4 minutos antes que el lacre sea efectivamente liberado.	9

[471] Programación Irá Liberar Después de 4 Minutos – Código Contact ID

[471] [____] Patrón: 3407 (En el campo zona es enviado el nivel del lacre que irá asumir)

Cuatro dígitos con el código Contact ID del evento. Programar 0000 para deshabilitar el envio de ese evento.

[472] Programación Lacrada – Código Contact ID

[472] [____] Patrón: 3408 (En el campo zona es enviado el nivel del lacre)

Cuatro dígitos con el código Contact ID del evento. Programar 0000 para desabilitar el envio de esse evento.

AGENDAS

Utilizando el reloj integrado del sistema, es posible programar operaciones automáticas como armar, desarmar, activar y desactivar PGMs, enviar eventos o restringir el acceso de determinados usuarios.

En el total, se puede configurar hasta 34 agentamientos, con horario de inicio y fin.

Caso el reloj sea alterado en un tiempo inferior a 15 minutos, las acciones agentadas entre el horario antiguo y el nuevo serán ejecutadas. Si la alteración en el reloj es superior a 15 minutos, el sistema considera que el reloj estaba desconfigurado y los agentamientos que irían ocurrir en el período son ignorados. Si el reloj está con la hora errada, los agentamientos no son ejecutados.

[830 A 863] TIPO DE LA AGENDA

[830 a 863] [__] Patrón: 0 (Deshabilitado)

[830] [__] Agenda 1	[842] [__] Agenda 13	[854] [__] Agenda 25
[831] [__] Agenda 2	[843] [__] Agenda 14	[855] [__] Agenda 26
[832] [__] Agenda 3	[844] [__] Agenda 15	[856] [__] Agenda 27
[833] [__] Agenda 4	[845] [__] Agenda 16	[857] [__] Agenda 28
[834] [__] Agenda 5	[846] [__] Agenda 17	[858] [__] Agenda 29
[835] [__] Agenda 6	[847] [__] Agenda 18	[859] [__] Agenda 30
[836] [__] Agenda 7	[848] [__] Agenda 19	[860] [__] Agenda 31
[837] [__] Agenda 8	[849] [__] Agenda 20	[861] [__] Agenda 32
[838] [__] Agenda 9	[850] [__] Agenda 21	[862] [__] Agenda 33
[839] [__] Agenda 10	[851] [__] Agenda 22	[863] [__] Agenda 34
[840] [__] Agenda 11	[852] [__] Agenda 23	
[841] [__] Agenda 12	[853] [__] Agenda 24	

0 – Deshabilitado

Esse agendamento no está sIendo usado.

1 – Armar y Desarmar

Cuando el reloj atingir el horario de inicio, el usuario configurado en la función de complemento (Funciones 864 hasta 897) irá armar el sistema. Cuando el reloj atingir el horario final, el usuario irá desarmar el sistema.

Se puede configurar solamente el horario de inicio o solamente el horario final (programando el otro Horario con FF:FF). En ese caso el agentamiento puede solo armar o solo desarmar el sistema.

Las particiones que serán armadas o desarmadas son las particiones que el usuario tiene acceso.

Si el usuario esté configurado para permitir arme forzado, en el momento del agentamiento él irá armar el sistema en el modo forzado.

Caso existan zonas de la central abiertas en el momento de armar, el sistema no irá armar si no for configurado el arme forzado del usuario.

Solamente son válidos usuarios 0001 hasta 0100.

2 – Accionar PGM

A pgm a ser controlada debe ser programada en la función de complemento de la agenda (Funciones 864 hasta 897). Los valores posibles son 0001 hasta 0255.

En el horario de inicio, la PGM acciona. En el horario final la PGM desactiva.

Se puede configurar solamente el Horario de inicio o solamente el Horario final (programando el otro Horario con FF:FF). Em ese caso, se puede hacer con que el agentamiento solamente accione o desactive la PGM.

3 – Enviar Evento

El evento enviado sigue el formato Contact ID programado en el complemento de la agenda (Funciones 864 a 897). Los valores posibles son 1000 hasta FFFF.

El evento es enviado tanto en el Horario de inicio como en el Horario final, con el valor 00 para la partición y 000 para la zona/usuario.

Se puede configurar solamente el horario de inicio o solamente el Horario final (programando el otro Horario con FF:FF). En ese caso, el evento es enviado solamente en el horario válido.

