



Manual de instalação e programação do Advisor Advanced AT5x500A(-IP)

Copyright	© 2021 Carrier. Todos os direitos reservados. As especificações podem ser alteradas sem aviso prévio.
Marcas comerciais e patentes	Aritech, o nome e logótipo Advisor Advanced ATSx500A(-IP) são marcas comerciais da Carrier Fire & Security.
	Outros nomes comerciais utilizados neste documento podem ser marcas comerciais ou marcas comerciais registadas dos fabricantes ou vendedores dos respectivos produtos.
Fabricante	Carrier Fire & Security Americas Corporation, Inc. 13995 Pasteur Blvd Palm Beach Gardens, FL 33418, USA
	Representante de fabrico autorizado na UE: Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands
Avisos e isenções de responsabilidade dos produtos	<p>ESTES PRODUTOS ESTÃO PREVISTOS PARA SEREM VENDIDOS E INSTALADOS POR PROFISSIONAIS QUALIFICADOS. A CARRIER FIRE & SECURITY NÃO PODE APRESENTAR QUALQUER GARANTIA DE QUE QUALQUER PESSOA OU ENTIDADE QUE COMPRE OS SEUS PRODUTOS, INCLUINDO QUALQUER “DISTRIBUIDOR AUTORIZADO” OU “REVENDEDOR AUTORIZADO”, TEM FORMAÇÃO OU EXPERIÊNCIA ADEQUADA PARA INSTALAR CORRETAMENTE PRODUTOS RELACIONADOS COM A SEGURANÇA E A PROTEÇÃO CONTRA INCÊNDIOS.</p> <p>AVISO! Os produtos para alarme de incêndio e deteção de fumo usados com os sistemas Advisor Advanced destinam-se a ser utilizados exclusivamente por conveniência e não devem ser utilizados como produtos de proteção da vida. A combinação não cumpre com os requisitos legais para os produtos de proteção da vida ou para utilização como sistemas de deteção de incêndios. A Carrier não aceita qualquer responsabilidade por danos derivados da utilização incorreta dos produtos.</p> <p>Para mais informações sobre isenções de garantia e sobre a segurança dos produtos, consulte https://firesecurityproducts.com/policy/product-warning/ ou faça a leitura do código QR.</p>
	
Versão	Este documento refere-se às seguintes versões de firmware do Advisor Advanced ATSx500A(-IP): MR_4.7
Certificação	<p></p> <p>EN 50131-1 Requisitos do sistema EN 50131-3 Equipamento de controlo e de indicação EN 50131-6 Fontes de alimentação EN 50136-1-1 Sistemas de alarme - Sistemas de transmissão de alarmes</p> <p>ATS1500A(-IP): Grau de segurança 2, classe ambiental II ATS3500A(-IP): Grau de Segurança 3, classe ambiental II ATS4500A-IP: Grau de Segurança 3, classe ambiental II</p> <p>Nota: o painel ATS1500A(-IP)-MM pode ser atualizado para o grau de segurança 3 utilizando o kit de tamper ATS-MM-TK.</p> <p>Modo de funcionamento conforme a EN 50136-2: 2013.</p>

A transmissão dos eventos para a estação central ocorre por meio de procedimentos de passagem de acordo com a EN 50136-2: 2013.

Testado por VdS Schadeverhütung GmbH

Importante: Para cumprir as normas acima referidas, é necessário configurar o sistema de acordo com as definições indicadas no Capítulo 8 "Normas" na página nº 367 em diante.

Este produto não foi concebido em conformidade com as normas EN 50134 e EN 54.

Directivas da União Europeia

A Carrier Fire & Security declara que estes dispositivo se encontra em conformidade com os requisitos e disposições aplicáveis da Diretiva 2014/30/EU e/ou 2014/35/EU. Para mais informações consulte firesecurityproducts.com ou www.aritech.com.

REACH

O produto pode conter substancias da Lista de Candidatos de concentração acima de 0.1% w/w, de acordo com a lista de Candidatos publicada recentemente no site ECHA.

Informações de utilização segura podem ser encontradas em <https://firesecurityproducts.com/en/content/intrusion-intro>



2012/19/EU (directiva WEEE, sobre Resíduos de Equipamentos Eléctricos e Electrónicos): Os produtos marcados com este símbolo não podem ser eliminados como lixo municipal não separado na União Europeia. Para uma reciclagem adequada, devolva este equipamento ao fornecedor local aquando da compra de um novo equipamento equivalente, ou coloque-o num ponto de recolha designado para o efeito. Para mais informações, consulte: recyclethis.info

Documentação de produto

Por favor consulte o link seguinte para obter a versão eletrónica da documentação do produto.



Este link irá direcioná-lo para a página regional da EMEA. Nesta página pode solicitar o acesso ao portal seguro, onde todos os manuais se encontram armazenados.

<https://firesecurityproducts.com/en/contact>

Informação de contacto

firesecurityproducts.com ou www.aritech.com

Índice

	Prefácio	iii
Capítulo 1	Instalação e programação rápida	1
	Instalação rápida	2
	Programação rápida	4
Capítulo 2	Instalação	7
	Informação de instalação geral	8
	Manutenção	17
	Montagem	20
	Ligação à terra	22
	Blindagem	23
	Cablagem do Advisor Advanced	24
	Configuração	32
	Especificações	37
Capítulo 3	Funções do sistema	45
	Lista de funções	47
	Zonas	49
	Áreas	55
	Arme e desarme	57
	Inibir e isolar	60
	Teclas	62
	Dispositivos	67
	Utilizadores	69
	Grupos de utilizadores	72
	PIN	77
	Saídas	79
	Controlo de acesso	80
	Filtros de condições	87
	Triggers	89
	Calendário	90
	Eventos	93
	Testes e diagnósticos	95
	Reportes de alarme	100
	Funções de utilizador programáveis	105
	Arme automático	109
	Programação de dispositivos sem fios	110
	Utilizar câmaras	117
	Reset técnico	121
	Desarme / ATM Temporizado	122
	Áudio de duas vias	123
	UltraSync	126
	Aplicação móvel	129

	Segurança dos dados do cartão	130
Capítulo 4	Programação	133
	O menu do Advisor Advanced	134
	Acesso remoto	141
	Arranque inicial	142
Capítulo 5	Referência de menu	145
	1 Serviço	148
	2 Disp.BUS	174
	3 Gestão utlz	201
	4 Zonas e áreas	211
	5 Menu Porta	241
	6 Outputs e filtros	267
	7 Calendário	275
	8 Sistema	283
	9 Comunicação	316
Capítulo 6	Software	353
	Programar o Advisor Advanced através do software de configuração	354
	Actualização de firmware Advisor Advanced	356
Capítulo 7	Resolução de problemas	361
	Procedimento de recuperação	362
	Resolução de problemas do dispositivo	363
Capítulo 8	Normas	367
	Opções afectadas pelas normas EN 50131	368
	Opções afectadas por outros regulamentos	375
Anexo A	Eventos do Advisor Advanced	379
Anexo B	Códigos de reporte utilizados no Advisor Advanced	399
	Glossário	413
	Índice remissivo	419
	Mapa de programação	429

Prefácio

Este documento inclui uma perspectiva geral do produto e instruções detalhadas que explicam como instalar e programar o sistema Advisor Advanced.

Para utilizar este documento com eficácia tem de dispor das seguintes qualificações mínimas:

- Conhecimentos básicos sobre sistemas de alarme e componentes
- Conhecimentos básicos de instalações eléctricas e de ligações eléctricas de baixa tensão

Leia estas instruções e toda a documentação auxiliar na totalidade antes de instalar este produto ou trabalhar com ele.

Nota importante

Este manual fornece informações sobre todos os painéis de controlo Advisor Advanced e IP Advisor Advance em todas as variações. O “painel de controlo Advisor Advanced” refere-se a todas as versões do Advisor Advanced ou IP Advisor Advanced, salvo quando especificado em contrário.

Lista de variantes do painel

Tabela 1: Lista de variantes do painel ATsx500A(-IP)

Modelo	Cobertura	Dimensões (mm)	Peso (kg)
ATS1500A-MM	Metal	MM, 315 x 388 x 85	5,2
ATS1500A-IP-MM	Metal	MM, 315 x 388 x 85	5,2
ATS1500A-SM	Metal	SM, 250 x 250 x 86	2,8
ATS1500A-IP-SM	Metal	SM, 250 x 250 x 86	2,8
ATS1500A-LP	Plástico	LP, 257 x 400 x 112	2,6
ATS1500A-IP-LP	Plástico	LP, 257 x 400 x 112	2,6
ATS3500A-MM	Metal	MM, 315 x 388 x 85	5,2
ATS3500A-IP-MM	Metal	MM, 315 x 388 x 85	5,2
ATS3500A-LP	Plástico	LP, 257 x 400 x 112	2,6
ATS3500A-IP-LP	Plástico	LP, 257 x 400 x 112	2,6
ATS4500A-IP-MM	Metal	MM+, 315 x 445 x 88	5,4
ATS4500A-IP-LM	Metal	LM, 465 x 480 x 160	10,9

Notas

- Algumas versões podem não estar disponíveis.
- O peso não inclui as baterias.

Limitação de responsabilidade

Dentro dos limites permitidos pela lei aplicável, a Carrier não assume qualquer responsabilidade por quaisquer oportunidades de negócio ou lucros perdidos, perda de utilização, interrupção de negócios, perda de dados ou quaisquer outros danos directos, indirectos ou especiais, sob qualquer teoria de responsabilidade, seja com base em contrato, garantia, negligência, responsabilidade do produto ou outros actos ilícitos. Uma vez que algumas jurisdições não permitem a exclusão ou limitação de responsabilidade por danos directos ou indirectos, a limitação anterior poderá não ser aplicável ao seu caso. De qualquer modo, a responsabilidade total da Carrier não ultrapassará o preço de compra do produto. A limitação precedente aplicar-se-á dentro dos limites permitidos pela lei aplicável, independentemente de a Carrier ter sido advertida para a possibilidade de tais danos e independentemente de qualquer reparação cumprir ou não o seu propósito essencial.

É obrigatório proceder à instalação em conformidade com o presente manual, com os códigos aplicáveis e com as instruções das autoridades competentes.

Embora tenham sido adoptadas todas as precauções durante a preparação do presente manual, com vista a garantir a exactidão do respectivo conteúdo, a Carrier não assume qualquer responsabilidade por erros ou omissões.

Mensagens de advertência

As mensagens de advertência advertem para condições ou práticas que podem produzir resultados indesejáveis. As mensagens de advertência utilizadas no presente documento são mostradas e descritas abaixo.

AVISO: as mensagens de aviso advertem para perigos que podem resultar em lesões ou morte. Indicam as acções a adoptar ou a evitar para impedir lesões ou morte.

Cuidado: as mensagens de cuidado advertem para possíveis danos no equipamento. Indicam as acções a adoptar ou a evitar para impedir os referidos danos.

Nota: as mensagens em forma de nota advertem para a perda eventual de tempo ou esforço. Descrevem como evitar essa perda. As notas são também utilizadas para realçar informações importantes que devem ser lidas.



Sinal de segurança que identifica acções ou práticas exigidas pela norma de segurança EN 60950.

Avisos e precauções



Cuidado: Peças quentes! Risco de queimaduras. Queimaduras nos dedos ao manusear as peças. Deixe as peças arrefecer antes de manusear.



AVISO! Tensão perigosa! Risco de ferimentos ou morte. O fusível pode estar na posição neutra. A rede elétrica deve estar desligada para remover a energia aos condutores de fase.



AVISO! Risco de incêndio, explosão ou mau funcionamento da proteção se a bateria for substituída por outra de tipo incorreto. A eliminação de uma bateria pelo fogo, a sua colocação dentro de um forno quente, deixá-la num ambiente envolvente com uma temperatura extremamente alta, sujeitá-la a uma pressão atmosférica extremamente baixa, esmagá-la ou cortá-la mecanicamente pode resultar em explosão ou vazamento de líquido ou gás inflamável.



AVISO! Se a tampa da caixa for removida, não existe proteção contra incêndio causado eletricamente que possa ocorrer durante o mau funcionamento do sistema.

A tampa da caixa deve ser remontada de acordo com estas instruções de instalação após cada interferência de um utilizador.

Capítulo 1

Instalação e programação rápida

Resumo

Este capítulo apresenta passos básicos de ligação e programação do painel de controlo Advisor Advanced e dispositivos auxiliares.

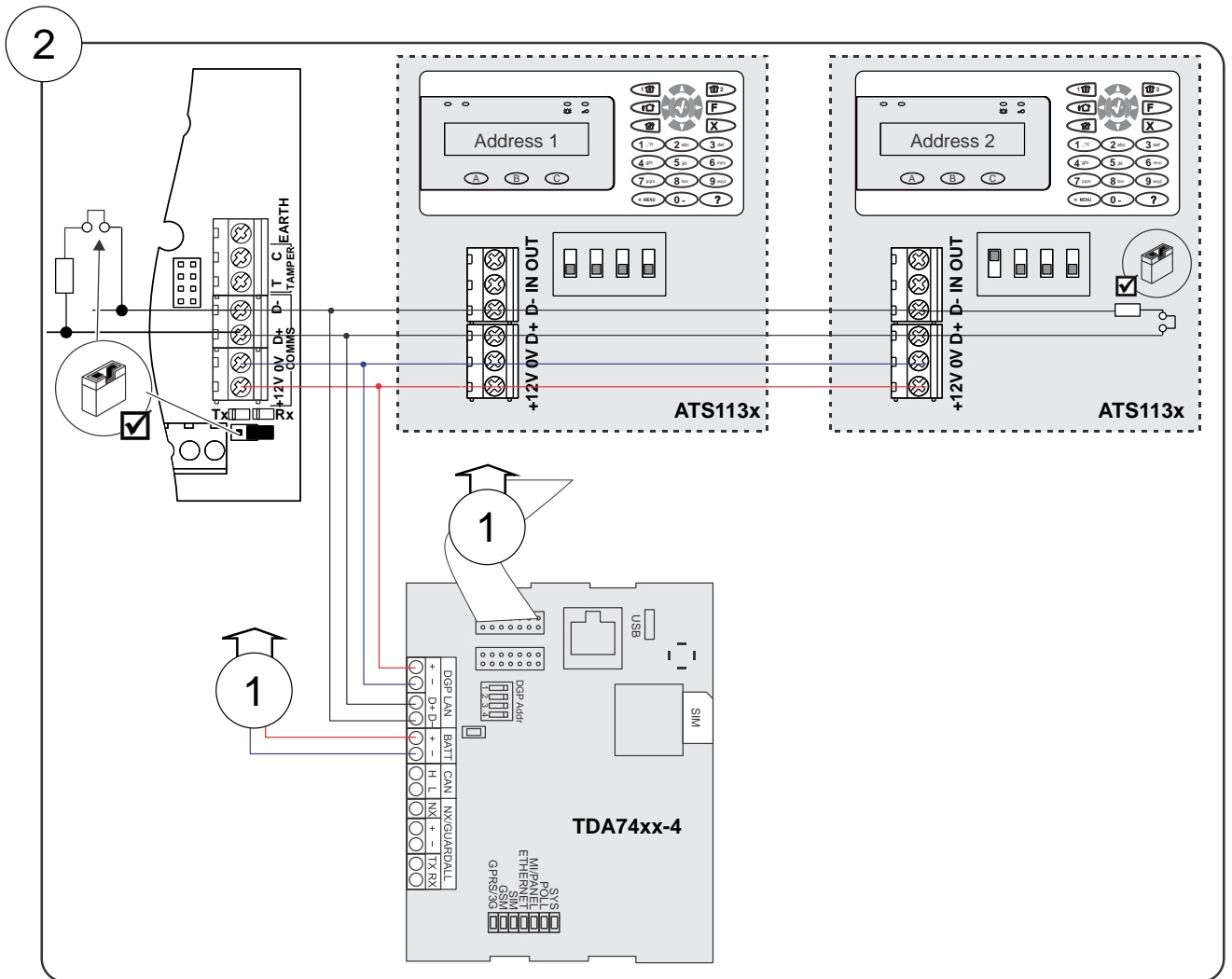
Para uma descrição mais detalhada do processo de instalação, consulte o Capítulo 2 “Instalação” na página nº 7.

Para informações sobre programação, consulte o Capítulo 4 “Programação” na página nº 133 e o Capítulo 5 “Referência de menu” na página nº 145.

Índice

Instalação rápida 2

Programação rápida 4



Programação rápida

Arranque inicial

Nota: consulte “O menu do Advisor Advanced” na página nº 134 para uma explicação do menu.

Ligue a alimentação do painel. Os menus e mensagens adicionais são apresentados na tabela abaixo.

Display	Instruções
---------	------------

INFORMAÇÕES Instal. neces	Prima Enter para continuar.
1>Idioma painel	Seleccione Inglês.
2>Predefinições	Escolha EN 50131 Grau 3.
3>Hora&data	Defina a data e hora actuais.
4>UltraSync	Defina opções UltraSync.

Se necessário, ative a conectividade UltraSync e depois introduza a palavra-passe UltraSync. Se o UltraSync estiver ativado, a comunicação do painel será configurada através da segurança da “cloud”.

5>Outras opç	Defina outras opções do painel.
--------------	---------------------------------

Podem ser definidas as seguintes opções:

- Método de coação
- Tamanho do PIN
- Modo de alteração do PIN

Consulte também “Arranque inicial” na página nº 142.

6 Instalar >Cancelar<	Escolha OK
Alterar PIN Installer	Pressione Enter para continuar
Novo PIN >_	Digite o novo PIN de instalador e pressione Enter

Vericar >_	De seguida, digite novamente o PIN para verificação.
Alterar PIN Supervisor	Pressione Enter para continuar
Novo PIN >_	Digite o novo PIN de supervisor e pressione Enter
Vericar >_	De seguida, digite novamente o PIN para verificação.

O painel reinicia-se.

Configuração automática

Auto Config? >Sim<	Prima Enter para continuar.
RAS 1-16 BUS1 R-?----- DGP 1-15 BUS1 -?----- Aud 1-16 BUS1 ---?-----	Aguarde até o painel configurar todos os dispositivos bus e zonas.
Adicionado R:1 D:0 Z:8 A:0	Prima Enter para continuar.

Activar entrada em modo técnico

Carrier F&S QUI 05 Mar 12:21	Digite o PIN de supervisor e pressione Menu.
1>Opções de zona 2 Isolator	Vá para o menu 8.8 Manutenção em
8>Manutenção em Activar?	Active o tempo de acesso do instalador

Prima Cancelar, Cancelar para sair de sessão.

Entrada de menu de programação

Carrier F&S QUI 05 Mar 12:21	Digite o PIN de instalador e pressione Menu.
Inib. reportes >Não<	Prima Enter para continuar.

```
Inibir tampers
Desarmar áreas
```

```
1>Serviço
2 Disp.BUS
```

É apresentado o menu do instalador.

Alterar a chave de encriptação

Cuidado: recomenda-se vivamente alterar a chave de encriptação predefinida.

Vá a 9.4.3 Código de encriptação 1 e 9.4.4 Código de encriptação 2 (página 347).

```
3 Cód Encript.1
>000000000000<
```

Introduza a chave de encriptação 1.

```
4 Cód Encript.2
>000000000000<
```

Introduza a chave de encriptação 2.

Configuração de zonas

Cuidado: Selecione o esquema de numeração pretendida antes de programar as zonas. Ver “8.7.9 Esquema Objeto” na página nº 308 para mais informações

Vá para 4.1 Zonas (página 211).

```
4>Zonas&Áreas
```

Prima Enter.

```
1>Zonas
```

Prima Enter.

```
0>Adicionar zona
1 Zona 1
```

Selecione uma zona.

Para cada zona utilizada no sistema, introduza o nome da zona em 4.1.n.1 Nome da zona (página 212).

```
1 Nome da zona
>Zona 1 <
```

A seguir, defina o tipo de zona em 4.1.n.2 Tipo de zona (página 213).

```
02 Tipo de zona
>Entrada/Saida1<
```

Adicionar utilizadores

Vá para o menu 3.1 Utilizadores (página 201).

```
0>Adicionar utlz
1 Instalador
```

Prima Enter para adicionar um utilizador.

```
Modo Adicionar
>Manual<
```

Prima Enter.

```
INFORMAÇÕES
Utlz adicion
```

```
1>Nome de utlz
Utilizador 3
```

Prima Enter.

```
1 Nome de utlz
>Utilizador 3 <
```

Introduza um novo nome de utilizador.

Configure outras opções do utilizador:

- 3.1.n.2 PIN (página 202)
- 3.1.n.3 Cartão utilizador (página 203)
- 3.1.n.6 Grupos utlz (página 204), etc.

Repita para outros utilizadores.

Ao sair da configuração do utilizador, confirme o bloqueio dos dados do utilizador.

```
Bloq.Info.Utl?
>Cancelar<
```

Selecione OK e confirme.

Configuração de áreas

Vá para 4.2 Áreas (consulte a página 227).

Altere o nome da área em 4.2.n.1 Nome da área (consulte a página 228).

```
1 Nome da área
>Área 1 <
```

Introduza um novo nome de área.

Configure outras opções da área:

- 4.2.n.2 Tempo de saída (página 228)
- 4.2.n.3 Tempo de entrada (página 229), etc.

Cuidado: antes de activar 4.2.n.5.4 Desarme Duplo (página 232), certifique-se de adicionar utilizadores que possam ajudar no desarme. Consulte “Adicionar utilizadores” acima.

Configuração da central receptora

Configure o caminho de comunicação em 9.3 Opções de via (página 328).

```
1>RTPC
3 GSM/SMS/GPRS
```

Selecione o caminho necessário e configure-o consoante o hardware utilizado.

A seguir, vá para o menu 9.1 Central Receptora (página 316).

```
0>Adicionar CRA
1 CRA 1
```

Adicione uma nova CRA, ou selecione uma existente. Configure os parâmetros seguintes:

- 9.1.n.1 Nome CRA (página 317)
- 9.1.n.2 Via de transm (página 317)
- 9.1.n.3 Protocolo (página 317)
- 9.1.n.5 Contas (página 318)
- Outras opções, consoante o caminho de comunicação utilizado.

Teste a comunicação utilizando o menu 1.2.6.n.6 Teste manual (página 160), em que <n> é o número da central receptora configurada.

```
Chamar CRA 1...
Pronto
```

Normas

Se necessário, siga as instruções do Capítulo 8 “Normas” na página nº 367 para configurar outras opções exigidas pelas normas e regulamentos aplicáveis.

Capítulo 2

Instalação

Resumo

Este capítulo apresenta uma panorâmica geral do produto e instruções detalhadas de instalação dos componentes do seu sistema Advisor Advanced.

Nota: toda a instalação de hardware necessária deve ser efectuada por um técnico qualificado, cumprindo todos os códigos aplicáveis.

Índice

Informação de instalação geral	8
Caixas do Advisor Advanced	8
Layout do Advisor Advanced	12
Teclados e leitores	13
Manutenção	17
Ligação à corrente eléctrica	17
Instalação de bateria	18
Substituição da bateria	18
Montagem	20
Directrizes gerais de instalação	20
Ligação à terra	22
Blindagem	23
Cablagem do Advisor Advanced	24
Cablagem preferida do databus do sistema	24
Ligação do databus do sistema	24
Ligação das zonas	25
Valores de resistências de fim de linha	27
Tipos de ligação EOL	29
Ligação da sirene	30
Outras ligações	30
Configuração	32
Valores predefinidos do painel	32
Configuração de zonas	32
Saídas	32
Endereçamento de zonas, saídas e portas	33
Especificações	37
Corrente auxiliar e capacidade da bateria	41

Informação de instalação geral

As caixas com orifícios de montagem (item 1) estão apresentadas nas figuras abaixo.

O item 2 indica a localização do pilar do tamper de remoção de parede.

Todas as dimensões são fornecidas em mm.

