


# Manual de Programação e instalação

## Central VW16Z 4G IP – VW16Z 4G – VW16Z IP

**V7.34 – R4.10 – Julho 2026**

www.viawebsystem.com.br

**Produto**: VW16Z 4G IP e VW16Z 4G
**Modelo**: VW_GPRS_BG95-M3
Incorpora produto homologado pela Anatel sob número 13721-22-04635
**Modelo:** VW_GPRS_EG915U
Incorpora produto homologado pela Anatel sob número 17660-22-04635

País de origem: Brasil
Fabricante: SI – Sistemas Inteligentes Eletrônicos Ltda.

# Índice


***Principais Características*** ..... **8**
Especificação detalhada interface de rede: ..... 8
Suporte a protocolo de autenticação 802.1X ..... 8
***Instalação*** ..... **9**
***Periféricos*** ..... **9**
***Fixação*** ..... **9**
***Placa Central*** ..... **10**
***VIAWEB Studio*** ..... **11**
***Operação do Alarme*** ..... **11**
Armar e Desarmar o sistema ..... 11
Operando Via página Web ..... 11
Operando Via Teclado ..... 12
***Programando a Central*** ..... **13**
Por teclado ..... 13
Via cabo serial – Software VIAWEB download ..... 15
***Página Web*** ..... **15**
Identificando o dispositivo na rede ..... 15
Página inicial ..... 16
Botões de menu ..... 16
***MONITORAMENTO (Comunicador Internet)*** ..... **17**
[ 020 ] Intervalo de Ping IP (Keep Alive) ..... 17
[ 040 ] Intervalo de Ping 4G (Keep Alive) ..... 17
[ 023 a 025 ] ID ISEP ..... 17
[ 026 a 028 ] Porta TCP do Servidor ..... 17
[ 029 a 031 ] Endereço do Servidor ..... 17
[ 034 a 036 ] Endereço do servidor (para teclado LED) ..... 18
[ 066 a 073 ] Número da Conta da Partição ..... 18
[ 032 ] Horário do Primeiro Teste de Internet ..... 18
[ 033 ] Intervalo de Teste Internet ..... 18
[ 440 ] Evento de Acesso Remoto – Código Contact ID ..... 18
[ 473 ] Evento de Acesso via Cabo Serial – Código Contact ID ..... 18
[ 018 ] Partição e Zona dos eventos internos ..... 18
[ 086 ] Servidor VIAWEB #3 como backup do Servidor VIAWEB #1 – opção (Bit) 3 ..... 19
[ 086 ] Bloqueia o acesso remoto da conexão com os servidores #1, #2 e #3 (Bit) 6, 7 e 8 ..... 19
[ 363 ] Ajuste do relógio e Teste periódico – opções (bits) 1, 5, 7 e 8 ..... 19
***Formato de comunicação*** ..... **20**
[ 001 a 003 ] Sequências de Comunicação ..... 20
[ 004 a 006 ] Filtro de Eventos Partições ..... 21
[ 007 a 012 ] Filtro de Eventos das Sequências ..... 21
[ 013 a 015 ] Tentativas de Envio das Sequências ..... 21
[ 016 ] Primeiro Periférico de Comunicação Auxiliar (meio de comunicação 04) ..... 21
[ 017 ] Segundo Periférico de Comunicação Auxiliar (meio de comunicação 05) ..... 21
***IP (Ethernet)*** ..... **22**
[ 051 ] Endereço IP na Rede ..... 22
[ 052 ] Gateway ..... 22
[ 053 ] Máscara de Sub Rede ..... 22
[ 054 ] Endereço MAC (Somente Leitura) ..... 22
[ 021 e 022 ] Servidores DNS ..... 22
[ 055 ] DHCP ..... 23

[ 056 ] Servidor NTP....23
[ 057 ] Fuso horário....24
***4G....25***
[ 037 e 038 ] Seleciona Operadora (para teclado de LED)....25
[ 041 e 541 ] PIN do SIM CARD 1 e 2....26
[ 042 e 542 ] APN do SIM CARD 1 e 2....26
[ 043 e 543 ] Usuário SIM CARD 1 e 2....26
[ 044 e 544 ] Senha SIM CARD 1 e 2....26
[ 045 e 545 ] Número do ICCID do SIM CARD 1 e 2 (somente leitura)....26
[ 502 e 503 ] KBytes Trafegados SIM CARD 1 e 2 (somente leitura)....26
[ 046 ] Versão do Módulo 4G (somente leitura)....26
[ 076 ] Estado Geral da Comunicação....26
***ZONAS....27***
[ 107 ] Configuração das Zonas....27
[ 108 ] Velocidade das Zonas....33
[ 091 a 106 ] Tipo das Zonas....33
*Instantânea – todas as opções apagadas....34*
*Temporizada 1 – opção 1....34*
[ 121 e 123] Tempo de Entrada e Saída 1....34
*Temporizada 2 – opção 2....34*
[ 122 e 124] Tempo de Entrada e Saída 2....34
[ 120 ] Partições que Bipam durante a Temporização....34
*Seguidora – opção 1 e 2....34*
*Preventiva – opção 3....34*
[ 127 ] Tempo de Zona Preventiva....35
*24 Horas – opção 4....35*
*Silenciosa – opção 5....35*
*Controle Remoto – opção 6....35*
[ 187 a 202 ] Partições de Controle Remoto....35
*Restauro – opção 7....36*
*Anti-Sequestro – opção 5 e 6....36*
[ 125 ] Tempo de Zona Anti-Sequestro....36
*Anti-Invasão – opção 4, 5 e 6....36*
[ 126 ] Tempo de Zona Anti-Invasão....36
*Auto Exclusão – opção 8....36*
[ 113 ] Número de Disparos para Auto Exclusão....36
[ 109 e 110 ] Zonas com Chime....36
[ 111 e 112 ] Zonas sem Exclusão....37
[ 114 e 115 ] Zonas Cruzadas....37
[ 116 ] Número de Zonas Cruzadas abertas para Disparo....37
[ 119 ] Zona Esquecida Aberta (Zona 2)....37
[ 423 ] Zona Esquecida Aberta – Código Contact ID....37
[ 117 e 118 ] Inversão do estado das zonas....37
[ 1501 a 1628 ] Nome das Zonas....38
***SENHAS....38***
Cadastrando senhas....38
Cadastrando senhas por teclado....38
Cadastrando senhas via Página WEB....38
[ 220 ] Número de Dígitos das Senhas....39
[ 221 ] Senha de Programação....39
[ 222 a 285 ] Partições que o Usuário tem Acesso (01 a 64)....39
[ 348 ] Senha de Coação....39

[ 349 e 350 ] Usuários temporários (senhas 029 e 030)....39
[ 352 ] Senha de Download....40
[ 047 a 050] Horário de Funcionamento das Senhas com Horário Restrito....40
[ 400 ] Dias da semana de Funcionamento das Senhas com Horário Restrito....40
[ 363 ] Inibir senha de programação quando central está armada - (bit) 2....40
[ 1401 a 1464 ] Nome dos Usuários....40
***GRUPOS DE USUÁRIOS....41***
[ 601 a 664 ] Grupo do usuário – Tipos de Grupos....41
[ 399 ] Grupo desabilita o rearme por inércia....41
[ 322 ] Grupo arme forçado....42
[ 323 ] Grupo não exclui zona....42
[ 324 ] Grupo horário restrito....42
***PARTIÇÕES....42***
[ 204 ] *Sistema Particionado*....42
[ 171 a 186 ] Partições das Zonas....43
[ 591 a 598 ] Nomes das Partições....44
[ 203 ] Partição 8 Comum....44
***AUTO ATIVA....44***
[ 131 a 138 ] Horário de Auto Ativa....44
[ 206 a 209 e 358 a 361 ] Horário de Auto Desativa....44
[ 130 ] Dias da Semana com Auto Desativa....44
[ 139 a 146 ] Ativação por Inércia das Partições....45
[ 159 a 166 ] Horário em que as Partições Ativam por Inércia....45
[ 167 a 170 ] Dias da Semana em que as Partições Ativam por Inércia....45
[ 465 ] Falha no auto arme – Código Contact ID....45
[ 147 a 154 ] Horário em que as partições estão sempre armadas....46
[ 155 a 158 ] Dias da semana para as partições sempre armadas....46
[ 491 a 494 ] Tempo de rearme das partições sempre armadas....46
[ 205 ] Partições para Auto Ativa (auto ativa do teclado)....47
[ 363 ] Anular Auto Ativação com zona aberta – opção (bit) 4....47
***SIRENES....47***
[ 210 e 211 ] Tempo de Sirene....47
[ 213 e 214 ] Partições que Disparam a Sirene....47
[ 216] Bip de Sirene....47
[ 219 ] Supervisão de Sirene....47
[ 082 ] Problemas que disparam a sirene....48
***Servidor DDNS e APP VIAWEB Mobile....48***
Programando *VIAWEB* Mobile por funções....48
[ 571 ] Habilita cadastro automático VIAWEB Direct....48
[ 570 ] VIAWEB Direct – Chave Criptográfica....48
[ 580 ] Habilita Dynamic DNS....48
[ 581 ] Endereço Externo (Hostname)....49
[ 582 ] Usuário Dynamic DNS....49
[ 583 ] Senha Dynamic DNS....49
[ 584 ] Resultado Dynamic DNS....49
VIAWEB Direct....50
VIAWEB Cloud....51
*AlarmeNET.com*....52
***AVANÇADO....53***
[ 000 ] Versão do Firmware da Central....53
[ 081 ] Opções de Envio de Testes e de Bateria....53
[ 355 e 357 ] Permissão de Acesso Remoto....53

[ 520 ] Permissão de Acesso à Navegação WEB....54
[ 366 ] Teclas Especiais 1 e 2....54
[ 039 ] Estado da comunicação....54
[ 365 ] Retardo de falha de AC....54
[ 363 ] Programação de Senhas Aleatórias – opção (bit) 3....55
[ 363 ] Salva a lista de periféricos ligados ao Innovabus – opção (bit) 6....56
Lacre da programação (somente para empresas de monitoramento)....56
[ 019 ] Lacre de Programação....56
[ 471 ] Programação irá liberar após 4 minutos – Código Contact ID....57
[ 472 ] Programação lacrada – Código Contact ID....57
[ 364 ] Interface de Integração (Rádio Monitoramento) - opções 7 e 8....57
[ 077 ] Atalho de Programação....58
***AGENDAS....59***
Ação que a agenda irá executar....59
[ 830 a 863 ] Ações a executar....59
[ 864 a 897 ] Complemento da agenda....60
Em que momento a agenda executa a ação inicial?....60
[ 898 a 931 ] Horário de início da agenda....60
[ 932 a 965 ] Horário final da agenda....60
[ 966 a 999 ] Dias da semana da agenda....60
Em que momento a agenda executa a ação final?....60
[ 665 a 698 ] Duração da ação....60
Combinação das condições....60
[ 286 a 319 ] Combinação das condições....60
Funções das agendas....61
Condições Supervisionadas....62
[ 384 a 398 ] Condição supervisionada....62
[ 521 a 535 ] Calendário de Feriados....65
[ 363 ] Diversos....65
***RESET....66***
Reset das senhas Mestre e de programação....66
Reset total da programação....66
[ 362 ] Trava de Reset....66
[ 362 ] Reinicialização de Barramento....66
[ 362 ] Resetar a programação de um periférico individualmente....66
***CONTACT – ID (Códigos dos Eventos do Alarme)....67***
[ 401 a 476 ] Códigos dos Eventos em Contact-ID....68

**Produto**: VW16Z 4G IP e VW16Z 4G
**Modelo**: VW_GPRS_BG95-M3
Incorpora produto homologado pela Anatel sob número 13721-22-04635

País de origem: Brasil
Fabricante: SI – Sistemas Inteligentes Eletrônicos Ltda.

# PRINCIPAIS CARACTERÍSTICAS

**As Centrais VW16Z 4G IP e VW16Z 4G NÃO possuem entrada de linha telefônica.**

- 16 Zonas na placa (8+8), com divisão resistiva, expansível;
- 8 partições;
- 64 senhas, expansível;
- 8 grupos para senhas;
- 2 saídas para automação (PGMs), expansível;
- 8 periféricos gerenciáveis no barramento + 24 autogerenciáveis;
- Saída de sirene de 2,5A;
- Saída auxiliar 1,2A;
- Fonte supervisionada automática 110/127/220V;
- Armazena 2048 eventos (buffer);
- 34 agendas avançadas e 15 condições supervisionadas;
- Comunicação via chip de dados (4G)* e rede TCP/IP (ethernet);**
- 2 bandejas para SIM Cards;*
- Programação via teclado, VIAWEB Studio e VIAWEB Download;
- Atualização de firmware via 4G*, IP** e cabo serial;
- Universal Plug and Play;**
- Compatível com os aplicativos: VIAWEB Mobile, VIAWEB Studio e AlarmeNET.com

*Central VW16Z 4G IP e VW16Z 4G ** Central VW16Z 4G IP e VW16Z IP

## ESPECIFICAÇÃO DETALHADA INTERFACE DE REDE:

- Interface ethernet compatível com IEEE 802.3
- 10Base-T Full e Half-Duplex (porta de 10Mbps)
- TCP/IP v4 e v6
- Protocolos: Arp (IPv4); ICMPv4 (Apenas resposta a PING); ICMPv6; IP (v4 e V6); TCP; UDP; NTP (client); UPNP; HTTP (servidor); DNS client (suporte a records AAAA e A); DHCP; DHCPv6; DynDNS (VIAWEBservice e NOIP).

## SUPORTE A PROTOCOLO DE AUTENTICAÇÃO 802.1X

Para que as centrais modelos VW16Z 4G IP e VW16Z IP possam conectar-se em redes com autenticação 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC), é preciso:

Utilizar um mini roteador modelo " GL.iNet-AR300M16" ou o "nanopi R3S". O roteador deve ter sua saída WAN ligada à rede e a saída LAN ligada ao conector ethernet da central. O roteador então deve ser configurado para autenticar na rede via o protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC) e permitir acesso à central.

# INSTALAÇÃO

## Bateria

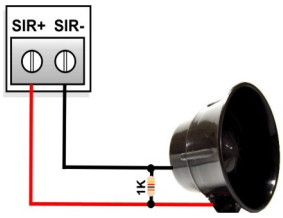
É importante que seja ligada ao sistema uma bateria de “back-up” para que em caso de falha na energia elétrica, o sistema continue funcionando corretamente. Recomendamos o uso de bateria selada recarregável de 12V 7Ah de boa qualidade. A central disponibiliza dois cabos para a conexão da bateria 13,8V , onde o vermelho deve ser ligado ao positivo (+) e o preto ao negativo (-) da bateria.

## Rede Elétrica

Conectar o chicote elétrico na placa e à rede elétrica.
Ao ser energizada o led vermelho começa a piscar.

## Sirene

Nos terminais SIR+ e SIR- a central disponibiliza ao instalador uma tensão de 13,8 V e 2,5A com a bateria conectada, para a instalação da sirene. Essa saída tem uma proteção contra curto-circuito ou corte de sirene quando programada.




Para que a supervisão de sirene funcione corretamente, conecte um resistor de **1K** em paralelo, o mais próximo possível da sirene.

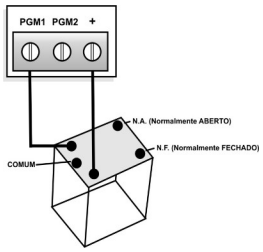
## Saída de Alimentação Auxiliar e Barramento

A saída auxiliar permite no máximo 1,2A. Nos terminais ( + ) e ( c ) a central disponibiliza ao instalador uma tensão de 13,8V para os sensores que podem ser ligados à central.

O barramento disponibiliza nos terminais **VM** e **PR** uma tensão de 12V usado para alimentação e no **VD** e **AM** a tensão é de aproximadamente 3,8V usado para comunicação.

## Saídas Programáveis (PGM1 e PGM2)

A central possui duas saídas programáveis. Essas saídas disponibilizam uma tensão negativa de no máximo 100mA para a ligação de um relé que fará o acionamento de equipamentos para automação.




# PERIFÉRICOS

Os teclados, expansores de zonas e módulos VIAWEB são periféricos interligados à central através do sistema de barramento **VD** e **AM**. Cada periférico tem um endereço dentro do barramento do sistema e a alimentação dos teclados precisa ser ligada ao **VM** e **PR** da central.

# FIXAÇÃO

Escolha um local arejado para a fixação da caixa da central, onde exista energia elétrica, internet e **NÃO VISÍVEL A PESSOAS ESTRANHAS.**

## Cuidados para Fixação da Placa

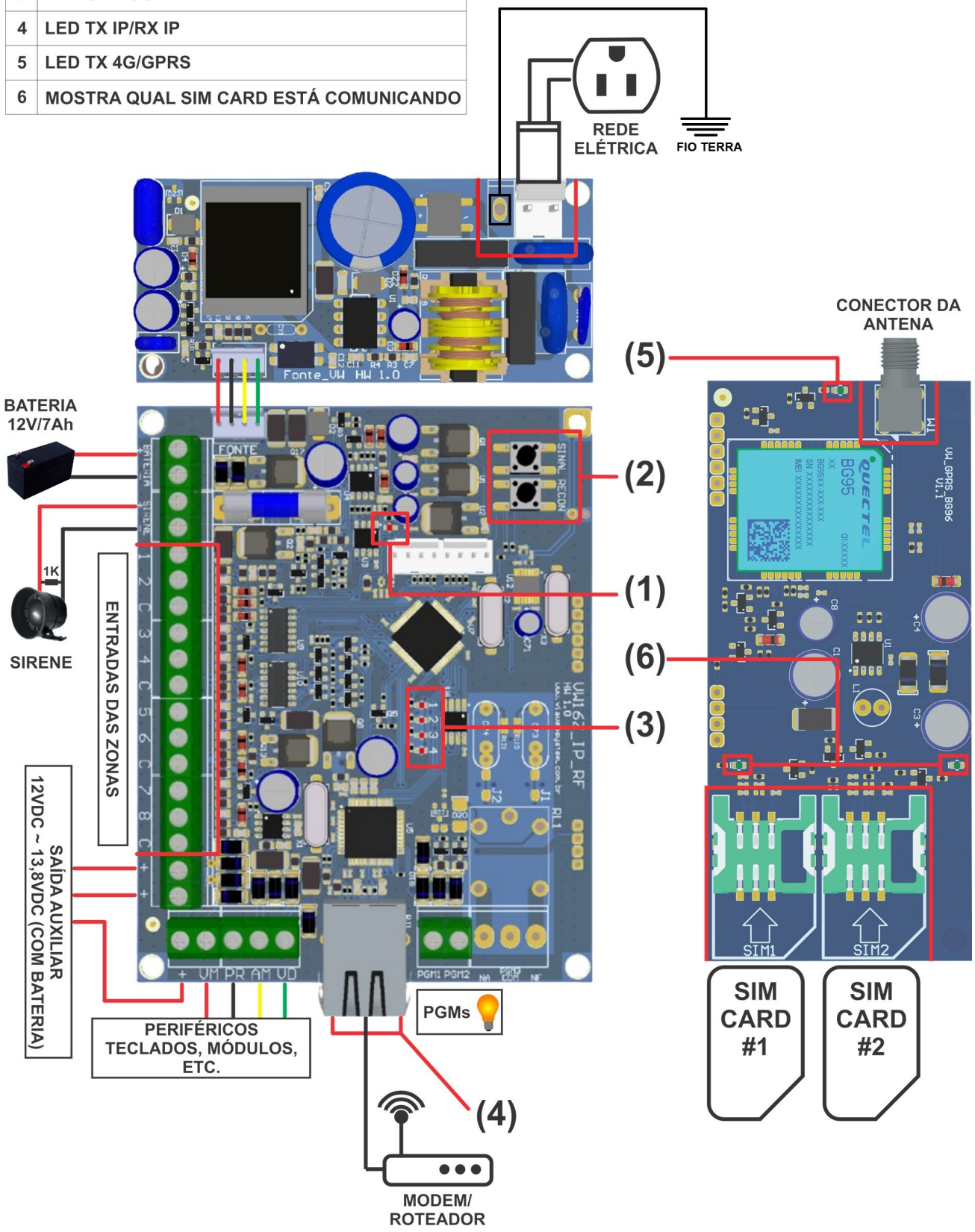
Ao fazer a instalação de sensores e periféricos, procure não deixar os fios passando sobre a placa.

## Aterramento

Para melhor proteção, equipamentos eletrônicos em geral precisam de um aterramento. A central tem um local especial para a ligação do aterramento.(ver figura)

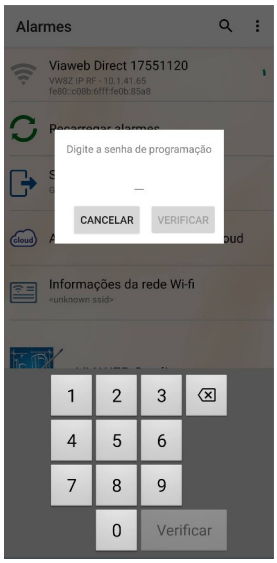
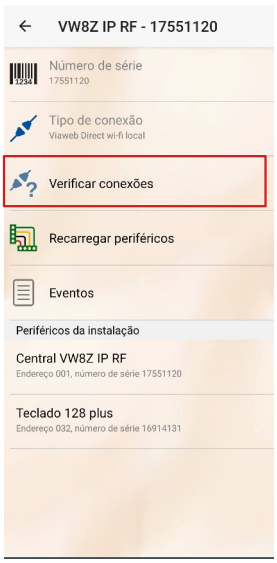
# PLACA CENTRAL

| | |
|---|---|
| 1 | LED BAT |
| 2 | TECLA SINAL/TECLA RECON |
| 3 | LED STATUS |
| 4 | LED TX IP/RX IP |
| 5 | LED TX 4G/GPRS |
| 6 | MOSTRA QUAL SIM CARD ESTÁ COMUNICANDO |



# VIAWEB Studio

A programação da Central VW16Z 4G IP poderá ser feita usando o aplicativo VIAWEB Studio. Conecte a central VW16Z 4G IP na rede local, depois para inserir o equipamento no APP, siga os passos abaixo:

| 1º Conectar o celular na mesma rede da central, no APP irá aparecer um ícone cinza (sinal de Wi-Fi) | 2º Digite a senha de programação, de fábrica 5353 | 3º Pronto! O equipamento foi adicionado via Direct. Agora toque na instalação para Habilitar o Cloud | 4º Toque em “Verificar conexões” | 5º Toque em “Ativar VIAWEB Cloud” |
|---|---|---|---|---|
|  |  |  |  |  |

# Operação do Alarme

## Armar e Desarmar o sistema

**Formas de armar ou desarmar o sistema:**
Por senhas: utilizando o navegador Web, um teclado ou o aplicativo VIAWEB Mobile.
Por controle remoto: Utilizando o Receptor VW1664-PTK no barramento.
**Senha de arme e desarme e cadastro de usuários (senha mestre) de fábrica: 1515**
Obs.: Para alteração de senhas e cadastro de usuários consulte página 38.
**A central não arma o sistema se houver alguma zona imediata da central pronta (aberta) para disparar (violada).**

## Operando Via página Web

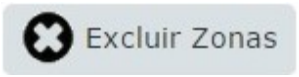
**Para armar e desarmar o sistema pela página Web, é necessário colocar a senha do usuário quando acessar a página.**
A seguinte tela irá aparecer:




Na foto, o primeiro botão indica o estado da partição. Quando passamos o mouse em cima desse botão, aparecem os dois botões abaixo para armar e desarmar.

Se o sistema for particionado, aparecerão as outras partições e as suas respectivas zonas.

Para alterar os nomes das partições nessa página, programar as funções de [ 591 ] a [ 598 ].

Para inibir os setores basta clicar em “ 

“e depois clicar nas zonas desejadas antes de armar.

Se você estiver na página “Configurar”, basta clicar  para acessar esta página.

## Operando Via Teclado

**Armar ou desarmar o sistema**

Basta o usuário digitar sua senha no teclado. Se o sistema estiver armado ele desarma e vice-versa.

**Programar o Relógio**

ENT + SENHA DE PROGRAMAÇÃO, USUÁRIO 001 OU 002 + EXC

[ _ _:_ _ ] HH:MM + [ _ _ /_ _ /_ _ ] DIA / MÊS / ANO

**Inibindo zonas**

Caso o sistema esteja desarmado, é possível inibir algumas zonas antes de armar. Uma zona inibida não irá gerar disparo, mesmo se violada. Para inibir uma zona, digite o número da zona no teclado, seguido da tecla EXC (excluir). Pode-se repetir o procedimento até que todas as zonas desejadas tenham sido excluídas. Em seguida digita-se a senha para armar.

Exemplo:

Inibir as zonas 1, 36 e armar com a senha 1234: 1 EXC 36 EXC 1234

**Armando por partições**

Caso o sistema seja particionado, ao digitar a senha, o usuário irá armar ou desarmar todas as partições que tem acesso. Caso o usuário deseje armar ou desarmar parcialmente o sistema deve digitar a partição desejada (1 a 8) seguida da tecla SIS (sistema). Pode-se repetir o procedimento até que todas as partições desejadas sejam selecionadas. Em seguida digita-se a senha para armar.