4 – Restringir acceso de usuario

Durante el período comprendido entre el Horario de inicio y el Horario final de la agenda, el usuario configurado en el complemento de la agenda no tendrá acceso al sistema.

Solamente son válidos usuarios 0001 hasta 0100.

Durante el período de restrición, al digitar la contraseña de ese usuario, se recibe la información de Contraseña inválida.

[864 a 897] Complemento de la Agenda

[864 a 897] [__/__/__/__] Patrón: 0000

[864] [__ __ __ __] Complemento de la agenda 1
[865] [__ __ __ __] Complemento de la agenda 2
[866] [__ __ __ __] Complemento de la agenda 3
[867] [__ __ __ __] Complemento de la agenda 4
[868] [__ __ __ __] Complemento de la agenda 5
[869] [__ __ __ __] Complemento de la agenda 6
[870] [__ __ __ __] Complemento de la agenda 7
[871] [__ __ __ __] Complemento de la agenda 8
[872] [__ __ __ __] Complemento de la agenda 9
[873] [__ __ __ __] Complemento de la agenda 10
[874] [__ __ __ __] Complemento de la agenda 11
[875] [__ __ __ __] Complemento de la agenda 12
[876] [__ __ __ __] Complemento de la agenda 13
[877] [__ __ __ __] Complemento de la agenda 14
[878] [__ __ __ __] Complemento de la agenda 15
[879] [__ __ __ __] Complemento de la agenda 16
[880] [__ __ __ __] Complemento de la agenda 17
[881] [__ __ __ __] Complemento de la agenda 18
[882] [__ __ __ __] Complemento de la agenda 19
[883] [__ __ __ __] Complemento de la agenda 20
[884] [__ __ __ __] Complemento de la agenda 21
[885] [__ __ __ __] Complemento de la agenda 22
[886] [__ __ __ __] Complemento de la agenda 23
[887] [__ __ __ __] Complemento de la agenda 24
[888] [__ __ __ __] Complemento de la agenda 25
[889] [__ __ __ __] Complemento de la agenda 26
[890] [__ __ __ __] Complemento de la agenda 27
[891] [__ __ __ __] Complemento de la agenda 28
[892] [__ __ __ __] Complemento de la agenda 29
[893] [__ __ __ __] Complemento de la agenda 30
[894] [__ __ __ __] Complemento de la agenda 31
[895] [__ __ __ __] Complemento de la agenda 32
[896] [__ __ __ __] Complemento de la agenda 33
[897] [__ __ __ __] Complemento de la agenda 34

[898 a 931] Horario de Inicio de la Agenda

[898 a 931] [__/__/__/__] Patrón: 0000

Se programa en horas y minutos (HH:MM). Para deshabilitar el Horario se debe programar FFFF.

[898] [__ : __] Inicio de la agenda 1
[899] [__ : __] Inicio de la agenda 2
[900] [__ : __] Inicio de la agenda 3
[901] [__ : __] Inicio de la agenda 4
[902] [__ : __] Inicio de la agenda 5
[903] [__ : __] Inicio de la agenda 6
[904] [__ : __] Inicio de la agenda 7
[905] [__ : __] Inicio de la agenda 8
[906] [__ : __] Inicio de la agenda 9
[907] [__ : __] Inicio de la agenda 10
[908] [__ : __] Inicio de la agenda 11
[909] [__ : __] Inicio de la agenda 12
[910] [__ : __] Inicio de la agenda 13
[911] [__ : __] Inicio de la agenda 14
[912] [__ : __] Inicio de la agenda 15
[913] [__ : __] Inicio de la agenda 16
[914] [__ : __] Inicio de la agenda 17
[915] [__ : __] Inicio de la agenda 18
[916] [__ : __] Inicio de la agenda 19
[917] [__ : __] Inicio de la agenda 20
[918] [__ : __] Inicio de la agenda 21
[919] [__ : __] Inicio de la agenda 22
[920] [__ : __] Inicio de la agenda 23
[921] [__ : __] Inicio de la agenda 24
[922] [__ : __] Inicio de la agenda 25
[923] [__ : __] Inicio de la agenda 26
[924] [__ : __] Inicio de la agenda 27
[925] [__ : __] Inicio de la agenda 28
[926] [__ : __] Inicio de la agenda 29
[927] [__ : __] Inicio de la agenda 30
[928] [__ : __] Inicio de la agenda 31
[929] [__ : __] Inicio de la agenda 32
[930] [__ : __] Inicio de la agenda 33
[931] [__ : __] Inicio de la agenda 34

[932 a 965] Horario Final de la Agenda

[932 a 965] [__/__/__/__] Patrón: 0000

Se programa en horas y minutos (HH:MM). Para deshabilitar el horario se debe programar FFFF.