Caixas do Advisor Advanced

Figura 1: Caixa pequena de metal (-SM)

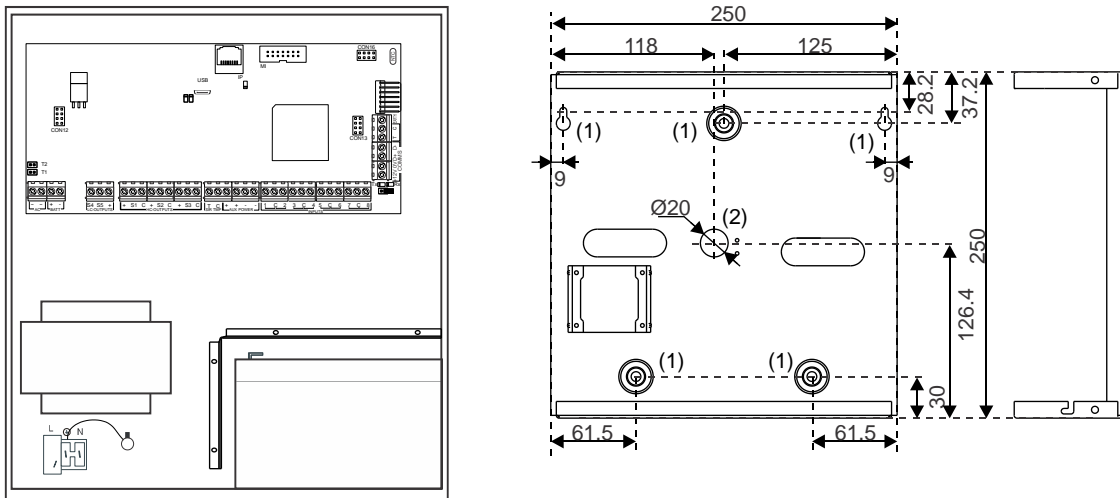


Figura 2: Caixa média de metal (-MM)

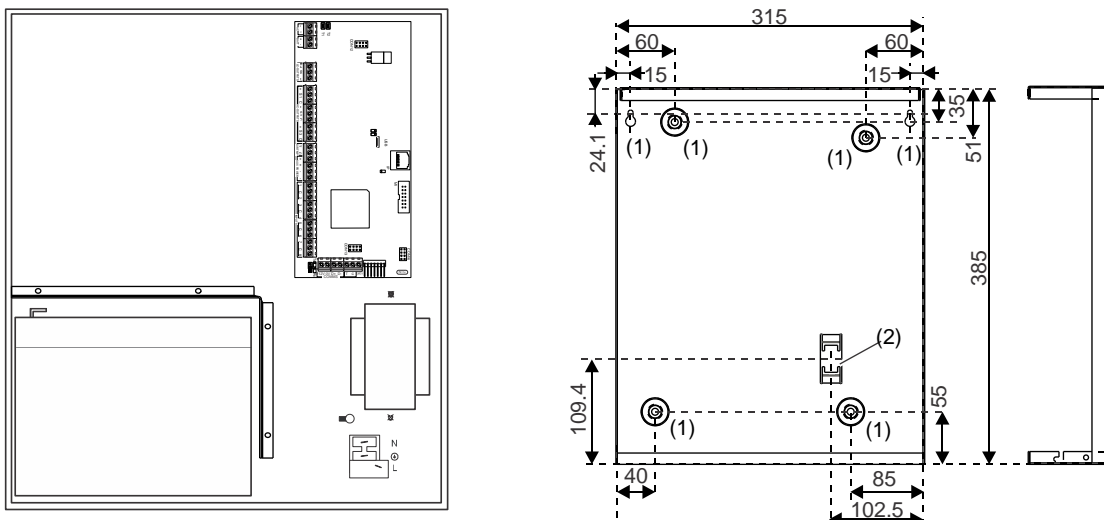


Figura 3: Caixa grande de policarbonato (-LP)

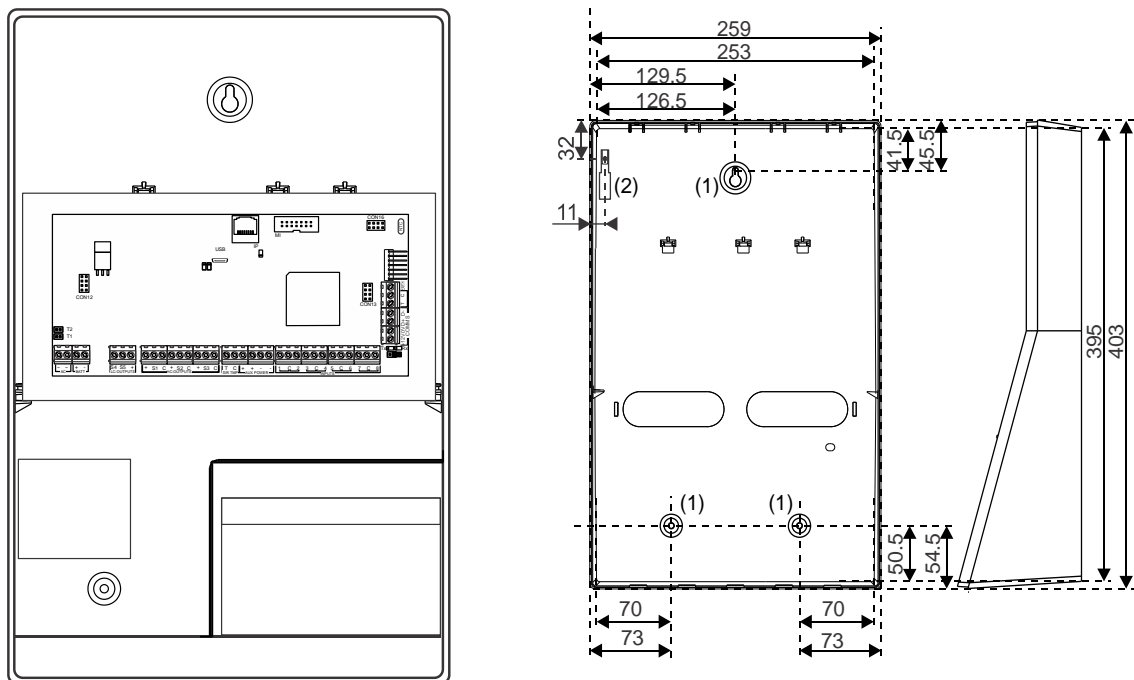


Figura 4: Caixa média de metal (-MM+)

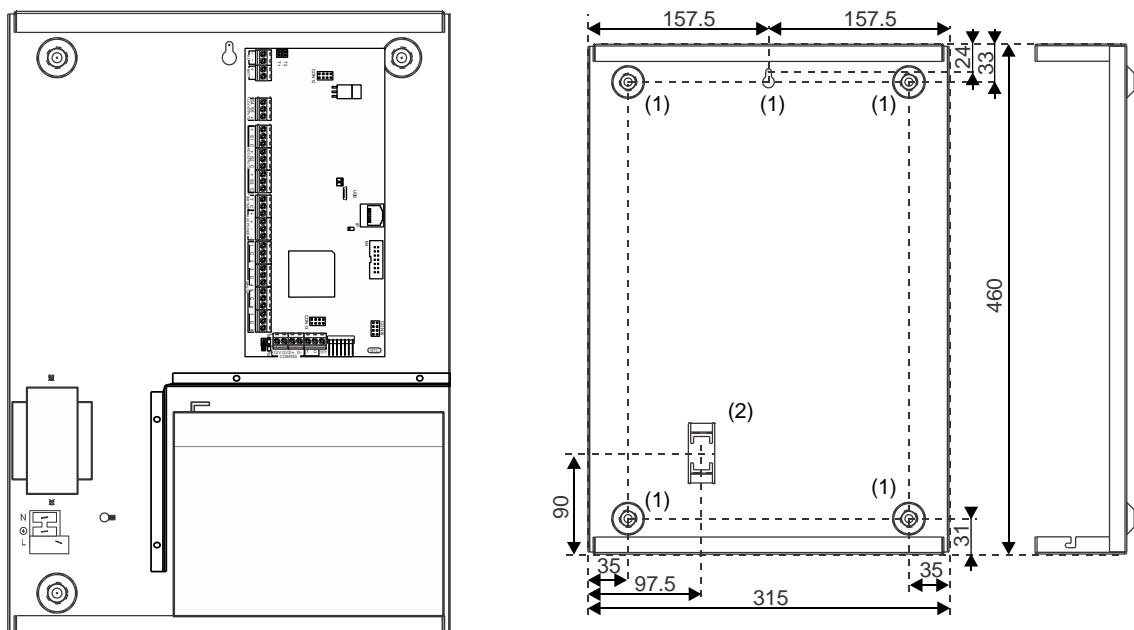
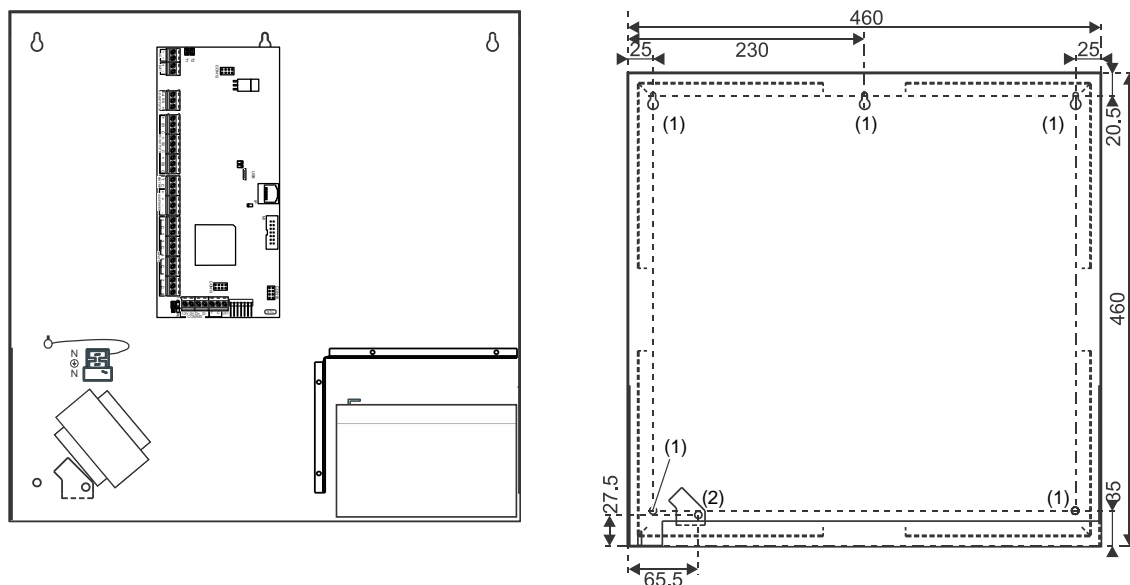


Figura 5: Caixa grande de metal (-LM)



Para mais detalhes sobre ligações e como ligar dispositivos ao Advisor Advanced, consulte “Cablagem do Advisor Advanced” na página nº 24.

Para obter mais informações relativas à conexão de tampers de remoção, consulte “Montagem de tamper de remoção” abaixo.

Montagem de tamper de remoção

Para caixas médias (MM e MM+) e caixas grandes (LM), siga os passos na Figura 6 na página nº 11. Para caixas de plástico grandes (LP), siga os passos na Figura 7 na página nº 11.

Figura 6: Suporte de tamper amovível de caixa média (MM e MM+) e grande (LM)

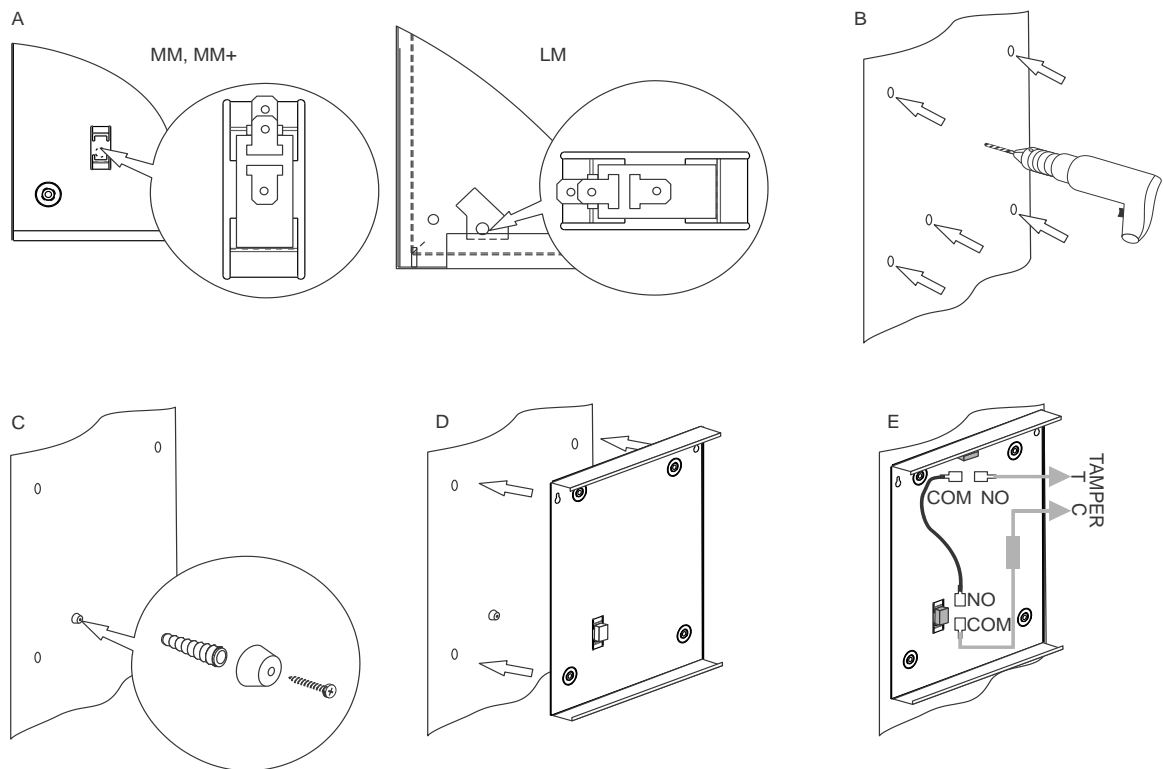
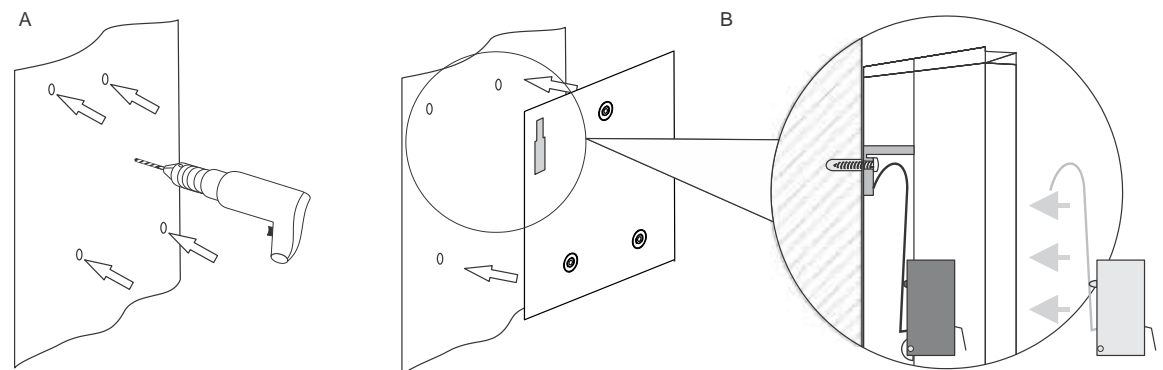
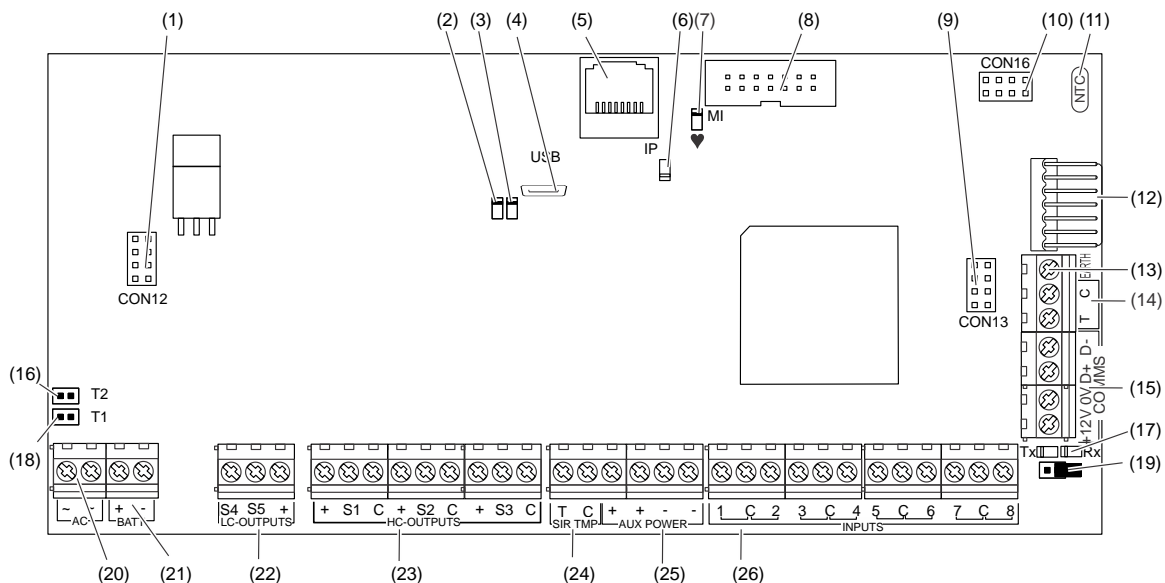


Figura 7: Suporte de tamper amovível de caixa de plástico grande (LP)



Layout do Advisor Advanced

Figura 8: Estrutura da PCI do Advisor Advanced ATSx500A(-IP)



- | | |
|---|---|
| <ul style="list-style-type: none"> (1) Interface para o expensor de saída (2) LED falha USB (3) LED alimentação USB (4) Conector USB (tipo micro-A/B) (5) Conector Ethernet RJ-45 (apenas ATS-IP) (6) LEDs de comunicação IP (apenas ATS-IP) (7) LED Heartbeat (8) Conector MI-bus para dispositivos MI (9) Interface para o expensor de entrada (10) Interface com módulo RTPC (11) Opcional: sensor de temperatura ambiente do compartimento (12) Conector de expensor de databus ATS670 (13) Terminal de terra do painel (14) Interruptor tamper externo (15) Ligações para databus do sistema RS-485 | <ul style="list-style-type: none"> (16) T2: Modo de actualização de firmware (DFU) (17) LEDs de comunicação databus do sistema RS-485 (18) T1: restaura o PIN predefinido do instalador (19) Jumper de terminação do databus do sistema (20) Terminal de fornecimento de energia CA (21) Ligação das baterias (22) Saídas de baixa corrente (OC) (23) Saídas de alta corrente (24) Interruptor tamper de sirene (25) Saída de alimentação auxiliar de 12 V CC (26) Entradas de zonas |
|---|---|

Teclados e leitores

Figura 9: Teclado ATS111xA

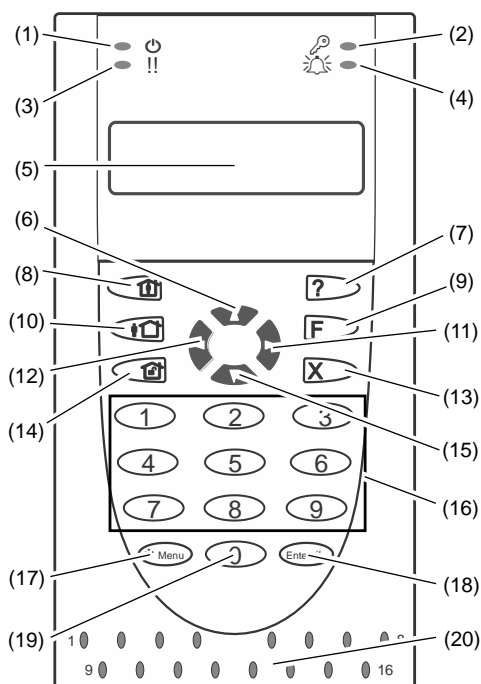
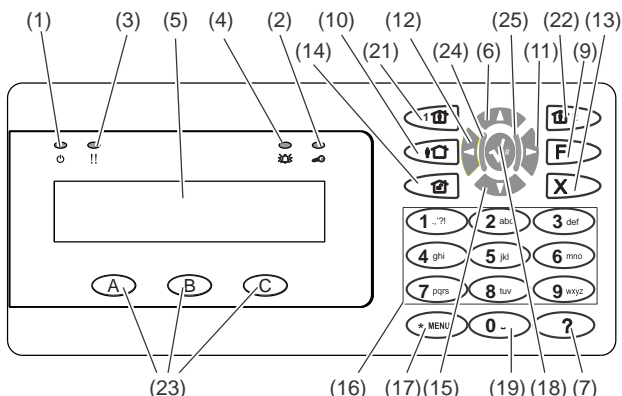


Figura 10: Teclado ATS113x



(1)	LED de corrente CA	A verde: corrente CA ligada
(2)	LED de acesso	Azul intermitente: leitura de cartão
(3)	LED de falha	A amarelo: falha activa do sistema Amarelo intermitente: alerta geral (EN 50131)
(4)	LED de alarme	A vermelho: condição de alarme activa
(5)	Visor LCD	Apresenta mensagens
(6)	▲ / Para cima	Percorrer os menus em sentido ascendente Alterar valor Eliminar
(7)	? / Ajuda	Mostrar ajuda Percorrer texto (só ATS113x)
(8)	Arme parcial	Armar parcialmente uma área Percorrer texto (só ATS111x)
(9)	F / Função	Mostrar falhas/zonas activas Modificador de teclas de funções Percorrer texto (só ATS113x)
(10)	Ligado	Armar totalmente uma área
(11)	► / Direita	Aceder ao menu seleccionado Deslocar o cursor para a direita
(12)	◀ / Esquerda	Voltar para o menu anterior Deslocar o cursor para a esquerda
(13)	X / Sair	Sair da função de utilizador actual Modificador do controlo de volume
(14)	Desligado	Desarmar uma área

(15)	▼ / Para baixo	Percorrer os menus em sentido descendente Alterar valor Retrocesso
(16)	Teclado alfanumérico	Teclas de 1 a 9, dados alfanuméricos. Consulte “Disposição do teclado” na página nº 139.
(17)	Menu	Pedir acesso aos menus
(18)	Enter	Concluir o passo Aceder à entrada de menu seleccionada
(19)	0	Tecla 0 Alternar a selecção
(20)	LEDs de área de 1 a 16	Ligado: área armada. Consulte também “Nota de indicação de controlo de acesso” na página nº 16. Desligado: área desarmada. Intermitente: condição de alarme da área.
(21)	Arme parcial 1	Arme parcial 1 das áreas
(22)	Arme parcial 2	Arme parcial 2 das áreas
(23)	A, B, C	Teclas de funções programáveis
(24)	LED1	LED 1 programável
(25)	LED2	LED 2 programável

Figura 11: Leitores ATS118x

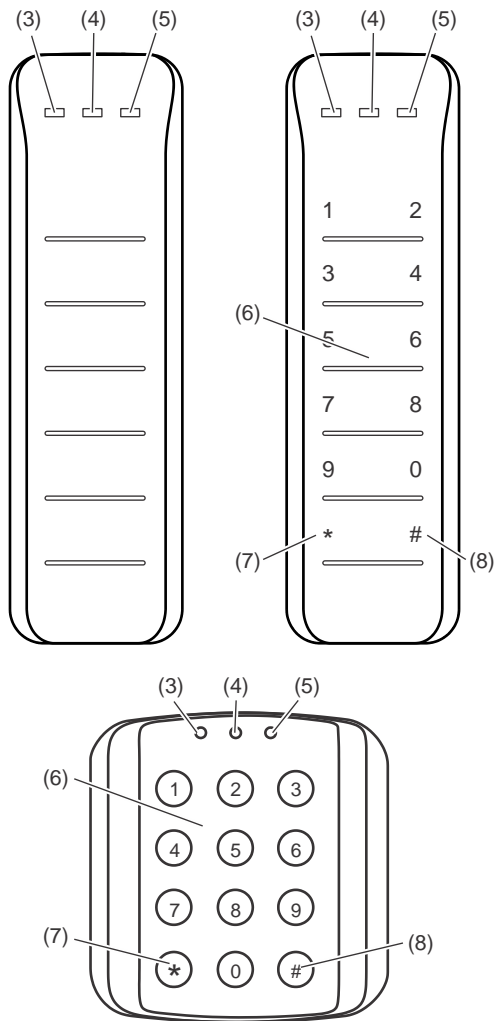


Figura 12: Leitores ATS1190/ATS1192

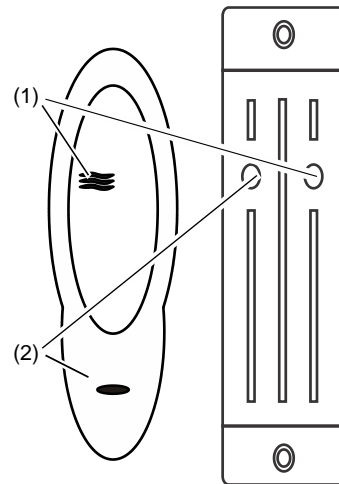


Figura 13: Leitor ATS1197 com teclado

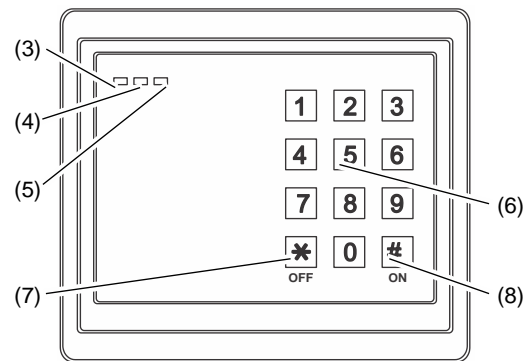
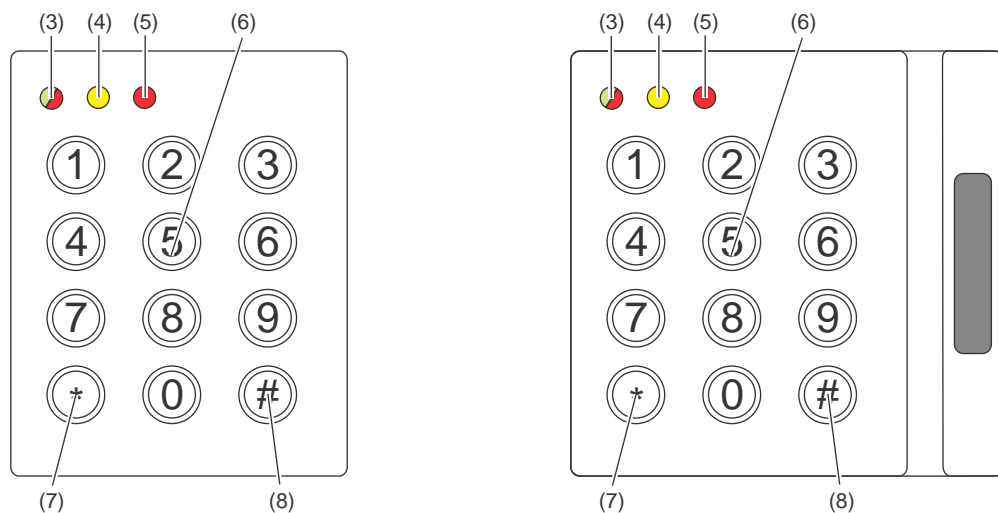


Figura 14: Leitores ATS1151/ATS1156



(1)	LED azul	Acesso concedido
(2)	LED vermelho	On (ligado): área armada Intermitente: alerta geral (EN 50131)

(3)	LED duplo	Verde aceso: Alimentação de CA ligada, todas as áreas não definidas Verde intermitente: corrente CA desligada, ou desbloqueada enquanto desarmada. Vermelho ligado: todas as áreas armadas. Consulte também “Nota de indicação de controlo de acesso” abaixo. Vermelho intermitente: desbloqueado durante o arme.
(4)	LED amarelo	Aceso: todas as zonas estão em estado normal/falha do sistema Nota: Esta funcionalidade depende das definições do sistema. Consulte “8.8.12 RAS LEDLaranja” na página 314. Intermitente: alerta geral (EN 50131) ATS125x: sempre ligado CDC4: falha do sistema
(5)	LED vermelho	Intermitente: alarme
(6)	Teclas numéricas	Teclas de 0 a 9, dados numéricos
(7)	Off	Desarmar uma área
(8)	On	Armar totalmente uma área

Nota de indicação de controlo de acesso

Os teclados e leitores de controlo de acesso, que estão ligados a controladores de portas e não ao painel de controlo, indicam áreas de formas diferentes:

- O LED duplo acende-se de vermelho quando é definida *qualquer* área associada.
- O LED da área 1 está ligado quando é definida *qualquer* área associada. Os LED de área de 2 a 16 não são utilizados.