Exemplos:

Armar as partições 1 e 8 com a senha 1234: 1 SIS 8 SIS 1234

Armar a partição 2, excluindo a zona 5: 5 EXC 2 SIS 1234

**Limpar os eventos da memória (limpar buffer)**

Esse comando limpa a memória de eventos (marca todos os eventos como enviados mas não exclui) e reinicia a comunicação da central.

ENTER + senha de programação ou usuário 001 ou 002 + CANCELAR

# PROGRAMANDO A CENTRAL

A Central VW16Z 4G IP é totalmente programável e possui inúmeras opções e funções. O valor padrão de fábrica das funções é ajustado para atender a maioria das instalações, reduzindo a necessidade de efetuar a programação de todas.

A central é programada através de funções. Nesse manual as funções são colocadas dentro de colchetes. Exemplo: **[ 204 ],** a função que determina se o sistema é particionado.

Existem dois tipos de funções:

- Funções que são programadas colocando uma **sequência de dígitos.**

No manual essas funções são representadas com o código da função seguido da quantidade de caracteres. Exemplo, função [ 121 ] [ __/__/__ ]; significa que a função 121 é preenchida com 3 dígitos. A função [ 121 ] é tempo de entrada nas zonas temporizadas. Nessa função colocamos "030" o que equivale a 30 segundos, ou a função [ 131 ] que determina o horário de autoativação da partição 1, podemos colocar nessa função "1500", o que corresponde a 15:00 ou três horas da tarde.

- Funções que são programadas **habilitando bits.**

Nesse tipo de função você deve deixar os bits (ou leds no caso do teclado) de 1 a 8 habilitados ou desabilitados dependendo da configuração desejada. No manual essas funções são representadas em tabelas com explicações da função de cada bit. Quando o bit não aparece na tabela, significa que ele não tem função.
Exemplo função [ 091 ] tipo da zona 1. Se nessa função o bit 1 estiver ativo, a zona 1 fica como temporizada, entretanto, se estiverem ativos os bits 2 e 6, a zona é desabilitada.

Existem quatro maneiras de programar a central VW16Z4G IP: **Pelo aplicativo VIAWEB Studio, por teclado, pelo software "VIAWEB Download" ou pela Página Web**.

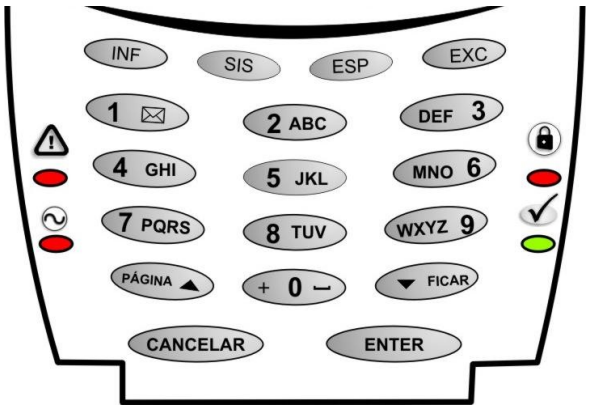
## POR TECLADO

**A senha de programação padrão de fábrica é 5353**

Para entrar no modo de programação pressione ENTER mais a senha de programação seguida da tecla ENTER.

- O teclado emitirá três bips rápidos confirmando que entrou na programação (o teclado emite um bip longo no caso de senha errada)
- Dentro do modo de programação, o led "" ficará piscando e os demais leds apagados.
- Digite o número de uma função (NÃO é necessário apertar ENTER), o teclado emitirá três bips rápidos confirmando que entrou na função (o teclado emite um bip longo no caso de função errada).
- O led "" ficará Aceso mostrando que o teclado está pronto para receber os valores a serem programados.
- Preste atenção na programação pois existem funções com valores com 3 dígitos, com 2 dígitos e múltipla escolha.
- Em algumas funções, após a entrada do valor, a central confirma automaticamente (emite três bips rápidos), caso contrário pressione ENT para confirmação.
- O led "" volta a piscar e os demais leds ficam apagados aguardando uma nova função.
- Para sair do modo de programação pressione ENT novamente.

Quando uma função contém mais do que um dígito, estes dígitos não podem ser vistos simultaneamente. Assim que uma função é acessada, o primeiro dígito é apresentado automaticamente. Dígitos adicionais (se existirem) podem ser apresentados pressionando-se a tecla EXC nos teclados de LED.




**Led** e acesos
O teclado está esperando para entrar com a senha de programação.

**Led** piscando
O teclado está esperando o número da função que será programada.

**Led** aceso e piscando
O teclado está esperando o valor que será programado na função.

**Led** piscando e piscando
O teclado está esperando o endereço do periférico para programação.

**ENT +** 5353 **+ ENT +** [ __ __ __ ] (Função 3 Dígitos) + valor

Há 5 formas de programar e visualizar a programação pelo teclado:

**1) Funções de um dígito**, em que se programa o valor desejado pressionando uma única tecla (Ex: função 091 tipo da zona 1).

O valor programado é representado pelo led aceso, sendo que o valor zero é representado pelo led 10. Para programar o novo valor pressionar a tecla desejada. Se quiser manter o valor atualmente mostrado, pressione a tecla EXC ou CANCELAR.

Essas funções podem assumir valores de 0 a F (hexadecimal). Para programar os valores acima de 9, utilizar a combinação de teclas: A – INF 1, B – INF 2, C – INF 3, D – INF 4, E – INF 5, F – INF 6.

**2) Funções de vários dígitos hexadecimais,** em que se programam vários dígitos seguidos (Ex: função 440 – evento Contact ID de 4 dígitos).

Em teclados de led, a programação pode ser visualizada um dígito por vez, sendo que cada led corresponde a um número e o led 10 corresponde ao zero. Para visualizar todos os números programados basta ir pressionando a tecla EXC. Para visualizar valores acima de 9 (A a F), primeiro irá aparecer a tecla INF (representada pelos leds 2 e 4 acesos simultaneamente) e ao pressionar EXC novamente, o próximo valor mostrado irá variar de 1 a 6, representando as letras de A a F.

Para programar um novo valor, deve-se pressionar as teclas desejadas. Se quiser manter um dos atuais valores mostrados pressione a tecla EXC.

Essas funções podem assumir valores de 0 a F (hexadecimal). Para programar os valores acima de 9, utilizar a combinação de teclas: A – INF 1, B – INF 2, C – INF 3, D – INF 4, E – INF 5, F – INF 6.

**3) Funções decimais,** em que se programa um número de 3 dígitos entre 000 e 255 (Ex: função 121 – tempo de entrada 1).

O valor nos teclados de led é mostrado pelos leds de 1 a 8 de forma binária.

O valor programado é dado pela soma dos leds acesos:

| LED | SOMA |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 4 |
| 4 | 8 |
| 5 | 16 |
| 6 | 32 |
| 7 | 64 |
| 8 | 128 |

Exemplo: Se os leds 1; 5 e 8 estiverem acesos o valor será:
1 + 16 + 128 = 145

**4) Funções de múltiplas opções,** em que cada led aceso de 1 a 8 representa uma opção (Ex: função [ 120 ] - partições que bipam temporização). Ao entrar nessa função os leds já mostram o valor programado. Para alterar o valor deve-se pressionar a tecla de 1 a 8 correspondentes à opção. Se o led acender, a opção está habilitada, se o led apagar, desabilitada. Para programar esta função, após escolher as opções deve-se pressionar ENTER.

**5) Funções de texto,** em que se programa uma mensagem (Ex: função 029 endereço do servidor VIAWEB 1). Essas funções somente são programadas por teclados de display. Ao tentar programar uma dessas funções com o teclado de leds, ouve-se um bip de erro. Para programar uma letra pressionar a tecla correspondente até que a letra desejada apareça no display. Para alterar entre letras maiúsculas, minúsculas e números, pressionar a tecla SIS. Ao terminar de digitar o texto, deve-se pressionar a tecla 0 até que o símbolo de <ENTER> apareça, esse símbolo é que marca o fim do texto.Pressionar ENTER para programar.

## Via cabo serial – Software VIAWEB download

Para programar via cabo serial e para mais informações, deve-se obter o software VIAWEB download, na área de “Guias e Manuais” do site www.viawebsystem.com.br.

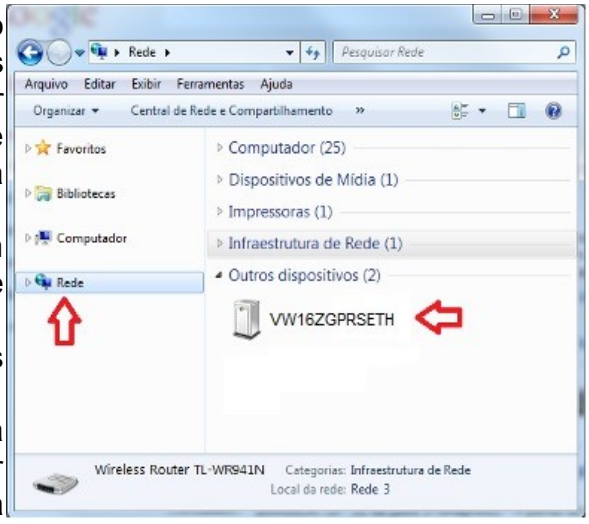
Para acessar a central via cabo serial é necessário senha de download (pág. 40).

# Página Web

## Identificando o dispositivo na rede

A Central com conector de rede possui recurso “Universal Plug and Play” (versões do Windows compatíveis: Vista ou superior). Isso significa que ao ser conectada na rede local ela será automaticamente detectada por computadores compatíveis com esta tecnologia.

Para identificar a central, em um computador com Windows, abra o explorador de arquivos, e depois clique na opção “rede” no menu à esquerda.




A central irá aparecer como “outros dispositivos de rede”. Dê um duplo clique para abrir a página inicial.

Caso a central não esteja aparecendo, verifique a conexão do cabo de rede, os leds verdes devem estar acesos ou piscando. Se o problema persistir, efetue a configuração manual dos parâmetros de rede em “Configuração manual dos parâmetros da rede” (pág. 22).

## Página inicial

Clicando duas vezes na central, ou digitando o endereço de rede interna dele em um navegador, aparecerá um pedido de autorização. O campo do usuário deve ser deixado em branco e no campo senha coloca-se a **senha de programação (padrão:5353)** ou a senha de usuário **mestre (padrão:1515)**.

Usando a senha de programação podemos apenas alterar a programação, usando a senha mestre, podemos alterar a programação, cadastrar usuários e armar/desarmar o sistema.

É disponibilizado o controle local através da página do dispositivo. Porém a conexão nesse caso possui apenas autenticação simples e não é segura para ser redirecionada para fora da rede interna.O acesso à página web pode ser desabilitado por programação (ver pág. 53).

## Botões de menu

| Controlar PGMs | Excluir Zonas | Eventos | Relatório |
|---|---|---|---|
| Abre a página de controle das PGMS do sistema. | Habilita a seleção das zonas para a exclusão ao armar. | Abre a página com os últimos 100 eventos registrados pelo sistema. | Abre a página com o relatório do status atual do sistema. |

| Configurar | Abre a página do assistente de configuração.<br>No assistente encontramos: |
|---|---|

| | | | |
|---|---|---|---|
|  | **Monitoramento**<br>Programar os dados da empresa de monitoramento quando o sistema é monitorado. |  | **Usuários**<br>Permite a visualização de usuários e programação de senhas. |
|  | **Rede e Internet**<br>Configurações de rede, internet e servidor de data e hora do módulo. |  | **VIAWEB Direct**<br>Configurações para conexão do módulo com o aplicativo. |
|  | **Controle do Sistema**<br>Volta para a página de controle do sistema. |  | **Programar**<br>Página para programação do sistema por funções. |

- Programando os campos da página Monitoramento, as funções [001], [023],[026],[029],[066] são automaticamente programadas. Ao apagar os campos e salvar, todas essas funções são desprogramadas.
- Na página Usuários podemos modificar ou cadastrar os usuários e suas senhas. Os nomes colocados aqui programam automaticamente as funções [601] a [700].
- Programando os campos da página Rede e Internet, as funções [051], [052],[053],[055], [021],[022],[056], [057] são automaticamente programadas. Ao apagar os campos e salvar, todas essas funções são desprogramadas.
- Programando os campos da página Viaweb Direct, as funções [003], [006],[011],[012],[570], [580], [582],[583] são automaticamente programadas. Ao apagar os campos e salvar, todas essas funções são desprogramadas.
- Na página Programar, no campo **endereço,** deixamos 001 para programar a central. Este campo é alterado quando precisamos programar outro periférico (teclados, módulos expansores, etc.). No campo **função** colocamos a função que desejamos programar e clicamos em carregar. No campo **valor** aparece o que está programado na função. Para alterar a programação basta inserir o novo valor e clicar em **salvar**.

# MONITORAMENTO (COMUNICADOR INTERNET)

O monitoramento é feito através das sequências de comunicação. Para mais informações sobre as sequências de comunicação verifique o item “Monitoramento de eventos por sequências de comunicação” na página 20.

Ao contratar uma empresa de monitoramento, você receberá as seguintes informações:

- IP do servidor do monitoramento (VIAWEB Receiver).
- Porta TCP do servidor do monitoramento (normalmente 1733).
- ID ISEP: Identificador único de 4 dígitos, serve para que a empresa de monitoramento identifique o seu equipamento na central de monitoramento.

**DICA:** Na página inicial de configuração da central, há a opção de configurar a empresa de monitoramento. Basta preencher os 3 campos acima e verificar na própria página se a conexão com a empresa foi estabelecida. Essa página faz a configuração automática da sequência de comunicação 1 e atribui o ID ISEP como sendo o número de conta para partição 1 (função [ 066 ]).

**Tela de programação da empresa de monitoramento.**

Ao configurar a conexão com uma empresa de monitoramento, a central mantém uma comunicação constante com o servidor de monitoramento, enviando imediatamente qualquer evento, falha ou informação gerada pelo sistema. Também é possível para a empresa de monitoramento efetuar acesso remoto à central. Toda vez que a empresa de monitoramento acessar o sistema de alarme, um evento é gerado. Esse evento é configurado na função [ 440 ].

## [ 020 ] INTERVALO DE PING IP (KEEP ALIVE)

**[ 020 ]** [ __/__/__ ] Padrão: 001 minuto

Periodicamente é enviado um pacote criptografado para o servidor VIAWEB verificando se este está respondendo corretamente. O intervalo de Ping pode ser qualquer valor de 001 a 015.

## [ 040 ] INTERVALO DE PING 4G (KEEP ALIVE)

**[ 020 ]** [ __/__/__ ] Padrão: 010 minutos

Como o Ping IP mas por 4G. O intervalo pode ser qualquer valor de 001 a 015 minutos.

## [ 023 A 025 ] ID ISEP

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

ID_ISEP: (número identificador da central ou Conta) deve ser cadastrado o mesmo ID_ISEP no Monitoramento (servidor VIAWEB Receiver).

## [ 026 A 028 ] PORTA TCP DO SERVIDOR

**[ 026 ]** [ __/__/__/__/__ ] Porta TCP do Servidor VIAWEB 1 Padrão: 01733
**[ 027 ]** [ __/__/__/__/__ ] Porta TCP do Servidor VIAWEB 2 Padrão: 01733
**[ 028 ]** [ __/__/__/__/__ ] Porta TCP do Servidor VIAWEB 3 Padrão: 01733

Porta TCP: Porta de conexão entre a central e o servidor VIAWEB.

## [ 029 A 031 ] ENDEREÇO DO SERVIDOR

Padrão: viawebmobile.com (máx. 30 caracteres)
**[ 029 ]** [ __/__/ … /__ ] IP FIXO ou End URL Servidor 1
**[ 030 ]** [ __/__/ … /__ ] IP FIXO ou End URL Servidor 2
**[ 031 ]** [ __/__/ … /__ ] IP FIXO ou End URL Servidor 3

IP FIXO ou Endereço URL do servidor VIAWEB (Receiver) que receberá os eventos via internet.

## [ 034 a 036 ] Endereço do servidor (para teclado LED)

**[ 034 ]** [ _/ _/ _/. _/ _/ _/. _/ _/ _/. _/ _/ _/ ] IP FIXO Servidor 1 Padrão: 000.000.000.000
**[ 035 ]** [ _/ _/ _/. _/ _/ _/. _/ _/ _/. _/ _/ _/ ] IP FIXO Servidor 2 Padrão: 000.000.000.000
**[ 036 ]** [ _/ _/ _/. _/ _/ _/. _/ _/ _/. _/ _/ _/ ] IP FIXO Servidor 3 Padrão: 000.000.000.000
IP FIXO do servidor VIAWEB que receberá os eventos via internet.
**Obs.:** Quando esta função é programada por teclado, a cada 3 dígitos é emitida uma confirmação sonora. Exemplo: para programar o IP 192.168.1.1 deve-se digitar 192 168 001 001

## [ 066 a 073 ] Número da Conta da Partição

**[ 066 ]** [ __/__/__/__ ] Número da Conta Partição 1 ou não particionado Padrão:0000
**[ 067 ]** [ __/__/__/__ ] Número da Conta Partição 2 Padrão:0000
**[ 068 ]** [ __/__/__/__ ] Número da Conta Partição 3 Padrão:0000
**[ 069 ]** [ __/__/__/__ ] Número da Conta Partição 4 Padrão:0000
**[ 070 ]** [ __/__/__/__ ] Número da Conta Partição 5 Padrão:0000
**[ 071 ]** [ __/__/__/__ ] Número da Conta Partição 6 Padrão:0000
**[ 072 ]** [ __/__/__/__ ] Número da Conta Partição 7 Padrão:0000
**[ 073 ]** [ __/__/__/__ ] Número da Conta Partição 8 Padrão:0000

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

Pode-se programar até 8 contas diferentes, sendo uma para cada partição. Quando a central não for particionada, programa-se apenas o número da conta da partição 1. O número pode de ser de 0000 até FFFF.

## [ 032 ] Horário do Primeiro Teste de Internet

**[ 032 ]** [ __/__/__/__ ] Padrão: 00:00
Horário em que deve ocorrer a primeira transmissão do evento de teste automático no dia.

## [ 033 ] Intervalo de Teste Internet

**[ 033 ]** [ __/__/__/__ ] Padrão: 00:00
Período de tempo para enviar teste, em horas e minutos.
Ex.: para a transmissão de 24 testes por dia, programa-se o intervalo de 1 hora.

## [ 440 ] Evento de Acesso Remoto – Código Contact ID

**[ 440 ]** [ __/__/__/__ ] Padrão: 1412
Código Contact ID do evento. Programar 0000 para desabilitar o envio desse evento.
Obs.: Senha de download encontra-se na pág. 40.

## [ 473 ] Evento de Acesso via Cabo Serial – Código Contact ID

**[ 473 ]** [ __/__/__/__ ] Padrão: 1410
Código Contact ID do evento. Programar 0000 para desabilitar o envio desse evento.

## [ 018 ] Partição e Zona dos eventos internos

**[ 018 ]** [ P / Z / Z / Z ] Padrão: 0000 [P = partição 1 dígito] [Z = zona 3 dígitos]
O sistema, conforme a programação, pode enviar diversos eventos internos: teste periódico, falha de bateria, falha de rede elétrica e outros.
Por padrão, quando esses eventos são gerados, a partição envia o valor zero e a zona envia o valor zero também.
Caso desejado, pode-se alterar o valor da partição e da zona a ser enviada com esses eventos.

## [ 086 ] Servidor VIAWEB #3 como backup do Servidor VIAWEB #1 – opção (Bit) 3

| | Descrição | Tecla/Led |
|---|---|---|
| [ 086 ] | Quando habilitado, permite o SERVIDOR VIAWEB #3 ser usado como Backup do SERVIDOR VIAWEB #1 com o mesmo IDISEP. OBS.: Para utilizar esta opção, a função 025 deve estar zerada. Essa função é utilizada quando um servidor VIAWEB possui dois IPs distintos. | 3 |

## [ 086 ] Bloqueia o acesso remoto da conexão com os servidores #1, #2 e #3 (Bit) 6, 7 e 8

| | Descrição | Tecla/Led |
|---|---|---|
| [ 086 ] | Se habilitado, bloqueia o acesso remoto de comandos vindos do servidor VIAWEB #1 | 6 |
| | Se habilitado, bloqueia o acesso remoto de comandos vindos do servidor VIAWEB #2 | 7 |
| | Se habilitado, bloqueia o acesso remoto de comandos vindos do servidor VIAWEB #3 | 8 |

## [ 363 ] Ajuste do relógio e Teste periódico – opções (bits) 1, 5, 7 e 8

| Padrão: Apagado (Desabilitado) | | Bit/Led |
|---|---|---|
| [ 363 ] | Se habilitado, periodicamente ajusta o relógio interno com o horário recebido do servidor VIAWEB 1. Lembre-se que o servidor VIAWEB precisa estar conectado em uma das sequências para que seja possível atualizar o relógio através dele. | 1 |
| | Se habilitado, quando o nível de sinal estiver sendo enviado no teste periódico (no campo zona), no campo partição, o valor representará a tecnologia. Sendo:<br>00 - GPRS<br>07 - 4G<br>08 - CAT-M1<br>09 – NB-IoT | 5 |
| | Quando habilitado, o evento de teste periódico (função 439) é enviado usando o ID_ISEP (funções 023 a 025) como número da conta. Se desabilitado, usa o número da conta da partição 1 (função 066). | 7 |
| | O campo zona do evento Contact ID do teste periódico é preenchido.<br>Se o equipamento possui 4G ou GPRS embarcado, preenche com o nível de sinal de 000 (0%) até 032 (100%).<br>Caso contrário, com a mínima tensão de alimentação lida em 0,1V. | 8 |

# FORMATO DE COMUNICAÇÃO

Funções abaixo automaticamente programadas pela “Página Web”

## [ 001 A 003 ] SEQUÊNCIAS DE COMUNICAÇÃO

**[ 001 ]** [ __/__/ … /__ ] Seq. de Com.1 (32 dígitos ou 16 meios)
**[ 002 ]** [ __/__/ … /__ ] Seq. de Com.2 (32 dígitos ou 16 meios)
**[ 003 ]** [ __/__/ … /__ ] Seq. de Com.3 (32 dígitos ou 16 meios)

| Opções | Meios de Comunicação |
|---|---|
| 00 | Fim da sequência de comunicação (quando utilizar menos que 16 meios) |
| 01 | Servidor VIAWEB 1 comunicação por GPRS ou 4G |
| 02 | Servidor VIAWEB 2 comunicação por GPRS ou 4G |
| 03 | Servidor VIAWEB 3 comunicação por GPRS ou 4G |
| 04 | Primeiro periférico de comunicação auxiliar (ver função 016) |
| 05 | Segundo periférico de comunicação auxiliar (ver função 017) |
| 51 | Servidor VIAWEB 1 via rede TCP/IPv4 ou IPv6 (ethernet) |
| 52 | Servidor VIAWEB 2 via rede TCP/IPv4 ou IPv6 (ethernet) |
| 53 | Servidor VIAWEB 3 via rede TCP/IPv4 ou IPv6 (ethernet) |
| 81 | Envio de notificações para VIAWEB Direct (disponível somente nas versões com cabo de rede) |
| 91* | Comunicação com módulos de rádio de outros fabricantes (para mais informações consultar página 57) |

Nessas funções indicamos para qual meio os eventos serão enviados e em que sequência.

**Exemplos: [ 001 ]** [**51 52 00** 0000 …] Na função 001 colocamos como meio principal Servidor VIAWEB 1 (empresa de monitoramento) e Servidor VIAWEB 2 como backup. Ou seja, se por algum motivo o servidor principal da empresa sair do ar, a sequência vai passar a enviar eventos para o servidor 2. Quando o servidor 1 voltar, a sequência volta a enviar eventos para o servidor 1 novamente.

**[ 002 ]** [ **81 00** 000000 …] Na função 002 colocamos para enviar os eventos para o VIAWEB direct (Aplicativo).

Note que as funções [001], [002] e [003] funcionam paralelamente, ou seja, a central envia eventos ao mesmo tempo para as três sequências.

**Atenção:** É possível programar até **3 servidores VIAWEB** diferentes. Cada servidor pode ser conectado usando a rede Ethernet (meios 51, 52 e 53).

Se duas ou mais sequências de comunicação forem programadas com o mesmo servidor VIAWEB por cabo e 4G ao mesmo tempo (51 e 01, 52 e 02 ou 53 e 03) o equipamento irá dar preferência a conexão via cabo (ethernet) e somente irá conectar via 4G (ou GPRS) se a conexão por cabo falhar.

Para manter as duas vias conectadas ao mesmo tempo deve-se programar servidores VIAWEB diferentes, por exemplo servidor VIAWEB 1 por cabo, usando 51 e servidor VIAWEB 2 por 4G, usando 02. Exemplo, se a sequência 1 for programada com [5100...] e a sequência 2 for programada com [0100...] a conexão será mantida online via cabo (ethernet). O 4G somente irá conectar caso a conexão via ethernet falhe.