[932] [__ : __] Fin de la agenda 1
[933] [__ : __] Fin de la agenda 2
[934] [__ : __] Fin de la agenda 3
[935] [__ : __] Fin de la agenda 4
[936] [__ : __] Fin de la agenda 5
[937] [__ : __] Fin de la agenda 6
[838] [__ : __] Fin de la agenda 7
[839] [__ : __] Fin de la agenda 8
[940] [__ : __] Fin de la agenda 9
[941] [__ : __] Fin de la agenda 10
[942] [__ : __] Fin de la agenda 11
[943] [__ : __] Fin de la agenda 12
[944] [__ : __] Fin de la agenda 13
[945] [__ : __] Fin de la agenda 14
[946] [__ : __] Fin de la agenda 15
[947] [__ : __] Fin de la agenda 16
[948] [__ : __] Fin de la agenda 17
[949] [__ : __] Fin de la agenda 18
[950] [__ : __] Fin de la agenda 19
[951] [__ : __] Fin de la agenda 20
[952] [__ : __] Fin de la agenda 21
[953] [__ : __] Fin de la agenda 22
[954] [__ : __] Fin de la agenda 23
[955] [__ : __] Fin de la agenda 24
[956] [__ : __] Fin de la agenda 25
[957] [__ : __] Fin de la agenda 26
[958] [__ : __] Fin de la agenda 27
[959] [__ : __] Fin de la agenda 28
[960] [__ : __] Fin de la agenda 29
[961] [__ : __] Fin de la agenda 30
[962] [__ : __] Fin de la agenda 31
[963] [__ : __] Fin de la agenda 32
[964] [__ : __] Fin de la agenda 33
[965] [__ : __] Fin de la agenda 34

[966 a 999] Días de la Semana de la Agenda

[966 a 999] Patrón: (Deshabilitados, todas las opciones desmarcadas)

Además del Horario de inicio y del Horario final, para que el agentamiento ocurra, los días de la semana deben estar habilitados en la agenda.

Opción 8 – Feriados:

Caso la opción 8 esté habilitada, el agentamiento irá ocurrir también en los feriados, independiente del día de la semana. Para configurar cuales días serán considerados feriados, verificar las funciones 521 a 535.

	Dom	Lun	Mar	Mier	Jue	Vier	Sáb	Feriados
[966] Días de la Semana Agenda 1	1	2	3	4	5	6	7	**8**
[967] Días de la Semana Agenda 2	1	2	3	4	5	6	7	**8**
[968] Días de la Semana Agenda 3	1	2	3	4	5	6	7	**8**
[969] Días de la Semana Agenda 4	1	2	3	4	5	6	7	**8**
[970] Días de la Semana Agenda 5	1	2	3	4	5	6	7	**8**
[971] Días de la Semana Agenda 6	1	2	3	4	5	6	7	**8**
[972] Días de la Semana Agenda 7	1	2	3	4	5	6	7	**8**
[973] Días de la Semana Agenda 8	1	2	3	4	5	6	7	**8**
[974] Días de la Semana Agenda 9	1	2	3	4	5	6	7	**8**
[975] Días de la Semana Agenda 10	1	2	3	4	5	6	7	**8**
[976] Días de la Semana Agenda 11	1	2	3	4	5	6	7	**8**
[977] Días de la Semana Agenda 12	1	2	3	4	5	6	7	**8**
[978] Días de la Semana Agenda 13	1	2	3	4	5	6	7	**8**