Manutenção

A manutenção do painel de controlo de intrusão só pode ser realizada por pessoal dedicado da assistência. O parafuso da caixa destina-se a proteger a o produto da utilização não intencional.

Para a caixa de metal, o parafuso já está instalado fora da embalagem. Para a caixa de plástico, o parafuso, disponível no interior da caixa, deve ser montado antes da primeira utilização.

Para abrir a caixa, retire o parafuso e abra a tampa.

Após a manutenção, volte a colocar a tampa e fixe-a com o parafuso.



Ligação à corrente eléctrica

A instalação eléctrica deve ser realizada por uma pessoa qualificada.

O isolamento sólido dos cabos da rede eléctrica do edifício deve cumprir as especificações técnicas e ambientais do equipamento.

O isolamento dos fios nos cabos ligados ao equipamento têm de estar em conformidade com as normas IEC 60332-1-2 e IEC 60332-1-3 ou IEC 60332-2-2, dependendo da área da seção transversal do fio, ou IEC TS 60695-11-21, independentemente da área da seção transversal.

Como alternativa, esses fios têm de estar em conformidade com a UL 2556 VW-1. A área da seção transversal do fio deve estar selecionada para suportar uma corrente de 2 A.

Utilize o terminal do conector de alimentação de energia para ligar a corrente eléctrica CA. Pode ser utilizado um cabo fixo ou um cabo de alimentação flexível para ligar à tomada de corrente com ligação à terra. Quando é utilizada uma cablagem fixa, insira um disjuntor específico na rede de distribuição de alimentação. Em todos os casos, a ligação à corrente eléctrica tem de estar em conformidade com os regulamentos locais.

Ligue sempre o fio de ligação à proteção de terra do edifício e certifique-se de que a ligação é fiável. Consulte também “Ligação à terra” na página 22.

Caso o equipamento esteja ligado à rede eléctrica utilizando instalações fixas, recomenda-se que o cabo terra seja mais comprido que a linha e o cabo neutro.

Ligue o cabo a entrar e neutro ao bloco de ligação de rede de acordo com a etiqueta. Isto garante que o cabo é protegido pelo fusível de rede e que a manutenção pode ser realizada pelo pessoal da assistência.

Certifique-se de que antes de efectuar a ligação à corrente, a fonte de alimentação de rede está desligada.

Ao instalar a energia da rede eléctrica, utilize buçins, braçadeiras de cabos, e acoplamentos PG16s, para garantir uma cablagem correta e minimizar o risco de danos nos fios durante a instalação e a utilização. Quando a alimentação de

corrente é estabelecida, utilize protectores de redução de tensão, tais como braçadeiras e PG16s de emparelhamento para assegurar uma cablagem adequada. Se forem utilizados multiconectores do orifício de entrada do produto é necessário utilizar também um bucim PG16 (ou superior) aprovado de acordo com UL-V2. A especificação PG16 indica os diâmetros mínimo e máximo dos cabos.

Em todos os casos, têm de ser cumpridos os regulamentos locais.

AVISO: Perigo de electrocussão. Para evitar lesões pessoais ou a morte provocadas por electrocussão, remova todas as fontes de energia e deixe descarregar a energia armazenada antes de instalar ou remover o equipamento.

Instalação de bateria

AVISO! A utilização de baterias do tipo incorreto, pode causar risco de incêndio, explosão ou de fuga química. Utilizar apenas os tipos de bateria indicados em “Especificações da fonte de alimentação” na página nº 37.

Para instalar a bateria, efetuar:

1. Certifique-se de que as definições do produto permitem-lhe abrir a tampa sem iniciar o alarme de sabotagem (tamper).
2. Certifique-se de que a alimentação de rede se encontra desligada, e remova a cobertura.
3. Se necessário, remova a antepara da bateria, desapertando quatro parafusos.
4. Ligue a bateria, deslizando os fios do produto no conectores.
5. Monte a proteção da bateria utilizando 4 parafusos.

ATENÇÃO! A proteção da bateria deve ser montada durante a operação normal do dispositivo.

Se for utilizada uma bateria BS131N (12 V / 18 Ah) numa caixa ATS1640 em combinação com o quadro expensor ATS7700 RTPC, é necessário que exista isolamento duplo. Utilize cabos correctamente isolados para cablagem RTPC, e utilize material termo-retráctil.

Substituição da bateria

Este produto pode conter uma (ou mais) bateria chumbo-ácido do tipo BS, selada, recarregável. Uma vez que a remoção de uma bateria poderá afectar as

definições de configuração do produto ou accionar um alarme, apenas um técnico qualificado deverá retirar as baterias.

Para retirar a bateria:

1. Certifique-se de que as definições do produto permitem-lhe abrir a tampa sem iniciar o alarme de sabotagem (tamper).
2. Desligue a alimentação de corrente, se necessário, e retire a tampa.
3. Se necessário, remova a antepara da bateria, desapertando quatro parafusos.
4. Desligue a bateria. Tenha em atenção que, consoante o modelo da bateria, os conectores poderão estar localizados de maneira diferente.
5. Retire a bateria do suporte.

Elimine a bateria em conformidade com os regulamentos ou normas locais.

Para informação sobre a substituição de baterias, consulte as especificações do produto ou entre em contacto com a assistência técnica.

Montagem

A unidade é montada com parafusos ou pinos através dos orifícios de montagem na secção da retaguarda da cobertura.



Importante: Quando o produto é montado na parede, certifique-se de que suporta pelo menos 3 vezes o peso do produto. O peso do produto é o produto propriamente dito mais a bateria e acessórios.

Certifique-se de que a unidade é montada numa superfície vertical, sólida e plana, de forma que a base não se dobre ou distorça quando os parafusos de montagem são apertados.

Deixe um espaço de 50 mm entre as coberturas do equipamento montadas lado a lado e 25 mm entre a cobertura e a parede lateral.

A bateria recarregável não deve ser instalada até que o painel de controlo esteja preso à superfície de fixação. Em circunstância alguma o painel pode ser transportado com uma bateria instalada.

Certifique-se de que os terminais dos fios estão isolados. Recomenda-se a utilização de braçadeiras para segurar os cabos de forma organizada.

AVISO! Utilizar cabos em conformidade com a IEC 60332-1-2 e IEC 60332-1-3, ou IEC 60332-2-2, ou IEC TS 60695-11-21, ou UL 2556 VW-1. Utilizar cabos e ligações que possam suportar no mínimo a corrente de 2 A.

Directrizes gerais de instalação

Os painéis de controlo Advisor Advanced foram concebidos, montados e testados em conformidade com os requisitos das normas relevantes actuais de segurança, emissão e imunidade relativamente a interferências eléctricas e electromagnéticas do ambiente.

Se as seguintes directrizes forem seguidas, o sistema proporcionará muitos anos de serviço fiável.

Para além das directrizes indicadas a seguir, durante a instalação do painel de controlo Advisor Advanced, é essencial seguir quaisquer requisitos locais dependentes do país aplicáveis à instalação. Apenas um electricista qualificado ou outra pessoa com qualificações adequadas deverá efectuar a ligação deste sistema à corrente CA ou à rede pública de telefone.

- Certifique-se de que existe uma boa ligação à terra para o sistema de alarme.
- Mantenha separados os cabos de baixa tensão e os cabos de alimentação de corrente. Utilize pontos separados de entrada de cabos para a caixa do painel de controlo.

- Se forem utilizados os orifícios superiores e/ou inferiores de entrada de cabos na caixa para encaminhar os cabos para o painel de controlo, utilize sempre um sistema adequado de tubos de encaixe através de uma caixa de junção e condutores. Para este efeito, utilize apenas materiais da classe de inflamabilidades adequada (HB ou superior).
- Para a ligação da corrente eléctrica, utilize o terminal do conector de alimentação através de uma cablagem permanente ou de um cabo de alimentação flexível para ligar à tomada de corrente com ligação à terra. Utilize sempre braçadeiras para prender o cabo de alimentação ao ponto de fixação próprio disponível junto ao terminal do conector de alimentação eléctrica.
 - Ao instalar a cablagem fixa e permanente, insira um disjuntor geral dedicado e de fácil acesso na rede de distribuição de energia.
 - Nunca tente soldar os fios de ligação da corrente eléctrica nas extremidades onde os mesmos são ligados aos conectores dos terminais.
- Evite enrolar os fios dentro da caixa do painel de controlo e encaminhe os cabos de maneira que os mesmos não fiquem por cima ou por baixo da placa de circuito impresso. Recomenda-se a utilização de braçadeiras para segurar os cabos de forma organizada dentro da caixa.
- A bateria utilizada nesta unidade deve ser feita de materiais da classe de flamabilidade adequada (HB ou superior).
- Qualquer circuito ligado directamente aos contactos de relés do equipamento ou aos contactos de relés externos através da saída electrónica do equipamento deverá estar qualificado como um circuito operativo SELV (safety extra-low voltage - ultra baixa tensão de segurança).
 - Não deve estar instalado um relé de comutação de alimentação eléctrica no interior da caixa do painel de controlo.
 - Coloque sempre um díodo de supressão (por ex., um 1N4001) através da bobina de relé.
 - Utilize apenas relés com um bom isolamento entre os contactos e a bobina.
 - O comprimento máximo de cabo para ligação de uma saída de colectador aberto não pode exceder 30 m. Para distâncias maiores, utilize a expansão de saída de relé (por exemplo, expansor de quatro relés ATS624).
- A folga mínima entre as coberturas do equipamento é de 50 mm (entre as saídas de ventilação do equipamento).
- Utilize apenas estas unidades num ambiente limpo e não em ar húmido. Os requisitos ambientais são fornecidos em “Especificações” na página nº 37.
- Para ligações nos terminais do painel, o “torque” recomendado é de 0,3 a 0,4 N·m. Este valor de “torque” é independente da espessura (AWG) dos fios utilizados. O valor de 0,4 N·m é também o valor máximo de “torque” permitido para este conector.

Ligação à terra

AVISO: Devem ser seguidos os procedimentos correctos de ligação à terra.

Ligar à terra uma caixa que contém vários dispositivos

Todos os dispositivos concebidos para o sistema têm ligações à terra através de pernos metálicos ligados à caixa metálica. Certifique-se de que estes pernos metálicos têm uma boa ligação à caixa (tenha atenção à pintura). As ligações à terra de todas as peças de equipamento do sistema podem ser utilizadas para a ligação da malha dos cabos blindados. Certifique-se de que todos os cabos de ligação de proteção internos fazem uma ligação fiável com o cabo de ligação à terra de proteção do edifício.

Ligar painéis à terra num só edifício

Num edifício, várias caixas ou dispositivos têm ligação à terra para um ponto de terra seguro.

O ponto de terra seguro do edifício tem de ser inspeccionado por um empreiteiro licenciado.

Ligar painéis à terra em vários edifícios

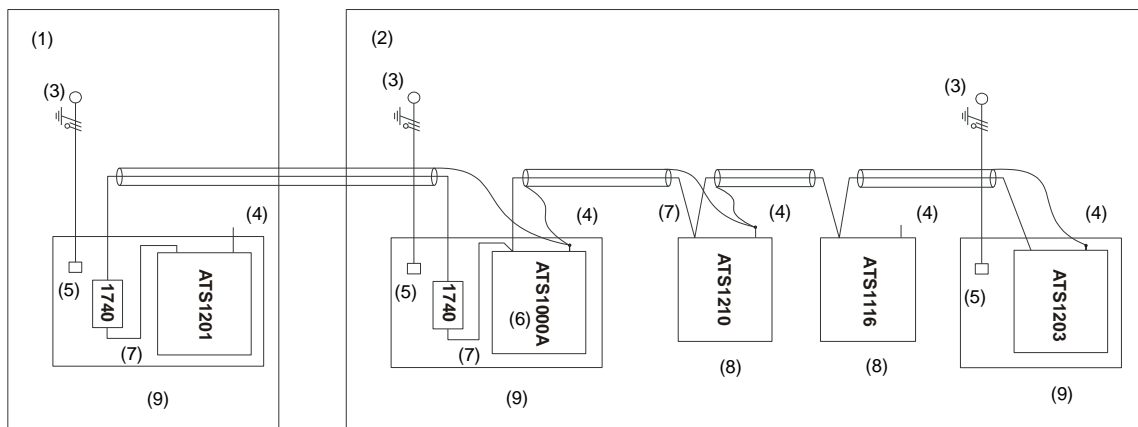
Se a cablagem se estender a vários edifícios, será utilizado no sistema mais do que um ponto de terra comum. Para isolar o databus do sistema, utilize isolador/repetidores ATS1740. Desta maneira o sistema está protegido contra variações da potencial terra.

Blindagem

A blindagem dos cabos blindados utilizados no sistema deverá ser ligada apenas a um lado do ponto de terra comum de um edifício (ver Figura 15 abaixo). Se um cabo databus blindado for encaminhado através de mais de um dispositivo plástico, a blindagem do cabo de entrada e de saída deve ser ligada.

Se for utilizada a ligação IP, certifique-se de que o cabo Ethernet FTP se mantém num único edifício. Utilize um router ou comutador para isolar os cabos Ethernet entre os vários edifícios.

Figura 15: Blindagem do sistema



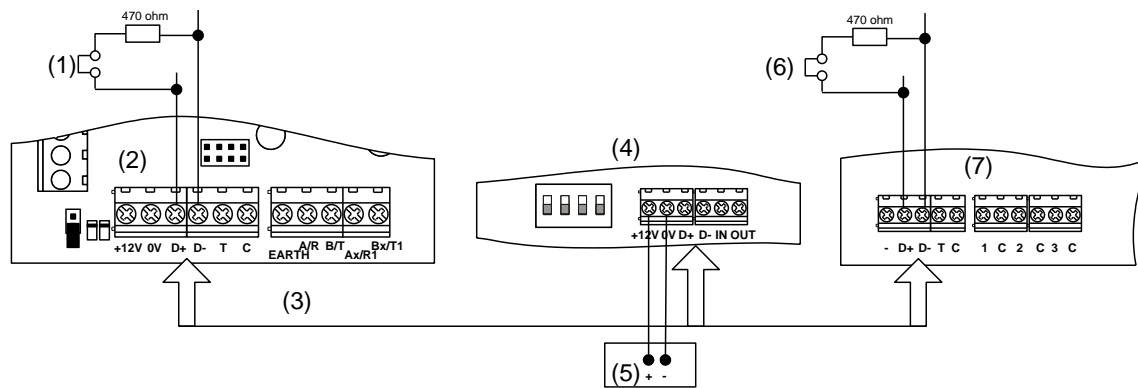
- | | |
|---|--|
| (1) Edifício 1 | (6) Painel de controlo Advisor Advanced. |
| (2) Edifício 2 | (7) Databus do sistema |
| (3) Alimentação de corrente eléctrica com terra local | (8) Dispositivo em caixa de plástico |
| (4) Borne de terra e blindagem | (9) Dispositivo em caixa metálica |
| (5) Conector de alimentação de corrente eléctrica | |

Cablagem do Advisor Advanced

Cablagem preferida do databus do sistema

O jumper de terminação (também chamado TERM link), ou DIP switch deve estar ON (ligado), ou deve ser instalada uma resistência de 470 Ω em cada um dos dispositivos nas extremidades do databus de ligação em cadeia. Numa configuração de ligação em estrela, o TERM link só é instalado nos dispositivos nas extremidades dos dois troços de cabo databus do sistema mais longos.

Figura 16: Cablagem do databus do sistema



- (1) TERM link instalado (primeiro dispositivo no databus local).
- (2) Variantes de painel de controlo Advisor Advanced.
- (3) O tipo de cabo de dados preferido é o WCAT 52 (dois pares entrançados).
- (4) Teclado LCD Advisor (o comutador TERM é definido como Desligado).
- (5) Fonte de alimentação separada de 12 V (necessária se o teclado estiver a mais de 100 m do painel ou do expansor mais próximo). Ligue o terminal negativo da fonte de alimentação ao fio “-” do databus.
- (6) TERM link instalado (último dispositivo no databus local).
- (7) Qualquer expansor remoto como o ATS1201(E) ou o ATS1210(E).

Ligação do databus do sistema

O databus do sistema é utilizado para ligar expansores remotos (para fornecer zonas extra) e teclados ao painel de controlo Advisor Advanced. Os dispositivos remotos podem encontrar-se a até 1,5 km de distância de um painel de controlo Advisor Advanced.

Os teclados e os expansores remotos devem ser ligados através de um cabo de dados blindado com dois pares entrançados da ligação do databus do sistema (recomenda-se o WCAT 52).

Recomendamos que utilize uma fonte de alimentação separada para um teclado, quando a distância entre o teclado e o dispositivo mais próximo for de mais de 100 metros.

Se o teclado for alimentado por uma fonte de alimentação separada, não ligue o “+” do databus do sistema. Ligue o “+” da fonte de alimentação local ao “+” do

teclado, e ligue os 0 volts da fonte de alimentação e os 0 volts do databus do sistema ao terminal do teclado marcado com um “-”. O número máximo e dispositivos permitidos no databus é indicado em “Características gerais” na página nº 39.

Dois databus do sistema (apenas ATS4500A)

Variantes específicas do painel permitem ligar mais dispositivos bus utilizando um segundo databus do sistema. Para instalar outro databus do sistema, utilize o segundo módulo de extensão RS485 LAN do painel,ATS670.

Os endereços de dispositivos ligados adicional (BUS2) são determinados pela adição de 16 ao endereço físico dos teclados, e 15 ao endereço dos expansores. Assim, BUS1 gere os teclados com os endereços de 1 a 16 e expansores de 1 a 15, enquanto que o BUS2 – teclados 17 a 32 e expansores de 16 a 30.

Nota: Os controladores de porta só podem ser instalados no BUS1.

Ligação das zonas

As entradas são configuradas como zonas EOL (fim de linha) padrão programadas livremente. Contudo, ao programar as zonas como zona dupla, todas as entradas da zona podem ser programadas para fornecer a indicação de alguns estados para a mesma zona.

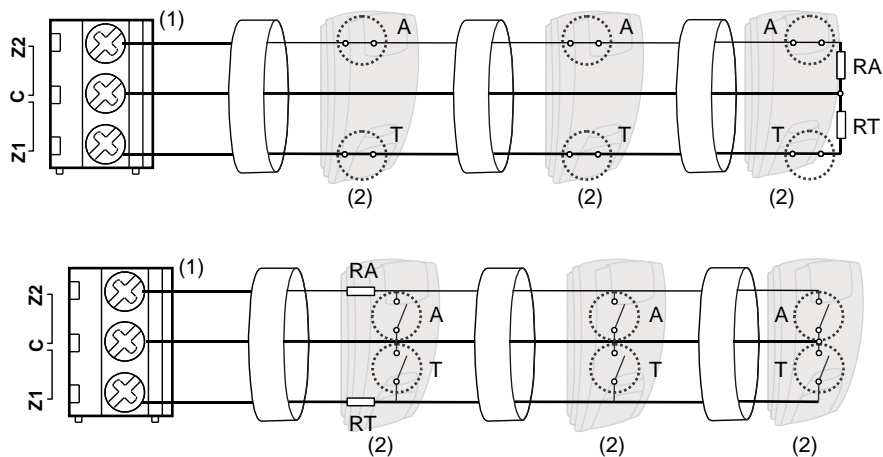
Consoante o modelo do detector, efectue o seguinte para configurar as zonas:

- Escolha o tipo de ligação EOL. Consulte “Tipos de ligação EOL” na página nº 29.
- Programe o modo de entrada. Consulte “8.6.1 Modo entrada” na página nº 302 para o painel, ou “2.2.2.n.4.5 Modo de input” na página nº 187 para os expansores.
- Defina os valores da resistência de fim de linha. Consulte “8.6.2 Resistência EOL” na página nº 302 para o painel, ou “2.2.2.n.4.6 EOL” na página nº 187 para os expansores.
- Configure a opção de anti-máscara. Consulte “4.1.n.6.7 Anti-Mask” na página nº 215.

Ligações de zona simples

Numa ligação de zona simples, são necessárias duas zonas, uma zona para o alarme e outra zona para o tamper. Os contactos de tamper são ligados em série com uma resistência EOL.

Figura 17: Exemplos de zona simples



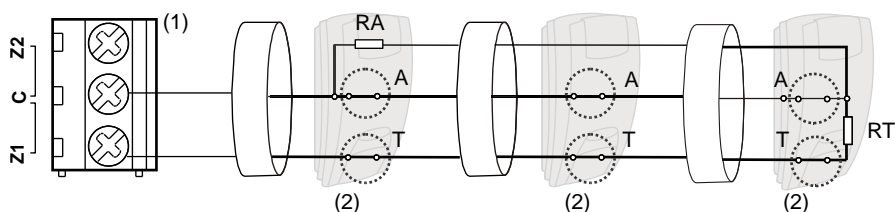
- | | |
|----------------------|------------------|
| (1) Terminal de zona | (2) Detector |
| C Terminal comum | A Relé de alarme |
| Z1 Entrada de zona 1 | T Relé de tamper |
| Z2 Entrada de zona 2 | |

Ligações de zona dupla

Na ligação de zona dupla, uma zona pode detectar alguns estados de detector. São utilizadas pelo menos duas resistências para definir estados de alarme e de tamper. Consoante as definições programadas, podem existir estados adicionais definidos como alarme de máscara ou falha de sensor. Esses estados podem ser os seguintes:

- Curto (tamper)
- Activo (alarme)
- Normal
- Máscara
- Falha de sensor
- Aberto (tamper)

Figura 18: Exemplo de zona dupla



- | | |
|----------------------|------------------|
| (1) Terminal de zona | (2) Detector |
| C Terminal comum | A Relé de alarme |
| Z1 Entrada de zona 1 | T Relé de tamper |
| Z2 Entrada de zona 2 | |

As ligações EOL possíveis são indicadas em “Tipos de ligação EOL” na página nº 29.

Valores de resistências de fim de linha

A lista que se segue contém os valores das resistências de fim de linha e possíveis estados de zona. São também indicados os valores de resistência e tensão medidos em toda a zona.

Consoante o tipo de entrada e a opção de anti-máscara, podem estar disponíveis os seguintes valores de EOL.