Outro exemplo, programar a sequência 1 com [5100...] e a sequência 2 com [0200...] fará com que o servidor VIAWEB 1 se mantenha online via cabo (ethernet) e o servidor VIAWEB 2 também se mantenha online via 4G.

* **Equipamentos que possuem Comunicação com módulos de rádio por serial:**
**Central VW16Z IP** versão 7.29 ou superior; **Central VW16Z IP LT** versão 6.71 ou superior; **Central VW8Z IP** versão 2.71 ou superior; **Módulo IP Mini / IP Mini 100 Mbps** versão 4.71 ou superior; **Central de Automação VW-DIN** versão 2.71 ou superior; **Central VW8Z IP RF** versão 2.71 ou superior

## [ 004 a 006 ] Filtro de Eventos Partições

Padrão: Todos Acesos (envia eventos de todas as partições)

| | 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 |

Esta função determina os eventos das partições que cada sequência vai enviar.

Exemplo: A sequência 1 pode enviar eventos somente das partições 1, 2, 3 e 4 e a sequência 2 pode enviar eventos somente das partições 5, 6, 7 e 8.

## [ 007 a 012 ] Filtro de Eventos das Sequências

Padrão: Todos Acesos (todos os eventos habilitados para todas as sequências)

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

CLASSIFICAÇÃO DOS CÓDIGOS DE EVENTOS:

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

**Mais informações ver pág. 67 Códigos de comunicação**

Cada led aceso corresponde ao grupo de eventos e restauros que serão transmitidos na sequência de comunicação e quando apagados não são enviados.

## [ 013 a 015 ] Tentativas de Envio das Sequências

**[ 013 ]** [ __/__/__ ] Tentativas Seq. de Comunicação 1 Padrão: 010
**[ 014 ]** [ __/__/__ ] Tentativas Seq. de Comunicação 2 Padrão: 010
**[ 015 ]** [ __/__/__ ] Tentativas Seq. de Comunicação 3 Padrão: 010

Após tentar enviar o evento sem sucesso pelo número de vezes programado, a central desiste de tentar enviar o evento, porém quando for gerado um novo evento, o módulo tentará novamente enviar todos os eventos que não foram enviados.

## [ 016 ] Primeiro Periférico de Comunicação Auxiliar (meio de comunicação 04)

**[ 016 ]** [ __/__/__ ] Endereço do Periférico Padrão: 048

Para utilizar o meio 04 (módulo de comunicação externo 1) em alguma sequência de comunicação (funções 001 a 003), deve-se antes colocar aqui o endereço no barramento deste módulo.

## [ 017 ] Segundo Periférico de Comunicação Auxiliar (meio de comunicação 05)

**[ 017 ]** [ __/__/__ ] Endereço do Periférico (meio 05) Padrão: 000

Para utilizar o meio 05 (módulo de comunicação externo 2) em alguma sequência de comunicação (funções 001 a 003), deve-se antes colocar aqui o endereço no barramento deste módulo.

Para utilizar os meios 04 ou 05, deve haver na mesma instalação algum módulo VIAWEB. Os módulos VIAWEB possuem endereços distintos conforme o modelo:
Módulo GPRS Universal, Módulo IP Universal, Módulo GPRS IP Universal, Módulo IP mini, Módulo 4G mini, Módulo 4G Universal e Módulo 4G IP Universal: **Endereço 048**.
Expansor VW16ZGPRS, VW16ZIP e VW16Z: **Endereço 002 a 010** (conforme programação).

# IP (ETHERNET)

**Funções abaixo automaticamente programadas pela "Página Web"**

A VW16Z 4G IP possui recursos para configurar-se automaticamente na rede ethernet em que for instalada. Porém, caso algum problema ocorra e não seja possível visualizar a central na rede pode-se efetuar a configuração manualmente.

## [ 051 ] ENDEREÇO IP NA REDE

**[ 051 ]** [ _ _ _/_ _ _/_ _ _/_ _ _ ] Endereço IP da Central Padrão: 010.001.001.169

Endereço válido dentro da intranet onde a central for instalada.

Caso a rede utilize um servidor DHCP para atribuir os IPs, deve-se programar o servidor DHCP para que não duplique o IP utilizado na central em outro dispositivo. Para saber qual o IP deve-se programar, consulte o administrador da rede.

## [ 052 ] GATEWAY

**[ 052 ]** [ _ _ _/ _ _ _/ _ _ _/ _ _ _ ] Endereço IP do Gateway Padrão: 010.001.001.001

Programar o IP do roteador ou Firewall que dá acesso à Internet. Para saber qual o IP deve-se programar, consulte o administrador da rede.

## [ 053 ] MÁSCARA DE SUB REDE

**[ 053 ]** [ _ _ _/ _ _ _/ _ _ _/ _ _ _ ] Máscara de Rede Padrão: 255.255.255.000

Para saber qual o valor da máscara de rede deve programar, consultar o administrador da rede.

## [ 054 ] ENDEREÇO MAC (SOMENTE LEITURA)

**[ 054 ]** [ __/__/ … /__ ] Endereço MAC Padrão: C08B6FXXXXXX

MAC: XXXXXX é um número único para cada equipamento.

## [ 021 E 022 ] SERVIDORES DNS

**[ 021 ]** [ _ _ _/ _ _ _/ _ _ _/ _ _ _ ] Servidor DNS Primário Padrão: 8.8.8.8
**[ 022 ]** [ _ _ _/ _ _ _/ _ _ _/ _ _ _ ] Servidor DNS Secundário Padrão: 8.8.4.4

Servidores DNS: servem para que a central possa encontrar o IP do servidor VIAWEB a partir do seu endereço URL na rede internet (ex.: www.viawebservice.com.br). Caso o DHCP esteja habilitado (opção 1 da função [ 055 ]), pode-se optar por utilizar o endereço de servidor DNS fornecido pela rede ou programado (opção 3 da função [ 055 ]). Esse campo é automaticamente programado quando habilitado o cadastro de aplicativo na página web.

## [ 055 ] DHCP

**[ 055 ]** [ 1 _ _ _ _ _ 7 _ ] Habilitados

| | Bit/Led | Descrição |
|---|---|---|
| **[ 055 ]** | **1** | Permite que as configurações da rede, (endereço IP, Gateway, máscara de rede e servidores DNS) sejam obtidos automaticamente da rede onde está instalado, desde que a rede possua um servidor DHCP ativo como, por exemplo, um modem roteador. Para saber se o DHCP está habilitado no modem, deve-se consultar o administrador da rede. |
| | 3 | O DNS via DHCP habilita a central a utilizar as configurações de DNS da rede onde está instalado. |
| | 4 | Desabilita uPNP – Ao habilitar essa opção os recursos universal Plug and Play do módulo serão desabilitados. O painel não será identificado na rede automaticamente. Essa opção é útil para redes com grande número de computadores, evitando tráfego desnecessário de dados. |
| | 5 | Desabilita NCSI – Ao habilitar essa opção o equipamento não detecta mais a presença de Internet, assumindo que a rede IP sempre tem acesso à Internet. Serve para eliminar tentativas de comunicação do equipamento com o servidor NCSI. |
| | 6 | Bloqueia recebimento de pacotes de Broadcast e Multicast – Diminui o tráfego de dados em caso de redes com muita latência. Habilitar essa opção impede o funcionamento do aplicativo VIAWEB Mobile e o uPNP. Permite que o módulo opere em redes com tráfego de dados extremo, mas não é compatível com todas as redes ou roteadores TCP/IP. |
| | **7** | Habilita IPV6. |
| | 8 | Modifica o protocolo TCP para compatibilizar com modelos de roteadores fora das normas. Alguns roteadores com falhas de implementação podem bloquear pacotes TCP cujo header não possua ao menos um option. Habilitar essa opção para contornar a falha destes roteadores. |

## [ 056 ] Servidor NTP

**[ 056 ]** [ __/__/ … /__ ]Servidor NTP (Padrão: a.ntp.br)

Endereço de servidor de sincronismo para o relógio interno da central. Máximo 30 caracteres. Para desabilitar o servidor NTP basta deixar o campo em branco.

## [ 057 ] Fuso horário

**[ 057 ]** [ __/__ ] Fuso horário Padrão: 12 – Brasília
Código de fuso horário para a atualização no 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 | **Brasília, Bahia, Amapá, Pará, Alagoas, Ceará, Maranhão, Paraíba, Pernambuco, Piauí, Rio Grande do Norte, Sergipe** |
| **13** | UTC – 3:00 | ***Com horário de verão. 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 Tempo universal | Costa do Marfim, Gana, Libéria |
| **17** | UTC + 1:00 | Europa Central, África Ocidental |
| **18** | UTC + 2:00 | África do Sul, Palestina, Líbia, Ruanda |
| **19** | UTC + 3:00 | Arábia 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 rede 4G | Centrais e módulos 4G |
| **38** | NTP desabilitado | |

***Estados Brasileiros com ajuste automático do Horário de Verão**

# *4 G*

## [ 037 e 038 ] Seleciona Operadora (para teclado de LED)

**[ 037 ]** [ __ ] Operadora SIM CARD 1 (Padrão: 0)
**[ 038 ]** [ __ ] Operadora SIM CARD 2 (Padrão: 0)

Quando a operadora é escolhida nessa função, automaticamente as funções [042][043][044] ou [542] [543] [544] serão programadas.

| | | | |
|---|---|---|---|
| 0 – TIM<br>APN: tim.br<br>Usuário: tim<br>Senha: tim | 4 – Claro Genérica<br>APN: generica.claro.com.br<br>Usuário: claro<br>Senha: claro | 8 – TMDATA VIVO<br>APN: tmdata.vivo.com.br<br>Usuário: tmdata<br>Senha: tmdata | C – Link Solution<br>APN: link.claro.br<br>Usuário: claro<br>Senha: claro |
| **1 – Claro**<br>**APN: claro.com.br**<br>**Usuário: claro**<br>**Senha: claro** | 5 – VIVO<br>APN: zap.vivo.com.br<br>Usuário: vivo<br>Senha: vivo | 9 – Full Time Claro<br>APN: ft.claro.com.br<br>Usuário: claro<br>Senha: claro | D – Link Solution<br>APN: linksol.vivo.com.br<br>Usuário: link<br>Senha: link |
| 2 – Datatem<br>APN: inlog.vivo.com.br<br>Usuário: datatem<br>Senha: datatem | 6 – TMDATA Claro<br>APN: tmdata.claro.com.br<br>Usuário: tmdata<br>Senha: tmdata | A – Full Time Tim<br>APN: telemetria.tim.br<br>Usuário: tim<br>Senha: tim | E – Datatem<br>APN: inlog.claro.com.br<br>Usuário: datatem<br>Senha: datatem |
| 3 – Oi<br>APN: gprs.oi.com.br<br>Usuário: oi<br>Senha: oi | 7 – TMDATA Tim<br>APN: tmdata.tim.br<br>Usuário: tmdata<br>Senha: tmdata | B – Grupo Lógico Claro<br>APN: logico.claro.com.br<br>Usuário: LOGICO<br>Senha: LOGICO<br>Obs.: Quando programada esta operadora, deve-se mudar as funções de USUÁRIO (043) e SENHA (044) para os 6 últimos dígitos do ICDD do chip | F – Virtueyes<br>APN: virtueyes.com.br<br>Usuário: virtu<br>Senha: virtu |

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

## [ 041 e 541 ] PIN do SIM CARD 1 e 2

**[ 041 ]** [ __/__/__/__ ] PIN do SIM CARD 1 Padrão: 0000
**[ 541 ]** [ __/__/__/__ ] PIN do SIM CARD 2 Padrão: 0000
Senha programada no SIM CARD, para que o VIAWEB reconheça o PIN, insira o chip em um aparelho celular e ative o código de segurança PIN nas configurações do celular.

## [ 042 e 542 ] APN do SIM CARD 1 e 2

**[ 042 ]** [ __/__/… /__ ] APN SIM CARD 1 Padrão: claro.com.br
**[ 542 ]** [ __/__/… /__ ] APN SIM CARD 2 Padrão: claro.com.br
APN: Nome do ponto de acesso da operadora celular GSM. (máx. 30 caracteres)

## [ 043 e 543 ] Usuário SIM CARD 1 e 2

**[ 043 ]** [ __/__/ … /__ ] Usuário SIM CARD 1 Padrão: claro (máx. 30 caracteres)
**[ 543 ]** [ __/__/ … /__ ] Usuário SIM CARD 2 Padrão: claro (máx. 30 caracteres)
Usuário: Fornecido pela operadora celular GSM para conexão 4G.

## [ 044 e 544 ] Senha SIM CARD 1 e 2

**[ 044 ]** [ __/__/ … /__ ] Senha SIM CARD 1 Padrão: claro (máx. 30 caracteres)
**[ 544 ]** [ __/__/ … /__ ] Senha SIM CARD 2 Padrão: claro (máx. 30 caracteres)
Senha: Fornecida pela operadora celular GSM para autenticação 4G.

## [ 045 e 545 ] Número do ICCID do SIM CARD 1 e 2 (somente leitura)

**[ 045 ]** [ __/__/ … /__ ] Número do ICCID SIM CARD 1
**[ 545 ]** [ __/__/ … /__ ] Número do ICCID SIM CARD 2
Número de identificação do SIM CARD (somente leitura).

## [ 502 e 503 ] KBytes Trafegados SIM CARD 1 e 2 (somente leitura)

**[ 502 ]** [ __/ __/ __/ __ ] KBytes Trafegados SIM CARD 1
**[ 503 ]** [ __/ __/ __/ __ ] KBytes Trafegados SIM CARD 2
Mostra a quantidade de Kilo Bytes trafegados no SIM CARD.
Programando "0000" ou desligando o equipamento, zera-se o contador.

## [ 046 ] Versão do Módulo 4G (somente leitura)

**[ 046 ]** [ versão do módulo ]
Utilizado apenas para leitura da versão do módulo.

## [ 076 ] Estado Geral da Comunicação

Somente leitura. Cada um dos 8 BITs apresenta uma informação:

| BIT (LED) | Habilitado (aceso) | Desabilitado (apagado) |
|---|---|---|
| **1** | Indica que o servidor 1 está online | Indica que o servidor 1 está offline |
| **2** | Indica que o servidor 2 está online | Indica que o servidor 2 está offline |
| **3** | Indica que o servidor 3 está online | Indica que o servidor 3 está offline |
| **4** | Conectado ao cabo de rede TCP/IP | Há problemas no cabo de rede TCP/IP |
| **5** | Acesso à internet OK | Há problemas no acesso à internet |
| **6** | SIM CARD 1 tem acesso à internet | SIM CARD 1 ausente ou sem internet |
| **7** | SIM CARD 2 tem acesso à internet | SIM CARD 2 ausente ou sem internet |
| **8** | Nível de sinal de ao menos um LED | Sem sinal celular |

# ZONAS

A Central VW16Z 4G IP possui 8 entradas de zona, permitindo a instalação de até 16 zonas distintas. Caso a instalação possua mais que 8 sensores, estes podem ser agrupados. Se ainda assim for necessário um número maior de zonas, pode-se instalar expansores de zonas, ampliando a capacidade da central até 128 zonas.

**DICA:** Recomenda-se agrupar no máximo dois (2) sensores na mesma zona. Também recomenda-se não agrupar sensores com tecnologias de detecção diferentes na mesma zona, separando magnéticos, IVPs, Micro-ondas, sensores de barreira, etc…

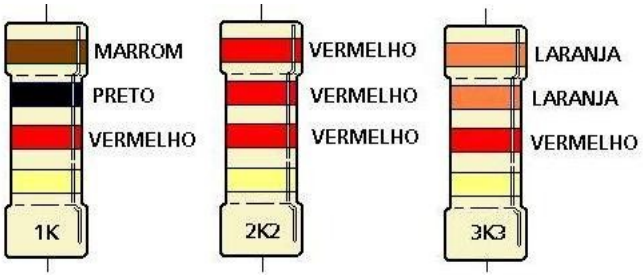
**Instalação dos sensores nas zonas:**

Existem 8 formas diferentes de instalar os sensores nas zonas. A forma de instalação deve estar de acordo com o valor da função 107.

## [ 107 ] Configuração das Zonas

**[ 107 ]** [ __/__ ] Padrão: 04 (16 zonas normalmente fechadas sem resistor de fim de linha e sem tamper)

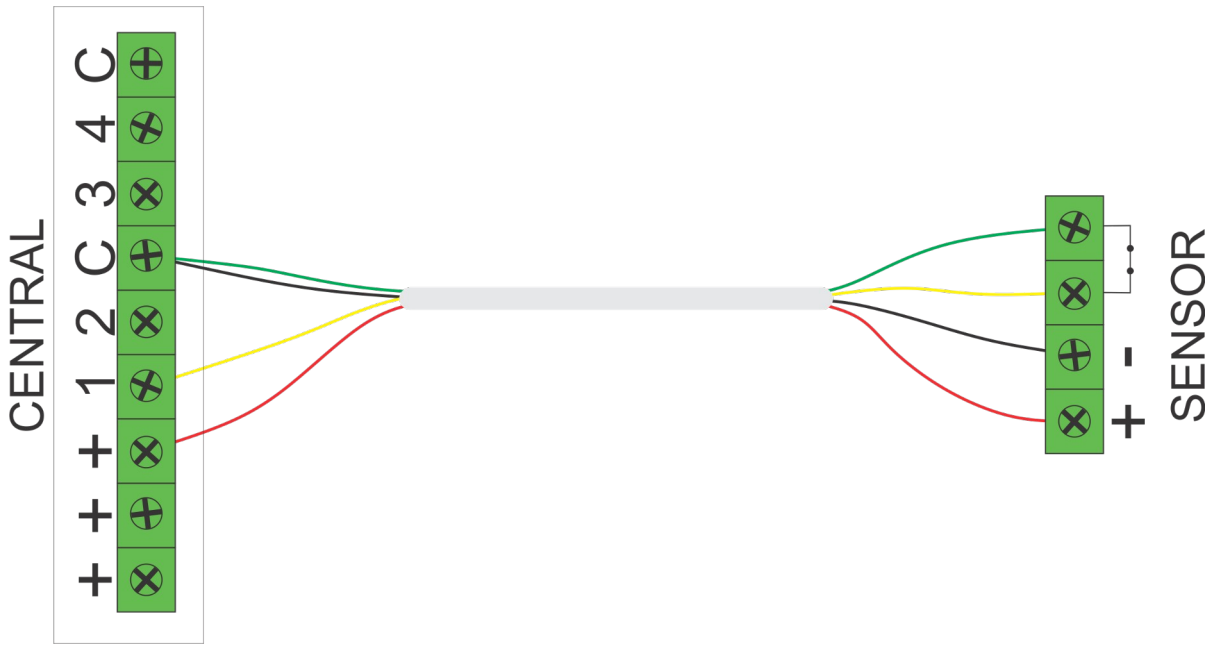
O resistor de fim de linha, quando instalado, permite que a central detecte falha de tamper (quando há rompimento no cabo do sensor ou abertura da caixa do sensor) e curto circuito (quando há sabotagem no fio do sensor).




A central possibilita o funcionamento de 8 ou 16 zonas com ou sem resistor de fim de linha (RFL).

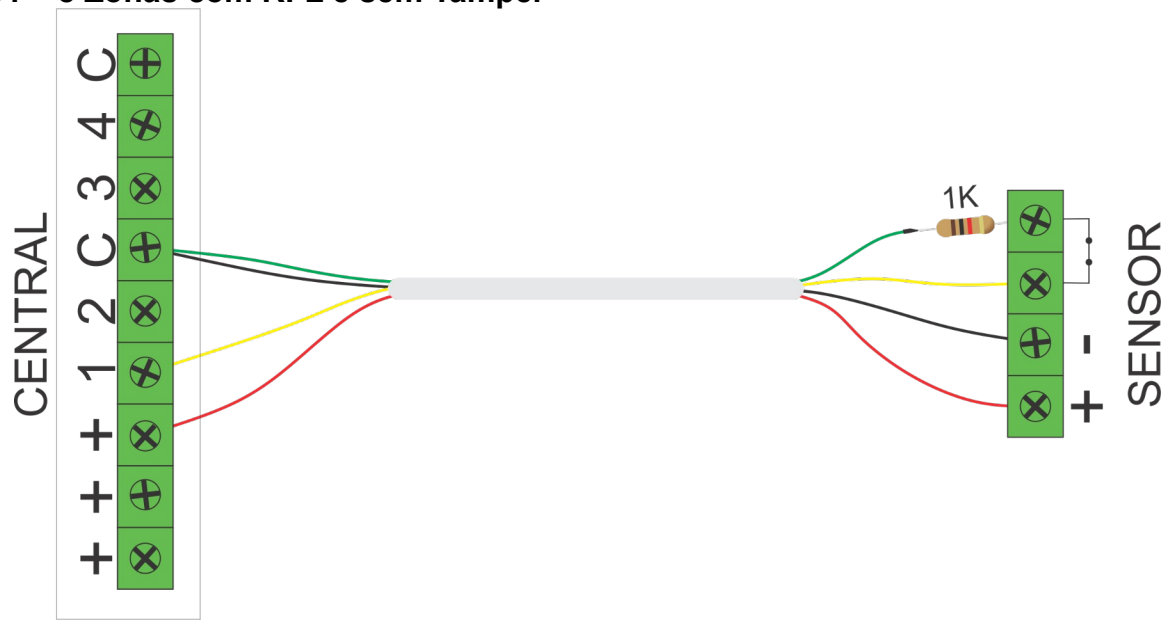
Essas possibilidades estão divididas em 10 diferentes modos:

**MODO 00 – 8 Zonas sem RFL e sem Tamper**



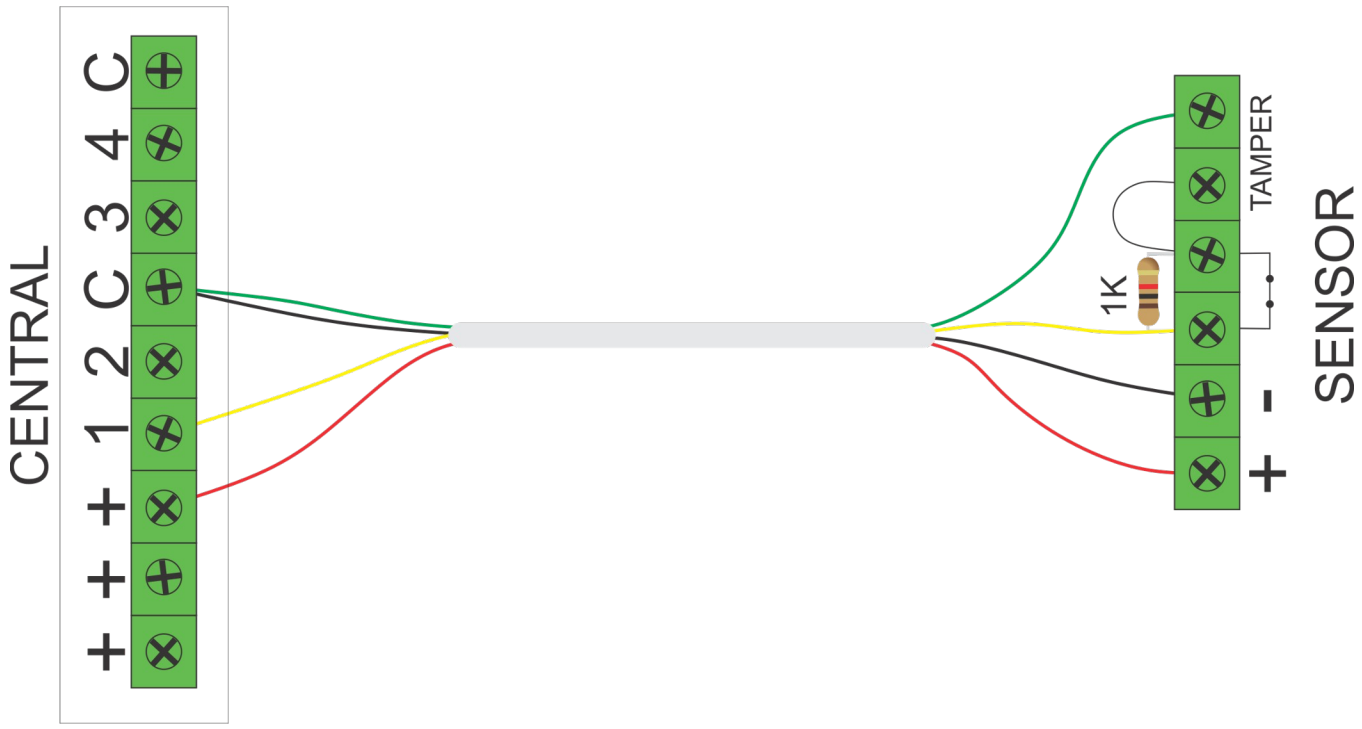

Esta programação não detecta curto na fiação e nem tamper, permite que a central reconheça a abertura e o fechamento do sensor. Esta programação não funciona para sensores NA (normalmente aberto), pois assim a central estará sempre em disparo, porém é possível inverter o estado do sensor para NF (normalmente fechado). Ver função 117.