[979] Días de la Semana Agenda 14	1	2	3	4	5	6	7	**8**
[980] Días de la Semana Agenda 15	1	2	3	4	5	6	7	**8**
[981] Días de la Semana Agenda 16	1	2	3	4	5	6	7	**8**
[982] Días de la Semana Agenda 17	1	2	3	4	5	6	7	**8**
[983] Días de la Semana Agenda 18	1	2	3	4	5	6	7	**8**
[984] Días de la Semana Agenda 19	1	2	3	4	5	6	7	**8**
[985] Días de la Semana Agenda 20	1	2	3	4	5	6	7	**8**
[986] Días de la Semana Agenda 21	1	2	3	4	5	6	7	**8**
[987] Días de la Semana Agenda 22	1	2	3	4	5	6	7	**8**
[988] Días de la Semana Agenda 23	1	2	3	4	5	6	7	**8**
[989] Días de la Semana Agenda 24	1	2	3	4	5	6	7	**8**
[990] Días de la Semana Agenda 25	1	2	3	4	5	6	7	**8**
[991] Días de la Semana Agenda 26	1	2	3	4	5	6	7	**8**
[992] Días de la Semana Agenda 27	1	2	3	4	5	6	7	**8**
[993] Días de la Semana Agenda 28	1	2	3	4	5	6	7	**8**
[994] Días de la Semana Agenda 29	1	2	3	4	5	6	7	**8**
[995] Días de la Semana Agenda 30	1	2	3	4	5	6	7	**8**
[996] Días de la Semana Agenda 31	1	2	3	4	5	6	7	**8**
[997] Días de la Semana Agenda 32	1	2	3	4	5	6	7	**8**
[998] Días de la Semana Agenda 33	1	2	3	4	5	6	7	**8**
[999] Días de la Semana Agenda 34	1	2	3	4	5	6	7	**8**

Ejemplo: Programar una agenda para Restringir usuario 003 das 12:00 a las 13:30 horas, de lunes a viernes.

Programar las siguientes funciones:
830 = 4
864 = 0003 (Número del usuario)
898 = 12:00 (Horario de inicio)
932 = 13:30 (Horario de fin)
966 = Opciones 2 a 6 habilitados (lunes a viernes)

En el exemplo, a partir de las 12:00, el usuario 003 no tiene más acceso a la central. Cuando el reloj marcar el Horario final (13:30) el usuario 3 vuelve a tener acceso.

[521 a 535] Calendário de Feriados

En esas funciones son definidos 15 feriados anuales con dia y mes. En los días de feriado, funciones de Auto Activa y Auto Desactiva se comportan como Domingo.

[521] [D / D / M / M] Feriado 1 [526] [D / D / M / M] Feriado 6 [531] [D / D / M / M] Feriado 11
[522] [D / D / M / M] Feriado 2 [527] [D / D / M / M] Feriado 7 [532] [D / D / M / M] Feriado 12
[523] [D / D / M / M] Feriado 3 [528] [D / D / M / M] Feriado 8 [533] [D / D / M / M] Feriado 13
[524] [D / D / M / M] Feriado 4 [529] [D / D / M / M] Feriado 9 [534] [D / D / M / M] Feriado 14
[525] [D / D / M / M] Feriado 5 [530] [D / D / M / M] Feriado 10 [535] [D / D / M / M] Feriado 15

RESET

Reset de las Contraseñas Maestras y de Programación

Para que las contraseñas maestras e de programación vuelvan para los valores de fábrica siga los pasos:

- Alimente la central (el reset solo funciona en los primeros 4 minutos)
- Mantenga el botón multifuncional* pulsado por 10 segundos.
- El led de status de la central LD3 y LD4 van parpadear lentamente.
- Solté el botón.

Después de ese procedimiento las contraseñas retornan al Patrón de fábrica:

Contraseña de Programación: 5353 Contraseña Maestra 001: 1515

Reset Total de la Programación

Para que Los valores de todas las Funciones vuelvan para los patrones de fábrica siga los pasos:

- Mantenga ambos los botones* pulsados por 20 segundos.
- En 10 segundos los leds 1 e 2 empiezan a parpadear indicando que hubo reset de las contraseñas (si el equipamiento es central de Alarma), aguarde más 10 segundos sin soltar el botón.
- Los leds quedan encendidos indicando que el equipamiento está retornando a los valores de fábrica.
- Solté el botón. **AGUARDE LOS LEDS VOLVEREN A PARPADEAR PARA RETIRAR LA ALIMENTACIÓN**, **Caso contrário el reset no será completado.**

*La posición del “Botón multifuncional” y del “Led de status de la central” están en la página 11.