EOL	Detalhes de ligação [1]	Medição [2]	Estado da zona					
			Curto	Máscara	Normal	Alarme	Falha	Aberto
Simples NC (Item 1)								
Sem EOL		R (kΩ)	—	—	<1	>1	—	—
		U (V)	—	—	<3,5	>3,5	—	—
Nota: os valores de outras EOL são iguais a Duplo, mas todos os intervalos excepto normal são intervalos de alarmes.								
Simples NO (Item 2)								
Sem EOL		R (kΩ)	—	—	>19,66	<19,66	—	—
		U (V)	—	—	>11,14	<11,14	—	—
Nota: os valores de outras EOL são iguais a Duplo, mas todos os intervalos excepto normal são intervalos de alarmes.								
Duplo								
10K (Item 4)		R (kΩ)	<3,33	3,33– 6,67	6,67– 13,33	13,33– 26,67	—	>26,67
		U (V)	<5,70	5,70– 8,10	8,10– 10,20	10,20– 11,70	—	>11,70
4K7 (Item 3)		R (kΩ)	<1,00	—	1,00– 6,67	6,67– 16,84	—	>16,84
		U (V)	<2,41	—	2,41– 8,07	8,07– 10,74	—	>10,74
4K7 (Item 4)		R (kΩ)	<1,00	1,00– 3,42	3,42– 6,67	6,67– 16,84	—	>16,84
		U (V)	<2,41	2,41– 5,79	5,79– 8,07	8,07– 10,74	—	>10,74
4K7 (Item 7)		R (kΩ)	<1,00	16,84– 55,00	1,00– 6,67	6,67– 11,75	11,75– 16,84	>55,00
		U (V)	<2,41	10,74– 12,70	2,41– 8,07	8,07– 9,82	9,82– 10,74	>12,70
2K2 (Item 4)		R (kΩ)	<0,73	0,73– 1,47	1,47– 2,93	2,93– 5,87	—	>5,87
		U (V)	<1,90	1,90– 3,30	3,30– 5,30	5,30– 7,70	—	>7,70

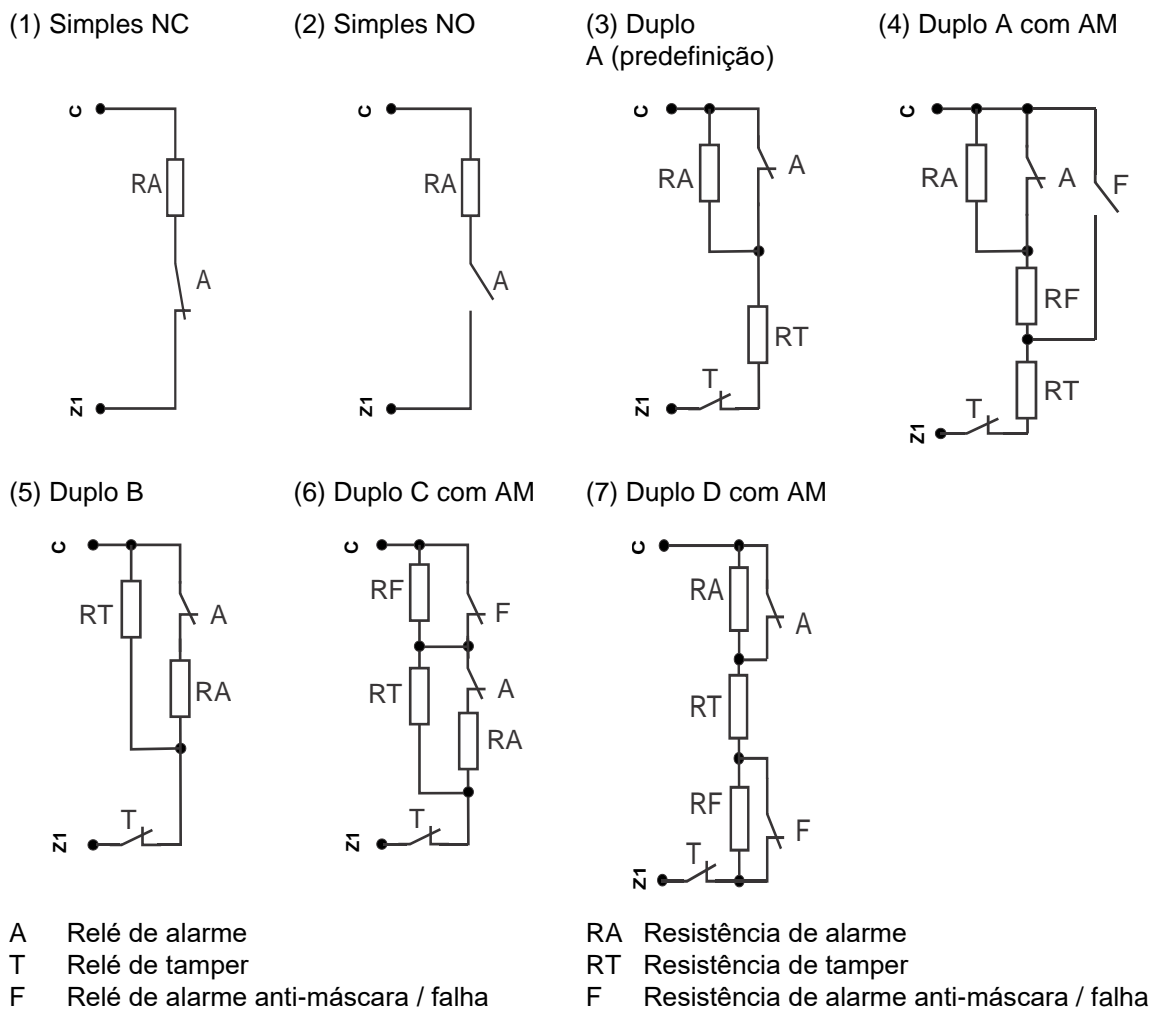
EOL	Detalhes de ligação [1]	Medição [2]	Estado da zona					
			Curto	Máscara	Normal	Alarme	Falha	Aberto
6K8	(Item 4)	R (kΩ)	<2,27	2,27– 4,53	4,53– 9,07	9,07– 18,13	—	>18,13
	RA=6,8 kΩ, RT=3,4 kΩ, RF=3,4 kΩ	U (V)	<4,50	4,50– 6,80	6,80– 9,10	9,10– 11,00	—	>11,00
5K6	(Item 4)	R (kΩ)	<1,87	1,87– 3,73	3,73– 7,47	7,47– 14,93	—	>14,93
	RA=5,6 kΩ, RT=2,8 kΩ, RF=2,8 kΩ	U (V)	<3,90	3,90– 6,10	6,10– 8,50	8,50– 10,50	—	>10,50
3K74	(Item 4)	R (kΩ)	<1,25	1,25– 2,45	2,45– 4,99	4,99– 9,98	—	>9,98
	RA=3,74 kΩ, RT=1,87 kΩ, RF=1,87 kΩ	U (V)	<2,90	2,90– 4,80	4,80– 7,10	7,10– 9,40	—	>9,40
3K3	(Item 4)	R (kΩ)	<1,10	1,10– 2,20	2,20– 4,40	4,40– 8,80	—	>8,80
	RA=3,3 kΩ, RT=1,65 kΩ, RF=1,65 kΩ	U (V)	<2,60	2,60– 4,40	4,40– 6,70	6,70– 9,00	—	>9,00
2K	(Item 4)	R (kΩ)	<0,67	0,67– 1,33	1,33– 2,67	2,67– 5,33	—	>5,33
	RA=2 kΩ, RT=1 kΩ, RF=1 kΩ	U (V)	<1,70	1,70– 3,00	3,00– 5,00	5,00– 7,30	—	>7,30
1K5	(Item 4)	R (kΩ)	<0,50	0,50– 1,00	1,00– 2,00	2,00– 4,00	—	>4,00
	RA=1,5 kΩ, RT=0,75 kΩ, RF=0,75 kΩ	U (V)	<1,30	1,30– 2,40	2,40– 4,10	4,10– 6,30	—	>6,30
2K2+4K7	(Item 3)	R (kΩ)	<3,60	—	3,60– 5,60	5,60– 8,20	—	>8,20
	RA=2,2 kΩ, RT=4,7 kΩ	U (V)	<6,00	—	6,00– 7,50	7,50– 8,80	—	>8,80
1K	(Item 7)	R (kΩ)	<0,51	4,52– 40,00	0,51– 1,52	1,52– 2,94	2,94– 4,52	>40,00
	RA=1 kΩ, RT=1 kΩ, RF=12 kΩ	U (V)	<1,35	6,24– 12,33	1,35– 3,36	3,36– 5,29	5,29– 6,74	>12,33
8K2	(Item 5)	R (kΩ)	<1,50	—	1,50– 5,84	5,84– 14,25	—	>14,25
	RA=8,2 kΩ, RT=8,2 kΩ	U (V)	<3,33	—	3,33– 7,52	7,52– 10,33	—	>10,33
8K2	(Item 6)	R (kΩ)	<1,50	14,25– 45,00	1,50– 5,84	5,84– 10,07	10,07– 14,25	>45,00
	RA=8,2 kΩ, RT=8,2 kΩ, RF=8,2 kΩ	U (V)	<3,33	10,33– 12,48	3,33– 7,52	7,52– 9,37	9,37– 10,33	>12,48

- [1] Consulte a Figura 19 abaixo.
- [2] Resistência de zona R (kΩ), tensão de zona U (V).
- O estado não está disponível

Tipos de ligação EOL

As seguintes ligações de EOL são utilizadas para diferentes tipos de entrada e valores de EOL. Consulte “Valores de resistências de fim de linha” na página nº 27 para obter mais informações.

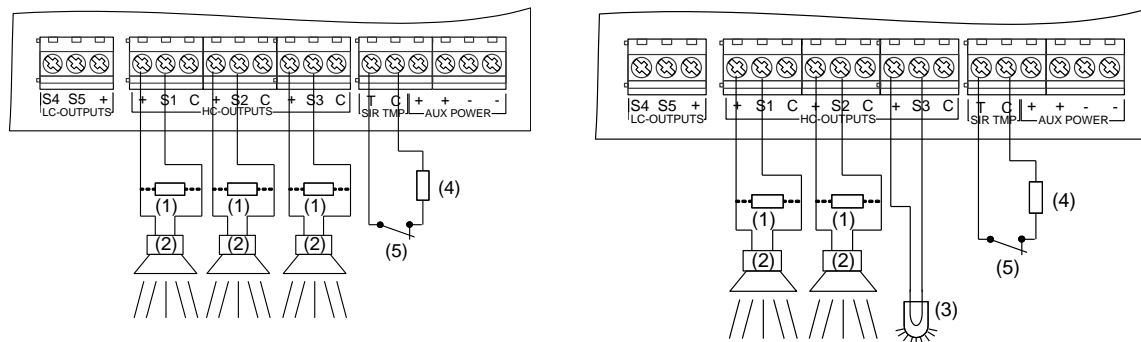
Figura 19: Tipo de ligação



Cuidado: Ao usar os tipos de ligação (4), (6) e (7), a opção de anti-máscara da zona tem de estar habilitada. As outras zonas têm de ter esta opção desabilitada. Consulte “4.1.n.6.7 Anti-Mask” na página nº 215.

Ligação da sirene

Figura 20: Exemplos de ligação da sirene



- (1) Resistência do EOL da sirene (1 kΩ). Tem de ser instalada se a sirene não contiver uma resistência incorporada.
- (2) Sirene.

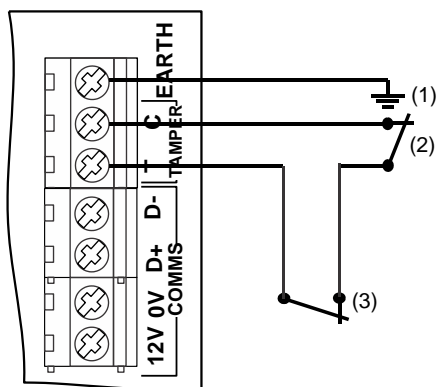
- (3) Flash.
- (4) Resistência EOL de tamper da sirene.
- (5) Tamper da sirene (normalmente fechado).

Nota: A saída da sirene pode ser configurada como interna ou externa. Isto é efectuado através das definições do painel, e não através da configuração do hardware do painel. Consulte “Atribuições de saídas predefinidas” na página nº 33 e “Saídas” na página nº 79.

Outras ligações

Ligação de tamper

Figura 21: Ligação à terra e tamper no ATsx500A(-IP)



- (1) Ligação à terra
- (2) Tamper externo (normalmente fechado)
- (3) Tamper tipo “pry-off” (remoção) opcional (normalmente fechado) exigido pelos regulamentos EN 50131 Grau 3 e VdS-C

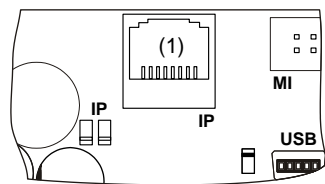
Ligação RTPC

Para ligar a RTPC nos painéis de controlo ATsx500A(-IP), utilize o módulo ATS7700 RTPC. Consulte a *Ficha de Instalação do Módulo ATS7700 RTPC* para mais informações.

Cuidado: Se a linha RTPC for fornecida através da rede ADSL, certifique-se de que é utilizado pelo menos o separador/filtro, caso contrário a qualidade da comunicação RTPC poderá ser muito baixa para um reporte fiável.

Ligação da Ethernet

Figura 22: Ligação da Ethernet



(1) RJ45 Ethernet

A porta Ethernet é uma ligação de base IEEE 802.3u que suporta velocidades de ligação 10BASE-T ou 100BASE-TX.

Para as ligações Ethernet utilize apenas cabo do tipo FTP Cat 5e.

Configuração

Valores predefinidos do painel

Ao ligar o painel pela primeira vez, o sistema pede-lhe para escolher as predefinições apropriadas. Escolha as definições correctas de acordo com os regulamentos locais. O painel conclui então o processo de instalação. Para mais detalhes, consulte “Arranque inicial” na página nº 142.

Nota: Pelo menos um teclado com um LCD deve ser ligado ao databus do sistema.

Configuração de zonas

Expansão interna

O número de zonas ligadas directamente ao painel de controlo pode ser expandido utilizando o módulo ATS608. A capacidade máxima de zonas internas para cada painel de controlo é indicada na “Especificações > Características gerais” na página nº 39.

Expansão externa

Podem ser utilizados expansores para expandir os painéis de controlo Advisor Advanced com zonas externas. O número máximo de zonas para cada painel de controlo é indicado na “Especificações > Características gerais” na página nº 39.

Um expansor padrão pode ter oito zonas ligadas ao mesmo. Algumas zonas podem ser expandidas em incrementos de 8, até 32, portanto um expansor pode ter 8, 16, 24 ou 32 zonas.

Nota: A capacidade de zonas é o número de zonas configuráveis do sistema. Essas zonas podem estar localizadas em qualquer entrada disponível. Consulte “Especificações > Características gerais” na página nº 39.

Saídas

Na PCI de um painel existem 5 saídas. Pode ser utilizado um expansor de saídas para acrescentar outras 16 saídas ao interior do painel.

São utilizados controladores de saídas para expandir o número de saídas de um expansor. Um controlador de saídas do expansor expande as saídas para 8. Um expansor pode ter dois controladores de saídas ligados, aumentando as saídas para um máximo de 16 por expansor.

Um teclado só pode ter uma saída na versão de painel actual.

O número máximo de saídas para cada painel de controlo é indicado na “Especificações > Características gerais” na página nº 39.

Notas

- A saída de baixa corrente S4 está activa quando o sistema está pronto a armar. A saída de baixa corrente S5 está activa quando o sistema está armado.
- Defina a saída de teclado 7 para activar o som contínuo de besouro do teclado, ou a saída 8 para activar o som intermitente.

Saídas de sirene

O endereço das saídas de sirene do painel de controlo Advisor Advanced iniciam-se em 1 (consulte a Tabela 2 abaixo).

Em expansores com saídas de sirene, a saída 16 é a saída de sirene.

Para activar a saída de sirene, a saída programada deve ter atribuído o filtro de condição necessário (definido por um evento de alarme ou um evento de sirene, consoante as definições de preferências). Para mais detalhes, consulte “Saídas” na página nº 79.

Atribuições de saídas predefinidas

As atribuições de saídas predefinidas são indicadas na Tabela 2 abaixo.

Tabela 2: Atribuições de saídas predefinidas

Saída	Nome	Tipo	Função de saída predefinida
Painel 1	S1	Saída de alta corrente	EN 50131 Grau 3: Saída de sirene interna S1 VdS: Saída de sirene externa S1
Painel 2	S2	Saída de alta corrente	EN 50131 Grau 3: Saída de sirene externa S1 VdS: Saída de sirene externa S2
Painel 3	S3	Saída de alta corrente	EN 50131 Grau 3: Saída de sirene programável VdS: Saída de estroboscópio externo S3
Painel 4	S4	Saída de baixa corrente	A1 pronto a armar
Painel 5	S5	Saída de baixa corrente	A1 armado
Teclado 7	—	Virtual	Som contínuo do besouro
Teclado 8	—	Virtual	Som intermitente do besouro

Nota: as atribuições de saídas poderão necessitar de ajustes para estar em conformidade com as normas EN 50131 ou VdS.

Endereçamento de zonas, saídas e portas

Zonas e saídas

A tabela abaixo mostra o endereçamento de zonas e saídas no sistema Advisor Advanced.

Nota: esta é a numeração predefinida num esquema clássico de numeração. Para alterá-lo e criar objectos com uma numeração independente das entradas ou saídas físicas, utilize o menu “8.7.9 Esquema Objeto” na página nº 308.

Tabela 3: Numeração de zonas e saídas

Dispositivo	Zonas	Saídas	Dispositivo	Zonas	Saídas
Painel	1–8	1–8	2 placas de relé ATS1810	N/A	17–24 [1]
Expansor de entrada (ATS608)	9–16	N/A	Expansor de saída (ATS62x)	N/A	9–16 [2]
DGP 1	17–48	17–48	Teclado 1	N/A	1001–1008
DGP 2	49–80	49–80	Teclado 2	N/A	1009–1016
DGP 3	81–112	81–112	Teclado 3	N/A	1017–1024
DGP 4	113–144	113–144	Teclado 4	N/A	1025–1032
DGP 5	145–176	145–176	Teclado 5	N/A	1033–1040
DGP 6	177–208	177–208	Teclado 6	N/A	1041–1048
DGP 7	209–240	209–240	Teclado 7	N/A	1049–1056
DGP 8	241–272	241–272	Teclado 8	N/A	1057–1064
DGP 9	273–304	273–304	Teclado 9	N/A	1065–1072
DGP 10	305–336	305–336	Teclado 10	N/A	1073–1080
DGP 11	337–368	337–368	Teclado 11	N/A	1081–1088
DGP 12	369–400	369–400	Teclado 12	N/A	1089–1096
DGP 13	401–432	401–432	Teclado 13	N/A	1097–1104
DGP 14	433–464	433–464	Teclado 14	N/A	1105–1112
DGP 15	465–480 [3]	465–496	Teclado 15	N/A	1113–1120
DGP 16 [4]	497–528	497–528	Teclado 16	N/A	1121–1128
DGP 17	529–560	529–560	Teclado 17 [4]	N/A	1129–1136
DGP 18	561–592	561–592	Teclado 18	N/A	1137–1144
DGP 19	593–624	593–624	Teclado 19	N/A	1145–1152
DGP 20	625–656	625–656	Teclado 20	N/A	1153–1160
DGP 21	657–688	657–688	Teclado 21	N/A	1161–1168
DGP 22	689–720	689–720	Teclado 22	N/A	1169–1176
DGP 23	721–752	721–752	Teclado 23	N/A	1177–1184
DGP 24	753–784	753–784	Teclado 24	N/A	1185–1192
DGP 25	785–816	785–816	Teclado 25	N/A	1193–1200
DGP 26	817–848	817–848	Teclado 26	N/A	1201–1208
DGP 27	849–880	849–880	Teclado 27	N/A	1209–1216
DGP 28	881–912	881–912	Teclado 28	N/A	1217–1224
DGP 29	913–944	913–944	Teclado 29	N/A	1225–1232

Dispositivo	Zonas	Saídas	Dispositivo	Zonas	Saídas
DGP 30	945–976	945–976	Teclado 30	N/A	1233–1240
			Teclado 31	N/A	1241–1248
			Teclado 32	N/A	1249–1256

- [1] Os estados das saídas 17 a 24 são duplicados nos relés ATS1810 e nas saídas do DGP 1.
- [2] Ao utilizar o cartão de relé ATS624 com o expansor ATS1810 ligado, o estado da saída 8 do expansor é invertido.
- [3] Entradas 17 a 32 do expansor 15 não podem ser utilizadas.
- [4] Não é possível ligar mais do que 15 expansores e 16 teclados a um databus do sistema. Para ligar mais dispositivos bus a um painel, é necessário instalar um segundo módulo de extensão LAN RS485 do painel, ATS670. Consulte também “Dois databus do sistema” na página nº 25.

Portas

Existem dois tipos de portas: tipo inteligente e tipo padrão. As portas padrão (1 a 16) são controladas pelo painel de controlo. Os teclados ou leitores 1 a 32 ligados aos databus do sistema do painel de controlo Advisor Advanced, são utilizados para funções simples de controlo de acesso.

As portas inteligentes (17 a 64) são controladas por controladores de portas. Os teclados ou leitores ligados aos databus locais dos controladores de portas designam-se por “leitores de controladores de portas (leitores CP)” e são utilizados para funções avançadas de controlo de acesso.

Consulte “Portas” na página nº 80 para obter mais informações.

A Tabela 4 abaixo mostra a numeração de portas, zonas e saídas para controladores de portas.

Tabela 4: Numeração de portas, zonas e saídas dos controladores de portas

Controlador de portas	Portas	Zonas	Saídas
1	17-20	17-48	17-48
2	21-24	49-80	49-80
3	25-28	81-112	81-112
4	29-32	113-144	113-144
5	33-36	145-176	145-176
6	37-40	177-208	177-208
7	41-44	209-240	209-240
8	45-48	241-272	241-272
9	49-52	273-304	273-304
10	53-56	305-336	305-336
11	57-60	337-368	337-368
12	61-64	369-400	369-400

A Tabela 5 abaixo mostra a atribuição predefinida de zonas e saídas para controladores de portas.

Tabela 5: Atribuição predefinida de zonas e saídas para controladores de portas

Função	Porta	Controlador de portas											
		1	2	3	4	5	6	7	8	9	10	11	12
Relé de desbloqueio	1ª porta	17	49	81	113	145	177	209	241	273	305	337	369
	2ª porta	18	50	82	114	146	178	210	242	274	306	338	370
	3ª porta	19	51	83	115	147	179	211	243	275	307	339	371
	4ª porta	20	52	84	116	148	180	212	244	276	308	340	372
Zona nº	1ª porta	17	49	81	113	145	177	209	241	273	305	337	369
	2ª porta	19	51	83	115	147	179	211	243	275	307	339	371
	3ª porta	21	53	85	117	149	181	213	245	277	309	341	373
	4ª porta	23	55	87	119	151	183	215	247	279	311	343	375
N.º de zona DOTL	1ª porta	17	49	81	113	145	177	209	241	273	305	337	369
	2ª porta	19	51	83	115	147	179	211	243	275	307	339	371
	3ª porta	21	53	85	117	149	181	213	245	277	309	341	373
	4ª porta	23	55	87	119	151	183	215	247	279	311	343	375
Nº zona pedido de saída	1ª porta	18	50	82	114	146	178	210	242	274	306	338	370
	2ª porta	20	52	84	116	148	180	212	244	276	308	340	372
	3ª porta	22	54	86	118	150	182	214	246	278	310	342	374
	4ª porta	24	56	88	120	152	184	216	248	280	312	344	376
N.º de zona de shunt	1ª porta	17	49	81	113	145	177	209	241	273	305	337	369
	2ª porta	19	51	83	115	147	179	211	243	275	307	339	371
	3ª porta	21	53	85	117	149	181	213	245	277	309	341	373
	4ª porta	23	55	87	119	151	183	215	247	279	311	343	375

A Tabela 6 abaixo mostra a atribuição predefinida de leitores de databus locais dos controladores de portas a portas específicas.

Tabela 6: Atribuição predefinida de portas para controladores de portas

Função do leitor	Leitor de ENTRADA	Leitor de ENTRADA 2	Leitor de SAÍDA	Leitor de SAÍDA 2
1ª porta	1	5	9	13
2ª porta	2	6	10	14
3ª porta	3	7	11	15
4ª porta	4	8	12	16

Especificações

Para uma lista dos modelos de painéis, consulte “Lista de variantes do painel” na página nº iii.