**MODO 01 – 8 Zonas com RFL e sem Tamper**



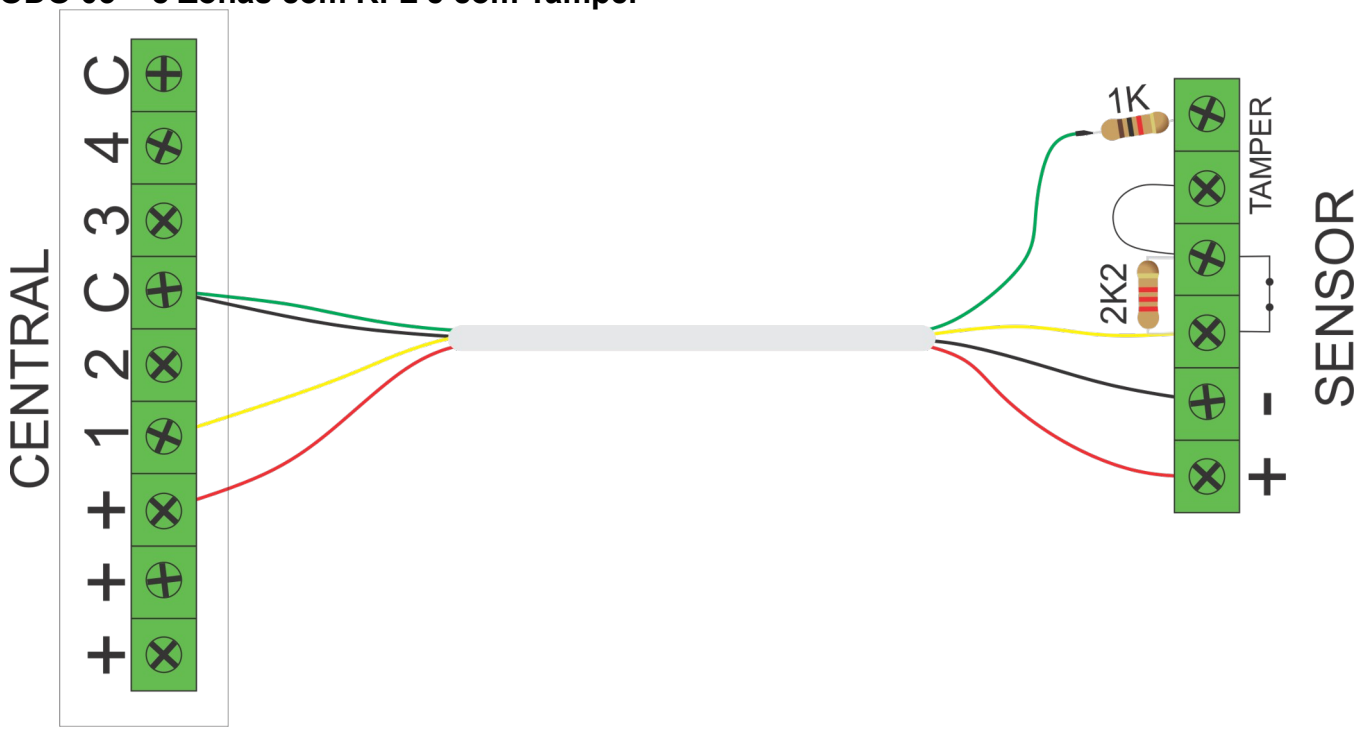

Quando a instalação não necessita de reconhecimento de tamper, mas com detecção de curto na fiação (resistor de fim de linha – RFL). Os sensores podem ser NF (normalmente fechado) ou NA (normalmente aberto), para os sensores NA é necessário mudar a ligação do resistor de série para paralelo, ou inverter o estado da zona, ver função 117.

**MODO 02 – 8 Zonas sem RFL e com Tamper**



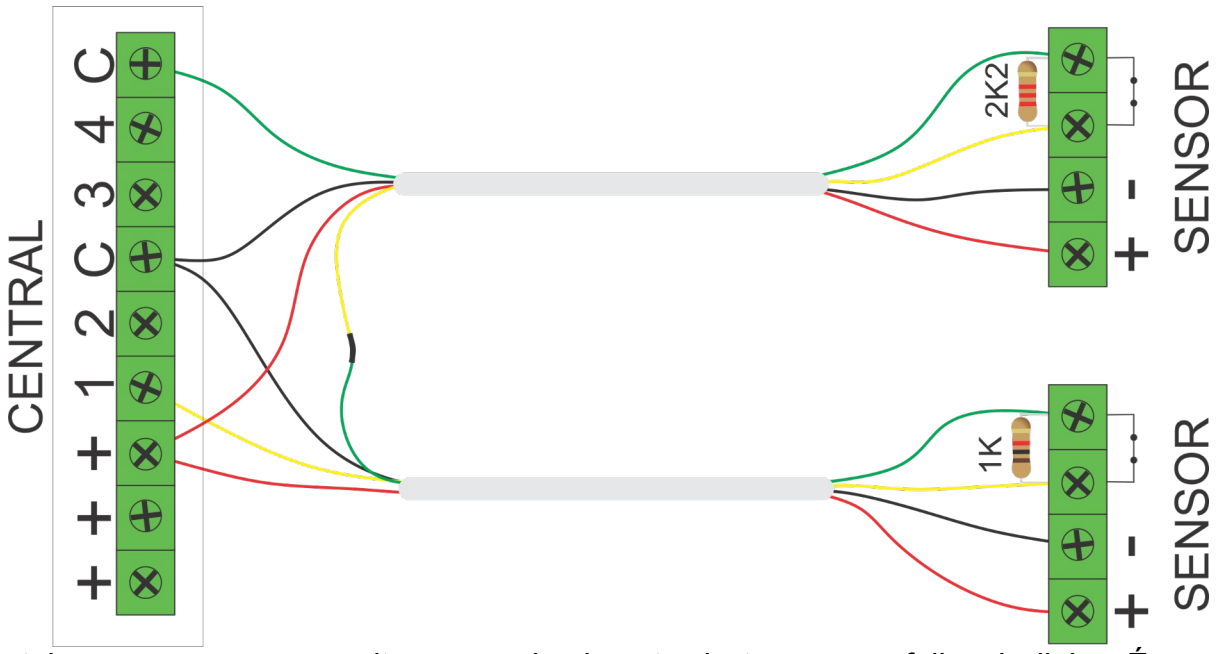

Quando a instalação tem a necessidade de reconhecimento de tamper e sem resistor de fim de linha, isso é possível utilizando um resistor de 1K em paralelo com o relé do sensor. A central reconhece a abertura da tampa do sensor ou o corte da fiação.

**MODO 03 – 8 Zonas com RFL e com Tamper**



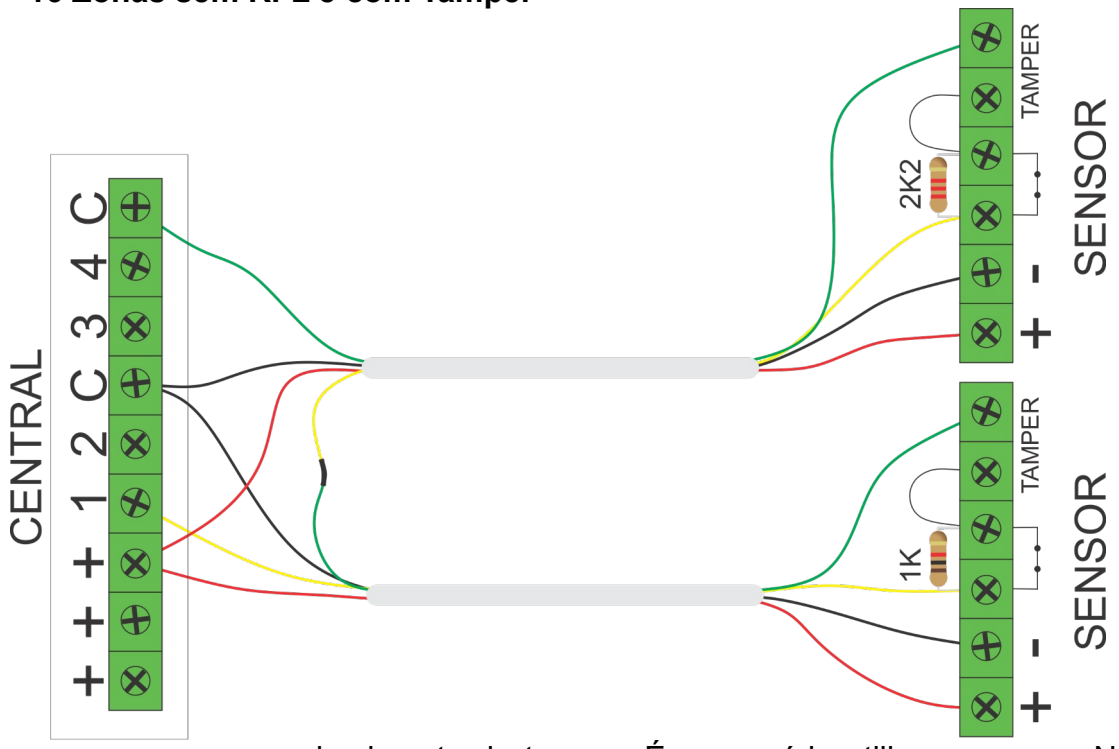

Se a instalação necessita o reconhecimento de tamper e falhas de linha (curto na fiação) e alarmes, é necessário a utilização de sensores normalmente fechados, colocando um resistor de 1K em série com a fiação do alarme e um resistor de 2K2 em paralelo com o relé do sensor. Para os sensores NA é possível inverter o estado da zona, ver função 117.

**MODO 04 – 16 Zonas sem RFL e sem Tamper**



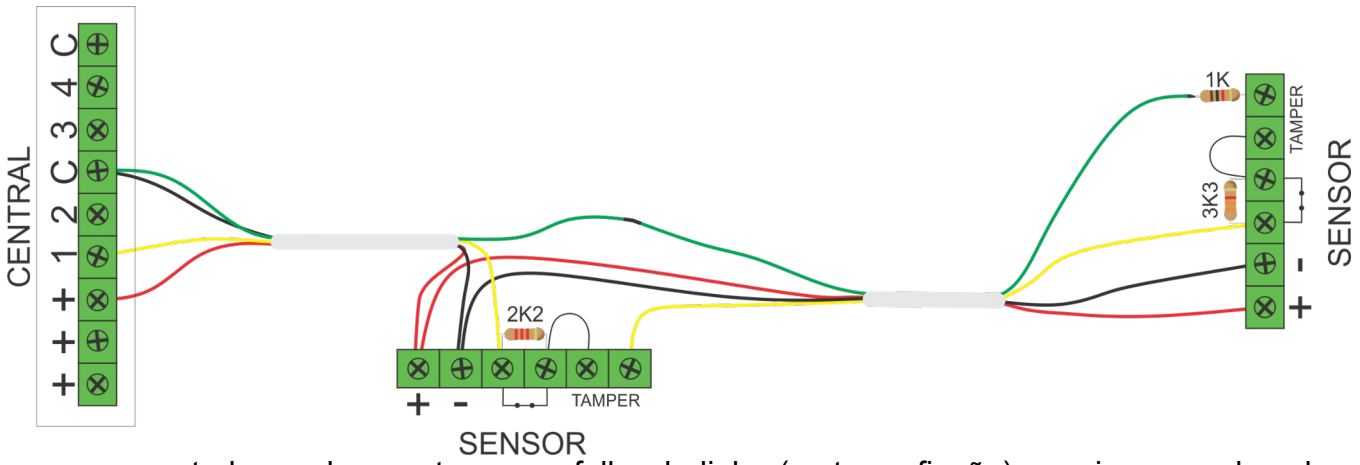

Para instalação que não necessita o reconhecimento de tamper ou falha de linha. É necessário utilizar sensores NF. Para as zonas de 1 a 8 usar resistor de 1K e as zonas de 9 a 16 usar resistor de 2K2. A central vai reconhecer a abertura e fechamento de cada uma das 16 zonas. Para os sensores NA é possível inverter o estado da zona, ver função 117.

**MODO 05 – 16 Zonas sem RFL e com Tamper**



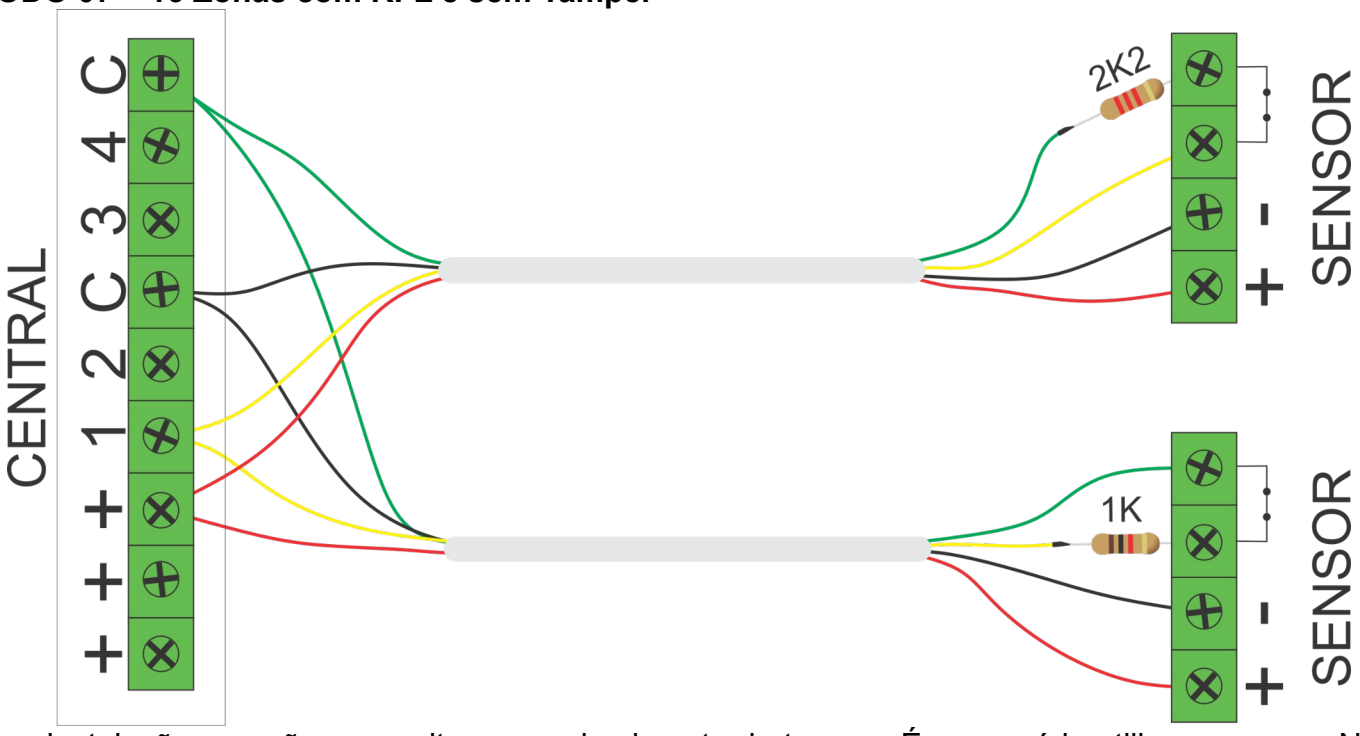

Para utilizar zonas com o reconhecimento de tamper. É necessário utilizar sensores NF, para as zonas de 1 a 8 usar resistor de 1K em paralelo com o relé do sensor e as zonas de 9 a 16 usar resistor de 2K2 em paralelo com o relé do sensor. A central vai reconhecer a abertura e fechamento de cada uma das 16 zonas, abertura da tampa do sensor e cortes na fiação.

**MODO 06 – 16 Zonas com RFL e com Tamper**



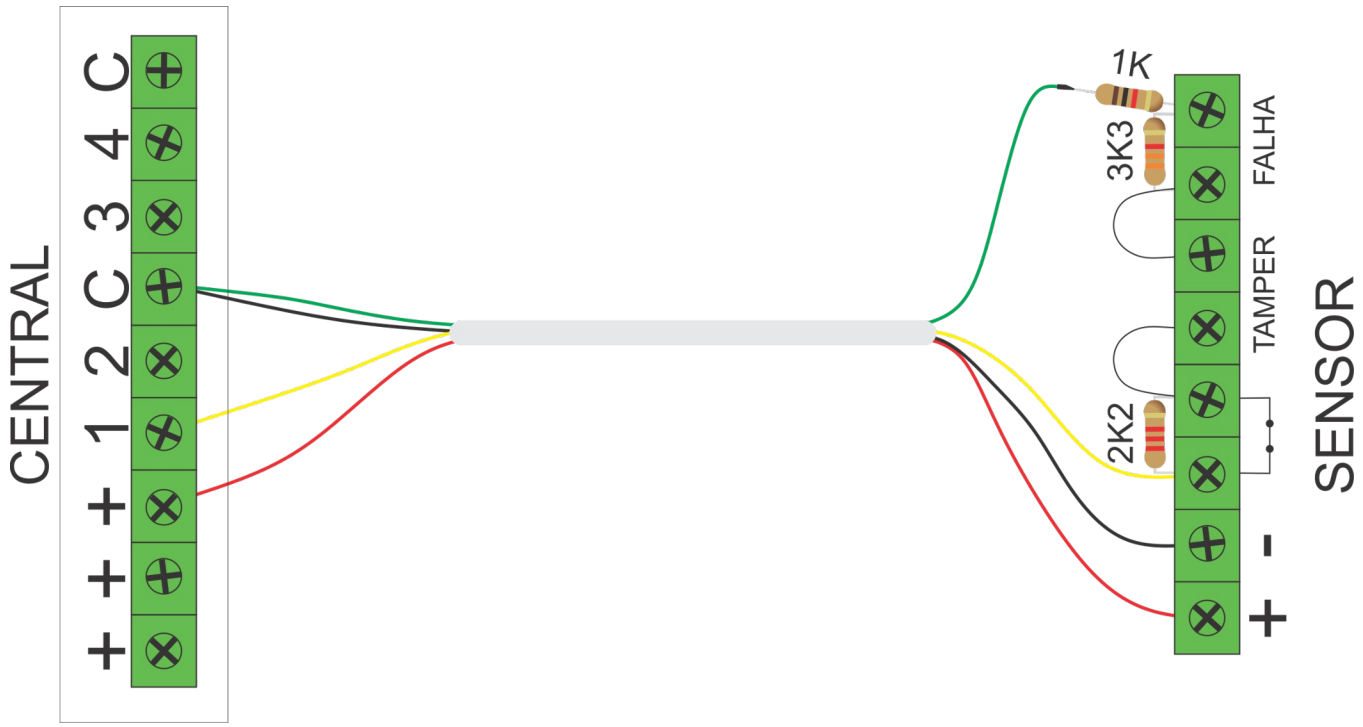

Para que a central reconheça o tamper e falha de linha (curto na fiação), precisa ser colocado um resistor de 1K em série com a entrada da zona e utilizar um resistor de 2K2 em paralelo para as zonas de 1 a 8 e para as zonas de 9 a 16 o resistor de 3K3 em paralelo no relé dos sensores.

**MODO 07 – 16 Zonas com RFL e sem Tamper**



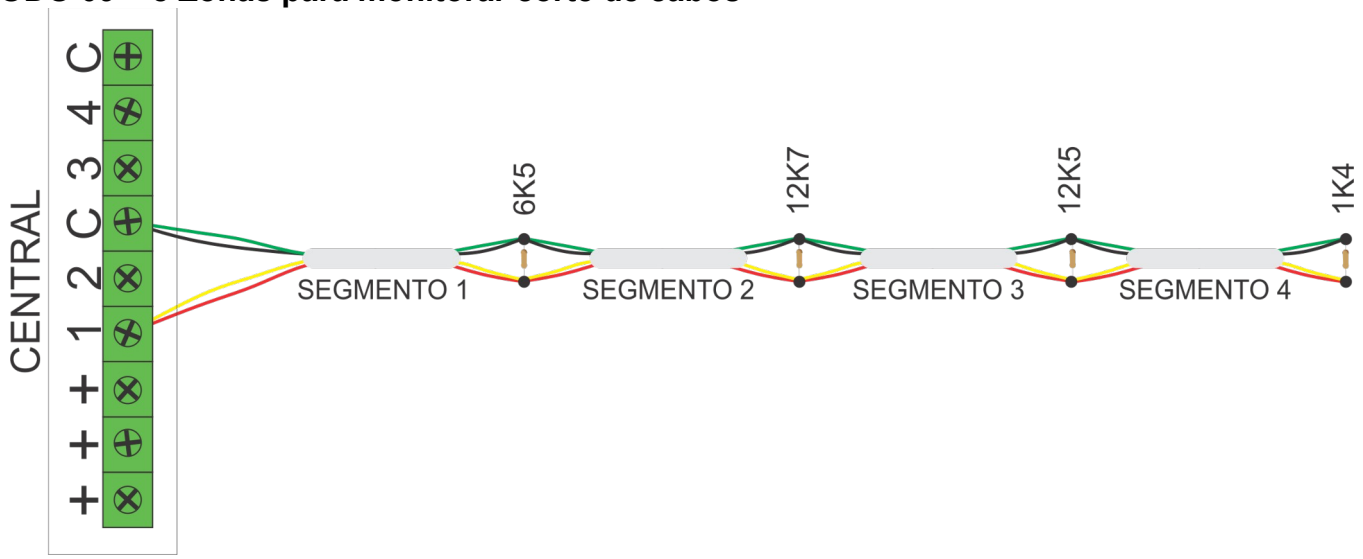

Para instalação que não necessita o reconhecimento de tamper. É necessário utilizar sensores NF, para zonas de 1 a 8 usar resistor de 1K e as zonas de 9 a 16 usar resistor de 2K2. A central vai reconhecer a abertura e fechamento de cada uma das 16 zonas. Para os sensores NA é possível inverter o estado da zona, ver função 117.

**MODO 08 – 8 Zonas com RFL, com Tamper e falha (TEOL)**




Para que a central reconheça o tamper e a falha de linha (curto na fiação) precisa ser colocado um resistor de 1K em série com a entrada da zona e utilizar um resistor de 2K2 em paralelo ao contato do relé. Usar um resistor de 3K3 em paralelo com a saída de falha (AM ou trouble).

**MODO 09 – 8 Zonas para monitorar corte de cabos**




O modo 9 é uma forma de utilização especial das zonas. Desenvolvido especificamente para monitorar corte de cabos, permite detectar em qual dos 4 segmentos o cabo foi cortado.

Deve-se configurar as zonas para funcionarem 24 horas com restauro (opções 4 e 7 das funções 091 a 106). Pode-se inibir o disparo da sirene se desejado, configurando a zona como silenciosa (opção 5).

Possui supervisão de curto, gerando evento de falha de curto caso o cabo monitorado seja circuitado.

Para cada segmento cortado um evento é gerado:
Segmento #4: Disparo da zona.

Código programado nas funções 402 a 409 e restauro, nas funções 442 a 449.
Segmento #3: Disparo da zona alta (equivalente ao TROUBLE do modo 8)
Código programado nas funções 410 a 417 e restauro, nas funções 450 a 457
Segmento #2: Evento de falha de loop
Código programado na função 477 e restauro, na função 478
Segmento #1: Falha de Tamper
Código programado na função 418 e restauro na função 458
Curto-circuito:
Código programado na função 432 e restauro na função 467

**MODO 10 – Desabilita todas as zonas com fio.**

## [ 108 ] Velocidade das Zonas

**[ 108 ]** [ __/__/__ ] Padrão: 005 (0,5 segundos)
Tempo em décimos de segundo, para que a central reconheça abertura ou fechamento das zonas, o tempo pode variar de 001 a 020.

## [ 091 a 106 ] Tipo das Zonas

Para facilitar a instalação, a zona 1 já vem programada como temporizada. Todas as zonas têm a opção “Auto Exclusão” habilitada por padrão.

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

**[ 1 ]** – Temporizada 1
**[ 2 ]** – Temporizada 2
**[ 3 ]** – Preventiva
**[ 4 ]** – 24 Horas
**[ 5 ]** – Silenciosa
**[ 6 ]** – Controle Remoto
**[ 7 ]** – Restauro
**[ 8 ]** – Auto Exclusão
**[ 1 e 2 ]** – Seguidora
**[ 2 e 6 ]** – Zona desabilitada
**[ 5 e 6 ]** – Entrada “Anti-sequestro”
**[4, 5 e 6 ]** – Anti-invasão
**[4, 5 e 7 ]** – Pânico

Dentro de cada função selecione o tipo da zona com as teclas de 1 a 8 (led aceso: tipo selecionado).
A seguir uma descrição detalhada de cada opção:

### Instantânea – todas as opções apagadas

Quando nenhum led estiver aceso, a zona dispara imediatamente após a abertura, se a central estiver armada.

### Temporizada 1 – opção 1

A zona possui duas temporizações: entrada 1 e saída 1.

Tempo de Entrada: tempo que o usuário tem para desarmar o sistema via teclado antes que o mesmo gere o disparo da zona.

Tempo de Saída: Tempo que o usuário tem para sair do local após armar o sistema.