Ojo.: En el reset total todas las contraseñas también vuelven a los valores de fábrica

[362] Trava de Reset

[362] [__/__/__] Patrón: 000

Cuando es programado el valor 147 en esa función, se torna imposible restaurar la programación y las contraseñas de fábrica (reset) de la central hasta que se programe en esta función un valor distinto de 147.

CÓDIGOS DE LOS EVENTOS DE LA ALARMA (CONTACT – ID)

La VW16ZGPRSIP informa inmediatamente a la central de monitoreo (cuando programada) todas las alteraciones en su estado, situación de las particiones, fallas y restauros, programaciones, etc. Todas esas informaciones pueden ser reportadas en todas las vías de comunicación disponibles (ethernet TCP/IPv4). Inclusive cuando si utilizan módulos externos (VWGPRS o expansores).

Esas informaciones enviadas permiten a la central de monitoreo perfecta identificación de cual panel envió la comunicación, vinculado a la fecha y hora del evento, y permite identificar diversos tipos de ocurrencias.

Eses eventos son identificados tanto en la central de monitoreo cuanto en el servidor VIAWEB SERVICE por el protocolo CONTACT-ID. Basicamente, un evento de Contact-id es generado de esa manera:

CCCC	QXXX	YY	ZZZ
Cliente	Evento	Partición	Complemento

CCCC – Cliente:

Esta es la identificación del cliente en la empresa de monitoreo.
(programado en las funciones de [066] hasta [073]).

Q – Qualifier do evento:

Es el dígito que define si el código es un evento (desarme, disparo, Falla, etc.), o un restauro (arme, restauración de disparo, restauración de Falla, etc.). 1 = EVENTO y 3 = RESTAURO.

XXX – Código del evento:

Cada evento tiene un código Patrón distinto. En la tabla abajo encontramos los códigos generados por la central y el campo caso necesiten de alteración.

YY – Partición:

Cuando el sistema es particionado indica en cual la partición ocurrió el evento.

ZZZ – Complemento:

Referente al evento. Por ejemplo, en el caso de disparo, ese campo mostra la zona que fue disparada, o cuando el sistema es armado, ese campo indica cual usuario armó el sistema.

OJO.: La alteración de los eventos en los campos abajo puede dificultar la interpretación de los eventos tanto por la aplicación cuanto por la central de monitoreo.

La aplicación Viaweb Mobile “traduce” automáticamente el evento Contact-id, no siendo necesaria la alteración de los campos abajo.

Caso el evento programado en los campos abajo no esté dentro de los padrones, cuando generado, en la aplicación aparecerá solamente el valor programado y no la descripción de él.

Algunos códigos Contact-ID usados para identificación de las ocurrencias pueden ser programados. Las Funciones 401 a 476 sirven para alterar o cancelar eses códigos.

[401 a 476] Códigos de los Eventos en Contact - ID

0000 = Desabilita o evento

Alarmes

[401] [1 /1 / 3 / 0] Alarma de Robo
[402] [1 / 1 / 3 / 0] Disparo de zona 1
[403] [1 / 1 / 3 / 0] Disparo de zona 2
[404] [1 / 1 / 3 / 0] Disparo de zona 3
[405] [1 / 1 / 3 / 0] Disparo de zona 4
[406] [1 / 1 / 3 / 0] Disparo de zona 5
[407] [1 / 1 / 3 / 0] Disparo de zona 6
[408] [1 / 1 / 3 / 0] Disparo de zona 7
[409] [1 / 1 / 3 / 0] Disparo de zona 8
[410] [1 / 1 / 3 / 0] Disparo de zona 9
[411] [1 / 1 / 3 / 0] Disparo de zona 10
[412] [1 / 1 / 3 / 0] Disparo de zona 11
[413] [1 / 1 / 3 / 0] Disparo de zona 12
[414] [1 / 1 / 3 / 0] Disparo de zona 13
[415] [1 / 1 / 3 / 0] Disparo de zona 14
[416] [1 / 1 / 3 / 0] Disparo de zona 15
[417] [1 / 1 / 3 / 0] Disparo de zona 16
[418] [1 / 1 / 4 / 4] Violación de Tamper **- SMS**
[419] [1 / 1 / 0 / 0] Emergencia Médica **- SMS**
[420] [1 / 1 / 1 / 0] Incendio **- SMS**
[421] [1 / 1 / 2 / 0] Emergencia Silenciosa **- SMS**
[422] [1 / 1 / 2 / 1] Coacción