Especificações de alimentação eléctrica

Tensão de entrada de corrente	230 V CA +10%, -15%, 50/60 Hz ±10%
Consumo de corrente a 230 V CA:	
ATS1500A(-IP)	Máx. 150 mA
ATS3500A(-IP), ATS4500A-IP	Máx. 300 mA
Saída do transformador	
ATS1500A-SM/LP	20 VAC, 31 VA
ATSx500A(-IP)-MM/MM+/LM	23 VAC, 58 VA
ATS3500A(-IP)-LP	22 VAC, 53 VA
Fabricante e tipo do transformador	
ATS1500A(-IP)-SM/LP	Aritech 1070366
ATSx500A(-IP)-MM/MM+/LM	Aritech 22-183
ATS3500A(-IP)-LP	Aritech 22-167

Especificações da fonte de alimentação

Tipo de fonte de alimentação	Tipo A em conformidade com EN 50131-6 Tipo I em conformidade com VdS 2115
Tensão [1]	13,8 V $\overline{=}$ ±0,2 V
Corrente de alimentação eléctrica:	
ATS1500A(-IP)	1,10 A máx. a 13,8 V $\overline{=}$ ±0,2 V
ATS3500A(-IP)	2,10 A máx. a 13,8 V $\overline{=}$ ±0,2 V
ATS4500A-IP	2,65 A máx. a 13,8 V $\overline{=}$ ±0,2 V
Consumo da placa principal (alarme/inativo):	
ATSx500A	100 mA a 13,8 V $\overline{=}$ ±0,2 V
ATSx500A-IP	150 mA a 13,8 V $\overline{=}$ ±0,2 V
Corrente máxima disponível no sistema [2]:	
ATS1500A	1.000 mA a 13,8 V $\overline{=}$ ±0,2 V
ATS1500A-IP	950 mA a 13,8 V $\overline{=}$ ±0,2 V
ATS3500A	2.000 mA a 13,8 V $\overline{=}$ ±0,2 V
ATS3500A-IP	1.950 mA a 13,8 V $\overline{=}$ ±0,2 V
ATS4500A-IP	2.500 mA a 13,8 V $\overline{=}$ ±0,2 V
Saída de alimentação auxiliar (AUX. POWER) [3]	13,8 V $\overline{=}$ ±0,2 V, 1 A máx.
Saída de alimentação da bateria (BAT) [4]	13,8 V $\overline{=}$ ±0,2 V, 2,5 A máx.

Tipo de bateria	Bateria de ácido de chumbo, recarregável: [5] 7,2 Ah, 12 V nom. (BS127N) 12 Ah, 12 V nom. (BS130N) 18 Ah, 12 V nom. (BS131N) 26 Ah, 12 V nom. (BS129N) 36 Ah, 12 V nom. (BS134N)
Duração da bateria em utilização em modo de espera [6]:	
Típico	3 anos em condições de carga flutuante a 20 °C
Máximo	5 anos
Ciclo de utilização de duração da bateria	200 ciclos com descarga de 100% 225 ciclos com descarga de 80% 500 ciclos com descarga de 50%
Tipo de cabos da bateria	Aritech 160319999-1
Tensão máxima na fonte de alimentação, saída de alimentação de energia auxiliar e saída de alimentação da bateria	14,5 V _{DC}
Condição de bateria baixa	De 9,5 V _{DC} a 10,5 V _{DC}
Teste de bateria, nível [7]	11,2 V
Tensão mínima (carregamento da bateria) na fonte de alimentação, saída de alimentação de energia auxiliar e saída de alimentação da bateria [8][9]	9,45 V _{DC}
Tensão de ondulação máxima V _{pp} [10]	100 mV (típico), 300 mV (máx.)
Valor de accionamento de sobretensão [11]	15,5 V _{DC} (mín.)
Tensão de falha da fonte de alimentação	< 9,45 V durante 10 s

- [1] A tensão normal é monitorizada em conformidade com os regulamentos de EN 50131 Grau 3 e VdS-C.
- [2] Corrente disponível para saídas de alimentação auxiliar e de carregamento da bateria.
- [3] Corrente permanente máxima para alimentar dispositivos externos do equipamento de controlo na ausência de condições de alarme. A soma da corrente de saída auxiliar e da corrente de saída COMM não pode exceder a corrente máxima especificada em “Corrente auxiliar e capacidade da bateria” na página nº 41.
- [4] A saída de bateria fornece protecção contra curto-circuito da bateria (em conformidade com os requisitos VdS).
- [5] As caixas aplicáveis para baterias específicas são especificadas em “Corrente auxiliar e capacidade da bateria” na página nº 41.
- [6] A temperatura alta e vários ciclos de carga podem reduzir significativamente o tempo de vida útil da bateria. Consulte as especificações da bateria para obter mais informações.
- [7] Se, durante um teste da bateria manual ou programado, a tensão da bateria ficar abaixo limiar, o teste de bateria falha.
- [8] Um mecanismo de protecção contra descarga profunda controla a tensão da bateria e desliga a bateria se a tensão descer abaixo do valor indicado, conforme exigido pelos regulamentos de EN 50131 Grau 3 e VdS-C.
- [9] É gerada uma mensagem de falha específica quando qualquer saída falha.
- [10] Tensão de ondulação máxima apenas quando a bateria está a ser carregada.
- [11] Um mecanismo de protecção contra sobretensão controla a tensão da fonte de alimentação e desliga a PSU se a tensão subir acima do valor indicado, conforme exigido pelos regulamentos de EN 50131 Grau 3 e VdS-C.

Características gerais	ATS1500A(-IP)	ATS3500A(-IP)	ATS4500A-IP
Combinações de código	De 10.000 (4 dígitos) a 10 milhares de milhões (10 dígitos)		
Resistência fim-de-linha	1,5 kΩ, 2 kΩ, 2,2 kΩ, 3,3 kΩ, 3,74 kΩ, 4,7 kΩ (predefinição), 5,6 kΩ, 6,8 kΩ, 10 kΩ		
Zonas no equipamento	8 (expansível até 16 com 1X ATS608)		
Número máximo de zonas	32	128	512
Saídas no equipamento	5 (expansível para 9 com 1X ATS624, ou para 21 com 1X ATS626). Consulte “Saídas standard no equipamento” na página nº 40.		
Número máximo de saídas	128		
Áreas	4	8	64
Grupos área	—	—	64
Número máximo de RAS / teclados	8	16	32 [1]
Número máximo de DGP / expansores	7	15	30 [1]
[1] É necessário instalar um segundo módulo de extensão RS485 LAN do painel, ATS670 para ligar mais de 16 RASs e 15 DGPs.			
Número máximo de utilizadores	2000, que inclui: -1000 utilizadores com dados completos -1000 utilizadores apenas com cartões		
Número máximo de utilizadores (para utilizadores com funcionalidade SMS e reporte de voz)	16	64	128
Inibir / isolar / limite de shunt, máx.	32	128	512
Programas	24		
Janelas de tempo	4 por programa		
Dias especiais	8		
Ações por programa	20		
Capacidade de registo de eventos Nota: consulte também “Eventos” na página nº 93.	24500, que inclui: - 10000 eventos obrigatórios - 1500 eventos não obrigatórios - 10000 eventos de acesso - 1000 eventos de instalador - 1000 eventos de comunicador - 1000 eventos estendidos		
Retenção de dados (registo, definições de programação)	20 anos		
Funcionalidades de controlo de acesso	ATS1500A(-IP)	ATS3500A(-IP)	ATS4500A-IP
Controladores de portas suportados	7	12	12
Portas padrão	4	8	16

Portas inteligentes:			
CDC4 modo standard	28	48	48
CDC4 modo alargado	28	96	96
Regiões	256		
Grupos de portas	128		
Pisos	64		
Grupos de pisos	128		
Número máximo de utilizadores (com controladores de portas ligados):			
CDC4	65532		
ATS125x sem IUM	2000		
ATS1250 com ATS1831 IUM	17488		
ATS1250 com ATS1832 IUM	65532		

Nota: as funcionalidades de SMS e reporte de voz só estão disponíveis para um número limitado de utilizadores. O número máximo de utilizadores com funcionalidade total de controlo e reporte é indicado em “Características gerais” na página nº 39.

Caraterísticas de áudio

Número máximo de dispositivo de áudio	8	16	32
---------------------------------------	---	----	----

Caraterísticas UltraSync

Número máximo de notificações push	16
------------------------------------	----

Ligação da Ethernet (ATSx000-IP)

Norma suportada	IEEE 802.3u
Velocidade	10BASE-T ou 100BASE-TX
Duplex	Half-duplex e full-duplex
Cablagem	Cabo FTP (par entrançado com blindagem envolvente) Cat 5e ou melhor
Auto-negociação	MDIX

Saídas standard no equipamento

S1, S2, S3	Saída electrónica de corrente alta , classificação: 1 A a 13,8 V
S4, S5 [1]	Saída electrónica de corrente baixa, classificação: 50 mA a 13,8 V

[1] O comprimento máximo de cabo para conexão de saída de baixa corrente não pode exceder 30 m. Para distâncias maiores, utilize a expansão de saída de relé (por exemplo, expansor de quatro relés ATS624).

Características ambientais

Temperatura de operação	0 a +40°C
Temperatura testada em conformidade com EN 50131	-10 a +55°C
Humidade	95% sem condensação
Grau de protecção IP	IP31
Cor	Bege

Dimensões	Consulte “Lista de variantes do painel” na página nº iii
Grau e classe EN 50131	ATS1500A(-IP): Grau 2, Classe II ATS3500A(-IP): Grau 3, Classe II ATS4500A-IP: Grau 3, Classe II Nota: ATS1500A(-IP)-MM pode ser actualizado para uma configuração EN de Grau 3 com a utilização do kit de tamper ATS-MM-TK. ATS1500A(-IP)-SM pode ser actualizado para uma configuração EN de Grau 3 com a utilização do kit de tamper ATS-SM-TK.
Classe de segurança	Classe I
Tipo de caixa	Caixa (cumpre UL94V-0)
Tipos de cabos de ligação à terra	Aritech 160558999-1
Categoria de sobretensão	Categoria II
Altitude máxima, ou pressão de ar mínima	2000 m acima do nível médio do mar

Fusíveis do painel de controlo

Bateria	ATS1500A(-IP), ATS3500A(-IP): 2 A, com rearme ATS4500A(-IP): 3 A, com rearme
Aux. 12 V	1 A, com rearme
Databus do sistema	1 A, com rearme
Sirene 1, saída de corrente alta S1	1 A, com rearme
Sirene 2, saída de corrente alta S2	1 A, com rearme
Sirene 3, saída de corrente alta S3	1 A, com rearme
Alimentação eléctrica, fusível de alimentação eléctrica	ATS1500A(-IP)-SM/LP: Lento T-160 mA, 230 VAC, Aritech 33-119 ATS1500A(-IP)-MM, ATS3500A(-IP), ATS4500A-IP: Lento T-315 mA, 230 VAC, Aritech 33-118

O fusível de rede faz parte do bloco de terminais de rede Aritech 120494888.

AVISO: Antes de retirar o fusível de alimentação eléctrica, a alimentação de corrente tem de ser desligada (consultar “Ligação à corrente eléctrica” na página nº 17).

Corrente auxiliar e capacidade da bateria

Tabela 7: Corrente auxiliar máxima disponível do ATS1500A(-IP)

Bateria, Ah:			7,2	12	18
Caixa aplicável			SM, MM, LP	LP	MM
Aprovação de segurança / Grau	Tempo de descarga (h)	Tempo de carregamento (h)	Corrente auxiliar, mA		
EN Grau 2	12	72	450	750	750

Bateria, Ah:			7,2	12	18
Caixa aplicável			SM, MM, LP	LP	MM
Aprovação de segurança / Grau	Tempo de descarga (h)	Tempo de carregamento (h)	Corrente auxiliar, mA		
INCERT Grau 2	24	48	150	350	570
INCERT Grau 3	60	24	—	—	150
EN Grau 3, VdS-B	30	24	90	250	350
NF&A2P Grau 2 (EN+RTC)	36	72	—	180	350
NF&A2P Grau 3 (EN+RTC), VdS-C	60	24	—	—	150

Tabela 8: Corrente auxiliar máxima disponível do ATS3500A(-IP)

Bateria, Ah:			7,2	12	18
Caixa aplicável			MM, LP	LP	MM
Aprovação de segurança / Grau	Tempo de descarga (h)	Tempo de carregamento (h)	Corrente auxiliar, mA		
EN Grau 2	12	72	450	850	1350
INCERT Grau 2	24	48	150	350	600
INCERT Grau 3	60	24	—	—	150
EN Grau 3, VdS-B	30	24	90	250	450
NF&A2P Grau 2 (EN+RTC)	36	72	—	180	350
NF&A2P Grau 3 (EN+RTC), VdS-C	60	24	—	—	150

Tabela 9: Corrente auxiliar máxima disponível do ATS4500A-IP

Bateria, Ah:			12	18	25	36
Caixa aplicável			LM	MM+, LM	LM	LM
Aprovação de segurança / Grau	Tempo de descarga (h)	Tempo de carregamento (h)	Corrente auxiliar, mA			
EN Grau 2	12	72	850	1350	1600	1600
INCERT Grau 2	24	48	350	600	890	1350
INCERT Grau 3	60	24	—	150	260	450
EN Grau 3, VdS-B	30	24	250	450	675	1000
NF&A2P Grau 2 (EN+RTC)	36	72	180	350	540	850
NF&A2P Grau 3 (EN+RTC), VdS-C	60	24	—	150	260	450

Nota: a bateria 18 Ah bloqueia alguns orifícios de entrada na caixa MM.

Exemplo de ATS1500A(-IP) EN Grau 2

Quando utilizar backup de bateria conforme especificado para EN Grau 2 utilizando uma bateria de 12 Ah, a corrente auxiliar máxima disponível é de 750 mA.

Exemplo de AT3500A(-IP) EN Grau 3

Quando utilizar backup de bateria conforme especificado para EN Grau 3 utilizando uma bateria de 18 Ah, a corrente auxiliar máxima disponível é de 450 mA.

Esta corrente é a corrente total máxima disponível que pode ser utilizada para componentes auxiliares, tais como:

- DGPs / RASs no databus do sistema Advisor Advanced
- Detectores na saída de alimentação auxiliar
- Dispositivos de comunicação via bus MI (ex. GSM, IP)

Corrente utilizada temporariamente, como por exemplo: As sirenes e os estroboscópios não estão incluídos.

O valor nominal dos fusíveis tem de ser considerado.

Informação do estado da bateria

São disponibilizados diversos modos de detecção, para entender o estado de uma bateria.

Será utilizado um pequeno teste de bateria, para detectar, dentro de 10 segundos, o seguinte:

- Falha de bateria (ou falta de bateria), para informar o instalador de que não existe bateria ou de que a bateria ligada está fraca. O evento será registado e notificado.
- Bateria fraca, assim que a bateria fica abaixo de 10,5 V com ou sem corrente. O evento será registado, notificado e comunicado.

Será utilizado um outro teste de bateria, uma vez por dia, para entender ainda melhor o estado da bateria. Caso a bateria acabe, será registada, notificada e comunicada uma mensagem de falha de bateria.

Monitorização do sistema

O sistema proporciona a monitorização dos seguintes itens:

Tabela 10: Itens monitorizados

Função de monitorização	Mensagem	Causa
Corrente AC	Falha na alimentação de corrente	Perda de fonte de alimentação externa [1][2]
Bateria	Bateria baixa	Tensão baixa da bateria [1]

Função de monitorização	Mensagem	Causa
	Falha do teste de bateria	Bateria gasta Falha do carregador da bateria
	Falha de saída de alimentação/fusível	Sobrecarga da saída
Saídas de alimentação	Falha de saída de alimentação/fusível	Fusível queimado Perda de fusível Curto-circuito Sobrecarga
Fonte de alimentação	Falha de saída de alimentação/unidade de potência	Falha da unidade de potência Sobretensão
Tampers	Tamper de dispositivo	Sabotagem do dispositivo

- [1] Falha de corrente e Bateria fraca acabará por resultar na Protecção contra descarga profunda da bateria.
- [2] É apresentada uma mensagem de falha da rede elétrica caso ocorrem problemas com a alimentação CA ou falhas na PSU. Visualize o registo de eventos do painel para identificar a origem da falha.

Capítulo 3

Funções do sistema

Resumo

Esta secção apresenta e descreve todas as funcionalidades e funções dos painéis de controlo Advisor Advanced.

Nota: funcionalidades específicas poderão não estar disponíveis consoante a variante do painel, a versão de firmware ou a configuração do hardware.

Índice

Lista de funções	47
Zonas	49
Tipos de zonas	49
Áreas	55
Arme e desarme	57
Desarme retardado	58
Inibir e isolar	60
Inibir	60
Isolamento	60
Inibição de zonas	60
Teclas	62
Sequências de teclas comuns do teclado LCD	62
Sequências de teclas comuns do teclado sem LCD	64
Teclas de funções	65
Dispositivos	67
Bus - enumeração	67
Adicionar um teclado com um endereço superior	67
Teclados	68
Expansores	68
Dispositivos de áudio	68
Utilizadores	69
Utilizadores predefinidos	69
Bloqueio de dados do utilizador	70
Grupos de utilizadores	72
PIN	77
Saídas	79

Controlo de acesso	80
Controlador de portas	80
Portas	80
Grupos de portas	81
Pisos	81
Grupos de pisos	81
Funções básicas de controlo de acesso	82
Funções avançadas de controlo de acesso	82
Lógica de macros dos controladores de portas	83
Impulso bloqueio e desbloqueio	84
Filtros de condições	87
Triggers	89
Calendário	90
Menu de atalhos de programa	91
Eventos	93
Registo	93
Programação	93
Testes e diagnósticos	95
Walk test	95
Outros testes	98
Reportes de alarme	100
Princípios de reportes de alarme	100
Ordem dos reportes	101
Falha de comunicação (FTC)	102
Áudio de duas vias	103
Funções de utilizador programáveis	105
Arme automático	109
Programação de dispositivos sem fios	110
Aprendizagem de sensores sem fios	110
Aprendizagem de comandos	112
Sensores RF de duas zonas	114
Activação do dispositivo	115
Utilizar câmaras	117
Configuração	117
Diagnóstico	119
Resolução de problemas	119
Reset técnico	121
Desarme / ATM Temporizado	122
Áudio de duas vias	123
UltraSync	126
Aplicação móvel	129
Segurança dos dados do cartão	130

Lista de funções

A Tabela 11 abaixo apresenta uma lista alfabética de funções do Advisor Advanced e as referências descritivas.

Tabela 11: Lista de funções

Função	Referência
Aplicação móvel	“Aplicação móvel” na página nº 129
Áreas	“Áreas” na página nº 55
Arme	“Arme e desarme” na página nº 57
Arme automático	“Arme automático” na página nº 109
Arme parcial	“Arme e desarme” na página nº 57
ATM	“Desarme / ATM Temporizado” na página nº 122
Áudio de duas vias	“Áudio de duas vias” na página nº 123
Calendário	“Calendário” na página nº 90
Câmaras	“Utilizar câmaras” na página nº 117
Canal seguro	“Segurança dos dados do cartão” na página nº 130
Controlo de acesso	“Controlo de acesso” na página nº 80
Desarme	“Arme e desarme” na página nº 57
Desarme temporizado	“Desarme / ATM Temporizado” na página nº 122
Diagnósticos	“Testes e diagnósticos” na página nº 95
Dispositivos sem fios	“Programação de dispositivos sem fios” na página nº 110
Entradas	“Zonas” na página nº 49
Eventos	“Eventos” na página nº 93
Expansores / DGPs	“Dispositivos” na página nº 67, “Expansores” na página nº 68
Filtros de condições	“Filtros de condições” na página nº 87
Funções de utilizador programáveis	“Funções de utilizador programáveis” na página nº 105
Grupos de utilizadores	“Grupos de utilizadores” na página nº 72
Inibir	“Inibir e isolar” na página nº 60
Isolamento	“Inibir e isolar” na página nº 60
Modo seguro	“Segurança dos dados do cartão” na página nº 130
PIN	“PIN” na página nº 77
Portas	“Portas” na página nº 80
Reporte	“Reportes de alarme” na página nº 100
Saídas	“Saídas” na página nº 79
Shunt	“Inibição de zonas” na página nº 60, “Shunt de porta” na página nº 82
Teclados / RASs	“Dispositivos” na página nº 67, “Teclados” na página nº 68
Teclas	“Teclas” na página nº 62
Testes	“Testes e diagnósticos” na página nº 95
Triggers	“Triggers” na página nº 89

Função	Referência
UltraSync	“UltraSync” na página nº 126
Utilizadores	“Utilizadores” na página nº 69
Walk test	“Walk test” na página nº 95
Zonas	“Zonas” na página nº 49

Zonas

Zona é um sinal eléctrico de um dispositivo de segurança ou de um grupo de dispositivos (detector PIR, contacto de porta) para o sistema Advisor Advanced. Cada dispositivo pode ser identificado por um número ou um nome de zona. Por exemplo, zona 14, Porta de saída de emergência.

A ligação de zonas é descrita no Capítulo 2 “Instalação” > “Ligação das zonas” na página nº 25.

Para informações sobre a configuração de zonas, consulte “Configuração de zonas” na página nº 32.

O endereçamento de zonas é descrito em “Endereçamento de zonas, saídas e portas” na página nº 33.

A programação de zonas é efectuada através de “4.1 Zonas” na página nº 211 (do Capítulo 5 “Referência de menu”).

Tipos de zonas

Estão disponíveis os seguintes tipos de zonas.

1. Alarme

Não gera nenhum alarme quando a área está desarmada.

Gera um alarme quando a área está armada.

Exemplo: porta interna, PIR (detector de movimento).

2. Entrada/Saída 1

Não gera nenhum alarme quando a área está desarmada.

Quando a área está armada, o temporizador de saída é iniciado e a activação da zona não gera qualquer alarme. Se a zona for activada quando o tempo de saída tiver expirado, inicia-se a temporização de saída. Só é gerado um alarme quando o tempo de entrada tiver expirado.

Exemplo: porta da frente.

É necessário programar o tempo de entrada/saída. Para mais informações, consulte “4.2 Áreas” na página nº 227.

3. Acesso

Não gera nenhum alarme quando a área está desarmada.

Gera um alarme quando a área é armada e não estiver a funcionar qualquer temporizador de saída ou de entrada.

Exemplo: PIR na entrada com um contacto de porta na porta de entrada.

É necessário programar o tempo de entrada/saída. Para mais informações, consulte “4.2 Áreas” na página nº 227.

4. Incêndio

Gera um alarme de incêndio, independentemente do estado da área.

O alarme de incêndio causa um som de sirene de impulso. Este alarme tem maior prioridade do que um alarme de intrusão.

Exemplo: detector de fumo.

AVISO! Os produtos para alarme de incêndio e deteção de fumo usados com os sistemas Advisor Advanced destinam-se a ser utilizados exclusivamente por conveniência e não devem ser utilizados como produtos de proteção da vida. A combinação não cumpre com os requisitos legais para os produtos de proteção da vida ou para utilização como sistemas de deteção de incêndios. Consulte também Capítulo 8 “Normas” > “Opções afectadas por outros regulamentos” na página nº 375.

5. Pânico

Gera um alarme de pânico, independentemente do estado da área.

Exemplo: botão de pânico.

Consulte também “8.8.1 Modo de pânico” na página 309.

6. 24H

Gera um alarme de intrusão, independentemente do estado da área.

7. Tamper (Sabotagem)

Gera um alarme de tamper (sabotagem), independentemente do estado da área.

Exemplo: tampers de painel.

8. Terminador de saída

Este tipo de zona é utilizado para terminar um tempo de saída. Se a zona mudar de activa para normal, o tempo de saída é terminado e a(s) área(s) são totalmente armadas assim que expira o retardo de arme final (consulte também “8.1.3.5 Rtd.arme final” na página nº 286).

9. Comutador

Quando a zona é comutada, a área fica armada/desarmada/armada parcialmente, consoante a opção de zona seleccionada.

Exemplo: comutador junto à porta da frente.

Consulte as opções “4.1.n.6.16 Chave latch” na página nº 217, “4.1.n.6.17 Arme por chave” na página nº 217, “4.1.n.6.18 Desarme por chave” na página nº 217.

10. Médico

Gera um alarme médico, independentemente do estado da área.

11. Técnico

Gera um alarme técnico, independentemente do estado da área.

Exemplo: sensor de temperatura.

Consulte as opções “4.1.n.6.19 Arme total técnico” na página nº 217, “4.1.n.6.20 Desarme técnico” na página nº 218.

12. Falha via tx

Monitoriza o dispositivo de reporte externo.

13. Porta corta-fogo

Se não estiver presente um alarme de incêndio, gerar um alarme de intrusão independentemente do estado da área. Caso contrário, não será gerado um alarme de intrusão.

Nota: A ativação do alarme sonoro interno depende da opção da zona de “Campainha”. Consulte “4.1.n.6.9 Campainha” na página 215.

Exemplo: portas corta-fogo ou portas de emergência.

Consulte também “4. Incêndio” na página nº 50.

14. Flh.230VAC aux

Monitoriza o fornecimento de corrente eléctrica auxiliar.

15. Falha bat.aux

Monitoriza a bateria de fornecimento de alimentação auxiliar.