## [ 121 e 123] Tempo de Entrada e Saída 1

**[ 121 ]** [ __/__/__ ] Tempo de Entrada 1 Padrão: 010 segundos
**[ 123 ]** [ __/__/__ ] Tempo de Saída 1 Padrão: 030 segundos

O tempo pode variar de 001 a 254 segundos.

### Temporizada 2 – opção 2

A zona possui duas temporizações: entrada 2 e saída 2.

Tempo de Entrada: tempo que o usuário tem para desarmar o sistema via teclado antes que o mesmo gere o disparo da zona.

Tempo de Saída: tempo que o usuário tem para sair do local após armar o sistema.

## [ 122 e 124] Tempo de Entrada e Saída 2

**[ 122 ]** [ __/__/__ ] Tempo de Entrada 2 Padrão: 020 segundos
**[ 124 ]** [ __/__/__ ] Tempo de Saída 2 Padrão: 040 segundos

O tempo pode variar de 001 a 254 segundos.

## [ 120 ] Partições que Bipam durante a Temporização

| Padrão: Todos Acesos (Habilitados) | Bit / Led / Part. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [ 120 ] Partições que bipam | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Se a instalação possuir teclados, estes podem sinalizar através de bips quando alguma zona estiver temporizando. Os teclados bipam indicando o tempo de saída apenas se houver uma ou mais zonas da VW8ZIP RF temporizando e bipam o tempo de entrada quando qualquer zona temporizada for violada.

### Seguidora – opção 1 e 2

Se uma zona seguidora abrir sem que nenhuma outra zona esteja temporizando, seu disparo é imediato, caso contrário irá temporizar junto com a outra zona. Ao armar o sistema as zonas seguidoras seguem o tempo de saída #1.

### Preventiva – opção 3

Previne alarmes falsos. As zonas programadas como preventivas operam em conjunto; elas somente disparam se durante um determinado período de tempo:

abrirem mais de uma vez; permanecerem abertas; duas ou mais zonas abrirem.

O tempo é programado na função [ 127 ]. **NÃO** se deve programar a zona como preventiva se o sensor for do tipo magnético ou sensor de barreira.

## [ 127 ] Tempo de Zona Preventiva

**[ 127 ]** [ __/__/__ ] Padrão: 045 segundos
O tempo pode variar de 001 a 255 segundos.

## 24 Horas – opção 4

Ao ser aberta, sempre gera disparo, independente se a central ou partição está armada. Esta característica permite programar botões de pânico ou proteger áreas onde nunca deve haver violação (como sensores de barreira em muros, por exemplo).

## Silenciosa – opção 5

Ao disparar não toca a sirene, apenas gera disparo no teclado e envia evento. Esta característica habilitada em conjunto com a opção “24 horas” e o “Restauro” permite programar botões de pânico silenciosos.

## Controle Remoto – opção 6

A zona funciona como chave para armar e desarmar o sistema. Pode-se instalar uma chave ou receptor de controle remoto, desde que os contatos sejam do tipo NF (normalmente fechado). A chave ou receptor deve ser instalado da mesma forma que um sensor do alarme. Qualquer uma das zonas da VW8ZIP RF pode ser configurada como controle remoto.

Nesse caso o número da zona se torna o usuário do sistema. Por exemplo, se a zona 8 for programada para controle remoto, teremos a informação de que o usuário 8 foi quem armou ou desarmou o sistema. Caso o sistema seja particionado, então deve-se configurar quais partições o controle remoto pode armar ou desarmar.

## [ 187 a 202 ] Partições de Controle Remoto

| Padrão: Partição 1 | Bit / Led / Part. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [ 187 ] Partições do Controle Remoto Zona 1 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 188 ] Partições do Controle Remoto Zona 2 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 189 ] Partições do Controle Remoto Zona 3 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 190 ] Partições do Controle Remoto Zona 4 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 191 ] Partições do Controle Remoto Zona 5 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 192 ] Partições do Controle Remoto Zona 6 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 193 ] Partições do Controle Remoto Zona 7 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 194 ] Partições do Controle Remoto Zona 8 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 195 ] Partições do Controle Remoto Zona 9 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 196 ] Partições do Controle Remoto Zona 10 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 197 ] Partições do Controle Remoto Zona 11 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 198 ] Partições do Controle Remoto Zona 12 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 199 ] Partições do Controle Remoto Zona 13 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 200 ] Partições do Controle Remoto Zona 14 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 201 ] Partições do Controle Remoto Zona 15 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 202 ] Partições do Controle Remoto Zona 16 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Quando uma zona é programada para controle remoto, programa-se qual das partições o controle vai operar.

Entre na função correspondente à zona em que está ligado o receptor.

Para selecionar uma ou mais partições pressione a tecla correspondente a partição.

O led aceso indica partição selecionada, pressione ENT para confirmar.

### Restauro – opção 7

Restaura a zona e envia o evento de restauro logo após o fechamento. Se não for habilitado, o restauro é enviado somente quando a sirene parar de tocar.

### Anti-Sequestro – opção 5 e 6

Quando uma zona é aberta com a característica “anti-sequestro”, uma senha precisa ser digitada no teclado ou um controle remoto acionado durante o tempo de “anti-sequestro” função [ 125 ]. Caso isso não ocorra, a central irá reportar o evento de COAÇÃO função [ 422 ].

### [ 125 ] Tempo de Zona Anti-Sequestro

**[ 125 ]** [ __/__/__ ] Padrão: 000 segundos (Anti-sequestro desabilitada)

Tempo (de 000 à 255 segundos) antes de enviar disparo da zona caso uma zona anti-sequestro tenha sido aberta.

### Anti-Invasão – opção 4, 5 e 6

A zona anti-invasão funciona em conjunto com a zona anti-sequestro. Após abrir a zona anti-sequestro, é possível violar a zona anti-invasão uma vez sem que gere disparo. Se houver uma nova abertura ou a zona permanecer aberta pelo tempo de zona anti-invasão, dispara o sistema.

### [ 126 ] Tempo de Zona Anti-Invasão

**[ 126 ]** [ __/__/__ ] Padrão: 000 segundos

Tempo em segundos que a zona anti-invasão pode ficar aberta sem gerar disparo.

As zonas anti-sequestro e anti-invasão permitem que se configure um sistema de segurança para chegada de veículos em uma guarita de condomínio. Ao se aproximar do local, o morador aciona o controle remoto abrindo a zona anti-sequestro. Uma barreira instalada na zona anti-invasão irá permitir a passagem do veículo sem gerar disparo. Caso alguém aproveite a abertura do portão para entrar, antes ou depois do veículo, fará com que a zona anti-invasão dispare.

Da mesma forma, se o usuário acionou a zona anti-sequestro, mas não desarmou o sistema no tempo programado, um evento de coação é gerado, indicando que o usuário não conseguiu chegar em segurança.

A zona anti-invasão também pode ser instalada no fecho do portão, para evitar que se esqueça o portão aberto.

### Auto Exclusão – opção 8

A zona que disparar consecutivamente, no mesmo período de armado, o número de vezes da função [ 113 ], será automaticamente anulada. O evento de auto exclusão de zona é enviado.

### [ 113 ] Número de Disparos para Auto Exclusão

**[ 113 ]** [ __/__/__ ] Padrão: 005

Número de vezes consecutivas que uma zona configurada com auto exclusão, deve disparar dentro do tempo de armado para ser automaticamente anulada. Se alguma outra zona disparar, reinicia a contagem de disparos.

O número de disparos pode variar de 001 a 255.

### [ 109 e 110 ] Zonas com Chime

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 109 ] Chime nas Zonas (1 – 8) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Zona** |
| [ 110 ] Chime nas Zonas (9 – 16) | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | **Zona** |

Define quais as zonas que poderão funcionar também como anunciador de presença. Todas as zonas que forem programadas com o anunciador de presença habilitado poderão emitir um sinal sonoro nos teclados toda vez que forem abertas. Nos teclados de LED para que emita o sinal de uma determinada zona, fora do modo de programação, mantenha pressionada a tecla correspondente à zona até ouvir um bip de OK; repita o processo para desligar o sinal.

## [ 111 e 112 ] Zonas sem Exclusão

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 111 ] Zonas sem exclusão (1 – 8) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Zona** |
| [ 112 ] Zonas sem exclusão (9 – 16) | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | **Zona** |

Impede que essas zonas sejam excluídas ao armar o sistema.

## [ 114 e 115 ] Zonas Cruzadas

| Padrão: Todos Apagados (Desabilitados) | 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 | **Zona** |

Uma zona cruzada, somente gera disparo se for violada em conjunto com uma ou mais zonas cruzadas do mesmo equipamento. Ou seja, se a zona for programada como “cruzada” somente gera disparo se no momento da violação, outras zonas “cruzadas” estiverem violadas. Caso o número de zonas cruzadas violadas for inferior ao mínimo necessário (função 116), a zona abre sem gerar disparo. Caso alguma outra zona cruzada já tenha disparado, então as demais zonas cruzadas irão disparar independente do número de zonas abertas.

## [ 116 ] Número de Zonas Cruzadas abertas para Disparo

**[ 116 ]** [ __/__/__ ] Padrão: 000

Indica quantas zonas cruzadas (funções [114] e [115]) precisam abrir ao mesmo tempo para disparar.

## [ 119 ] Zona Esquecida Aberta (Zona 2)

**[ 119 ]** [ __/__/__ /__] Padrão: 0000 (MM:SS - Recurso desabilitado)

Nessa função programa-se o tempo (em minutos e segundos) em que a zona 2 pode permanecer aberta. Se a zona 2 permanecer aberta além do tempo programado, o evento programado no campo [423] é enviado. O campo partição do evento será a partição da zona 2 e o campo zona será 002.

## [ 423 ] Zona Esquecida Aberta – Código Contact ID

**[ 423 ]** [ __/__/__/__ ] Padrão: 0000 (evento desabilitado)

Quatro dígitos com o código Contact ID do evento.

## [ 117 e 118 ] Inversão do estado das zonas

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 117 ] Inverte Zonas (1 – 8) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Zona** |
| [ 118 ] Inverte Zonas (9 – 16) | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | **Zonas** |

Se a opção estiver habilitada, ocorre a inversão do estado da zona. A zona aberta será considerada fechada e a zona fechada será considerada aberta. Não há alteração no modo de ligação das zonas ou nos estados de tamper, corte e curto.

### [ 1501 a 1628 ] Nome das Zonas

**[ 1501 a 1628 ]** [ __/__/… /__ ] 16 caracteres Padrão: Setor xxx (onde xxx é o número do setor)

Esse é o nome dado às zonas que compõem a VW8ZIP RF. É enviado quando o usuário acessa a central pelo Navegador de Internet.

# SENHAS

A Central VW16Z 4G IP possui 64 senhas de usuário. Cada senha de usuário pode ter acesso a qualquer uma das oito partições do sistema. Isso significa que é possível ter senhas que armam uma partição, senhas que armam todas as partições ou mesmo senhas que não armam partição alguma.

As senhas representam os usuários do sistema, sendo a senha 1 para o usuário 001, senha 2 para o usuário 002 e assim sucessivamente.

Alguns periféricos como teclados podem incluir mais usuários ao sistema, que pode ser expandido. Esses usuários podem ter senhas adicionais, controles remotos ou cartões de acesso.

As senhas são usadas nos teclados, software VIAWEB Mobile ou navegador WEB, para armar, desarmar ou inibir zonas do sistema.

### Cadastrando senhas

O cadastro de novos usuários pode ser feito via teclado ou via navegador **WEB**. Os usuários 1 e 2 são considerados usuários “mestres”; somente esses usuários podem cadastrar novos usuários. No padrão de fábrica, o usuário 1 vem com a senha “1515” (ou “151515” se configurado para 6 dígitos) e o usuário 2 não possui senha.

### Cadastrando senhas por teclado

Para cadastrar novos usuários por teclado, execute a sequência:

ENT (senha mestre 1 ou 2) ENT

Se a senha for correta, ouve-se um bip de OK e o teclado entra no modo de cadastro.

Digita-se o número do usuário com 3 dígitos (001 até 100). Em seguida digita-se a senha que este usuário irá utilizar, ou pressionar CANCELAR para apagar a senha deste usuário.

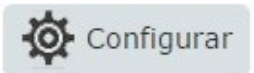
(número do usuário) (senha de 4, 5 ou 6 dígitos)

Se o código do usuário for cadastrado corretamente, ouve-se um bip de OK. Pode-se repetir a sequência: “número do usuário”, “código do usuário” até que todos os usuários sejam cadastrados. Ao fim do processo de cadastro deve-se pressionar **ENTER** para sair do modo de cadastro.

Exemplos:

1. Cadastrar usuário mestre 2: **ENTER 1515 ENTER 002 1234 ENTER**
2. Alterar usuário mestre 1: **ENTER 1515 ENTER 001 4321 ENTER**
3. Cancelar usuário 3: **ENTER 4321 ENTER 003 CANCELAR**
4. Cadastrar 2 usuários: **ENTER 4321 ENTER 004 4444 005 5555 ENTER**

## Cadastrando senhas via Página WEB

Abra o navegador WEB, clique em “ 

” e em seguida “  ”

## [ 220 ] Número de Dígitos das Senhas

**[ 220 ]** [ _ ] Padrão: 4 dígitos

Define quantos dígitos terão as senhas, se 4, 5 ou 6 dígitos. Essa função afeta todas as senhas, (Programação, Mestre e de Usuários).

OBS.: A senha de download sempre terá 6 dígitos.

## [ 221 ] Senha de Programação

**[ 221 ]** [ __/__/__/__/__/__ ] Padrão: 535353

A senha de programação permite alterar todas as funções da central. (zonas, partições, sirene, discagem, download), podendo ser de 4, 5 ou 6 dígitos, de acordo com a função [ 220 ].

## [ 222 a 285 ] Partições que o Usuário tem Acesso (01 a 64)

| Padrão: Partição 1 | Led \ Bit \ Partição | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [ 222 a 231 ] Usuários de 001 a 010 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 232 a 241 ] Usuários de 011 a 020 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 242 a 251 ] Usuários de 021 a 030 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 252 a 261 ] Usuários de 031 a 040 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 262 a 271 ] Usuários de 041 a 050 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 272 a 281 ] Usuários de 051 a 060 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 282 a 285 ] Usuários de 061 a 064 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Programa-se para cada senha, quais as partições ela terá acesso para armar ou desarmar. Para sistema não particionado a partição 1 deverá ser utilizada para permitir acesso.

## [ 348 ] Senha de Coação

| Padrão: Apagado (Desabilitado) | | **Led / Bit** |
|---|---|---|
| **[348]** | Habilita senha 064 do **painel de alarme** como senha de coação.<br>A senha 064 passa a operar como senha de coação, arma e desarma o sistema, todas as partições, e envia evento de coação. **(E121)** | 1 |
| | Habilita todas as senhas do **painel de alarme** para coação.<br>Qualquer senha que ao ser digitada tenha os dois últimos dígitos invertidos, gera coação. A senha continua armando e desarmando.<br>Ex: Senha 1 2 3 4, ao ser digitado 1 2 4 3 será gerado evento de coação.<br>OBS: Para evitar conflitos de senhas iguais deve-se habilitar esse modo antes de cadastrar os códigos das senhas. | 2 |

Coação é quando o usuário é “forçado” a desarmar a central. Nesse momento o usuário pode digitar a senha de coação para que o sistema desarme e ao mesmo tempo envie um evento de coação. O evento de coação é programado na função [ 422 ], evento 1121 é o padrão de fábrica para essa função.

## [ 349 e 350 ] Usuários temporários (senhas 029 e 030)

**[ 349 ]** [ __/__/__ ] Tempo de duração do usuário 29 Padrão: 000 (desabilitado)

**[ 350 ]** [ __/__/__ ] Tempo de duração do usuário 30 Padrão: 000 (desabilitado)

Tempo (de 000 à 255 horas) de duração da senha dos usuários temporários 29 e 30.

O valor 000, indica que essas senhas não são temporárias. Programar esses campos com a

quantidade de horas que a senha 29 ou 30 deverá durar.

O tempo de duração começa a contar no momento em que a função é programada ou quando a senha é cadastrada ou alterada.

## [ 352 ] Senha de Download

**[ 352 ]** [ __/__/__/__/__/__ ] Padrão: 363636 (6 dígitos)

A senha de download é a senha que permite a programação da central via cabo serial utilizando o software VIAWEB download. A senha que está na central deve ser a mesma do computador.

## [ 047 a 050] Horário de Funcionamento das Senhas com Horário Restrito

**[ 047 ]** [ __/__: __/__ ] Início do Primeiro Horário de Funcionamento das Senhas Padrão: 00:00
**[ 048 ]** [ __/__: __/__ ] Fim do Primeiro Horário de Funcionamento das Senhas
**[ 049 ]** [ __/__: __/__ ] Início do Segundo Horário de Funcionamento das Senhas
**[ 050 ]** [ __/__: __/__ ] Fim do Segundo Horário de Funcionamento das Senhas

As senhas pertencentes a grupos habilitados como horário restrito (Função 324) somente irão operar somente durante os dois intervalos de horário programados nessas funções.

## [ 400 ] Dias da semana de Funcionamento das Senhas com Horário Restrito

| [ 400 ] Dias da Semana das Senhas (Desabilitado) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Dom | Seg | Ter | Qua | Qui | Sex | Sáb | |
| **Tecla/Led** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

As senhas pertencentes a grupos habilitados como horário restrito (Função 324) podem ter dias da semana definidos para funcionar, sendo tecla 1 para domingo, 2 para segunda…até 7 para o sábado.

Nos dias habilitados nessa função as senhas somente irão funcionar durante um dos intervalos programados nas funções 047 a 050.

Para os demais dias da semana, as senhas podem não funcionar ou funcionar o dia todo, dependendo do valor habilitado na opção 8. Sendo:

**Opção 8 habilitada** – Nos demais dias, as senhas funcionam o dia todo.

**Opção 8 desabilitada** – Nos demais dias, as senhas não funcionam.

## [ 363 ] Inibir senha de programação quando central está armada - (bit) 2

| Padrão: Apagado (Desabilitado) | | Bit/Led |
|---|---|---|
| [ 363 ] | Se habilitado, a senha de programador somente irá funcionar se todas as partições estiverem desarmadas. Dessa forma pode-se impedir que o usuário altere a programação via teclado se a central estiver armada. | 2 |

## [ 1401 a 1464 ] Nome dos Usuários

**[ 1401 a 1464 ]** [ __/__/ …] (16 caracteres) Padrão: Usuário xxx (onde xxx é o número do usuário).

O nome cadastrado aqui aparece quando acessa a central pelo Navegador de Internet.

# GRUPOS DE USUÁRIOS

## [ 601 a 664 ] Grupo do usuário – Tipos de Grupos

Padrão: 1 (Grupo 1)

[ 601 ] [ __ ] Usuário 001 – Escolha Grupo de 1 a 8
[ 602 ] [ __ ] Usuário 002 – Escolha Grupo de 1 a 8
[ 603 ] [ __ ] Usuário 003 – Escolha Grupo de 1 a 8
[ 604 ] [ __ ] Usuário 004 – Escolha Grupo de 1 a 8
[ 605 ] [ __ ] Usuário 005 – Escolha Grupo de 1 a 8
[ 606 ] [ __ ] Usuário 006 – Escolha Grupo de 1 a 8
[ 607 ] [ __ ] Usuário 007 – Escolha Grupo de 1 a 8
[ 608 ] [ __ ] Usuário 008 – Escolha Grupo de 1 a 8
[ 609 ] [ __ ] Usuário 009 – Escolha Grupo de 1 a 8
[ 610 ] [ __ ] Usuário 010 – Escolha Grupo de 1 a 8
[ 611 ] [ __ ] Usuário 011 – Escolha Grupo de 1 a 8
[ 612 ] [ __ ] Usuário 012 – Escolha Grupo de 1 a 8
[ 613 ] [ __ ] Usuário 013 – Escolha Grupo de 1 a 8
[ 614 ] [ __ ] Usuário 014 – Escolha Grupo de 1 a 8
[ 615 ] [ __ ] Usuário 015 – Escolha Grupo de 1 a 8
[ 616 ] [ __ ] Usuário 016 – Escolha Grupo de 1 a 8
[ 617 ] [ __ ] Usuário 017 – Escolha Grupo de 1 a 8
[ 618 ] [ __ ] Usuário 018 – Escolha Grupo de 1 a 8
[ 619 ] [ __ ] Usuário 019 – Escolha Grupo de 1 a 8
[ 620 ] [ __ ] Usuário 020 – Escolha Grupo de 1 a 8
[ 621 ] [ __ ] Usuário 021 – Escolha Grupo de 1 a 8
[ 622 ] [ __ ] Usuário 022 – Escolha Grupo de 1 a 8
[ 623 ] [ __ ] Usuário 023 – Escolha Grupo de 1 a 8
[ 624 ] [ __ ] Usuário 024 – Escolha Grupo de 1 a 8
[ 625 ] [ __ ] Usuário 025 – Escolha Grupo de 1 a 8
[ 626 ] [ __ ] Usuário 026 – Escolha Grupo de 1 a 8
[ 627 ] [ __ ] Usuário 027 – Escolha Grupo de 1 a 8
[ 628 ] [ __ ] Usuário 028 – Escolha Grupo de 1 a 8
[ 629 ] [ __ ] Usuário 029 – Escolha Grupo de 1 a 8
[ 630 ] [ __ ] Usuário 030 – Escolha Grupo de 1 a 8
[ 621 ] [ __ ] Usuário 031 – Escolha Grupo de 1 a 8
[ 632 ] [ __ ] Usuário 032 – Escolha Grupo de 1 a 8
[ 633 ] [ __ ] Usuário 033 – Escolha Grupo de 1 a 8
[ 634 ] [ __ ] Usuário 034 – Escolha Grupo de 1 a 8
[ 635 ] [ __ ] Usuário 035 – Escolha Grupo de 1 a 8
[ 636 ] [ __ ] Usuário 036 – Escolha Grupo de 1 a 8
[ 637 ] [ __ ] Usuário 037 – Escolha Grupo de 1 a 8
[ 638 ] [ __ ] Usuário 038 – Escolha Grupo de 1 a 8
[ 639 ] [ __ ] Usuário 039 – Escolha Grupo de 1 a 8
[ 640 ] [ __ ] Usuário 040 – Escolha Grupo de 1 a 8
[ 641 ] [ __ ] Usuário 041 – Escolha Grupo de 1 a 8
[ 642 ] [ __ ] Usuário 042 – Escolha Grupo de 1 a 8
[ 643 ] [ __ ] Usuário 043 – Escolha Grupo de 1 a 8
[ 644 ] [ __ ] Usuário 044 – Escolha Grupo de 1 a 8
[ 645 ] [ __ ] Usuário 045 – Escolha Grupo de 1 a 8
[ 646 ] [ __ ] Usuário 046 – Escolha Grupo de 1 a 8
[ 647 ] [ __ ] Usuário 047 – Escolha Grupo de 1 a 8
[ 648 ] [ __ ] Usuário 048 – Escolha Grupo de 1 a 8
[ 649 ] [ __ ] Usuário 049 – Escolha Grupo de 1 a 8
[ 650 ] [ __ ] Usuário 050 – Escolha Grupo de 1 a 8
[ 651 ] [ __ ] Usuário 051 – Escolha Grupo de 1 a 8
[ 652 ] [ __ ] Usuário 052 – Escolha Grupo de 1 a 8
[ 653 ] [ __ ] Usuário 053 – Escolha Grupo de 1 a 8
[ 654 ] [ __ ] Usuário 054 – Escolha Grupo de 1 a 8
[ 655 ] [ __ ] Usuário 055 – Escolha Grupo de 1 a 8
[ 656 ] [ __ ] Usuário 056 – Escolha Grupo de 1 a 8
[ 657 ] [ __ ] Usuário 057 – Escolha Grupo de 1 a 8
[ 658 ] [ __ ] Usuário 058 – Escolha Grupo de 1 a 8
[ 659 ] [ __ ] Usuário 059 – Escolha Grupo de 1 a 8
[ 660 ] [ __ ] Usuário 060 – Escolha Grupo de 1 a 8
[ 661 ] [ __ ] Usuário 061 – Escolha Grupo de 1 a 8
[ 662 ] [ __ ] Usuário 062 – Escolha Grupo de 1 a 8
[ 663 ] [ __ ] Usuário 063 – Escolha Grupo de 1 a 8
[ 664 ] [ __ ] Usuário 064 – Escolha Grupo de 1 a 8

**As características são setadas em 8 grupos distintos cada um com uma função:**

## [ 399 ] Grupo desabilita o rearme por inércia

Usuários/Senhas que impedem o rearme por inércia. Grupo 1 a 8.

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 399 ] Grupo desabilita o rearme por inércia | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Grupo |

**Os usuários pertencentes a esse grupo podem desarmar partições programadas para rearmar por inércia e estas não mais rearmarão por inércia.**

## [ 322 ] Grupo arme forçado

Senhas que armam forçado. Grupo 1 a 8. Padrão somente grupo 1.
Os usuários que pertencem a este grupo podem armar ignorando as zonas abertas da central. Essas zonas somente irão gerar disparo se restaurarem e abrirem novamente após a ativação.