Restauros

[441] [0 / 0 / 0 / 0] Restauro Geral
[442] [3 / 1 / 3 / 0] Restauro de zona 1
[443] [3 / 1 / 3 / 0] Restauro de zona 2
[444] [3 / 1 / 3 / 0] Restauro de zona 3
[445] [3 / 1 / 3 / 0] Restauro de zona 4
[446] [3 / 1 / 3 / 0] Restauro de zona 5
[447] [3 / 1 / 3 / 0] Restauro de zona 6
[448] [3 / 1 / 3 / 0] Restauro de zona 7
[449] [3 / 1 / 3 / 0] Restauro de zona 8
[450] [3 / 1 / 3 / 0] Restauro de zona 9
[451] [3 / 1 / 3 / 0] Restauro de zona 10
[452] [3 / 1 / 3 / 0] Restauro de zona 11
[453] [3 / 1 / 3 / 0] Restauro de zona 12
[454] [3 / 1 / 3 / 0] Restauro de zona 13
[455] [3 / 1 / 3 / 0] Restauro de zona 14
[456] [3 / 1 / 3 / 0] Restauro de zona 15
[457] [3 / 1 / 3 / 0] Restauro de zona 16
[458] [3 / 1 / 4 / 4] Restauro de Tamper **- SMS**

Falhas

[423] [0 / 0 / 0 / 0] Zona esquecida aberta
[424] [1 / 3 / 0 / 0] Falla de Fuente Auxiliar
[425] [1 / 3 / 0 / 1] Falla de Energia Eléctrica **- SMS**
[426] [1 / 3 / 0 / 2] Falla de Bateria **- SMS**
[427] [1 / 3 / 3 / 3] F. Tensión en el Barramento **- SMS**
[428] [1 / 3 / 2 / 1] Falla de Sirena 1 **- SMS**
[429] [1 / 1 / 4 / 3] Falla de Módulo Expansor
[430] [1 / 3 / 5 / 0] Falla de Comunicación
[431] [1 / 3 / 5 / 1] Falla de Línea Telefónica – **SMS**
[432] [1 / 1 / 4 / 2] Corto circuito na zona **– SMS**
[465] [0 / 0 / 0 / 0] Falla de auto arme

Restauros

[459] [3 / 3 / 0 / 0] Restauro de Fuente Auxiliar
[460] [3 / 3 / 0 / 1] Restauro Energia Eléctrica **- SMS**
[461] [3 / 3 / 0 / 2] Restauro de Falla de Bateria **- SMS**
[462] [3 / 3 / 3 / 3] R. de F. Tensión en el Barramento
[463] [3 / 3 / 2 / 1] Restauro de Sirena 1 **- SMS**
[464] [3 / 1 / 4 / 3] Restauro de Módulo Expansor
[466] [3 / 3 / 5 / 1] Rest. de Línea Telefónica – **SMS**
[467] [3 / 1 / 4 / 2] Restauro de Corto Circuito **- SMS**

Desarmado

[433] [1 / 4 / 0 / 1] Desactivado por Contraseña **- SMS**
[434] [1 / 4 / 0 / 2] Partición Desac. Contraseña **- SMS**

Armados

[468] [3 / 4 / 0 / 1] Activado por Contraseña **-SMS**
[469] [3 / 4 / 0 / 2] Partición Act por Contraseña **- SMS**
[470] [3 / 4 / 0 / 3] Auto Activación **– SMS**
[473] [1 / 4 / 1 / 0] Acesso via Download **- SMS**
[474] [3 / 4 / 5 / 6] Activado Forzado

Exclusión

[436] [1 / 5 / 7 / 0] Exclusión de Zona **- SMS**
[437] [1 / 5 / 7 / 0] Auto Exclusión de Zona **- SMS**

Controle de Acesso

[440] [1 / 4 / 1 / 2] Ev. de acesso remoto pelo Viaweb
[471] [3 / 4 / 0 / 7] Programación lacrada, no campo zona irá o nível de lacre.
[472] [3 / 4 / 0 / 8] Programación irá liberar después 4 minutos, en el campo zona irá el nível que el lacre irá assumir.
[473] [0 / 0 / 0 / 0] Ev. de acesso por cabo serial