16. Key box

Monitoriza uma caixa que aloja uma chave das instalações. Permite uma abertura durante um breve período de tempo após o arme de uma área (especificado no temporizador da key box; consulte “8.1.4.5 Tempo key box” na página nº 287). Gera um alarme quando aberta fora deste período.

17. Reset técnico

A activação desta zona causa o reset técnico.

18. Entrada/Saída 2

Uma zona alternativa de entrada/saída.

Exemplo: porta traseira.

A zona de entrada/saída 2 inicia os temporizadores de entrada/saída alternativos. Consulte “4.2.n.2 Tempo de saída” na página nº 228 e “4.2.n.3 Tempo de entrada” na página nº 229.

Consulte também “2. Entrada/Saída 1” na página nº 49 para obter mais informações.

19. Shunt

A activação de zonas provoca a inibição (shunt) de todas as zonas de áreas que permitem a inibição. A inibição é permitida pela opção “4.1.n.6.36 Shunt” na página nº 222.

Consulte também “Inibição de zonas” na página nº 60.

20. PortCortaFogo-ES

Se a área não estiver desarmada, a zona funciona como “13. Porta corta-fogo” descrita na página nº 51.

Se a área estiver armada, a zona funciona como uma zona de entrada/saída. Consulte também “2. Entrada/Saída 1” na página nº 49 e “18. Entrada/Saída 2” na página nº 51.

Observe que no estado armado todos os filtros de condição mapeados para esta zona estão desativados.

Tabela 12: Opções de zonas disponíveis

Opções:	Tipo de zona	1. Alarme	2. Entrada/Saída 1	3. Acesso	4. Incêndio	5. Pânico	6. 24H	7. Tamper (Sabotagem)	8. Terminador de saída	9. Comutador	10. Médico	11. Técnico	12. Falha via tx	13. Porta corta-fogo	14. Flh.230VAC aux	15. Falha bat.aux	16. Key box	17. Reset técnico	18. Entrada/Saída 2	19. Shunt	20. PortCortaFogo-ES
4.1.n.6.1 Inibir		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
4.1.n.6.2 Isolar		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		-	-	+
4.1.n.6.3 Excl. em ArP1		-	-	-				-	-								-		-	-	
4.1.n.6.4 Excl. em ArP2		-	-	-				-	-								-		-	-	
4.1.n.6.5 Duplo impulso		-			-		-				-	-	-	-	-						-
4.1.n.6.6 Swinger shunt [1]		-	-	-		-	-				-		-	-	-	-			-	-	
4.1.n.6.7 Anti-Mask		-	-	-		-					-		-						-	-	
4.1.n.6.8 Empar. zona		-			-						-		-								-
4.1.n.6.9 Campainha		-	-	-							-		-						-	-	+
4.1.n.6.10 Soak test		-	-	-	-	-	-				-		-	-	-	-			-	-	-
4.1.n.6.11 Walk Test técnico		+	+	+	+	+	+				+	+	+	+	+	+			+	+	+
4.1.n.6.12 Walk Test utl		+	+	+		+	+				+	+		+	+	+			+	+	+
4.1.n.6.13 Sensor choque		-	-	-		-							-						-	-	
4.1.n.6.14 Prolongar EE			-																-	-	
4.1.n.6.15 Porta final			-	-															-	-	
4.1.n.6.16 Chave latch									-												

Opções:	Tipo de zona																				
	1. Alarme	2. Entrada/Saída 1	3. Acesso	4. Incêndio	5. Pânico	6. 24H	7. Tamper (Sabotagem)	8. Terminador de saída	9. Comutador	10. Médico	11. Técnico	12. Falha via tx	13. Porta corta-fogo	14. Filh.230VAC aux	15. Falha bat.aux	16. Key box	17. Reset técnico	18. Entrada/Saída 2	19. Shunt	20. PortCortaFogo-ES	
4.1.n.6.17 Arme por chave — arme total									-												
4.1.n.6.17 Arme por chave — arme parcial									-												
4.1.n.6.18 Desarme por chave									-												
4.1.n.6.19 Arme total técnico											+										
4.1.n.6.20 Desarme técnico											+										
4.1.n.6.21 Arme parcial técnico											+										
4.1.n.6.22 RAS LCD						-				-	-	-	-	-	-						-
4.1.n.6.23 Registo	•	•	•	•	•	•	•	+	+	+	•	•	+	+	+			•			
4.1.n.6.24 Reporte CRA	•	•	•	•	•	•	•	+	+	+	•	•	+	+	+			•			
4.1.n.6.25 Temp. Retardo											-	-			-	-					
4.1.n.6.26 REC no RAS																					
4.1.n.6.27 REC p/ Utiliz																					
4.1.n.6.28 Sensor tipo																					
4.1.n.6.29 Zona virtual																					-
4.1.n.6.30 Mantida abert																					-
4.1.n.6.31 ES verif arme																					
4.1.n.6.32 Alarme em AP1																					
4.1.n.6.33 Alarme em AP2																					
4.1.n.6.34 Reportar como																					
4.1.n.6.35 Auto Teste																					
4.1.n.6.36 Shunt	-	-				-								-							-
4.1.n.6.37 Ver isolados																				+	+
4.1.n.6.38 Stop Reporte	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4.1.n.6.39 Limitar relatórios	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

[1] Estas opções dependem das predefinições seleccionadas no arranque inicial do painel. Consulte também “Arranque inicial” na página nº 142.

Legenda:

- + (sim): A opção é programável, o valor predefinido é Sim.
- (não): A opção é programável, o valor predefinido é Não.
- (sempre): A opção não é programável, o valor é sempre Sim.

Tabela de referências de menu

Os menus seguintes aplicam-se às zonas.

Menu	Pág.	Descrição
2.2.2.n.3 Entradas DGP	186	Visualizar o intervalo de zonas do expansor selecionado
4.1 Zonas	211	Adicionar, remover e configurar zonas
4.5.n.2 Foto por zona	237	Seleciona zonas que podem acionar a câmara quando ativas.
5.1.n.6.1 Zona de porta	244	Atribui as zonas requeridas à porta selecionada
5.1.n.8.1 Zonas	259	Seleciona zonas que têm de ser inibidas na abertura de porta.
8.1.4 Zonas	286	Configura os temporizadores utilizados nas opções de configuração de zona
8.6 Opções de zona	302	Configura as opções de sistema para as zonas
8.7.6 Confir. alarme	305	Configura a confirmação de zona A e B (ACPO)
8.7.9 Esquema Objeto	308	Configura o esquema de numeração da zona

Áreas

Área é uma secção da instalação que tem requisitos de segurança específicos. O sistema Advisor Advanced permite a divisão de todas as instalações em áreas diferentes com diferentes requisitos de segurança. Cada área tem zonas atribuídas à mesma. Cada área é identificada por um número ou um identificador. Por exemplo: Área 1, Escritório principal, etc.

Cada área pode apresentar um dos seguintes estados:

- Armado
- Parcialmente armado
- Desarmado

Consulte “Arme e desarme” na página nº 57 para obter mais informações.

As áreas são configuradas em “4.2 Áreas” na página nº 227 do Capítulo 5 “Referência de menu”.

Grupos Área

Modelos de painéis específicos permitem agrupar áreas em grupos de áreas. Os utilizadores podem realizar operações de áreas com os grupos de áreas tal como com áreas: por exemplo, armar um grupo de áreas.

Os grupos de áreas são configurados em “4.3 Grupos Área” na página nº 233.

Nota: a disponibilidade dos grupos de áreas depende da variante do painel de controlo. Consulte “Especificações” na página nº 37 do Capítulo 2 “Instalação”.

Hierarquia das áreas

A hierarquia das áreas define a ordem pela qual as áreas de alta segurança devem ser armadas ou desarmadas. Um valor mais baixo significa uma hierarquia mais alta. As áreas com uma hierarquia mais alta devem ser armadas primeiro e desarmadas como as últimas.

Esta funcionalidade está disponível apenas nas áreas com uma hierarquia de áreas superior a 0.

Um exemplo são os cofres bancários. Deve ser impossível desarmar o cofre (hierarquia 1) antes da sala do cofre (hierarquia 2) ser desarmada. Além disso, não é possível armar a sala do cofre antes de armar o cofre.

A hierarquia das áreas é definida através do menu “4.2.n.6 Hierarquia” na página nº 232.

Tabela de referências de menu

Os menus seguintes aplicam-se às áreas.

Menu	Pág.	Descrição
2.2.1.n.3.4 Ver áreas, 2.2.1.n.3.5 Ver GA	177	Especifica que área e que grupo de área apresentará informações no teclado sem autorização do utilizador.

Menu	Pág.	Descrição
2.2.1.n.3.6 Áreas de controlo, 2.2.1.n.3.7 Controlar GA	177	Seleciona áreas e grupos de áreas que podem ser armados e desarmados pelo teclado.
2.2.1.n.3.14 LED1 ind. área, 2.2.1.n.3.15 LED2 ind. área	181	Atribui áreas a LED programáveis do teclado.
2.2.1.n.3.2 Tamper Área, 2.2.2.n.4.2 Tamper Área,	176	Determina que área recebe o tamper do dispositivo selecionado e eventos de falhas.
3.1.n.9 Seleccione Modo	205	Especifica se o utilizador opera em áreas ou grupos de áreas.
3.2.n.3 Áreas GU, 3.2.n.4 GU GA	209	Define áreas e grupos de áreas que o utilizador pode controlar.
4.1.n.5 Zona áreas	213	Atribui áreas à zona que tem de gerar o alarme quando é ativada e o estado da área, armada ou desarmada, satisfaz os requisitos do tipo de zona.
4.2 Áreas	227	Configura áreas.
4.3 Grupos Área	233	Atribui áreas a grupos de áreas.
5.1.n.6.3.1 Áreas de porta, 5.1.n.6.3.2 Grp Área Porta	244	Atribui a porta selecionada a áreas e grupos de áreas para indicação do estado da área nos leitores.

Arme e desarme

Cada área pode apresentar um dos seguintes estados:

- **Armado:** A condição de uma área em que uma alteração do estado de qualquer zona (de normal para activa) provoca um alarme. Uma instalação ou uma área só é armada quando está desocupada. Algumas zonas (como cofres) podem estar continuamente armadas.
- **Desarmado:** Uma condição de uma área, quando está ocupada e a actividade normal não acciona um alarme.
- **Parcialmente armado:** A condição de parte de uma área onde a alteração do estado de determinadas zonas (de normal para activa) provoca um alarme. Uma área ou instalação está armada parcialmente, quando está parcialmente desocupada, por exemplo, o exterior de uma casa está armada parcialmente, mas o interior ainda está desarmado.

Consulte também “Áreas” na página nº 55.

As áreas podem ser armadas ou desarmadas de uma das maneiras seguintes:

- Por utilizadores através de um teclado ou leitor. Consulte “Utilizadores” na página nº 69 e “Dispositivos” na página nº 67. As sequências de teclas disponíveis estão indicadas em “Teclas” na página nº 62.
- Por utilizadores através de um comando SMS. Para mais informações, consulte o *Guia de Referência do Controlo por SMS do Advisor Advanced*.
- Por operadores remotamente através de software de gestão. Consulte o Capítulo 6 “Software” na página nº 353.
- Automaticamente através da funcionalidade de arme automático. Consulte “Arme automático” na página nº 109 para obter mais informações.

Como utilizar o arme parcial

Quando um utilizador efectua um arme parcial, o sistema arma todas as áreas solicitadas, com todas as zonas de arme total (perímetro) supervisionadas, mas todas as zonas de arme parcial (interior) ignoradas. Como este modo é para segurança pessoal, o reporte para a central receptora depende da opção “8.4.3.1 Reporte BA” (consulte a página 296). Além disso, quaisquer alarmes que ocorram enquanto o arme parcial está aplicado, são tratados como alarmes locais que activam sirenes, besouros do teclado (se activados) e indicadores do teclado.

Se estiverem várias áreas atribuídas a uma zona, esta não é armada até que todas as áreas atribuídas sejam armadas. Se estiver atribuída à zona uma mistura de áreas de arme parcial e áreas de arme total, a zona obedece à condição de arme parcial.

Desarme retardado

O desarme de uma área pode ser retardado. O desarme retardado é utilizado em aplicações bancárias, como o abastecimento de máquinas ATM (caixas multibanco) e a abertura de cofres.

Durante o retardo o teclado ou leitor da área estão bloqueados. A mensagem seguinte é apresentada no ecrã LCD do teclado:

Retardo Desarme
Aguarde

Num teclado ou leitor sem LCD, o retardo do desarme é indicado por um LED de área intermitente lento.

O período de retardo é definido em “4.2.n.4.3 Retardo Desarme” na página nº 231.

Não é possível ignorar manualmente o retardo.

Tabela de referências de menu

Os menus seguintes são aplicáveis para arme, arme parcial e desarme.

Menu	Pág.	Descrição
2.2.1.n.3.6 Áreas de controlo, 2.2.1.n.3.7 Controlar GA	177	Seleciona áreas e grupos de áreas que podem ser armados e desarmados pelo teclado.
2.2.1.n.3.8.1 Modo cartão e PIN	178	Seleciona um método de autorização para o teclado.
2.2.1.n.3.8.3 1 x arme/desarme	178	Define se o teclado selecionado permite armar ou desarmar áreas com um único badge.
2.2.1.n.3.8.4 3xCartão arma	179	Define se o teclado selecionado permite armar áreas com um badge triplo.
2.2.1.n.3.12 Arme rápido	181	Permite armar áreas sem ter de introduzir o PIN ou o cartão.
3.1.n.9 Seleccione Modo	205	Especifica se o utilizador opera em áreas ou grupos de áreas.
3.2.n.3 Áreas GU, 3.2.n.4 GU GA	209	Define áreas e grupos de áreas que o utilizador pode controlar.
4.2.n.2 Tempo de saída	228	Define temporizadores de saída de área.
4.2.n.3 Tempo de entrada	229	Define temporizadores de entrada de área.
4.2.n.4.3 Retardo Desarme	231	Define temporizador para desarme retardado.
4.2.n.5 Opç.arm/desarm	231	Define várias opções de arme e desarme do sistema.
5.1.n.6.3 Controlo de Alarme	244	Define as opções de controlo de alarme para a porta selecionada.
8.1.3.5 Rtd.arme final	286	Define o tempo de atraso entre a conclusão do arme de uma área por um terminador de saída ou o arme final da porta e a área a ser armada.
8.4 Opções de arme	295	Define as condições de arme.

Menu	Pág.	Descrição
8.7.7 Desarme Fácil	307	Se ativado, pode desarmar instalações introduzindo um PIN ou passando um cartão válido sem premir outras teclas.
8.9 DesarmTemp/ATM	314	Configura as opções de interface do ATM (caixa automática), por exemplo atraso de desarme e atraso de desarme estendido.

Inibir e isolar

Um dispositivo avariado pode ser inibido ou isolado.

Inibir

Uma zona foi inibida de indicar estado normal ou activo. Passa a estar excluída de funcionar como parte integrante do sistema durante um determinado tempo. Contudo, os tampers são ainda monitorizados.

A zona fica inibida até ao desarme seguinte.

Uma zona pode ser inibida automaticamente ao utilizar a funcionalidade de arme forçado. É configurada através do menu “8.4.4 Arme forçado” na página nº 297 do Capítulo 5 “Referência de menu”.

Isolamento

Uma zona ou um dispositivo bus são inibidos de indicar estado normal ou activo. São excluídos de funcionar como parte do sistema permanentemente, até o isolamento ser retirado pelo gestor ou instalador.

Inibição de zonas

O procedimento de inibição (shunt) impede que as zonas activas gerem um alarme durante um determinado período de tempo.

Uma zona pode ser inibida da seguinte maneira:

- Manualmente, pelo instalador. Utilize o menu “1.2.1.9 Shunt Zonas” na página nº 153.
- De acordo com um calendário. Consulte “Calendário” na página nº 90 para obter mais informações.
- Através de um filtro de condições. Consulte “Filtros de condições” na página nº 87 para obter mais informações.
- Através de uma zona com tipo shunt. Consulte “Tipos de zonas” na página nº 49 para obter mais informações.

Cuidado: existe um limite ao número de zonas que podem ser inibidas em simultâneo. O limite é definido em “4.2.n.7.3 Limite de Shunt” na página nº 233.

Durante o tempo de inibição, a zona é inibida.

Se a zona ainda estiver activa depois de o tempo de inibição ter expirado, a zona irá gerar um alarme, dependendo no tipo de zona e o estado da área.

Para utilizadores específicos (consoante as suas opções de utilizador), a inibição está activa durante um tempo de inibição estendido.

Antes do temporizador de inibição expirar, pode ser emitido um aviso.

Tabela de referências de menu

Os menus seguintes aplicam-se a inibição, isolamento e shunt de zona.

Menu	Pág.	Descrição
1.2.1.9 Shunt Zonas	153	Inibe manualmente as zonas.
2.2.1.n.3.10 Isolar teclado	180	Isola os eventos de falha de tamper no teclado selecionado (o teclado permanece funcional).
2.2.2.n.4.4 Isolar DGP	187	Isola os eventos de falha de tamper no expansor selecionado (o expansor permanece funcional).
4.1.n.3 Isolado	213	Isola ou retira o isolamento da zona selecionada.
4.1.n.6.1 Inibir	214	Se definido como Sim, esta zona pode ser inibida pelos utilizadores.
4.1.n.6.2 Isolar	214	Se definido como Sim, esta zona pode ser isolada pelos utilizadores.
4.1.n.6.6 Swinger shunt	215	Se definido como Sim, o número de alarmes a partir desta zona está limitado ao número especificado para um ciclo de arme/desarme.
4.1.n.6.36 Shunt	222	Se definido como Sim, a zona pode ser isolada.
4.1.n.6.37 Ver isolados	222	Se definida como Ligado, os utilizadores são avisados sobre esta zona estar isolada ao tentar armar ou desarmar a área apropriada.
4.2.n.7 Limites	232	Limita o número de elementos do sistema que podem ser isolados ou inibidos de uma vez.
4.5.n.5 Isolado	239	Isola a câmara selecionada.
8.6.4 Swinger shunt	303	Define o número de alarmes de uma zona até ser inibida.

Teclas

O método de autorização depende das definições do sistema. Consulte “2.2.1.n.3.8 Opções de controlo” na página nº 178 para obter mais informações.

Nota: se introduzir um código PIN incorrecto três vezes, o teclado é bloqueado durante 120 segundos.

Sequências de teclas comuns do teclado LCD

Tabela 13: Sequências de teclas comuns do teclado de LCD

Acção	Método programado	Sequência de teclas	[1]	
Arme [2]	Armar com tecla	Ligado	<input type="checkbox"/>	
		Ligado, PIN, Enter	<input type="checkbox"/>	
	Armar com cartão	Cartão	<input type="checkbox"/>	
		Ligado, cartão	<input type="checkbox"/>	
		3 x cartão	<input type="checkbox"/>	
	Armar com cartão e PIN	Ligado, cartão, PIN, Enter	<input type="checkbox"/>	
		Cartão, PIN, Ligado	<input type="checkbox"/>	
	Desarme [2][3]	Desarmar com PIN	Desligado, PIN, Enter	<input type="checkbox"/>
			PIN	<input type="checkbox"/>
			PIN, Desligado	<input type="checkbox"/>
Desarmar com cartão		Cartão	<input type="checkbox"/>	
		Desligado, cartão	<input type="checkbox"/>	
Desarmar com cartão e PIN		Desligado, cartão, PIN, Enter	<input type="checkbox"/>	
		Cartão, PIN, Desligado	<input type="checkbox"/>	
		Cartão, PIN	<input type="checkbox"/>	
Arme parcial		Armar parcialmente com tecla	Arme parcial	<input type="checkbox"/>
	Arme parcial, PIN, Enter		<input type="checkbox"/>	
	Armar parcialmente com cartão	PIN, Arme parcial	<input type="checkbox"/>	
		Cartão	<input type="checkbox"/>	
		Arme parcial, cartão	<input type="checkbox"/>	
	Armar parcialmente com cartão e PIN	3 x cartão	<input type="checkbox"/>	
		Arme parcial, cartão, PIN, Enter	<input type="checkbox"/>	
		Cartão, PIN, Arme parcial	<input type="checkbox"/>	
Acesso a portas [2][3]	Acesso a portas com PIN	PIN, Enter	<input type="checkbox"/>	
	Acesso a portas com cartão	Cartão	<input type="checkbox"/>	
	Acesso a portas com cartão e PIN	Cartão, PIN, Enter	<input type="checkbox"/>	

Acção	Método programado	Sequência de teclas	[1]
Acesso ao menu [2]	Acesso ao menu com PIN	Menu, PIN, Enter	<input type="checkbox"/>
		PIN, Menu	<input type="checkbox"/>
	Acesso ao menu com cartão	Menu, cartão	<input type="checkbox"/>
	Acesso ao menu com cartão e PIN	Menu, cartão, PIN, Enter	<input type="checkbox"/>
Cartão, PIN, Menu		<input type="checkbox"/>	
Coacção [4]	Coacção com PIN	Qualquer tecla de arme (Ligado/Desligado/Arme Parcial), código de coacção, Enter	<input type="checkbox"/>
		Código coacção, qualquer tecla de arme	<input type="checkbox"/>
	Coacção com cartão e PIN	Qualquer tecla de arme (Ligado/Desligado/Arme Parcial), código de coacção, cartão, Enter	<input type="checkbox"/>
		Cartão, código de coacção, qualquer tecla de arme	<input type="checkbox"/>
Alterar volume do besouro do teclado	Aumentar o volume	X + Direita	<input type="checkbox"/>
	Diminuir o volume	X + Esquerda	<input type="checkbox"/>
Pânico [5]	Alarme de pânico	1 + 3	<input type="checkbox"/>
Sair [6]	Sair rapidamente da programação	Menu + Sair	<input type="checkbox"/>
Alarmes activos [7]	Apresentar zonas activas e falhas que devem ser confirmadas	Função, Função	<input type="checkbox"/>
Memória de alarmes [7]	Apresentar alarmes que ocorreram quando definidos	Enter, Enter	<input type="checkbox"/>

- [1] Utilize a caixa de selecção para assinalar as opções disponíveis para este sistema.
- [2] A funcionalidade depende de “2.2.1.n.3.8.1 Modo cartão e PIN” na página nº 178.
- [3] A funcionalidade depende de “8.7.7 Desarme Fácil” na página nº 307.
- [4] A funcionalidade depende de “8.7.3 Método coacção” na página nº 304.
- [5] A funcionalidade do alarme de pânico depende da opção “8.8.1 Modo de pânico” descrita na página nº 309. Depende também da opção “2.2.1.n.3.21 Teclas 1+3” descrita na página nº 183.
- [6] A função só funciona se não existir uma mensagem que requeira uma resposta ou acção do utilizador. Está desactivada, por exemplo, durante a aprendizagem de dispositivos sem fios.
- [7] A funcionalidade depende de “8.3.3 Lista de alarmes” na página nº 294.

Sequências de teclas comuns do teclado sem LCD

Tabela 14: Sequências de teclas comuns do teclado sem LCD

Acção	Método programado	Sequência de teclas	[1]
Arme [2]	Armar com PIN	Ligado, PIN, Ligado	<input type="checkbox"/>
		PIN, Ligado [6]	<input type="checkbox"/>
	Armar com cartão	Cartão [6]	<input type="checkbox"/>
		Ligado, cartão	<input type="checkbox"/>
		3 x cartão	<input type="checkbox"/>
	Armar com cartão e PIN	Ligado, cartão, PIN, Ligado	<input type="checkbox"/>
Cartão, PIN, Ligado [6]		<input type="checkbox"/>	
Desarme [2][3]	Desarmar com PIN	Desligado, PIN, Ligado	<input type="checkbox"/>
		PIN	<input type="checkbox"/>
		PIN, Desligado [6]	<input type="checkbox"/>
	Desarmar com cartão	Cartão	<input type="checkbox"/>
		Desligado, cartão	<input type="checkbox"/>
	Desarmar com cartão e PIN	Desligado, cartão, PIN, Ligado	<input type="checkbox"/>
		Cartão, PIN, Desligado [6]	<input type="checkbox"/>
		Cartão, PIN	<input type="checkbox"/>
	Arme parcial	Armar parcialmente com cartão	Cartão
3 x cartão			<input type="checkbox"/>
Acesso a portas [2]	Acesso a portas com PIN	PIN, Ligado [6]	<input type="checkbox"/>
		PIN, Desligado [6]	<input type="checkbox"/>
	Acesso a portas com cartão e PIN	Cartão [6]	<input type="checkbox"/>
		Cartão, PIN, Ligado [6]	<input type="checkbox"/>
Coacção [4]	Coacção com PIN	Qualquer tecla de arme (Ligado/Desligado), código de coacção, Enter	<input type="checkbox"/>
		Código coacção, qualquer tecla de arme	<input type="checkbox"/>
	Coacção com cartão e PIN	Qualquer tecla de arme (Ligado/Desligado), código de coacção, cartão, Enter	<input type="checkbox"/>
		Cartão, código de coacção, qualquer tecla de arme	<input type="checkbox"/>
	Pânico [5]	Alarme de pânico	1 + 3

[1] Utilize a caixa de selecção para assinalar as opções disponíveis para este sistema.