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 322 ] Grupo arme forçado (1 – 8) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Grupo** |

## [ 323 ] Grupo não exclui zona

Senhas que não excluem zonas. Grupo 1 a 8. Padrão todos excluem.

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 323 ] Grupo não exclui zona (1 – 8) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Grupo** |

## [ 324 ] Grupo horário restrito

Controles com horário restrito. Grupo 1 a 8. Padrão todos sem restrição.
** Programar dias da semana na função 400 e horário nas funções 047 a 050

| Padrão: Todos Apagados (Desabilitados) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 324 ] Grupo horário restrito (1 – 8) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Grupo** |

# PARTIÇÕES

## [ 204 ] *Sistema Particionado*

| Padrão: **Todos desabilitados (Apagado)** | | Bit/Led |
|---|---|---|
| [ 204 ] | Sistema particionado | 1 |
| | Partição 2 como partição interna | 2 |
| | Não arma com falha de periférico | 3 |
| | Armar mesmo com a sirene tocando | 4 |
| | Tempo de inércia das partições contado em horas (Funções 139 a 146) | 5 |

**Sistema Particionado (opção 1):**

Quando habilitada, permite particionar o sistema. Pode-se definir quais senhas terão acesso a quais partições e quais zonas farão parte de quais partições. O painel possui 8 partições com funcionamento independente. Se o sistema não for particionado todas as zonas ficam atribuídas automaticamente a partição 1. ***Habilitar os teclados para armar/desarmar as partições (acionamento parcial).***

**Partição 2 como partição interna (opção 2):**

Ao armar a partição 1, a partição 2 espera por movimento nas zonas da partição 1 durante o tempo de saída 1 (função 123). Se uma ou mais zonas da partição 1 abrirem durante esse tempo a partição 2 irá armar automaticamente. Se não houver nenhum movimento em nenhuma zona da partição 1, a partição 2 não arma.

Se ao final do tempo de espera, a partição 1 estiver em disparo, a partição 2 não arma.

Ao desarmar a partição 1, a partição 2 irá desarmar também.

A partição 2 ainda pode ser armada ou desarmada por outros meios (senhas, controle remoto, etc…)

**Aplicação:**

Quando o usuário arma a partição 1 e deixa o local (violando zonas temporizadas da partição 1) a partição 2

entende que não há pessoas na área interna e arma.
Quando o usuário arma a partição 1, mas permanece no local (não sai para as áreas externas e não viola nenhuma zona da partição 1) a partição 2 percebe essa condição e se mantém desarmada.
Caso o usuário arme a partição 1 e ocorra um disparo (violação de uma zona não temporizada por exemplo) a partição 2 irá se manter desarmada para evitar novos disparos indesejados.
Se alguma zona da partição 2 for esquecida aberta, ocorrerá disparo após o arme da partição

**Modo de configuração:**

Essa opção deve ser habilitada em conjunto com a opção 1 (sistema particionado).
Os usuários e controles devem ter acesso apenas a partição 1, deixando a partição 2 armar e desarmar automaticamente.
Todas as zonas externas devem ser configuradas para a partição 1.
Todas as zonas internas devem ser configuradas para a partição 2.
A partição 1 deve possuir ao menos uma zona temporizada, para que seja possível ao usuário sair do local após armar a partição 1 sem gerar disparo.

**Não arma com falha de periférico (opção 3):**

Quando habilitada não arma nenhuma partição do sistema se houver falha de periférico.

Para armar, o usuário deverá executar o comando de arme forçado (usando um teclado 128s ou Touch). A senha deverá ter permissão de arme forçado.

Ao armar o sistema junto com o evento de armado, irá enviar novamente o evento de falha de periférico (padrão E143) de todos os periféricos com falha. Essa opção é desabilitada no reset (padrão de fábrica).

Evento falha de periférico/falha no módulo expansão (pág. 68).

**Periférico** – equipamentos que estão ligados no barramento iNNOVAbus (teclados, expansores, módulos, etc.)

**Armar mesmo com a sirene tocando (opção 4):**

Quando desabilitada, a central irá evitar armar qualquer partição caso a sirene esteja disparada.

Se habilitado a central poderá ser armada, mesmo com a sirene em disparo.

**Tempo de inércia das partições contado em horas (opção 5):**

Se habilitado o valor programado nas funções 139 a 146 corresponderá à horas sem movimento e não a minutos.

## [ 171 a 186 ] Partições das Zonas

Padrão: 1 (partição 1)

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

Quando particionado o sistema, definimos aqui a qual partição a zona pertence.

**1 -** **Zona para a Partição 1** ( Padrão )
**2 -** Zona para a Partição 2
**3 -** Zona para a Partição 3
**4 -** Zona para a Partição 4
**5 -** Zona para a Partição 5
**6 -** Zona para a Partição 6
**7 -** Zona para a Partição 7
**8 -** Zona para a Partição 8

Quando utilizada a partição comum, (função [ 203 ]), as zonas programadas para a partição 8 somente serão ativadas quando as partições programadas na função [ 203 ] estiverem ativadas.

## [ 591 a 598 ] Nomes das Partições

**[ 591 ]** [ __/__/ … /__/__ ] (16 caracteres) Padrão: Partição x (onde x é o número da partição)
Nomes das partições.

## [ 203 ] Partição 8 Comum

| Padrão: Desabilitado todos os leds apagados | Led \ Bit \ Partição | | | | | | |
|---|---|---|---|---|---|---|---|
| **[ 203 ]** Partições em comum com a Partição 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

Quando for habilitado o sistema particionado, existe a possibilidade da partição de número 8 armar somente quando as outras partições em conjunto com ela estiverem também armadas. Quando alguma das partições for desarmada, a partição 8 desarma junto até que todas as outras sejam armadas novamente.

Para programar qual ou quais partições devem funcionar em conjunto, deixe os leds referentes às partições acesos.

Para que a partição 8 funcione independente, os leds devem estar todos apagados.

# AUTO ATIVA

## [ 131 a 138 ] Horário de Auto Ativa

Padrão: FF:FF (hh:mm) desabilitado
[ 131 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 1
[ 132 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 2
[ 133 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 3
[ 134 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 4
[ 135 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 5
[ 136 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 6
[ 137 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 7
[ 138 ] [ __/__/__/__ ] Horário de Auto ativa da Partição 8

Programando um horário válido nesses campos (0000 até 2359), o sistema arma independente do estado das zonas. Se alguma zona imediata estiver aberta, imediatamente após armar, um disparo será gerado. Para desprogramar preencha com FFFF (INF+6).

## [ 206 a 209 e 358 a 361 ] Horário de Auto Desativa

Padrão: FF:FF (hh:mm) desabilitado
[ 206 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 1
[ 207 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 2
[ 208 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 3
[ 209 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 4
[ 358 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 5
[ 359 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 6
[ 360 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 7
[ 361 ] [ __/__/__/__ ] Horário de Auto Desativa da Partição 8

Programando um horário válido nesses campos (0000 até 2359), a partição correspondente à função irá desarmar nesse horário. Os dias da semana em que as partições serão desarmadas automaticamente devem ser programados na função [ 130 ].

## [ 130 ] Dias da Semana com Auto Desativa

| Padrão: Desabilitado todos os leds apagados | Dom | Seg | Ter | Qua | Qui | Sex | Sáb | Dia |
|---|---|---|---|---|---|---|---|---|
| [ 130 ] Dias da Semana com Auto Desativa | 1 | 2 | 3 | 4 | 5 | 6 | 7 | **Led\Bit** |

Determina quais dias da semana o auto desativa (funções **[ 206 a 209 e 358 a 361 ]**) irá funcionar. Os dias que não estiverem marcados de 1 a 7 não desativam.

## [ 139 a 146 ] Ativação por Inércia das Partições

**Padrão: 000 (Desabilitado)**
[ 139 ] [__/__/__] Tempo para Armar por Inércia da Partição 1 ou não particionado
[ 140 ] [__/__/__] Tempo para Armar por Inércia da Partição 2
[ 141 ] [__/__/__] Tempo para Armar por Inércia da Partição 3
[ 142 ] [__/__/__] Tempo para Armar por Inércia da Partição 4
[ 143 ] [__/__/__] Tempo para Armar por Inércia da Partição 5
[ 144 ] [__/__/__] Tempo para Armar por Inércia da Partição 6
[ 145 ] [__/__/__] Tempo para Armar por Inércia da Partição 7
[ 146 ] [__/__/__] Tempo para Armar por Inércia da Partição 8

Esse é o tempo (000 a 255), em minutos ou horas (conforme a opção 5 da função 204) para que a partição ative se não houver movimento nas zonas dessa partição. Programar 000 para desabilitar.

## [ 159 a 166 ] Horário em que as Partições Ativam por Inércia

[ 159 ] [ __/__/__/__ ] Início da ativação por Inércia da Partição 1 Padrão: FF:FF
[ 160 ] [ __/__/__/__ ] Início da ativação por Inércia da Partição 2 Padrão: FF:FF
[ 161 ] [ __/__/__/__ ] Início da ativação por Inércia da Partição 3 Padrão: FF:FF
[ 162 ] [ __/__/__/__ ] Início da ativação por Inércia da Partição 4 Padrão: FF:FF

[ 163 ] [ __/__/__/__ ] Fim da ativação por Inércia da Partição 1 Padrão: FF:FF
[ 164 ] [ __/__/__/__ ] Fim da ativação por Inércia da Partição 2 Padrão: FF:FF
[ 165 ] [ __/__/__/__ ] Fim da ativação por Inércia da Partição 3 Padrão: FF:FF
[ 166 ] [ __/__/__/__ ] Fim da ativação por Inércia da Partição 4 Padrão: FF:FF

As partições de 1 a 4 podem ser programadas para que o auto ativa por inércia funcione apenas em um determinado período do dia. As partições de 5 a 8 se forem programadas para auto ativar por inércia, funcionam 24 horas.
No horário de início, o tempo sem movimento começa a ser contado. No horário final, se o sistema estiver armado, permanece armado.

## [ 167 a 170 ] Dias da Semana em que as Partições Ativam por Inércia

| Padrão: Desabilitado todos os leds apagados | Dom | Seg | Ter | Qua | Qui | Sex | Sáb | | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 167 ] Dias da Semana da Partição 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| [ 168 ] Dias da Semana da Partição 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| [ 169 ] Dias da Semana da Partição 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| [ 170 ] Dias da Semana da Partição 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |

As partições de 1 a 4 com horário de ativação por inércia, podem ter dias da semana definidos para funcionar, sendo tecla 1 para domingo, 2 para segunda, 3 para terça até 7 para o sábado.
Os dias que não estiverem marcados nos leds de 1 a 7 poderão ter o auto ativa funcionando 24 horas ou desabilitado, dependendo da tecla/led 8. Sendo:
**Led 8 Aceso:** Nos demais dias opera 24horas.
**Led 8 Apagado:** Nos demais dias, desabilitado.

## [ 465 ] Falha no auto arme – Código Contact ID

**[ 465 ]** [ __/__/__/__ ] Padrão: 0000 (desabilitado)
Quatro dígitos com o código Contact ID do evento.

## [ 147 a 154 ] Horário em que as partições estão sempre armadas

As partições de 1 a 4 podem ser programadas para ficarem sempre armadas durante um determinado período do dia e durante determinados dias da semana. É possível desarmá-la momentaneamente, porém, passado o tempo programado a partição rearma, independente do estado das zonas, que caso esquecidas abertas irão gerar disparo.
Padrão: FF:FF
[ 147 ] [ __/__: __/__ ] Início do Horário Sempre Armado da Partição 1
[ 148 ] [ __/__: __/__ ] Início do Horário Sempre Armado da Partição 2
[ 149 ] [ __/__: __/__ ] Início do Horário Sempre Armado da Partição 3
[ 150 ] [ __/__: __/__ ] Início do Horário Sempre Armado da Partição 4

**No início do horário de funcionamento, se a partição estiver desarmada, ela será armada automaticamente. Nesse caso, o sistema mantém na memória que o sistema foi armado automaticamente e no fim do horário de funcionamento, a partição será desarmada automaticamente.**

[ 151 ] [ __/__: __/__ ] Fim do Horário Sempre Armado da Partição 1
[ 152 ] [ __/__: __/__ ] Fim do Horário Sempre Armado da Partição 2
[ 153 ] [ __/__: __/__ ] Fim do Horário Sempre Armado da Partição 3
[ 154 ] [ __/__: __/__ ] Fim do Horário Sempre Armado da Partição 4

**Após esse horário, a partição não será mais armada automaticamente.**

## [ 155 a 158 ] Dias da semana para as partições sempre armadas.

| Padrão: Desabilitado todos os leds apagados | Dom | Seg | Ter | Qua | Qui | Sex | Sáb | | Bit / Led |
|---|---|---|---|---|---|---|---|---|---|
| [ 155 ] Dias da Semana da Partição 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| [ 156 ] Dias da Semana da Partição 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| [ 157 ] Dias da Semana da Partição 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| [ 158 ] Dias da Semana da Partição 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |

Determina quais dias da semana a partição ficará sempre armada, sendo tecla 1 para domingo, 2 para segunda até 7 para o sábado. Os dias que não estiverem marcados nos leds de 1 a 7 poderão ter o auto arme funcionando por todo o dia ou desabilitado, dependendo da opção 8.
Sendo:
**Opção 8 Aceso:** Nos demais dias auto arme opera o dia todo.
**Opção 8 Apagado:** Nos demais dias desabilitado.

## [ 491 a 494 ] Tempo de rearme das partições sempre armadas.

Padrão: 000 minuto
[ 491 ] [ __/__/__ ] Tempo de Rearme da Partição 1
[ 492 ] [ __/__/__ ] Tempo de Rearme da Partição 2
[ 493 ] [ __/__/__ ] Tempo de Rearme da Partição 3
[ 494 ] [ __/__/__ ] Tempo de Rearme da Partição 4

Se o valor programado for zero, é impossível desarmar a partição durante o período de sempre armado. Caso contrário, a partição poderá ser desarmada e permanecerá desarmada pelo período programado em minutos nestas funções. Passado esse tempo a partição irá armar novamente, independente de haver movimento nas zonas ou zonas abertas. Caso alguma zona esteja violada no momento do auto arme, o sistema irá disparar.

## [ 205 ] Partições para Auto Ativa (auto ativa do teclado)

| Padrão: **Apagado (Desabilitado)** | Bit / Led / Part. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [ 205 ] Partições para Auto Ativa | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Define as partições que serão ativadas pelas funções de auto ativa dos teclados.

**Obs.: Não está disponível para os teclados 128 Plus LCD, 32 Light leds e 16 plus leds.**

## [ 363 ] Anular Auto Ativação com zona aberta – opção (bit) 4

| Padrão: Apagado (Desabilitado) | | Bit/Led |
|---|---|---|
| **[ 363 ]** | Se habilitado, o auto arme por inércia de qualquer partição não irá armar se alguma zona da central for disparar. Nesse caso o sistema reinicia a contagem de tempo e envia o evento programado na função [ 465 ], “Falha no auto arme” informando a partição que não armou. | 4 |

# SIRENES

## [ 210 e 211 ] Tempo de Sirene

[ 210 ] [ __/__: __/__ ] Tempo da Sirene 1 Padrão: 05:00 (mm:ss)
[ 211 ] [ __/__: __/__ ] Tempo da Sirene 2 Padrão: 00:00

Definir quanto tempo em minutos e segundos que a sirene permanecerá ativa após o disparo de um alarme. (00:00 sem sirene) o tempo pode variar de 00:01 a 99:99 minutos.

**OBS.:** A sirene 2 é uma sirene virtual. Pode ser utilizada como condição supervisionada na programação da agenda avançada para que o disparo de uma ou mais partições por ela ative alguma PGM ou execute algum comando do sistema.

## [ 213 e 214 ] Partições que Disparam a Sirene

| Padrão: **Todos Acesos (Habilitados)** | Bit / Led / Part. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [ 213 ] Partições que disparam a Sirene 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| [ 214 ] Partições que disparam a Sirene 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Pode-se particionar a sirene, fazendo com que ela dispare apenas se zonas de algumas partições dispararem.

Assim podemos ter partições que disparam uma sirene e partições que disparam outra.

**Lembre-se:** periféricos antigos como expansores ou zonas de teclados podem não ser compatíveis com o particionamento da sirene. Nesse caso a sirene 1 irá sempre tocar, independente da partição.

## [ 216] Bip de Sirene

| Padrão: **Todos Acesos (Habilitado)** | Bit / Led / Part. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **[ 216 ]** Partições com Bip na Sirene 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

**Um bip :** Sistema Armado
**Dois bips :** Sistema Desarmado

## [ 219 ] Supervisão de Sirene

| Padrão: **Todos Acesos (Habilitado)** | Bit / Led |
|---|---|
| **[219 ]** Supervisão | 1 |

Quando desabilitada, não envia mensagem de problema para a central de monitoramento, apenas no teclado da central será possível verificar quando a sirene está com problema.

A supervisão funciona sempre devido ao sistema de proteção contra curto-circuito da central. Deve-se colocar o resistor de 1K em paralelo com a sirene.

### [ 082 ] Problemas que disparam a sirene

Padrão: Todos (desabilitados)

| | Bit/Led | Descrição |
|---|---|---|
| [ 082 ] | 1 | Falha de bateria |
| | 2 | Falha de rede elétrica |
| | 3 | Falha de sirene |
| | 4 | Sobrecarga no barramento |
| | 5 | Falha de comunicação |
| | 6 | Falha de fiação/tamper |
| | 7 | Falha de periférico |

Se a partição 1 estiver armada no momento em que a falha selecionada ocorrer, as sirenes programadas para disparar a partição 1 irão disparar.

## Servidor DDNS e APP VIAWEB Mobile

### Programando *VIAWEB* Mobile por funções

- **Funções abaixo automaticamente programadas pela "Página Web" ou cadastrando o alarme pelo app "VIAWEB MOBILE" ou "VIAWEB STUDIO"**
- Para envio de eventos para o aplicativo, programa-se o valor "81" em uma das sequências de comunicação

Se preferir, em vez de programar o acesso ao VIAWEB direct pela página web, podemos programar por teclado ou por software de programação (VIAWEB Download).

### [ 571 ] Habilita cadastro automático VIAWEB Direct

Deve-se programar o valor 1 para habilitar o cadastro automático.

A partir do momento em que o modo é habilitado, o usuário tem até 4 minutos para efetuar o cadastro automático de um novo VIAWEB Mobile.

Quando um novo aplicativo é cadastrado, a função sai do modo de cadastro automaticamente.

### [ 570 ] VIAWEB Direct – Chave Criptográfica

[ 570 ] [ __/__/… /__ ] Padrão: FFFFFFFF… (VIAWEB direct desabilitado) (32 caracteres)

Caso o cadastro automático não esteja habilitado, ao abrir o APP (conectado no Wi-Fi da mesma rede da VW16Z 4G IP, um ícone cinza irá aparecer, ao clicar nesse ícone e uma chave criptográfica será gerada. Essa chave deverá ser programada nesta função.

Caso a VW16Z 4G IP já possua uma chave, ao ser cadastrado um novo dispositivo essa mesma chave deve ser inserida no app.

Estando programada corretamente o APP irá abrir e estará pronto para acessar a central.

### [ 580 ] Habilita Dynamic DNS

[ 580 ] [ __/__/__ ] Padrão: 000 Desabilitado.

Define-se qual serviço de DNS será utilizado para a central. A vantagem do serviço VIAWEB DNS é que nele podem ser feitas personalizações em eventos e o envio de notificação de offline.

OPÇÕES: 000 – Desabilitado; **001 – VIAWEB DDNS**; 002 – NO-IP.ORG

## [ 581 ] Endereço Externo (Hostname)

[ 581 ] [ __/__/ … /__ ] (30 caracteres) Padrão: n<<número de série >>.viawebservice.com.br

Domínio com até 30 caracteres especificando o endereço cadastrado no serviço de Dynamic DNS. De fábrica esta função vem com endereço próprio no VIAWEB DNS.
Exemplos: meumodulo.no-ip.org; meumodulo.noip.me.

**OBS.: Se usar o DDNS VIAWEB, não é necessário alterar essa função**

## [ 582 ] Usuário Dynamic DNS

[ 582 ] [ __/__/… /__ ] Padrão: Número de série do equipamento

Usuário ou e-mail cadastrado no serviço de Dynamic DNS (até 30 caracteres).

**OBS.: Se usar o DDNS VIAWEB, não é necessário alterar essa função**

## [ 583 ] Senha Dynamic DNS

[ 583 ] [ __/__/ … /__ ] Padrão: Ajustado de fábrica, único para cada equipamento.

Senha cadastrada no serviço de Dynamic DNS (até 30 caracteres).

**OBS.: Se usar o DDNS VIAWEB, não é necessário alterar essa função**

## [ 584 ] Resultado Dynamic DNS

[ 584 ] [ __/__/ … /__ ] (30 caracteres) Função apenas de leitura.

É possível verificar o resultado da atualização do serviço Dynamic DNS, lendo o valor desta função.

**Possíveis valores:**

| Valor apresentado na função: | Interpretação |
|---|---|
| good | Atualização do IP concluída com sucesso. |
| nochg | Revalidação do IP concluída, sem alteração. |
| DDNS desabilitado | Programado o valor 000 na função 580. |
| Timeout conexão | Não foi possível abrir conexão com o servidor. |
| Serviço inválido | Programado valor diferente de 000, 001, e 002 na função 580. |
| URL Inválida | Provedor do serviço não disponível (ex. no-ip fora do ar). |
| Timeout memória | Não foi possível ler os parâmetros da memória (endereço, usuário, senha). |
| Timeout envio de dados | Não foi possível enviar dados para atualização do IP. |
| nohost | Valor programado na função 581 está inválido. |
| badauth | Valor programado na função 582 ou 583 está inválido. |
| badagent | Falha geral na utilização do serviço (programar 000 na função 580 e entrar em contato com o suporte imediatamente). |
| !donator | Atualização indisponível – limitações no cadastro desta conta junto ao no-ip. |
| abuse | Muitas atualizações em um curto espaço de tempo, programar 000 na função 580, por no mínimo 1 hora antes de reativar o serviço. |
| 401 Unauthorized | Valor programado na função 582 ou 583 está inválido. |

Disponível para Smartphones iOS ou Android.

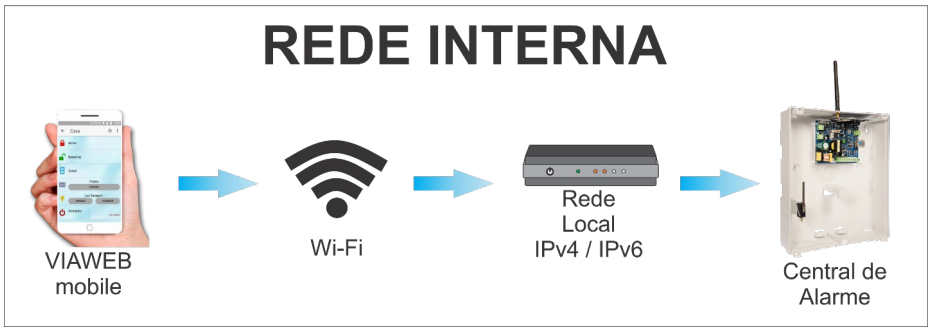
É possível controlar a central VW16Z 4G IP através do aplicativo VIAWEB Mobile. O controle pode ser feito onde você estiver, de qualquer lugar com acesso à Internet.

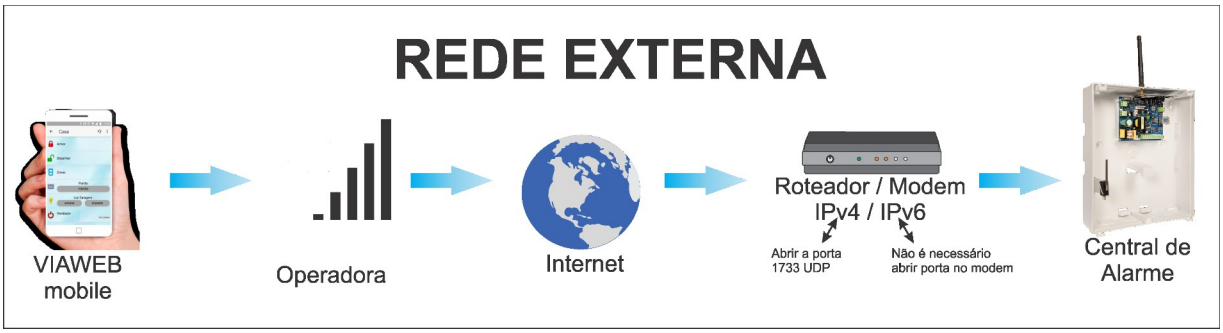
Baixe o aplicativo diretamente do Smartphone, através da loja de aplicativos correspondente.

O aplicativo VIAWEB Mobile permite utilizar tecnologias distintas para acessar e controlar o sistema, o “VIAWEB direct” e/ou “VIAWEB Cloud”.

## VIAWEB Direct

Essa tecnologia permite a conexão direta entre o sistema de alarme VIAWEB e o aplicativo móvel. O Smartphone comunica-se diretamente com e executa os comandos na Central VW16Z 4G IP.