Testes

[438] [1 / 6 / 0 / 2] Test Automático **- SMS**
[439] [1 / 6 / 0 / 3] Test Internet

PGM

[475] [0 / 0 / 0 / 0] Evento da PGM 1
[476] [0 / 0 / 0 / 0] Evento da PGM 2

Indice por Funciones

[000] Versión del Firmware de la Central....64
[001 a 003] Secuencias de Comunicación....22
[004 a 006] Filtro de Eventos Particiones....23
[007 a 012] Filtro de Eventos de las Secuencias....23
[013 a 015] Tentativas de Envio de las Secuencias....24
[016] Primero Periférico de Comunicación Auxiliar (Medio de Comunicación 04)....24
[017] Segundo Periférico de Comunicación Auxiliar (Medio de Comunicación 05)....24
[018] Partición y Zona dos Eventos Internos....20
[019] Lacre de Programación....67
[020] Intervalo de Ping....18
[021 y 022] Servidores Dns....18, 25
[023 a 025] ID ISEP....18
[026 a 028] Puerta Tcp Do Servidor....19
[029 a 031] Dirección del Servidor....19
[032] Horario del Primero Test de Internet....19
[033] Intervalo de Test Internet....19
[034 a 036] Dirección del Servidor (Para Teclado Led)....19
[037 y 038] Selecciona Operadora Sim Card #1 y #2 (Para Teclado de Led)....28
[041 y 541] Pin Do Sim Card #1 y #2....29
[042 y 542] Apn Gprs Sim 1 y Sim 2....29
[044 y 544] Contraseña Gprs Sim 1 y Sim 2....29
[045 y 545] Número del ICCID del Sim Card 1 y 2 (solamente lectura)....29
[046] Versión del Módulo Gprs (solamente lectura)....29
[047 a 050] Horario de Funcionamento de las Contraseñas con Horario Restringido....47
[051] Dirección Ip Na Red....25
[052] Gateway....25
[053] Máscara de Red....25
[054] Dirección Mac (Solamente Lectura)....25
[055] DHCP....26
[056] Servidor Ntp....26
[057] Huso Horario....26
[058] Intervalo del Test de Línea Cuando la Partición 1 Está Armada....32
[059] Intervalo del Test de Línea Cuando la Partición 1 Está Desarmada....32
[060] Horario del Primero Test de Línea Telefónica....31
[061] Intervalo del Test de Línea Telefónica....31
[066 a 073] Número de la Cuenta de la Partición....19
[074] Detector de Línea Telefónica....31
[075] Retardo na Falla de Línea Telefónica....33
[081] Opiciones de la Línea....32
[082] Problemas que Disparam a Sirena....53
[086] Ganho de transmissão e Servidor #3 como backup....66
[086] Opiciones de Transmisión....33
[086] Servidor Viaweb #3 como backup do Servidor Viaweb #1 - opción (Bit) 3....20
[091 a 106] Tipo de las Zonas....38
[107] Configuración de las Zonas....34
[108] Velocidad de las Zonas....38
[109 y 110] Zonas Com Chime....41
[111 y 112] Zonas Sin Exclusión....41
[113] Número de Disparos Para Auto Exclusión....41
[114 y 115] Zonas Cruzadas....42
[116] Número de Zonas Cruzadas Abiertas Para Disparo....42
[119] Zona Olvidada Abierta (Zona 2)....42