[2] A funcionalidade depende de “2.2.1.n.3.8.1 Modo cartão e PIN” na página nº 178.

[3] A funcionalidade depende de “8.7.8 Desarme Fácil” na página nº 307.

[4] A funcionalidade depende de “8.7.3 Método coacção” na página nº 304.

[5] A funcionalidade do alarme de pânico depende da opção “8.8.1 Modo de pânico” descrita na página nº 309.

[6] Determinadas sequências de chaves podem ter funções em conflito. Nesta situação, a funcionalidade depende da opção “2.2.1.n.3.8.5 Modo tecla/cartão”, descrita na página nº 179.

Quando se pode introduzir um PIN, o teclado emite dois sinais sonoros e os LEDs vermelho e verde piscam. Quando uma operação falha, o teclado emite sete sinais sonoros.

Teclas de funções

Utilize a Tabela 15 abaixo para descrever a funcionalidade e disponibilidade das teclas de funções.

Consulte também “2.2.1.n.3.13 Teclas Função” na página nº 181.

Tabela 15: Teclas de funções

Acção	Tecla	[1]
	A	<input type="checkbox"/>
	B	<input type="checkbox"/>
	C	<input type="checkbox"/>
	F1 (F + 1)	<input type="checkbox"/>
	F2 (F + 2)	<input type="checkbox"/>
	F3 (F + 3)	<input type="checkbox"/>
	F4 (F + 4)	<input type="checkbox"/>

[1] Utilize a caixa de selecção para assinalar as funções disponíveis para este sistema.

Tabela de referências de menu

Os menus seguintes aplicam-se às configurações de teclas.

Menu	Pág.	Descrição
2.2.1.n.3.8.1 Modo cartão e PIN	178	Seleciona um método de controlo.
2.2.1.n.3.8.3 1 x arme/desarme	178	Define se o teclado seleccionado permite armar ou desarmar áreas com uma passagem de cartão.
2.2.1.n.3.8.4 3xCartão arma	179	Define se o teclado seleccionado permite armar áreas com três passagens de cartão.
2.2.1.n.3.12 Arme rápido	181	Permite armar áreas sem ter de introduzir o PIN ou o cartão.
2.2.1.n.3.13 Teclas Função	181	Atribui uma função programável pelo utilizador a qualquer uma das teclas de funções disponíveis.
2.2.1.n.3.18 REC no RAS	182	Seleciona um teclado LCD adicional que apresente uma mensagem de confirmação após o desarme do sistema.
2.2.1.n.3.21 Teclas 1+3	183	Ativa um alarme de pânico através da combinação das teclas 1 e 3.
3.1.n.9 Seleccione Modo	205	Especifica se o utilizador opera em áreas ou grupos de áreas.

Menu	Pág.	Descrição
5.1.n.3.5.1 Cartão e PIN	251	Especifica qual o método requerido para abrir a porta a partir do leitor selecionado.
5.1.n.3.5.2 Dois cartões	251	Define se são necessários dois cartões ou PIN de utilizador para obter acesso.
5.1.n.6.3.6 Tipo Controlo	255	Especifica o tipo de controlo de alarme que está disponível para a porta selecionada.
8.1.3.2 Cartão e PIN	285	Define o tempo máximo de atraso entre a apresentação do cartão e a introdução do PIN.
8.7.7 Desarme Fácil	307	Se ativado, pode desarmar instalações introduzindo um PIN ou passando um cartão válido sem premir outras teclas.

Dispositivos

Existem os seguintes tipos de dispositivos bus:

- São utilizados Teclados para proporcionar controlo do sistema, como armar ou desarmar áreas. Consoante o tipo de teclado, poderão estar disponíveis funções adicionais, como ecrãs LCD, menus para ajustar a hora e a data, etc.
- Expansores são utilizados para proporcionar entradas e saídas remotas.
- Os leitores são ligados a controladores de portas e são utilizados para controlar portas inteligentes. Consulte “Controlo de acesso” na página nº 80 para obter mais informações.
- Dispositivos de áudio: para a verificação áudio, são utilizados dispositivos de áudio de duas vias. Consulte “Áudio de duas vias” na página nº 123 para obter mais informações.

Bus – enumeração

Os dispositivos utilizam DIP switches para definir o endereço bus. O Advisor Advanced utiliza geralmente o número de teclado/expansor. Para a dependência entre o endereço do dispositivo e o respectivo número, consulte o manual de instalação do dispositivo bus aplicável. O endereço do dispositivo programado pode ser visualizado em “2.2.1.n.2 Endereço BUS” (teclado), “2.2.2.n.2 Endereço BUS” (expansor), e “2.2.4.n.2 Endereço áudio”.

Consulte também Capítulo 2 “Instalação > Endereçamento de zonas, saídas e portas” na página nº 33.

Adicionar um teclado com um endereço superior

Se o número programado num teclado for superior ao número máximo permitido pelo sistema, o teclado não poderá ser adicionado. No entanto, é possível alterar este endereço a partir do painel através do menu interno do teclado. Adicionar um número de teclados superior abre um menu simplificado que contém apenas uma entrada do menu do teclado.

Por exemplo, para programar o teclado com o número programado 16 num sistema com 8 teclados:

1. Adicione teclado 16. Abre-se o menu “2.2.1.n.4 Menu RAS” (descrito na página nº 184).
2. Aceda ao menu do teclado.
3. Altere o endereço do teclado para 7. Consulte o manual aplicável do teclado.
4. Adicione o teclado 7.

Teclados

Um dispositivo que é o painel de controlo do utilizador para opções de segurança de áreas ou de pontos de acesso (portas). O teclado pode ser uma consola (teclado LCD utilizado para programar o painel de controlo, efectuar opções do utilizador, ver alarmes, etc.) ou qualquer outro dispositivo que possa ser utilizado para efectuar a função de segurança, como armar/desarmar, abrir portas, etc.

Os teclados e leitores podem também ser designados como estações de arme remotas (RASs).

Os teclados são configurados em “2.2.1 Dispositivos RAS” na página nº 175 do Capítulo 5 “Referência de menu”.

Expansores

Os expansores são dispositivos que expandem o número de entradas ou saídas do sistema Advisor Advanced. Existem dois tipos de expansores:

- Expansores internos: placas de expansão instaladas dentro da caixa do painel de controlo.
- Expansores externos: dispositivos bus que recolhem dados de outros dispositivos de segurança dentro de uma área e que os transferem para o painel de controlo Advisor Advanced. São também designados como expansores ou painéis de recolha de dados (DGPs).

A instalação e ligação dos expansores é descrita no Capítulo 2 “Instalação” na página nº 7.

As opções dos expansores são definidas em “2 Disp.BUS” na página nº 174 do Capítulo 5 “Referência de menu”.

Dispositivos de áudio

Os dispositivos de áudio de duas vias permitem ao operador da central recetora ouvir áudio ao vivo a partir das instalações protegidas e em alarme e responder de volta.

Consulte “Áudio de duas vias” na página nº 123 para obter mais informações.

Tabela de referências de menu

Os menus seguintes aplicam-se aos dispositivos bus.

Menu	Pág.	Descrição
2 Disp.BUS	174	Visualiza e configura os dispositivos bus.
8.5.2 Opções de DGP	301	Definições de controlador de portas.

Utilizadores

Os utilizadores são identificados no sistema Advisor Advanced por um número exclusivo, que está associado ao PIN ou cartão do utilizador.

Nota: se o sistema for compatível com EN 50131, só pode editar as suas próprias definições e configurar apenas utilizadores acabados de adicionar. Consulte “Bloqueio de dados do utilizador” na página nº 70 para obter mais informações.

Para cada utilizador, o sistema regista o seguinte:

- Número
- Nome
- PIN
- Número de ID do cartão
- Número de telefone
- Grupo de utilizadores (que determina as opções a que o utilizador pode aceder)
- Grupo de portas (que determina as regiões a que o utilizador pode aceder)
- Idioma
- Várias opções programadas

Nota: O seu próprio grupo de utilizadores pode não permitir-lhe programar PINs. Se autorizar a utilização desta opção, poderão ainda haver restrições quanto aos grupos de utilizadores que lhe é permitido actualizar.

O número máximo de utilizadores no sistema é definido em “Especificações” na página nº 37.

Nota: Ligando controladores de portas ao sistema Advisor Advanced aumenta o número máximo de utilizadores no sistema (consulte “Especificações > Funcionalidades de controlo de acesso” na página nº 39 para obter mais informações). No entanto, os utilizadores adicionais não têm os registos seguintes:

- Número de telefone
- Idioma

Utilizadores predefinidos

Existem dois utilizadores predefinidos no sistema.

- O instalador é utilizado para introduzir a configuração do sistema Advisor Advanced. O grupo de utilizadores que lhe é atribuído é o “grupo de instaladores”.
- Um utilizador com o nome predefinido de Supervisor, que pode conceder acesso ao menu de instalação ao técnico de manutenção. O grupo de utilizadores que lhe é atribuído é o “grupo de supervisores”. O PIN predefinido do supervisor é 1122.

Nota: Se o comprimento do PIN estiver configurado para mais de 4 dígitos, são acrescentados zeros aos valores PIN predefinidos. Por exemplo, se o sistema estiver configurado para um PIN de 6 dígitos, o PIN do supervisor é 112200.

Se a opção “8.2.8.1 Muitos instaladores” na página nº 292 estiver ativada, podem ser configurados alguns instaladores no painel. No entanto, apenas um instalador pode ter sessão iniciada a partir de um teclado de cada vez.

Consulte também “Grupos de utilizadores” na página nº 72.

Bloqueio de dados do utilizador

Quando um sistema está configurado em conformidade com EN 50131, o utilizador não está autorizado a modificar as definições de um utilizador existente (a não ser as de si próprio). Um novo utilizador só pode ser configurado quando é adicionado e um utilizador existente só pode ser removido. Os instaladores só podem modificar as suas próprias definições, e os outros utilizadores podem modificar as suas próprias definições através de menus do utilizador (para mais informações, consulte o *Guia do Utilizador do Advisor Advanced* e o *Manual do Gestor do Advisor Advanced*).

Depois de um novo utilizador ter sido adicionado através do menu “3.1.0 Adicionar utilizador” na página nº 201, o instalador pode configurar este utilizador. Concluída a modificação e depois de o instalador sair do menu de utilizador, aparece o seguinte pedido de confirmação:

```
Bloq.Info.Util?
  >Cancelar<
```

Escolha OK para confirmar a configuração do novo utilizador. Depois da confirmação, apenas este utilizador poderá modificar as suas próprias definições.

Caso contrário, seleccione Cancelar para voltar à configuração de utilizador.

Tabela de referências de menu

Os menus seguintes aplicam-se aos utilizadores.

Menu	Pág.	Descrição
1.2.11 Verificar cartão	167	Ler dados de um cartão de utilizador.
1.6 Manutenção em	172	Desativa a função de acesso do instalador antes de expirar o tempo de acesso.
3 Gestão utlz	201	Adicionar, editar ou eliminar utilizadores e grupos de utilizadores.
4.4.n.2 Util Atribuído	235	Atribui um utilizador existente ao comando seleccionado.
5.1.n.9.4 Opções HSU	261	Configura as opções de utilizador de alta segurança.
8.2 Opções de técnico	288	Configura opções que se aplicam a funções de manutenção e de instalação.

Menu	Pág.	Descrição
8.8.5 Aprende cartão	310	Selecione um keypad ou uma porta para a aprendizagem de cartões de utilizador.
9.1.n.4 Destino	324	Configura a comunicação GSM com os utilizadores.

Grupos de utilizadores

Um grupo de utilizadores permite aos utilizadores controlar as opções de alarme do sistema Advisor Advanced (também designado por controlo de alarmes). Isto confere flexibilidade ao determinar o acesso e controlo do sistema por parte do utilizador.

Um utilizador pode ter mais de um grupo de utilizadores atribuído. Neste caso, se qualquer um destes grupos conceder permissão para uma opção específica, o utilizador tem esta permissão.

Por exemplo: um utilizador tem dois grupos de utilizadores atribuídos: “R&D” e “Gestores”. Se o grupo de utilizadores “Gestores” permitir a inibição, mas o grupo “R&D” não o permitir, o utilizador pode inibir uma zona.

Nota: o sistema inclui sempre um grupo de instaladores.

Tipos de grupos de utilizadores

O tipo de grupo de utilizadores define quais as opções de grupo de utilizadores permitidas aos utilizadores que pertencem a um grupo deste tipo. Por exemplo, um guarda não tem autorização para adicionar utilizadores, enquanto que um utilizador normal não pode alterar a data e a hora.

Existem os seguintes tipos de grupos de utilizadores:

- Utilizador normal
- Supervisor
- Instalador
- Vigilante
- Desarme Temporizado/ATM
- Só Reset
- Historial

Estes tipos devem cumprir a norma EN 50131. O tipo de grupo de utilizadores define as opções predefinidas do grupo de utilizadores, bem como as alterações permitidas.

Nota: apenas o grupo de utilizadores “Grupo de instaladores” é do tipo Instalador. Além disso, este é o único tipo possível para este grupo.

O tipo de grupo de utilizadores é definido em “3.2.n.2 Tipo de GU” na página nº 209.

A Tabela 16 na página nº 73 apresenta as opções predefinidas e permitidas (privilégios do utilizador) dos grupos de utilizadores.

Nota: nem todas as opções de só leitura são visíveis para tipos de grupos de utilizadores específicos.

Tabela 16: Tipos de grupos de utilizadores e opções permitidas [1]

#	Opção	Tipo de grupo de utilizadores						
		Utilizador normal	Supervisor	Instalador	Vigilante	Desarme Temporizado / ATM	Só Reset	Historial
1.	Arme total	Sim	Sim	Sim	Sim	[Sim]	[Não]	[Não]
2.	Arme parcial 1	Não	Sim	Sim	Sim	[Não]	[Não]	[Não]
3.	Arme parcial 2	Não	Sim	Sim	Sim	[Não]	[Não]	[Não]
4.	Desarmar	Sim	Sim	Sim	Sim	[Sim]	[Não]	[Não]
5.	Só Reset	Sim	Sim	Sim	Sim	[Sim]	[Não]	[Não]
6.	Inibir	Sim	Sim	Sim	Sim	Não	Sim	[Não]
7.	Isolar	[Não]	Sim	[Sim]	[Não]	[Não]	[Não]	[Não]
8.	Hora e data	[Não]	Sim	[Sim]	Sim	[Não]	[Não]	[Não]
9.	Adicionar utlz	[N]	T	[T]	[N]	[N]	[N]	[N]
	N: nenhum R: restrito T: todos							
10.	Arme forçado	Não	Sim	Sim	[Não]	Não	[Não]	[Não]
11.	Alterar PIN	Sim	Sim	[Sim]	Sim	Não	[Não]	[Não]
12.	Walk Test	Não	Sim	[Sim]	Sim	[Não]	[Não]	[Não]
13.	Reset técnico	[Não]	Sim	[Sim]	Não	[Não]	[Não]	[Não]
14.	Código de coacção	Não	Sim	Sim	Não	Não	[Não]	[Não]
15.	Testes de reporte	[Não]	Sim	[Sim]	[Não]	[Não]	[Não]	[Não]
16.	Ligação remota	Não	Sim	[Sim]	[Não]	[Não]	[Não]	[Não]
17.	Limpeza	Não	Não	[Não]	[Não]	[Não]	[Não]	[Não]
18.	Lista áreas GU	Não	Sim	[Sim]	Não	Não	[Não]	[Não]
19.	Aceder menu	Sim	Sim	[Sim]	Sim	[Sim]	Sim	Sim
20.	Acesso instalador	[Não]	Sim	[Não]	[Não]	Sim	[Não]	[Não]
21.	Eventos acesso	Não	Sim	[Sim]	Sim	Sim	Sim	Sim
22.	Stop Reporte	Não	Sim	[Sim]	[Não]	[Não]	[Não]	[Não]
23.	Reporte SMS	Não	Sim [1]	Sim	[Não]	[Não]	[Não]	[Não]
24.	Controlo SMS	Não	Sim [1]	Sim	[Não]	[Não]	[Não]	[Não]
25.	Cartão e PIN P: apenas PIN C: apenas cartão CP: cartão ou PIN	CP	CP	CP	CP	CP	CP	CP
26.	Sem reporte OP/CL	Não	Não	[Não]	[Não]	[Não]	[Não]	[Não]

#	Opção	Tipo de grupo de utilizadores						
		Utilizador normal	Supervisor	Instalador	Vigilante	Desarme Temporizado / ATM	Só Reset	Historial
27.	Programa acesso N: nenhum V: ver CV: controlar/ver	V	CV	<CV>	CV	<N>	<N>	<N>
28.	Aprender comandos	[Não]	Sim	[Sim]	[Não]	[Não]	[Não]	[Não]
29.	Foto Teste CRA	Não	Sim	Sim	Não	[Não]	[Não]	[Não]
30.	Apagar imagem	Não	Sim	Sim	Não	[Não]	[Não]	[Não]
31.	Configuração da CRA	Não	Sim	[Sim]	Não	[Não]	[Não]	[Não]
32.	Shunt	Não	Não	[Sim]	[Não]	[Não]	[Não]	[Não]
33.	Ctrl Regiao	Não	[Sim]	Sim	Não	Não	Não	[Não]
34.	Controlo porta	Não	[Sim]	Sim	Não	Não	Não	[Não]
35.	Reporte notif.	Sim	Sim	Sim	Sim	Sim	Sim	Sim
36.	Ctrl. Notific.	Sim	Sim	Sim	Sim	Sim	Sim	Sim

[valor]: A opção é apenas de leitura.

- [1] O valor poderá depender das predefinições seleccionadas durante o arranque inicial. Consulte “Arranque inicial” na página nº 142 para obter mais informações.
- [2] Consulte “Limitações dos privilégios do utilizador” abaixo para obter mais informações.
- [3] Os números de teclados permitidos dependem da variante do painel. Para mais informações, consulte “Características gerais” na página nº 39.

Para descrições detalhadas das opções dos grupos de utilizadores, consulte “3.2.n.6 Opções de GU” na página nº 210.

Limitações dos privilégios do utilizador

A opção Adicionar utlz determina se o utilizador pode adicionar novos utilizadores e que direitos de utilizador têm estes utilizadores acabados de criar.

- Nada: O utilizador não pode criar novos utilizadores.
- Restrito: O utilizador pode criar novos utilizadores, mas só pode definir permissões iguais ou inferiores às suas próprias permissões.

Por exemplo, se o seu grupo de utilizadores não permite alterar a data e a hora, não pode conceder essa permissão a qualquer utilizador por edição de um grupo de utilizadores, nem atribuir um utilizador a um grupo de utilizadores que tenha essa permissão. Isto afecta opções, assim como áreas. Por exemplo, se o utilizador só tem acesso à Área 1, não pode dar acesso à Área 2 a outro utilizador.

- Tudo: O utilizador pode criar novos utilizadores com quaisquer permissões. Consulte também “Bloqueio de dados do utilizador” na página nº 70.

Opções de grupos de utilizadores

As opções de grupos de utilizadores são definidas no menu “3.2.n.6 Opções de GU” na página nº 210.

Estão disponíveis as seguintes opções:

Tabela 17: Opções de grupo de utilizadores como privilégios do utilizador

#	Opção	Descrição
1.	Arme total	Arme das instalações.
2.	Arme parcial 1	Efectuar um arme parcial 1.
3.	Arme parcial 2	Efectuar um arme parcial 2.
4.	Desarmar	Desarmar.
5.	Só Reset	Confirme os alarmes sem desarmar o sistema.
6.	Inibir	Inibir zonas.
7.	Isolar	Isolar zonas, dispositivos bus, câmaras, etc.
8.	Hora e data	Alterar a data e a hora do sistema.
9.	Adicionar utlz (nenhum / restrito / todos)	Criar novos utilizadores (consulte também “Limitações dos privilégios do utilizador” na página nº 74)
10.	Arme forçado	Efectuar um arme forçado. A disponibilidade desta opção depende da configuração do sistema.
11.	Alterar PIN	Alterar o próprio PIN.
12.	Walk Test	Executar um Walk Test.
13.	Reset técnico	Executar um reset técnico.
14.	Código de coacção	Utilizar um código de coacção.
15.	Testes de reporte	Efectuar uma chamada de teste para uma determinada central receptora.
16.	Ligação remota	Responder a um pedido de acesso remoto.
17.	Limpeza	Deixar zonas inibidas após o desarme.
18.	Lista de áreas do grupo de utilizadores	Visualizar a lista de áreas.
19.	Aceder menu	Aceder ao menu do utilizador.
20.	Acesso Instalador	Conceder ao instalador acesso à configuração do sistema.
21.	Eventos acesso	Aceder aos registos do painel.
22.	Stop Reporte	Parar reportes em curso.
23.	Reporte SMS	Receber reportes SMS.
24.	Controlo SMS	Controlo do sistema através de mensagens SMS.

#	Opção	Descrição
25.	Modo Cartão e PIN	Definir o modo para um determinado grupo de utilizadores (se possível). Estão disponíveis os seguintes modos: <ul style="list-style-type: none"> • Apenas PIN • Apenas cartão • Cartão ou PIN
26.	Sem reporte OP/CL	Os eventos de abertura/fecho gerados por utilizadores do grupo de utilizadores não são reportados.
27.	Programa acesso	Acesso a um programa. Estão disponíveis as seguintes opções: <ul style="list-style-type: none"> • Nada: sem acesso • Ver: acesso restrito. Os utilizadores podem visualizar um programa e cancelar acções para o dia actual. • Configurar: acesso total.
28.	Aprender comando	Programar um comando.
29.	Foto Teste CRA	Activar accionamento remoto de imagens.
30.	Apagar imagem	Apagar imagens.
31.	Configuração da CRA	Configurar a comunicação da CRA.
32.	Shunt	Shunt Zonas.
33.	Ctrl Regiao	Mover utilizadores entre regiões.
34.	Controlo porta	Estado do controlo de portas: bloquear, desbloquear, abrir, abertura programada, activar e desactivar.
35.	Reporte notif.	Criar e receber notificações.
36.	Ctrl. Notific.	Editar e apagar notificações.

Tabela de referências de menu

Os menus seguintes aplicam-se a grupos de utilizadores.

Menu	Pág.	Descrição
3 Gestão utlz	201	Adicionar, editar ou eliminar utilizadores e grupos de utilizadores.
9.1.n.4 Destino	324	Configura a comunicação GSM com os utilizadores.

PIN

O PIN (sigla inglesa de Personal Identification Number - número de identificação pessoal) é um número de 4 a 10 dígitos atribuído a, ou seleccionado por, um utilizador. É necessário introduzir um PIN num teclado Advisor como um pré-requisito para efectuar a maioria das opções do Advisor Advanced. Na configuração do Advisor Advanced, o PIN está associado a um utilizador que identifica o detentor do PIN ao sistema.

A política de PINs no sistema Advisor Advanced pode ser configurada de uma das seguintes formas:

- Os PINs são gerados pelo sistema. O utilizador pode solicitar uma nova geração de PIN.

Um PIN é gerado seleccionando Sim e premindo Enter neste menu. O PIN gerado é visualizado até que Enter seja premido novamente.

- Os PINs são introduzidos manualmente.

Premindo Enter permite introduzir ou editar o PIN do utilizador seleccionado.

O modo de alteração do PIN pode ser definido no menu “8.7.5 Modo alt. PIN” (consulte a página 305).

O comprimento do PIN é programado utilizando “8.7.4 Comprim. PIN” na página nº 304. O número dos PINs disponíveis varia de 10000 (para PINs de 4 dígitos) a 10000000000 (para PINs de 10 dígitos).

Não existem PINs reservados para a utilização do sistema. Qualquer PIN pode ser gerado ou introduzido para ser utilizado. Os PINs devem ser exclusivos. Um PIN não pode ser atribuído a mais de um utilizador. O sistema não gera nem aceita a introdução de PINs já em utilização.

O PIN de utilizador seleccionado pode ser alterado em “3.1.n.2 PIN” na página nº 202, se os dados de utilizador não estiverem bloqueados. Consulte “Bloqueio de dados do utilizador” na página nº 70 para obter mais informações.

Consulte também “Teclas” na página nº 62.

Tabela de referências de menu

Os menus seguintes aplicam-se à configuração e ao uso do PIN.

Menu	Pág.	Descrição
2.2.1.n.3.8.1 Modo cartão e PIN	178	Seleciona um método de controlo.
2.2.1.n.3.9 Bloq. PIN ES	180	Se definido como Sim, não é possível utilizar um PIN durante o tempo de entrada.
2.2.1.n.3.12 Arme rápido	181	Permite armar áreas sem ter de introduzir o PIN ou o cartão.
3.1.n.2 PIN	202	Alterar o PIN do utilizador.
5.1.n.6.3.3.1 Baixa Segurança	245	Define quando a autorização do utilizador é alterada de cartão e PIN para cartão <i>ou</i> PIN.