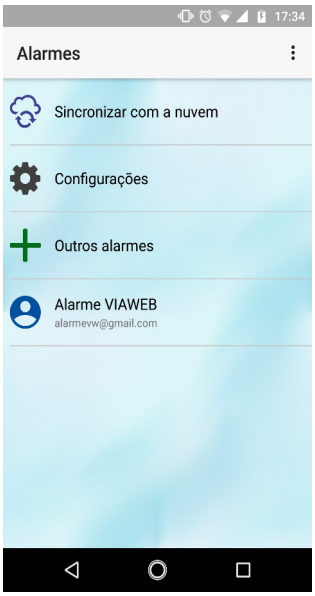
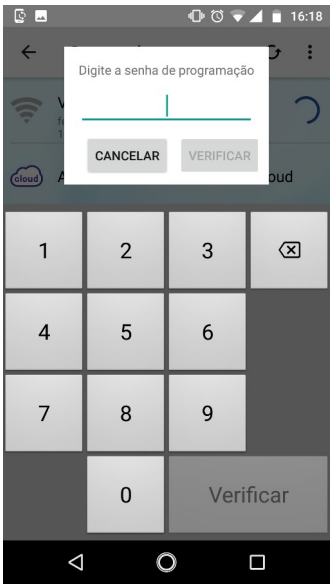




**Vantagens:**

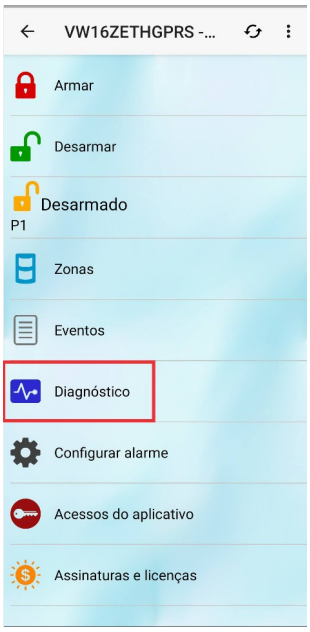
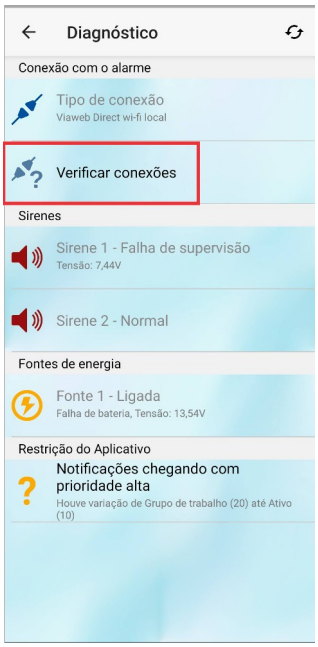
- Comunicação instantânea, rápida e direta.
- Protocolo criptografado AES CBC 128 bits, de alta segurança.
- Não depende de terceiros, servidores externos.

**Cadastro no Aplicativo:**

- No Smartphone, certifique-se que o aparelho está conectado na mesma rede que o módulo. Abra o APP e siga os passos:

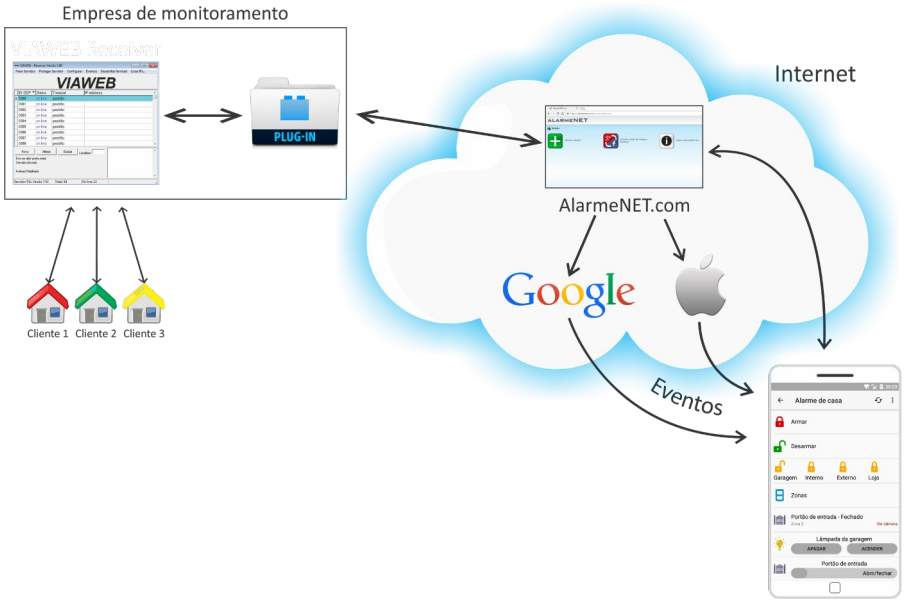
| 1° Entrar com o login social, Google ou Facebook | 2º Clicar em outros alarmes | 3º Clique no ícone cinza (sinal de wifi) | 4º Digite a senha de programação (5353 de fábrica) |
|---|---|---|---|
|  |  |  |  |

## VIAWEB CLOUD

| 1° Dentro da instalação, toque em “Diagnóstico” | 2° Depois toque em “Verificar Conexões” | 3° Toque em “Ajustar horário do alarme” e em seguida em “Ativar Viaweb Cloud” |
|---|---|---|
|  |  |  |

## ALARMENET.COM

Esta tecnologia utiliza a conexão da empresa de monitoramento para executar os comandos na central VIAWEB.

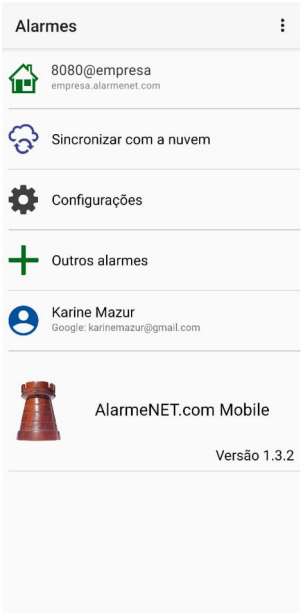



**Vantagens:**

- É possível armar e desarmar o sistema pela Página do servidor.
- Protocolo criptografado AES CBC 128 bits, de alta segurança.
- Permite acesso à qualquer painel ou módulo VIAWEB que esteja ONLINE na empresa.

**Cadastro no Aplicativo:**

- O usuário informa a empresa de monitoramento seu e-mail social (Google ou Facebook);
- A empresa cadastra este e-mail e a conta do cliente (ID ISEP) na página do AlarmeNET.com:

| | |
|---|---|
| O usuário faz o login no App AlarmeNET.com, usando a mesma conta que passou para a empresa | Pronto! O Alarme estará disponível na tela inicial. |
|  |  |

Para mais informações, consulte sua empresa de monitoramento.

# AVANÇADO

## [ 000 ] Versão do Firmware da Central

**[ 000 ]** [ _ _ _ _ ] Versão do firmware (função somente de leitura)

## [ 081 ] Opções de Envio de Testes e de Bateria

Padrão: Todos desabilitados

| | Bit/Led | Descrição | Selecionado | Apagado |
|---|---|---|---|---|
| [ 081 ] | 3 | Testes somente com central armada | Habilitado | **Desabilitado** |
| | 4 | Envio de Testes | Testes pela Internet | **Desabilitado** |
| | 8 | Desabilita teste de bateria | **Não executa teste de bateria** | Executa teste de bateria |

**Testes somente com central armada:** Se habilitado o envio do teste automático por ETH ou 4G (código Contact ID programado na função [438]) será feito apenas se uma ou mais partições estiverem armadas, caso contrário, o teste sempre será enviado.

**Envio de Testes:** Nesta função é definido se a central irá enviar teste de automático (código Contact ID programado na função [438]) pela internet. Nos itens 5, 6 e 7 define-se quais sequências de comunicação enviarão teste de linha.

**Não executa teste de bateria:** Se essa opção estiver ativa o equipamento não executa mais teste de bateria, ou seja, não reduz mais a tensão da fonte periodicamente para testar a presença ou não de uma bateria carregada. Habilitar essa opção caso o sistema não possua bateria de backup.

## [ 355 e 357 ] Permissão de Acesso Remoto

Restringe o acesso remoto à central, sendo:

**[ 355 ]** Permissão de acesso remoto por VIAWEB DOWNLOAD, SMS ou servidor VIAWEB
**[ 357 ]** Permissão de acesso remoto pela Página WEB ou VIAWEB DIRECT
Padrão: Todos (Habilitados)

| | Bit/Led | Níveis | Descrição |
|---|---|---|---|
| [ 355 ]<br>[ 357 ] | 1 | Monitoramento, PGM, Status | Se apagado, não é possível visualizar o status. |
| | 2 | Armar e Desarmar (Inibir) | Se apagado, não é possível armar, desarmar ou inibir zonas. |
| | 3 | Programar e Ler programação | Se apagado, não é possível alterar ou ler a programação. |
| | 4 | Ler Eventos | Se apagado, não é possível ler os eventos. |
| | 5 | Cadastrar e Ler Senhas | Se apagado, não é possível cadastrar ou ler senhas. |

*Disponível apenas na função [ 355 ]

## [ 520 ] Permissão de Acesso à Navegação WEB

**[ 520 ]** [ _ ] Padrão: 0

A Central VW16Z 4G IP permite controle e configuração a partir de qualquer navegador WEB. O acesso às páginas é feito a partir de autenticação básica HTML, sem criptografia. Esta autenticação é segura o suficiente para a maioria das aplicações em redes **domésticas**. Porém, nos casos em que a rede é pública, não confiável ou deseja-se um nível maior de monitoramento, pode-se desabilitar ou restringir o acesso ao navegador WEB.

| | |
|---|---|
| 0 | Permissão total de acesso, não há restrição para acesso ao navegador WEB. |
| 1 | Somente controle. Nesse caso, pode-se acessar a tela de controle, mas não é possível alterar as configurações. |
| 2 | Acesso restrito com chave. Nesse modo, o acesso fica totalmente bloqueado. Para liberar o acesso deve-se pressionar os dois botões (SINAL e RECON) na placa VW16Z 4G IP de 3 a 5 segundos. O acesso é liberado por 30 minutos ou até os botões serem pressionados novamente. |
| 3 | Acesso bloqueado. Não é possível acessar as páginas WEB da VW16Z 4G IP. |
| 4 | Acesso à página WEB fora da rede interna (inseguro) |

## [ 366 ] Teclas Especiais 1 e 2

[ 366 ] [ __/__ ] Padrão: 00 (Desabilitado).
**Obs.: Não está disponível para os teclados 128 plus, 32 light e 16 plus leds.**

| Função | Característica |
|---|---|
| 0 | Desabilitado |
| 1 | Emergência silenciosa |
| 2 | Alarme de furto |
| 3 | Incêndio |
| 4 | Emergência médica |
| 5 | Ativar PGM 1 |
| 6 | Desativar PGM 1 |
| 7 | Ativar PGM 2 |
| 8 | Desativar PGM 2 |
| 9 | Auto ativar partições da função [205] |

Esta função é programada através de dois dígitos. O primeiro dígito para a tecla especial 1 (ESP + 1) e o segundo para a tecla especial 2 (ESP + 2).

**Exemplo:**
Para enviar emergência silenciosa pela tecla especial 1 e auto armar pela especial 2 nessa função programe “19”.

## [ 039 ] Estado da comunicação

Informa o estado da conexão de rede e dos 3 servidores VIAWEB, para ser lido através do VIAWEB Studio.

## [ 365 ] Retardo de falha de AC

**[ 365 ] [ __/__/__ ]** Padrão: 000 minuto

Se programado o valor 000 o evento será enviado imediatamente, caso contrário o evento somente será enviado logo após o tempo programado. Há uma variação de aproximadamente 1 minuto evitando a transmissão simultânea de várias centrais em uma mesma localidade que ficou sem energia elétrica, o valor pode variar de 000 a 255.

## [ 363 ] Programação de Senhas Aleatórias – opção (bit) 3

| Padrão: Apagado (Desabilitado) | | Bit/Led |
|---|---|---|
| [ 363 ] | Modo de operação com senhas aleatórias. Se habilitado, as senhas de usuário 3, 4 e 5 são geradas aleatoriamente e trocadas automaticamente quando utilizadas. Ao desabilitar esse modo, as senhas de usuário 3, 4 e 5 são apagadas. Mais detalhes desse modo de operação são descritos abaixo. | 3 |

**Modo de operação com senhas aleatórias:**

Em determinadas soluções de segurança, algumas vezes é necessário que empresas ou pessoas que prestam serviços terceirizados, tenham acesso ao local protegido. Por exemplo, serviços de limpeza e conservação, manutenção periódica, reabastecimento de caixas e suporte. Nesses casos, pessoas alheias à área protegida precisam desarmar o sistema e passam a ter conhecimento de uma ou mais senhas de acesso.

Isso normalmente gera a insegurança de que uma ou mais pessoas desconhecidas retenham senhas e possam desarmar o alarme em momentos indesejados. A solução comum para esse problema é o desarme remoto do alarme pela empresa de monitoramento ou o acesso via Download e troca manual da senha utilizada. Essas soluções requerem intervenção manual do operador e estão sujeitas a falhas humanas.

Com esse modo de operação, o sistema passa a ter 3 senhas que somente são conhecidas pelo painel de alarme e pela empresa de monitoramento. Toda vez que uma das senhas é digitada, ela é trocada por outra, gerada aleatoriamente.

As senhas aleatórias são dos usuários 003, 004 e 005. No momento em que a opção 3 da função 363 é habilitada, essas 3 senhas são geradas aleatoriamente. Quando esta opção é desabilitada, essas senhas são apagadas automaticamente.

Para que o monitoramento receba a informação da nova senha, um evento em Contact ID com formato especial é enviado ao monitoramento. Os eventos em Contact ID possuem o seguinte formato: CCCC QEEE PP ZZZ, onde CCCC é a conta do cliente, Q o qualifier do evento, EEE o código do evento, PP a partição e ZZZ a zona correspondente do evento.

Ao gerar uma nova senha aleatória, o evento será enviado no formato abaixo:

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.

Onde [D1][D2][D3][D4][D5][D6] são os 6 dígitos da nova senha. Caso a senha possua menos de 6 dígitos, os últimos devem ser ignorados.

Como não existem eventos em contact ID cujo qualifier (Q) seja diferente de 1 ou 3, então no monitoramento é possível saber qual é o evento contendo a nova senha observando o valor do qualifier. 2 para a senha do usuário 003, 4 para a senha do usuário 004 e 6 para a senha do usuário 005.

Portanto, para que o monitoramento saiba qual é a senha atual, basta ver quais foram os últimos eventos contact ID recebidos com qualifier 2, 4 ou 6.

## [ 363 ] Salva a lista de periféricos ligados ao Innovabus – opção (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 |

## Lacre da programação (somente para empresas de monitoramento)

Em instalações de alta segurança, uma vez que o sistema tenha sido configurado, programado e seu funcionamento garantido, pode-se desejar evitar que se faça qualquer tipo de alteração nele. Com a função de lacre, pode-se garantir que a programação não foi alterada, mesmo por alguém com conhecimento das senhas de programação e download ou acesso ao servidor VIAWEB.

Para aumentar a segurança e evitar programações indesejadas, o lacre só pode ser alterado através do software de programação VIAWEB download.

Uma vez lacrado, o acesso do software de programação VIAWEB download fica restrito à conexão VIAWEB. Logo somente deve-se lacrar a central após ela ter sido programada e encontrar-se ONLINE com o VIAWEB Receiver. Caso contrário, existe a possibilidade de não mais ser possível entrar em programação.

Todos os periféricos compatíveis com esta nova tecnologia de lacre irão lacrar-se também da mesma forma que a central. Os periféricos sem suporte a lacre não sofrerão alterações no funcionamento.

Atenção: Uma vez ativado o lacre (programado com os valores 1, 5 ou 9), só será possível desabilitar o lacre definitivamente fazendo um reset na programação da central. Caso a central esteja com trava de reset, deve-se liberar o lacre (programando a função 019 com 1) e depois destravar o reset. Note que se o equipamento não estiver online, e for lacrado com a trava de reset, não será mais possível acessar sua programação, nem resetá-lo, e este deverá ser encaminhado para manutenção.

## [ 019 ] Lacre de Programação

| **Padrão 0 desabilitado** | | **Tecla Led** |
|---|---|---|
| [ 019 ] | Valor padrão de fábrica, o **lacre está desativado** e a programação da central pode ser alterada normalmente. | 0 |
| | **Abertura de lacre:** Programar 1 fará com que o evento de “Programação irá liberar” (função 471) seja enviado. Caso nenhuma programação seja feita nessa função, após 4 (quatro) minutos o lacre será liberado, e será possível alterar a configuração da central normalmente. Após 30 minutos o lacre volta automaticamente para o valor 5. | 1 |
| | **Lacra** a programação apenas da fonte **Power Bank**. | 2 |
| | **Lacre total:** Programar esse valor fará com que o evento de “Programação Lacrada” (função 472) seja enviado. Quando o lacre nesse nível estiver ativado:<br>**a)** Não aceita a senha de programação.<br>**b)** Bloqueia acesso ao download via cabo serial.<br>**c)** Somente aceita liberação do lacre se esta for feita através do VIAWEB Receiver (VIAWEB download conectado por servidor VIAWEB).<br>**d)** Não é possível cancelar a discagem ou limpar o Buffer de comunicação. | 5 |
| | **Lacre parcial:** Tem o mesmo efeito do lacre total, com exceção de que ainda é possível alterar a programação através do VIAWEB download. Para garantir a eficiência do lacre não se deve deixar o lacre parcial programado indefinidamente. Assim que possível deve-se lacrar totalmente a central gravando 5 na função 019. Pode-se alterar o lacre de 5 (total) para 9 (parcial), mas deve-se aguardar 4 minutos antes que o lacre seja efetivamente liberado. | 9 |

## [ 471 ] Programação irá liberar após 4 minutos – Código Contact ID

[ 471 ] [ ____ ]  Padrão: 3407 (no campo zona é enviado o nível do lacre que irá assumir)

Quatro dígitos com o código Contact ID do evento. Programar 0000 para desabilitar o envio desse evento.

## [ 472 ] Programação lacrada – Código Contact ID

[ 472 ] [ ____ ]  Padrão: 3408 (no campo zona é enviado o nível do lacre)

Quatro dígitos com o código Contact ID do evento. Programar 0000 para desabilitar o envio desse evento.

## [ 364 ] Interface de Integração (Rádio Monitoramento) - opções 7 e 8

A Central de modelo VW16Z IP possui uma interface universal para integração com equipamentos ou softwares de outros fabricantes, via HTTP ou cabo serial. Essa integração permite, entre outras coisas, comunicação direta com módulos de rádio de outros fabricantes.

**Para mais informações entre em contato com o fabricante do equipamento (Rádio) ou software integrado**. Se não utilizar um equipamento, software ou módulo de rádio de outro fabricante, manter essas opções desabilitadas.

| Padrão: Apagado (Desabilitado) | | Bit/Led |
|---|---|---|
| **[364]** | Habilitar ou não conforme instruções do integrador | 7 |
| | Habilitar ou não conforme instruções do integrador | 8 |

Equipamentos que possuem este recurso:

- Central VW16Z IP versão 6.71 ou superior
- Central VW8Z IP versão 2.71 ou superior
- Módulo IP Mini / IP Mini 100 Mbps versão 4.71 ou superior
- Central de Automação VW-DIN versão 2.71 ou superior
- Central VW8Z IP RF versão 2.71 ou superior

* Para os demais modelos de central, é possível fazer a integração com o rádio instalando um Módulo IP Mini.

## [ 077 ] Atalho de Programação

[ 077 ] [ 000 ] Padrão: 000
Com a função 077 é possível programar com apenas um valor funcionalidades usuais do sistema.
Disponível para as centrais e versões a seguir:

| MODELO | VERSÃO |
|---|---|
| VW16Z 4G | 7.30 |
| VW16Z 4G IP | 7.30 |
| VW16Z IP (com fonte em placa separada) | 7.30 |
| VW DIN | 3.30 |
| VW8Z IP RF | 3.30 |

Atalhos disponíveis:
077 = 001 Programa PGM 1 para acionar com qualquer partição armada.
077 = 002 Programa PGM 2 para acionar com qualquer partição armada.
077 = 005 Programa PGM 1 para acionar por 3 segundos quando uma senha correta é digitada.
077 = 006 Programa PGM 2 para acionar por 3 segundos quando uma senha correta é digitada.
077 = 010 Programa PGM 1 para ativar das 19h às 06h.
077 = 011 Programa PGM 2 para ativar das 19h às 06h.
077 = 015 Programa PGM 1 para acionar por 3 segundos quando arma ou desarma a partição 1.
077 = 016 Programa PGM 2 para acionar por 3 segundos quando arma ou desarma a partição 1.
077 = 020 Programa PGM 1 para funcionar como sirene 2.
077 = 101 Programa sequência 1 para conectar com a nuvem VIAWEB via IP.
077 = 102 Programa sequência 2 para conectar com a nuvem VIAWEB via IP (mais usado).
077 = 103 Programa sequência 3 para conectar com a nuvem VIAWEB via IP.
077 = 104 Programa sequência 1 para conectar com a nuvem VIAWEB via IP com backup 4G.
077 = 105 Programa sequência 2 para conectar com a nuvem VIAWEB via IP com backup 4G (mais usado).
077 = 106 Programa sequência 3 para conectar com a nuvem VIAWEB via IP com backup 4G.
077 = 107 Programa sequência 1 para conectar com a nuvem VIAWEB via 4G.
077 = 108 Programa sequência 2 para conectar com a nuvem VIAWEB via 4G (mais usado).
077 = 109 Programa sequência 3 para conectar com a nuvem VIAWEB via 4G.
077 = 200 Programa funções gerais de uma solução para portaria de condomínio (ver detalhes no Guia Online).
As orientações detalhadas para uso da função 077 são apresentadas no Guia Online. **Clique aqui** para acessar no Guia o conteúdo sobre Atalhos de programação.
**Importante: Sempre que programar um atalho aguarde 2 minutos antes de acessar novamente a programação. Este tempo é necessário para que a central execute todos os passos da programação.**

# AGENDAS

O equipamento possui 34 agendas distintas. Cada agenda permite executar ações conforme o horário, data e situação atual do sistema. Elas permitem controlar PGMs, armar e desarmar o sistema ou enviar eventos.

Não é mais necessário ajustar o relógio se a agenda não tiver restrição de horário ou dias.

Para configurar uma agenda é necessário programar:

## AÇÃO QUE A AGENDA IRÁ EXECUTAR

Cada agenda possui duas funções para configurar a ação que será executada. Uma para determinar o tipo da ação e outra para determinar o complemento. Sendo:

**0 – Agenda desabilitada**

Essa agenda não está sendo usada. Não é necessário programar nada no complemento.

**1 – Armar e Desarmar**

A ação inicial é armar o sistema. A ação final é desarmar o sistema. No complemento devemos programar qual usuário (0001 a 0064) irá armar e desarmar.

As partições que serão armadas ou desarmadas são as partições que o usuário tem acesso. Se o usuário estiver configurado para permitir arme forçado, no momento do agendamento ele irá armar o sistema no modo forçado. Caso existam zonas da central abertas no momento de armar, o sistema não irá armar se não for configurado o arme forçado do usuário. Somente são válidos usuários 0001 a 0064, referente aos usuários do equipamento e não do sistema.

**2 – Ativar PGM**

A ação inicial é ativar a PGM. A ação final é desativar a PGM. No complemento devemos programar qual PGM será controlada (0001 a 0255).

Quando executada com tempo de PGM, permite recarregar o tempo, acionando a PGM novamente, se necessário, sem ter que aguardar desativar a PGM para um novo comando.

**3 – Enviar Evento**

A ação inicial será enviar um evento, não há ação final. No complemento devemos programar o código Contact ID do evento a ser enviado. Valores possíveis são 1000 a FFFF.

O campo usuário ou zona do evento será preenchido conforme as condições supervisionadas que acionaram a agenda, sendo:

- O usuário da senha digitada;
- A zona aberta supervisionada;
- A zona disparada supervisionada.

Caso a ação tenha sido disparada por duas condições e as duas possuam zona ou usuário, vale a informação da primeira condição.

**4 – Inverter PGM**

A ação inicial é inverter a PGM. A ação final é desinverter a PGM. No complemento devemos programar qual PGM será controlada (0001 a 0255).

**5 – Desativar PGM**

A ação inicial é desativar a PGM. A ação final é nada. No complemento devemos programar qual PGM será controlada (0001 a 0255).

**OBS.: Para que a agenda funcione corretamente, o relógio interno da central tem que estar ajustado.**

## [ 830 A 863 ] AÇÕES A EXECUTAR

[ _ ] Padrão: 0 Desabilitado

## [ 864 a 897 ] Complemento da agenda

[ _ _ _ _ ] Padrão: 0000

## Em que momento a agenda executa a ação inicial?

Deve-se programar o horário de início e horário de fim da agenda e os dias da semana em que a agenda é válida. Pode-se configurar também se a agenda irá ser válida durante os feriados. É necessário configurar quais condições serão supervisionadas no sistema (partições armadas, problemas, zonas, etc…) e configurar que combinação de condições cada agenda seguirá. Durante o período de validade da agenda, se a "combinação das condições" for verdadeira a ação inicial é executada imediatamente. Caso as condições não sejam válidas, a ação não é executada.