[120] Particiones Que Hacen Pitidos Durante la Temporización....39
[121 y 123] Tiempo de Entrada y Salida 1....38
[122 y 124] Tiempo de Entrada y Salida 2....39
[125] Tiempo de Zona Anti-Secuestro....40
[126] Tiempo de Zona Anti-Invasión....41
[127] Tiempo de Zona Preventiva....39
[130] Días de la Semana con Auto Desactiva....50
[131 a 138] Horario de Auto Activa....49
[139 a 146] Activación Por Inercia de las Particiones....50
[147 a 154] Horario en que las Particiones Están Siempre Armadas....51
[155 a 158] Días de la Semana en que las Particiones Están Siempe Armadas....52
[159 a 166] Horario en que las Particiones Activan Por Inercia....50
[167 a 170] Días de la Semana en que las Particiones Activam Por Inercia....51
[171 a 186] Particiones das Zonas....48
[187 a 202] Particiones de Control Remoto....40
[203] Partición 8 Comum....49
[204] Sistema Particionado....47
[205] Particiones Para Auto Activa (Auto Activa del Teclado)....50
[206 a 209 y 358 a 361] Horario de Auto Desactiva....49
[210 y 211] Tiempo de Sirena....52
[213 y 214] Particiones que Disparan la Sirena....52
[216 y 217] Bip de la Sirena....53
[219] Supervisión de la Sirena....53
[220] Número de Dígitos de las Contraseñas....44
[221] Contraseña de Programación....44
[222 a 321] Particiones que el Usuario Tiene Acceso (001 a 100)....44
[322 a 334] Contraseñas que Arman Forzado (Away)....45
[335 a 347] Contraseñas que no Excluyen Zonas....46
[348] Contraseña de Coacción....45
[349 y 350] Usuários Tiemporários (Contraseñas 029 y 030)....46
[351] Número de Tonos Para Download....33
[352] Contraseña de Download....45
[354] Llamada Dupla....33
[355 y 357] Permiso de Acceso Remoto....64
[362] Trava de Reset....72
[363] Ajuste del Reloj y Test Periódico - Opciones (BITS) 1, 7 y 8....20
[363] Anular Auto Activación con Zona Abierta – Opción (BIT) 4....51
[363] Diversos....66
[363] Habilita Callback no Download – opción (bit) 5....33
[363] Inibir Contraseña de Programación Cuando Central Está Armada - (Bit) 2....44
[363] Programación de Contraseñas Aleatórias - Opción (BIT) 3....65
[363] Salva la Lista de Periféricos Conectados al Innovabus - Opción (BIT) 6....65
[366] Teclas Especiales 1 y 2....64
[371 a 374] Eventos de las Pgms....54
[375 y 376] Operación Lógica De Las Pgms....55
[377 a 380] Complemento De Las PGM's (Tipo Valor)....56
[381 a 384] Complemento De Las PGM's (Tipo Función)....56
[385 y 386] Tiempo Das Pgms....56
[387 a 399] Contraseñas con Horario Restringido....46
[400] Días de la Semana de Funcionamiento de las Contraseñas con Horario Restringido....47
[401 a 476] Códigos de los Eventos en Contact - ID....74
[423] Zona Olvidada Abierta – Código Contact ID....42
[440] Evento de Acceso Remoto – Código Contact ID....20
[465] Falla en el Auto Arme – Código Contact Id....51
[471] Programación Irá Liberar Después de 4 Minutos – Código Contact I....67

[472] Programación Lacrada – Código Contact I.....67
[473] Evento de Acceso Via Cable Serial – Código Contact ID.....20
[481 a 488] Números Telefónicos / Números SMS.....31
[491 a 494] Tiempo de Rearme de las Particiones Siempre Armadas.....52
[502 y 503] Kbytes Trafegados Sim Card 1 y 2 (solamente lectura).....29
[512] Horario de Envio del Informe.....62
[513] Días de la Semana Para Envio de Informe.....62
[520] Permisión de Accesso a la Navegación Web.....28
[521 a 535] Calendário de Feriados.....71
[551] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 1.....61
[552] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 2.....61
[553] Direcciones de Correo Electrónico Para Recepción de Eventos y Informes 3.....62
[561] Servidor Smtp.....61
[562] Puerta Para Correo Electrónico (Servidor Smtp).....61
[564] Usuario Correo Electrónico.....61
[565] Contraseña Correo Electrónico.....61
[570] Viaweb Direct - Llave Criptográfica.....58
[571] Habilita Registro Automático Viaweb Direct.....58
[580] Habilita Dynamic Dns.....59
[581] Dirección Externa (HOSTNAME).....59
[582] Usuario Dynamic Dns.....59
[583] Contraseña Dynamic Dns.....59
[584] Resultado Dynamic Dns.....59
[591 a 598] Nombres de las Particiones.....49
[601 a 700] Nombre de los Usuarios.....44
[701 a 828] Nombre de las Zonas.....42
[830 a 863] Tipo de la Agenda.....68
[864 a 897] Complemento de la Agenda.....69
[898 a 931] Horario de Inicio de la Agenda.....69
[932 a 965] Horario Final de la Agenda.....70
[966 a 999] Días de la Semana de la Agenda.....70