## [ 898 a 931 ] Horário de início da agenda

[ _ _ _ _ ] Padrão: 0000
Programa-se em horas e minutos (HH:MM)

## [ 932 a 965 ] Horário final da agenda

[ _ _ _ _ ] Padrão: 2359
Programa-se em horas e minutos (HH:MM). A hora programada de fim é incluída no período da agenda.

## [ 966 a 999 ] Dias da semana da agenda

| Padrão: todos habilitados | Dom | Seg | Ter | Qua | Qui | Sex | Sáb | Fer |
|---|---|---|---|---|---|---|---|---|
| **[ 966 a 999 ]** Dias da semana da agenda | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Opções de 1 a 8, sendo 1 para domingo, 2 para segunda, 3 para terça, 4 para quarta, 5 para quinta, 6 para sexta, 7 para sábado e 8 para feriados (funções 521 a 535).

## Em que momento a agenda executa a ação final?

Isso dependerá do tempo programado na duração da ação.

Se for programado o tempo, ao final deste tempo a ação final é executada (usuário desarma, envia evento ou desativa a PGM).

Se o tempo programado for 0000 então a ação final será executada assim que a "combinação das condições" não for mais verdadeira ou a agenda não estiver mais dentro do período de validade (horário e dias da semana).

Se o tempo programado for FFFF então a ação final nunca será executada.

## [ 665 a 698 ] Duração da ação

[ _ _ _ _ ] Padrão: 0000
Programa-se em minutos e segundos (MM:SS). Para duração infinita deve-se programar FFFF.

## Combinação das condições

Pode-se combinar duas condições supervisionadas no sistema para executar a ação de uma agenda. Existem 15 condições configuráveis, identificadas de 1 – 9 e A – F. Programar 0 indica que não irá verificar a condição.

## [ 286 a 319 ] Combinação das condições

[ _ _ ] Padrão: 00
Programar a primeira condição (0 a F) e a segunda condição (0 a F). Para não verificar nenhuma condição ao executar a ação, deve-se programar 00.

## Funções das agendas

| Agenda | Ações a executar | Complemento da ação (usuário, PGM evento) | Horário de início hh:mm | Horário de fim hh:mm | Duração da ação mm:ss | Dias da semana (dom a sáb + feriados) | Combinação das condições |
|---|---|---|---|---|---|---|---|
| 1 | 830 | 864 | 898 | 932 | 665 | 966 | 286 |
| 2 | 831 | 865 | 899 | 933 | 666 | 967 | 287 |
| 3 | 832 | 866 | 900 | 934 | 667 | 968 | 288 |
| 4 | 833 | 867 | 901 | 935 | 668 | 969 | 289 |
| 5 | 834 | 868 | 902 | 936 | 669 | 970 | 290 |
| 6 | 835 | 869 | 903 | 937 | 670 | 971 | 291 |
| 7 | 836 | 870 | 904 | 938 | 671 | 972 | 292 |
| 8 | 837 | 871 | 905 | 939 | 672 | 973 | 293 |
| 9 | 838 | 872 | 906 | 940 | 673 | 974 | 294 |
| 10 | 839 | 873 | 907 | 941 | 674 | 975 | 295 |
| 11 | 840 | 874 | 908 | 942 | 675 | 976 | 296 |
| 12 | 841 | 875 | 909 | 943 | 676 | 977 | 297 |
| 13 | 842 | 876 | 910 | 944 | 677 | 978 | 298 |
| 14 | 843 | 877 | 911 | 945 | 678 | 979 | 299 |
| 15 | 844 | 878 | 912 | 946 | 679 | 980 | 300 |
| 16 | 845 | 879 | 913 | 947 | 680 | 981 | 301 |
| 17 | 846 | 880 | 914 | 948 | 681 | 982 | 302 |
| 18 | 847 | 881 | 915 | 949 | 682 | 983 | 303 |
| 19 | 848 | 882 | 916 | 950 | 683 | 984 | 304 |
| 20 | 849 | 883 | 917 | 951 | 684 | 985 | 305 |
| 21 | 850 | 884 | 918 | 952 | 685 | 986 | 306 |
| 22 | 851 | 885 | 919 | 953 | 686 | 987 | 307 |
| 23 | 852 | 886 | 920 | 954 | 687 | 988 | 308 |
| 24 | 853 | 887 | 921 | 955 | 688 | 989 | 309 |
| 25 | 854 | 888 | 922 | 956 | 689 | 990 | 310 |
| 26 | 855 | 889 | 923 | 957 | 690 | 991 | 311 |
| 27 | 856 | 890 | 924 | 958 | 691 | 992 | 312 |
| 28 | 857 | 891 | 925 | 959 | 692 | 993 | 313 |
| 29 | 858 | 892 | 926 | 960 | 693 | 994 | 314 |
| 30 | 859 | 893 | 927 | 961 | 694 | 995 | 315 |
| 31 | 860 | 894 | 928 | 962 | 695 | 996 | 316 |
| 32 | 861 | 895 | 929 | 963 | 696 | 997 | 317 |
| 33 | 862 | 896 | 930 | 964 | 697 | 998 | 318 |
| 34 | 863 | 897 | 931 | 965 | 698 | 999 | 319 |

## Condições Supervisionadas

Existem 15 condições programáveis que as agendas podem supervisionar. Para cada condição há uma função de programação conforme a tabela abaixo:

| Condição | Função | Condição | Função |
|---|---|---|---|
| 1 | 384 | 9 | 392 |
| 2 | 385 | A | 393 |
| 3 | 386 | B | 394 |
| 4 | 387 | C | 395 |
| 5 | 388 | D | 396 |
| 6 | 389 | E | 397 |
| 7 | 390 | F | 398 |
| 8 | 391 | | |

## [ 384 a 398 ] Condição supervisionada

[ _ _ _ _ _ _ _ ] Padrão: 000000

Para configurar uma condição a ser supervisionada pelas agendas deve-se preenchar a função conforme a tabela abaixo:

| Valor a programar nas funções | | |
|---|---|---|
| **Condição supervisionada** | **Valor** | **Observação** |
| Falha de comunicação do meio | 0200CC | Substitua “CC” pelo meio de comunicação desejado. Exemplo: para monitorar falha no servidor IP 1: “020051” |
| Comunicação do meio OK | 8200CC | |
| Senha digitada / Controle acionado (somente os usuários do periférico). ***Condição instantânea** | 030UUU | Substitua o “UUU” pelo usuário. Para qualquer usuário programe 000. Ex: para monitorar o acionamento do controle 32 = “030032” |
| Memória de disparo (lembra que houve um disparo até que se desarme e arme o sistema novamente) | 0400PA | Substitua “P” e “A” conforme o quadro de partições. Ex: Memória de disparo de todas as partições = 0400FF |
| Sem memória de disparo (lembra que houve um disparo até que se desarme e arme o sistema novamente). | 8400PA | |
| Todas essas partições armadas | 1000PA | Substitua “P” e “A” conforme o quadro de partições. Ex: Monitora o estado da partição 1 apenas = 100001 |
| Todas essas partições desarmadas | 9000PA | |
| Alguma dessas partições armadas | 1100PA | Substitua “P” e “A” conforme o quadro de partições. Ex: Monitora o estado da partição 1 apenas = 110001 |
| Alguma dessas partições desarmadas | 9100PA | |
| Zona aberta | 120ZZZ | Substitua “ZZZ” pela zona do sistema |
| Zona fechada | 920ZZZ | |
| Zona disparada | 130ZZZ | |
| Zona não disparada | 930ZZZ | |
| Movimento na zona ***Condição instantânea** | 121ZZZ | |

| | | |
|---|---|---|
| Uma ou mais zonas destas partições abriram<br>***Condição instantânea** | 1400PA | Substitua “P” e “A” conforme o quadro de partições.<br>Ex: Monitora o estado da partição 8 apenas = 100080 |
| Sirene disparada | 15000S | Substitua “S” pelo número da sirene. (Somente centrais possuem sirene 2). Ex: para monitorar a sirene = 150001 |
| Sirene em repouso | 95000S | |
| Partições disparadas | 1600PA | Substitua “P” e “A” conforme o quadro das partições.<br>Ex: Monitora o estado da partição 4 apenas = 100008 |
| Partições em repouso | 9600PA | |
| Partições temporizando | 1800PA | Substitua “P” e “A” conforme o quadro das partições.<br>Ex: Monitora o estado da partição 4 e 5 apenas = 100018 |
| PGM acionada | 200PGM | Substitua “PGM” pela PGM monitorada. São aceitos valores de 000 a 255.<br>Ex: Monitora o estado da PGM 5 = 200005 |
| PGM desacionada | A00PGM | |
| Evento enviado<br>***Condição instantânea** | 21QEEE | Substitua “QEEE” pelo código contact ID do evento.<br>Ex: Monitorar o evento de teste manual = 211601 |
| Comando de cancelar comunicação recebido<br>***Condição instantânea** | 270000 | Ao executar a sequência para cancelar a discagem no teclado ou enviar o comando “Limpar Buffer” via download. |
| Problemas no sistema | 2800PR | Substitua “P” e “R” conforme o quadro de problemas.<br>Ex: Monitorar problema de comunicação = 280010 |
| Sem problemas no sistema | A800PR | |
| Chave pressionada | 06000X | Substitua “X” por “1”para chave RECON pressionada |
| Chave não pressionada | 86000X | Substitua “X” por “1” para chave RECON não pressionada |

***Condição instantânea**: São válidas somente no exato momento que ocorrem. Logo combinar duas condições instantâneas na mesma agenda fará com que essa agenda nunca consiga executar sua ação inicial, uma vez que é improvável que as duas condições ocorram exatamente ao mesmo tempo. Da mesma forma, se houver uma ação final a ser executada assim que as condições não forem mais válidas, ela será executada imediatamente após a ação inicial.

| **Quadro de Partições** | | | | |
|---|---|---|---|---|
| **Partições a Incluir** | **Valor de P** | | **Partições a Incluir** | **Valor de A** |
| Nenhuma partição 5 a 8 | 0 | | Nenhuma partição 1 a 4 | 0 |
| Apenas partição 5 | 1 | | Apenas partição 1 | 1 |
| Apenas partição 6 | 2 | | Apenas partição 2 | 2 |
| Partição 5 e 6 | 3 | | Partição 1 e 2 | 3 |
| Apenas partição 7 | 4 | | Apenas partição 3 | 4 |
| Partição 5 e 7 | 5 | | Partição 1 e 3 | 5 |
| Partição 6 e 7 | 6 | | Partição 2 e 3 | 6 |
| Partição 5, 6 e 7 | 7 | | Partição 1, 2 e 3 | 7 |
| Apenas partição 8 | 8 | | Apenas partição 4 | 8 |
| Partição 5 e 8 | 9 | | Partição 1 e 4 | 9 |
| Partição 6 e 8 | A | | Partição 2 e 4 | A |
| Partição 5,6 e 8 | B | | Partição 1,2 e 4 | B |
| Partição 7 e 8 | C | | Partição 3 e 4 | C |
| Partição 5, 7 e 8 | D | | Partição 1, 3 e 4 | D |
| Partição 6, 7 e 8 | E | | Partição 2, 3 e 4 | E |
| Partição 5, 6, 7 e 8 | F | | Partição 1, 2, 3 e 4 | F |

| Quadro de Problemas | | | | |
|---|---|---|---|---|
| **Problemas a Incluir** | **Valor de P** | | **Problemas a Incluir** | **Valor de R** |
| Nenhuma Problema 5 a 8 | 0 | | Nenhuma Problema 1 a 4 | 0 |
| Apenas Problema 5 | 1 | | Apenas Problema 1 | 1 |
| Apenas Problema 6 | 2 | | Apenas Problema 2 | 2 |
| Problema 5 e 6 | 3 | | Problema 1 e 2 | 3 |
| Apenas Problema 7 | 4 | | Apenas Problema 3 | 4 |
| Problema 5 e 7 | 5 | | Problema 1 e 3 | 5 |
| Problema 6 e 7 | 6 | | Problema 2 e 3 | 6 |
| Problema 5, 6 e 7 | 7 | | Problema 1, 2 e 3 | 7 |
| Apenas Problema 8 | 8 | | Apenas Problema 4 | 8 |
| Problema 5 e 8 | 9 | | Problema 1 e 4 | 9 |
| Problema 6 e 8 | A | | Problema 2 e 4 | A |
| Problema 5,6 e 8 | B | | Problema 1,2 e 4 | B |
| Problema 7 e 8 | C | | Problema 3 e 4 | C |
| Problema 5, 7 e 8 | D | | Problema 1, 3 e 4 | D |
| Problema 6, 7 e 8 | E | | Problema 2, 3 e 4 | E |
| Problema 5, 6, 7 e 8 | F | | Problema 1, 2, 3 e 4 | F |

| Problema | Descrição |
|---|---|
| 1 | Falha de bateria |
| 2 | Falha de rede elétrica |
| 3 | Falha de sirene |
| 4 | Sobrecarga no barramento |
| 5 | Falha de comunicação |
| 6 | Falha de fiação/tamper |
| 7 | Falha de periférico |
| 8 | Falha de linha telefônica |

| Quadro de Grupos | | | | |
|---|---|---|---|---|
| **Grupos a Incluir** | **Valor de G** | | **Grupos a Incluir** | **Valor de R** |
| Nenhuma Grupo 5 a 8 | 0 | | Nenhuma Grupo 1 a 4 | 0 |
| Apenas Grupo 5 | 1 | | Apenas Grupo 1 | 1 |
| Apenas Grupo 6 | 2 | | Apenas Grupo 2 | 2 |
| Grupo 5 e 6 | 3 | | Grupo 1 e 2 | 3 |
| Apenas Grupo 7 | 4 | | Apenas Grupo 3 | 4 |
| Grupo 5 e 7 | 5 | | Grupo 1 e 3 | 5 |
| Grupo 6 e 7 | 6 | | Grupo 2 e 3 | 6 |
| Grupo 5, 6 e 7 | 7 | | Grupo 1, 2 e 3 | 7 |
| Apenas Grupo 8 | 8 | | Apenas Grupo 4 | 8 |
| Grupo 5 e 8 | 9 | | Grupo 1 e 4 | 9 |
| Grupo 6 e 8 | A | | Grupo 2 e 4 | A |
| Grupo 5,6 e 8 | B | | Grupo 1,2 e 4 | B |
| Grupo 7 e 8 | C | | Grupo 3 e 4 | C |
| Grupo 5, 7 e 8 | D | | Grupo 1, 3 e 4 | D |
| Grupo 6, 7 e 8 | E | | Grupo 2, 3 e 4 | E |
| Grupo 5, 6, 7 e 8 | F | | Grupo 1, 2, 3 e 4 | F |

## [ 521 a 535 ] Calendário de Feriados

Nessas funções são definidos 15 feriados anuais com dia e mês. Nos dias de feriado funções de Auto Ativa, Auto Desativa e Agenda se comportam como Domingo.

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

## [ 363 ] Diversos

| Padrão: Todos Apagados (Desabilitados) | | Bit/Led |
|---|---|---|
| [ 363 ] | Se habilitado, periodicamente ajusta o relógio interno com o horário recebido do servidor VIAWEB 1. Mais informações pag. 19 | 1 |
| | Se habilitado, a senha de programador somente irá funcionar se todas as partições estiverem desarmadas. Mais informações pag. 39 | 2 |
| | Modo de operação com senhas aleatórias. Se habilitado, as senhas de usuário 3, 4 e 5 são geradas aleatoriamente e trocadas automaticamente quando utilizadas. Mais informações pag. 55 | 3 |
| | Se habilitado, o auto arme por inércia de qualquer partição não irá armar se alguma zona da central for disparar. Nesse caso o sistema reinicia a contagem de tempo e envia o evento programado na função [ 465 ], “Falha no auto arme” informando a partição que não armou. Mais informações pag. 45 | 4 |
| | Se habilitado, quando o nível de sinal estiver sendo enviado no teste periódico (no campo zona), no campo partição, o valor representará a tecnologia. Sendo:<br>00 - GPRS<br>07 - 4G<br>08 - CAT-M1<br>09 – NB-IoT<br>Mais informações pag. 19 | 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. Mais informações pag. 56 | 6 |
| | Quando habilitado, o evento de teste periódico é enviado usando o ID_ISEP como número da conta. Se desabilitado, usa o número da conta da partição 1 (função 066). Mais informações pag. 19 | 7 |
| | O campo zona do evento Contact ID do teste periódico é preenchido.<br>Se o equipamento possui 4G ou GPRS embarcado, preenche com o nível de sinal de 000 (0%) até 032 (100%).<br>Caso contrário, com a mínima tensão de alimentação lida em 0,1V.; Mais informações pag. 19 | 8 |

# RESET

## Reset das senhas Mestre e de programação

Para que as senhas mestre e de programação voltem para os valores de fábrica siga os passos:

- Alimente a central (o reset só funciona nos primeiros 4 minutos)
- Mantenha ambos os botões pressionados (sinal e recon) pressionados por 10 segundos.
- O led de status da central LD3 e LD4 vão piscar lentamente.
- Solte o botão.

Após esse procedimento as senhas retornam ao padrão de fábrica:

**Senha de Programação: 5353** **Senha Master 001: 1515**

## Reset total da programação

Para que os valores de todas as funções voltem para os padrões de fábrica siga os passos:

- Mantenha ambos os botões pressionados (sinal e recon) por 20 segundos.
- Em 10 segundos os leds 3 e 4 começam a piscar indicando que houve reset das senhas (se o equipamento for central de alarme), aguarde mais 10 segundos sem soltar os botões.
- Os leds ficam acesos indicando que o equipamento está retornando aos valores de fábrica.
- Solte os botões. AGUARDE OS LEDS VOLTAREM A PISCAR PARA RETIRAR A ALIMENTAÇÃO, caso contrário o reset não será completado.

Obs.: No reset total todas as senhas também voltam aos valores de fábrica.

## [ 362 ] Trava de Reset

**[ 362 ]** [ __/__/__ ] Padrão: 000

Quando for programado o valor 147 nessa função, torna-se impossível restaurar a programação e as senhas de fábrica (reset) da central até que se programe nesta função um valor diferente de 147.

## [ 362 ] Reinicialização de Barramento

**[ 362 ]** [ __/__/__ ] Padrão: 000

Quando for programado o valor 236 nessa função, as centrais de alarme reiniciam todos os seus periféricos do barramento como se o sistema tivesse acabado de ser alimentado, reordenando periféricos, eliminando periféricos ausentes e aceitando periféricos novos, remove falhas de periférico.

## [ 362 ] Resetar a programação de um periférico individualmente

**[ 362 ]** [ __/__/__ ] Padrão: 000

Permite resetar a programação de um periférico individualmente. Se programado o valor 058, executa reset do periférico com endereço programado na função 017.

# CONTACT – ID (CÓDIGOS DOS EVENTOS DO ALARME)

A VW16Z 4G IP informa imediatamente à central de monitoramento (quando programada) todas as alterações em seu estado, situação das partições, falhas e restauros, programações, etc. Todas essas informações podem ser reportadas em todas as vias de comunicação disponíveis (ethernet TCP/IPv4). Inclusive quando utilizam-se módulos externos (VWGPRS ou expansores).

Essas informações enviadas permitem à central de monitoramento perfeita identificação de qual painel enviou a comunicação, vinculado à data e hora do evento, e permite identificar diversos tipos de ocorrências.

Esses eventos são identificados tanto na central de monitoramento quanto no servidor VIAWEB SERVICE pelo protocolo **CONTACT-ID**.

Basicamente, um evento de contact-id é gerado dessa maneira:

| CCCC | QXXX | YY | ZZZ |
|---|---|---|---|
| Cliente | Evento | Partição | Complemento |

CCCC – Cliente: Esta é a identificação do cliente na empresa de monitoramento (programado nas funções de [066] à [073]) .

Q – Qualifier do evento: É o dígito que define se o código é um **evento** (desarme, disparo, falha, etc.), ou um **restauro** (arme, restauração de disparo, restauração de falha, etc.).
1 = EVENTO e 3 = RESTAURO.

XXX – Código do evento: Cada evento tem um código padrão distinto. Na tabela abaixo encontramos os códigos gerados pela central e o campo caso necessitem de alteração.

YY – Partição: Quando o sistema é particionado indica em qual a partição ocorreu o evento

ZZZ – Complemento: Referente ao evento. Por exemplo, no caso de disparo, esse campo mostra a zona que foi disparada, ou quando o sistema é armado, esse campo indica qual usuário armou o sistema.

**OBS.: A alteração dos eventos nos campos abaixo pode dificultar a interpretação dos eventos tanto pelo aplicativo quanto pela central de monitoramento.**

O Aplicativo VIAWEB Mobile “traduz” automaticamente o evento Contact ID, não sendo necessária a alteração dos campos abaixo.

Caso o evento programado nos campos abaixo não esteja dentro dos padrões, quando gerado, no aplicativo aparecerá apenas o valor programado e não a descrição dele.

Alguns códigos Contact ID usados para identificação das ocorrências podem ser programados. As funções 401 a 476 servem para alterar ou cancelar esses códigos.

## [ 401 a 476 ] Códigos dos Eventos em Contact-ID

0000 = Desabilita o evento

### Alarmes

**[401]** [ 1 / 1 / 3 / 0 ] Alarme de Furto
**[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 ] Violação de Tamper
**[419]** [ 1 / 1 / 0 / 0 ] Emergência Médica
**[420]** [ 1 / 1 / 1 / 0 ] Incêndio
**[421]** [ 1 / 1 / 2 / 0 ] Emergência Silenciosa
**[422]** [ 1 / 1 / 2 / 1 ] Coação

### 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

### Falhas

**[423]** [ 0 / 0 / 0 / 0 ] Zona esquecida aberta
**[424]** [ 1 / 3 / 0 / 0 ] Falha de Fonte Auxiliar
**[425]** [ 1 / 3 / 0 / 1 ] Falha de Energia Elétrica
**[426]** [ 1 / 3 / 0 / 2 ] Falha de Bateria
**[427]** [ 1 / 3 / 3 / 3 ] F. de Tensão no Barramento
**[428]** [ 1 / 3 / 2 / 1 ] Falha de Sirene 1
**[429]** [ 1 / 1 / 4 / 3 ] Falha de Módulo Expansor
**[430]** [ 1 / 3 / 5 / 0 ] Falha de Comunicação
**[432]** [ 1 / 1 / 4 / 2 ] Curto circuito na zona
**[465]** [ 0 / 0 / 0 / 0 ] Falha de auto arme

### Restauros

**[459]** [ 3 / 3 / 0 / 0 ] Restauro de Fonte Auxiliar
**[460]** [ 3 / 3 / 0 / 1 ] Restauro de Energia Elétrica
**[461]** [ 3 / 3 / 0 / 2 ] Restauro de Falha de Bateria
**[462]** [ 3 / 3 / 3 / 3 ] Restauro de Falha de Tensão no Barramento
**[463]** [ 3 / 3 / 2 / 1 ] Restauro de Sirene 1
**[464]** [ 3 / 1 / 4 / 3 ] Restauro de Módulo Expansor
**[467]** [ 3 / 1 / 4 / 2 ] Restauro de Curto Circuito

### Desarmado

**[433]** [ 1 / 4 / 0 / 1 ] Desativado Por Senha
**[434]** [ 1 / 4 / 0 / 2 ] Partição Desativ. Por Senha

### Armados

**[468]** [ 3 / 4 / 0 / 1 ] Ativado Por Senha
**[469]** [ 3 / 4 / 0 / 2 ] Partição Ativada por Senha
**[470]** [ 3 / 4 / 0 / 3 ] Auto Ativação
**[473]** [ 1 / 4 / 1 / 0 ] Acesso via Cabo serial
**[474]** [ 3 / 4 / 5 / 6 ] Ativado Forçado

### Exclusão

**[436]** [ 1 / 5 / 7 / 0 ] Exclusão de Zona
**[437]** [ 1 / 5 / 7 / 0 ] Auto Exclusão de Zona

### Controle de Acesso

**[440]** [ 1 / 4 / 1 / 2 ] Ev. de acesso remoto pelo VIAWEB
**[471]** [ 3 / 4 / 0 / 7 ] Programação lacrada, no campo zona irá o nível do lacre.
**[472]** [ 3 / 4 / 0 / 8 ] Programação irá liberar após 4 minutos, no campo zona irá o nível que o lacre irá assumir.

### Testes

**[438]** [ 1 / 6 / 0 / 2 ] Teste Automático
**[439]** [ 1 / 6 / 0 / 3 ] Teste Internet

### PGM

**[475]** [ 0 / 0 / 0 / 0 ] Evento da PGM
**[476]** [ 0 / 0 / 0 / 0 ] Restauro da PGM

### Loop Zonas (função 107 modo 9)

**[477]** [ 1 / 3 / 5 / 6 ] Falha de loop
**[478]** [ 3 / 3 / 5 / 6 ] Restauro de loop