Menu	Pág.	Descrição
5.1.n.6.3.4.3 Bloq.PIN ES	246	Se definido como Sim, não é possível utilizar um PIN durante o tempo de entrada.
5.1.n.3.5.1 Cartão e PIN	251	Especifica qual o método requerido para abrir a porta a partir do leitor selecionado.
5.1.n.6.3.7 Se PIN arma	255	Configura o funcionamento da porta se a área é armada utilizando um PIN.
5.1.n.7.2 Baixa Segurança	258	Define quando a alteração do utilizador é alterada de cartão e PIN para cartão <i>ou</i> PIN.
8.1.3.2 Cartão e PIN	285	Define o tempo máximo de atraso entre a apresentação do cartão e a introdução do PIN.
8.1.3.6 Manutenção em	286	Configura o tempo de acesso do técnico quando concedido por um utilizador.
8.2.1 Aceit. necess	288	Define se é necessário que um utilizador conceda ao instalador acesso ao menu de programação.
8.2.5 Manutenção em	291	Desativar a função de acesso do instalador antes de expirar o tempo de acesso.
8.2.6 Código desafio	292	Ativa a funcionalidade de tentativas de código.
8.5.1.1 Cartão p/ PIN	300	Tempo permitido entre apresentar um cartão válido a um leitor de portas e introduzir um PIN válido no teclado.
8.7.4 Comprim. PIN	304	Altera o comprimento do PIN.
8.7.5 Modo alt. PIN	305	Seleciona o modo de alteração do PIN apropriado.
8.7.7 Desarme Fácil	307	Se habilitado, pode desarmar instalações introduzindo um PIN ou passando um cartão válido sem premir outras teclas.

Saídas

As saídas Advisor Advanced são elementos lógicos que controlam saídas físicas (relés e colectores abertos). As saídas físicas são utilizadas para controlar portas, sirenes e para controlo de outros dispositivos.

Consulte o Capítulo 2 “Instalação” na página nº 7 para mais informações sobre saídas físicas.

As saídas Advisor Advanced são atribuídas a saídas físicas e são configuradas no menu “6 Outputs e filtros” descrito na página nº 267 do Capítulo 5 “Referência de menu”.

Estas saídas podem ser controladas por zonas, acções do utilizador, triggers, programa ou eventos do sistema utilizando filtros de condições. Consulte “Filtros de condições” na página nº 87 para obter mais informações.

Tabela de referências de menu

Os menus seguintes aplicam-se às saídas.

Menu	Pág.	Descrição
1.2.3.1 Teste de output	153	Verificar saídas e LED.
1.2.5.4 Modo Walktest	157	Verificar a funcionalidade de todo o sistema de alarme.
2.2.2.n.4.7 Módulos Output	194	Número de controladores de saída incluídos no controlador de portas.
6 Outputs e filtros	267	Configurar saídas.
8.1.2 Sirenes	284	Configurar temporizadores aplicáveis às sirenes interna e externa.
8.5.2.1 Mapear relés	301	Definir se as saídas de desbloqueio do controlador de portas podem ser controladas como saídas padrão.

Controlo de acesso

O sistema Advisor Advanced permite controlar o acesso dos utilizadores a regiões específicas utilizando portas. Existem os seguintes tipos de funções de controlo de acesso:

- A funcionalidade básica de controlo de acesso é controlar a função de alarme, inibindo para tal o contacto de porta quando um utilizador autorizado passa um cartão válido ou introduz um PIN válido, ou prime o botão de pedido de saída. Tais funções de controlo de acesso são disponibilizadas utilizando portas padrão.

Consulte “Shunt de porta” na página nº 82 para mais informações sobre shunts de porta.

Consulte também “Portas” abaixo, “Inibição de zonas” na página nº 60.

- As funções avançadas de controlo de acesso incluem anti-passback, regiões de alta segurança, etc. Estas funções só estão disponíveis ao utilizar portas inteligentes, as quais são controladas por controladores de portas (consulte “Controlador de portas” abaixo).

Consulte também “Funções avançadas de controlo de acesso” na página nº 82.

Controlador de portas

As funções avançadas de controlo de acesso são controladas por um controlador de portas, que é um expansor ligado ao bus do sistema ATS.

Um controlador de portas pode controlar até quatro portas inteligentes.

Actualmente, existem os seguintes controladores de portas: ATS1250, ATS125x (ATS1251, ATS1252, ATS1253, ATS1254), CDC4.

Cuidado: Certifique-se de que todos os controladores de porta instalados no bus do sistema são todos de apenas um tipo (CDC4 ou ATS1250/ATS125x) , para evitar conflitos de configuração.

Consulte “Expansores” na página nº 68 para mais informações sobre a instalação de expansores.

Portas

Uma porta é um elemento básico da funcionalidade de controlo de acesso. Existem dois tipos de portas:

- Porta padrão: Uma porta com um leitor ou um teclado atribuído a cada lado da porta, e um botão de pedido de saída para uma saída. A abertura não autorizada da porta causa um alarme de intrusão. Consulte “Funções básicas de controlo de acesso” na página nº 82.

- **Porta inteligente:** Uma porta que pode ser utilizada para o controlo de acesso avançado. Uma porta deste tipo tem até dois leitores e uma região atribuídos a cada lado, entrada e saída. Estas portas são controladas por controladores de portas. Consulte “Funções avançadas de controlo de acesso” na página nº 82.

Utilize o menu “5 Menu Porta” na página nº 241 para configurar portas.

Para o endereçamento predefinido de leitores, zonas de portas e saídas de bloqueio, consulte, “Endereçamento de zonas, saídas e portas” na página nº 33 no Capítulo 2 “Instalação”.

Nota: não é necessário configurar triggers para controlar bloqueios de porta. A saída definida no menu “5.1.n.4 Output Porta” na página nº 243 substitui a configuração de saída.

Grupos de portas

Os grupos de portas especificam quando é concedido acesso a uma porta específica. Os grupos de portas são atribuídos a utilizadores. Cada grupo de portas pode ter um período de tempo diferente (programa) quando pode ser concedido acesso a diferentes portas.

Os grupos de portas são programados em “5.2 Grupos portas” na página nº 261.

Os grupos de portas podem ser atribuídos a utilizadores em “3.1.n.8.1 Grupo de portas” na página nº 207.

Pisos

Um piso é um elemento da funcionalidade de controlo do elevador. Um piso é uma área comum para todas as cabinas de elevador.

Grupos de pisos

Os grupos de pisos especificam quando é concedido o acesso a um piso específico. Os grupos de pisos são atribuídos a utilizadores. Cada grupo de pisos pode ter um período de tempo (horário) diferente em que pode ser concedido o acesso a diferentes pisos.

Os grupos de pisos são usados em conjunto com os grupos de portas (ver “Grupos de portas” acima).

Os grupos de pisos são programados em “5.5 Grupos de pisos” na página 265.

Pode atribuir grupos de pisos a utilizadores em “3.1.N.8.2 Grupo de pisos” na página 207.

Funções básicas de controlo de acesso

Shunt de porta

O shunt de porta é um procedimento que inibe uma porta aberta, que poderia causar um alarme, por um tempo definido.

Uma porta pode ser inibida através de um teclado ou um leitor, ou por um controlador de portas. Consulte “5 Menu Porta” na página nº 241 para obter mais informações sobre shunts de porta.

Funções avançadas de controlo de acesso

Regiões

Uma região é uma área de controlo de acesso definida que possui portas que actuam como fronteiras. As regiões são utilizadas pelas funções de anti-passback para monitorizar em que regiões estão presentes utilizadores. As transferências de uma região para outra podem ser proibidas pelas definições de anti-passback.

Note que a região 1 é a região “fora”.

Utilize o menu “5.3 Regiões” na página nº 263 para editar regiões.

O menu “5.1.n.9.1 Regiões” na página nº 259 permite atribuir leitores de porta específicos a regiões.

Anti-passback

A função anti-passback permite que os utilizadores sejam transferidos de uma região para outra. Entrar numa região duas vezes consecutivas pode não ser possível, ou resultará no registo e reporte de um evento ao operador.

Estão disponíveis os seguintes tipos de anti-passback:

- Soft anti-passback: Um cartão ou PIN válido abre a porta quando utilizado para entrar na região pela segunda vez sem sair primeiro, mas é gerado um relatório.
- Hard anti-passback. Um cartão ou PIN válido *não* abre a porta quando utilizado para entrar na região pela segunda vez sem sair primeiro. Tentar fazê-lo gera um relatório.
- Regioes Anti-passback . Um cartão ou PIN válido *não* abre a porta quando utilizado para sair de uma região diferente da região em que se entrou anteriormente. Por exemplo, se o utilizador tiver entrado na região 3 a partir da região 2, será negada a sua tentativa de entrada na região 2 a partir da região 1. Tentar fazê-lo gera um relatório.

Utilize o menu “5.1.n.9.2 Anti-passback” na página nº 260 para programar o anti-passback para a porta seleccionada.

Alta segurança

As regiões de alta segurança (HSR) exigem que um determinado número de utilizadores de alta segurança (HSU) estejam presentes nas mesmas para permitir a entrada de utilizadores normais. Se um utilizador de alta segurança deixar a região, fazendo com que demasiado poucos HSU estejam presentes na mesma, é emitido um alarme precedido por um tempo de pré-aviso.

O sistema não permite que o utilizador normal permaneça na HSR sem HSU presentes, pelo que o último utilizador de alta segurança não poderá abandonar a área de alta segurança se utilizadores normais estiverem presentes na mesma.

Defina opções de HSU em “5.1.n.9.4 Opções HSU” na página nº 261.

Lógica de macros dos controladores de portas

Cada controlador de portas pode ser programado com macros lógica para controlar as suas saídas dependendo das entradas e flags.

Note que esta estrutura da lógica de macros é diferente da programação de filtros de condições do painel de controlo Advisor Advanced.

Nestas páginas são explicados os princípios da lógica de macros de controlo de porta.

Cuidado: é muito importante planear cuidadosamente a lógica de macros no papel, anotando todos os pormenores e a origem de cada zona e/ou dos event flags antes de proceder à programação.

Macros

Uma macro é um dispositivo de avaliação e tomada de decisão. Possui até quatro entradas e uma saída. Existem 32 macros disponíveis para cada controlador de portas.

As quatro entradas podem ser configuradas individualmente para activar a saída quando activa (OU) ou colectivamente juntas (E) para que duas ou mais entradas tenham de ser activadas para operar a saída.

Notas

- Todas as entradas podem ser invertidas individualmente, como opção, utilizando a função NOT.
- As entradas não utilizadas devem ser definidas como OU.

Os temporizadores das macros

A saída tem muitas opções temporizadas e uma latched. Cada uma das opções temporizadas pode ser programada em minutos ou segundos no intervalo entre 1 e 255.

- Desactivado: A macro está desactivada.

- Não temporizado : Segue apenas o resultado da equação lógica. Se uma entrada de macro (um event flag ou uma saída) para esta macro se alterar, a equação lógica será novamente calculada.
- Em impulso [seg]: Activa-se durante o tempo programado (em segundos) ou o período activo do resultado lógico, o que for mais curto.
- Em impulso [min]: Activa-se durante o tempo programado (em minutos) ou o período activo do resultado lógico, o que for mais curto.
- Em temporização [seg] : Activa-se durante o tempo programado (em segundos), independentemente da alteração da saída de macro.
- Em temporização [min]: Activa-se durante o tempo programado (em minutos), independentemente da alteração da saída de macro.
- ON retardo [seg] : Activa-se após o período de tempo programado (em segundos), a menos que o resultado da equação lógica já não seja válido.
- ON retardo [min] : Activa-se após o período de tempo programado (em minutos), a menos que o resultado da equação lógica já não seja válido.
- OFF retardo [seg] : Segue o resultado da equação lógica, mas permanece activo durante o tempo (em segundos) programado depois de o resultado da equação lógica deixar de estar activo.
- OFF retardo [min] : Segue o resultado da equação lógica, mas permanece activo durante o tempo (em minutos) programado depois de o resultado da equação lógica deixar de estar activo.
- Latched: Activa-se em qualquer uma das três primeiras entradas de macro na equação lógica e é reinicializado apenas pela quarta entrada de macro. Não são utilizadas quaisquer funções E/OU programadas.

Nota: no modo Latched, a entrada de rearme 4 não rearma a saída da macro enquanto alguma das entradas (1, 2 ou 3) estiver activa.

Impulso bloqueio e desbloqueio

Esta função é utilizada apenas em fechos electrónicos especiais que requerem que dois relés separados sejam activados (impulso) em alturas diferentes para abrir, e duas zonas separadas para monitorização.

Os dois relés necessários são retirados do relé especificado no menu “5.1 Portas” na página nº 241. “5.1.n.4 Output Porta” na página nº 243 especifica um relé, e o controlador de portas toma o número de relé sequencial seguinte para o segundo relé de que necessita para operar o bloqueio. Por exemplo; se a saída 17 for introduzida como um número de saída de desbloqueio e esta opção estiver definida como Sim, então as saídas 17 e 18 serão utilizadas para o bloqueio.

São também necessárias duas zonas para que esta operação funcione. Uma é para o contacto de abertura de porta normal (por exemplo, reed switch) e outra é para a monitorização do estado de bloqueio de porta proveniente do bloqueio

electrónico. As duas zonas necessárias são retiradas das opções “5.1.n.6.1.1 Zona de porta” na página nº 244 e “5.1.n.6.1.2 Segunda zona” na página nº 253.

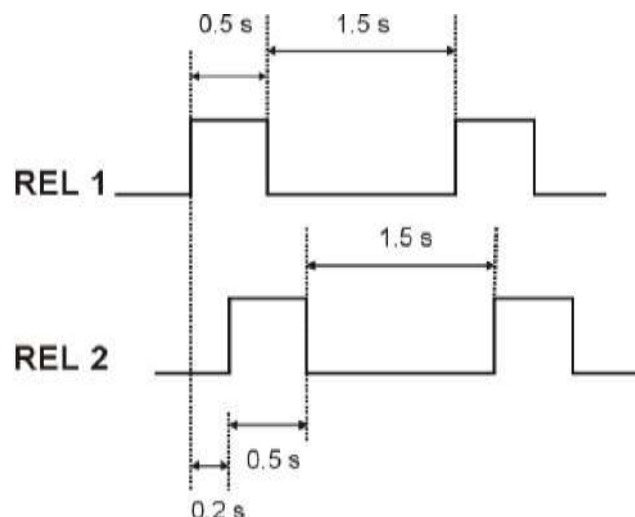
A função é programada em “5.1.n.6.2.3 Bloq/Dbloq Imp” na página nº 254.

A operação específica é a seguinte.

Procedimento de abertura de porta

Ao apresentar um utilizador válido neste leitor, o segundo relé recebe um impulso de ligação durante 0,5 segundos. 0,2 segundos depois de o segundo relé se ligar, o relé recebe um impulso de ligação durante 0,5 segundos. Se, de acordo com a monitorização de zona (explicada abaixo), a porta não se tiver aberto, continuará este procedimento durante o “5.1.n.5.1 Tempo de desbloqueio” descrito na página nº 243. Se for enviado um comando de “Desbloqueio de porta”, este procedimento será continuado permanentemente. O procedimento continua a cada 1,5 segundos. Consulte o diagrama de temporização na Figura 23 abaixo.

Figura 23

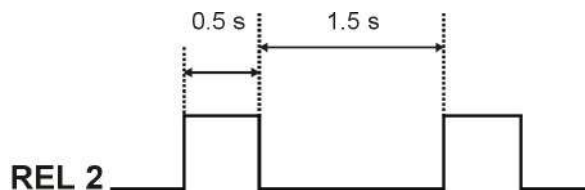


A diferença entre Abertura de porta e Desbloqueio de porta é: O comando de Abertura de porta desbloqueia apenas a porta durante o Tempo de desbloqueio, enquanto que o comando de Desbloqueio de porta abre a porta permanentemente até ser enviado um comando de Bloqueio de porta. Consulte também “1.2.13 Controlo porta” na página nº 168.

Procedimento de bloqueio de porta

O segundo relé recebe um impulso de ligação durante 0,5 segundos. Se, de acordo com a monitorização de zona (explicada abaixo), a porta não se tiver fechado, este procedimento continuará até se fechar. Consulte o diagrama de temporização na Figura 24 na página nº 86.

Figura 24



Monitorização de zonas

A primeira zona é o reed switch e a segunda zona vem do bloqueio electrónico que indica a posição de bloqueio de porta.

- Abertura de porta ou Desbloqueio de porta: se a segunda zona está activa e a primeira zona está normal.
- Bloqueio de porta: se a segunda zona está normal e a primeira zona está activa.

Tabela de referências de menu

Os menus seguintes aplicam-se ao controlo de acesso.

Menu	Pág.	Descrição
1.2.13 Controlo porta	168	Enviar um comando direto para uma porta específica.
2.2.2 Dispositivos DGP	185	Configurar os controladores de portas.
2.2.3 Leit Exp CP/CE	197	Configurar teclados e leitores ligados a um bus de controlador de portas locais.
3.1.n.8 Opções acesso	207	Configurar as opções de controlo de acesso para o utilizador selecionado.
5 Menu Porta	241	Adicionar, editar ou eliminar portas, grupos de portas e regiões.
8.5 Opções de acesso	299	Várias opções de controlo de acesso.

Filtros de condições

Um filtro de condição pode ser utilizado para controlar saídas ou grupos de utilizadores. Cada filtro dispõe de até quatro entradas, e uma saída.

Quatro entradas podem ser configuradas individualmente para activar o filtro quando activo (OR), ou colectivamente juntos (AND), pelo que duas ou mais entradas têm de ficar activadas para operar a saída. Uma entrada de filtro de condição pode ser uma área, uma zona, um evento, ou outra saída de filtro de condição, etc. Todas as dependências são então calculadas à vez.

Figura 25: Como funciona um filtro de condição



Exemplo da utilização de um filtro de condição

Acção necessária: quando a Área 1 está desarmada, introduzir o PIN correcto ou activar a fechadura abre a porta.

1. Seleccione um filtro de condição apropriado utilizando o menu "6.1.n Seleccionar filtro" na página nº 267.
2. Altere o nome do filtro para "Door open" no menu "6.1.n.1 Nome do filtro" na página nº 267.
3. No menu "6.1.n.2 Fórmula", programe o filtro de condição conforme indicado a seguir:

#	Evento ou operando	Descrição
1>	Teclado.1.7	PIN correcto, introduzido no teclado 1.
2	OU	
3	Zona.10.1	Zona activa 10, que é ligada ao computador de chave e é configurada no menu "4 Zonas e áreas".
4	E	
5	Área.1.3	Área 1 desarmada.

4. No menu “6.2 Outputs”, na página nº 269, defina os valores seguintes:

- Seleccione o filtro “Abrir porta” para a saída 10. A saída 10 pode ser utilizada para desbloquear a porta.
- Seleccione o modo Um Impulso.
- Configure o tempo de retardo para 00:00'00.
- Configure o tempo de activação para 00:00'05 s.

Tabela de referências de menu

Os menus seguintes aplicam-se aos filtros de condições.

Menu	Pág.	Descrição
4.5.n.3 Foto p/ filtro	238	Configura os filtros de condições que acionam a câmara.
6.1 Filtros de condição	267	Adicionar, editar e eliminar filtros de condições.
6.2.n.4 Iniciar filtro	270	Especifica um filtro de condições que ativa a saída.
6.2.n.5 Parar filtro	270	Especifica um filtro de condições opcional que desativa a saída.
7.2.n.7 Filtro	281	Atribuir um filtro de condições opcional que ativa o programa.

Triggers

Podem existir até 255 triggers no sistema. Podem ser utilizados em filtros de condições para controlar saídas remotamente. Para mais informações, consulte “Filtros de condições” na página nº 87.

Cada trigger possui alguns flag independentes que podem ser definidos ou redefinidos. Estes flag podem ser controlados de diferentes formas, por exemplo:

- Programa Advisor Advanced. Consulte “Calendário” na página nº 90.
- Comandos por SMS. Para mais informações, consulte o *Guia de Referência do Controlo por SMS do Advisor Advanced*.
- Botões de comando. Os botões de comando podem ser atribuídos a triggers nas definições do expansor sem fios. Para mais informações sobre programação de botões de comando, consulte “Programação de dispositivos sem fios” na página nº 110.
- Software de PC compatível com o Advisor Advanced. Consulte Capítulo 6 “Software” na página nº 353.

Para a lista completa de eventos que pode alterar flag específicos, consulte Anexo A “Eventos do Advisor Advanced” on page 379, grupo “Trigger”.

Consulte “Eventos” na página nº 93 para obter mais informações sobre eventos accionados.

Tabela de referências de menu

Os menus seguintes aplicam-se aos acionadores.

Menu	Pág.	Descrição
1.2.3.2 Est. Trigger	154	Alterar manualmente os estados de flag dos trigger.
6.3 Triggers	273	Adicionar, editar e eliminar triggers.

Calendário

O calendário permite configurar a execução automática de determinadas acções numa data e hora específicas. As configurações do painel podem ser automaticamente ajustadas de acordo com o programa.

O calendário é configurado através do menu “7 Calendário” na página nº 275 do Capítulo 5 “Referência de menu”.

A funcionalidade do calendário baseia-se em programas.

Programas

Cada programa inclui datas de início e de fim, janelas de tempo e acções a realizar. Também define os dias especiais, e o filtro que ativa acções nesta janela horária.

O número máximo de programas, acções, janelas de tempo e dias especiais no sistema é indicado em “Especificações > Características gerais” na página nº 39.

Os programas são definidos pelos parâmetros seguintes.

- **Data:** As datas de início e a de fim determinam um período de tempo em que o programa é válido, ou dois dias em que as acções estarão activadas, consoante a configuração da janela de tempo.
- **Tempo:** É possível definir até 4 janelas de tempo para cada programa.

Cuidado: as janelas de tempo não devem ser coincidentes.

A janela de tempo é determinada pelas horas de início e de fim do dia, e por dias da semana seleccionados.

Atenção: Defina sempre o tempo de fim quando utiliza a janela de tempo, com um dos seguintes: Período Acesso Habilitado, RTE No período, Baixa Segurança no período, e Período Desbloqueado. O tempo de fim não definido (00:00) pode originar comportamentos não especificados.

Se não for seleccionado nenhum dia da semana, a janela de tempo será válida apenas nos dias de início e de fim do programa (programa não recorrente). Caso contrário, o programa será repetido todas as semanas (programa recorrente).

Nota: o programa não recorrente permite apenas a definição de uma janela de tempo.

- **Lista de acções:** Uma lista de acções que têm de ser realizadas pelo sistema quando o programa está activo. Consulte “Acções” na página nº 91.
- **Tempo de dia especial:** Janelas de tempo alternativas que se tornam válidas se o dia actual for um dia especial. Consulte “Dias especiais nos programas” na página nº 91.
- **Filtro:** Um filtro condicional que habilita acções na janela horária quando se torna verdadeiro. Consulte também “Filtros de condições” na página nº 87.

Acções

Uma acção é uma função programada pelo utilizador, que pode ser executada automaticamente pelo sistema de acordo com o programa configurado.

Cada acção tem as seguintes definições:

- Nome
- Função de utilizador: Consulte “Funções de utilizador programáveis” na página nº 105.

Acções contrárias

Cada acção tem uma acção contrária que é oposta a essa acção. Por exemplo:

- A acção contrária de arme de área é desarme de área
- A acção contrária de desinibir zona é inibir zona
- A acção contrária de comutar trigger é comutar trigger, etc.

A acção contrária é definida automaticamente no programa se o fim da janela de tempo estiver definida. Neste caso, a acção é executada no início da janela de tempo e a acção contrária é executada no fim da janela de tempo. Se o fim da janela de tempo não estiver definida (00:00), a acção contrária não será activada.

Dias especiais nos programas

É possível atribuir janelas de tempo de dias especiais a cada programa. Se um programa tiver uma janela de tempo de dias especiais definida, esta será também activada nos dias especiais.

Cuidado: os dias especiais só podem ser configurados em programas recorrentes, que tenham dias da semana seleccionados e que sejam repetidos anualmente.

Os dias especiais são atribuídos a datas no menu “7.1 Ver” na página nº 275.

Nota de hora de Verão

As acções planeadas entre as 2:00 e as 3:00 na alteração da hora de Verão não ocorrem quando os relógios são adiantados e ocorrem duas vezes quando os relógios são atrasados.

Para obter mais informações sobre a programação de hora de Verão consulte “8.1.1 Hora e data” na página nº 283.

Menu de atalhos de programa

A partir da maioria dos elementos do sistema é possível aceder ao menu de atalhos de programa que permite atribuir rapidamente até dois programas ao elemento de sistema seleccionado, por exemplo, área, grupo de utilizadores, etc.

```
1>Sel 1º progr
  Não utilizado
```

Seleccionar um programa permite aceder a uma lista de programas definidos no sistema.

```
0>Adic Z.Horária
1 Programa 1
```

Quando é seleccionado um programa para o elemento seleccionado, ou quando é criado um novo, o sistema adiciona uma acção ao programa seleccionado. A acção contém o elemento seleccionado.

Para editar programas, utilize o menu “7.2 Programas” na página nº 276.

Nota: os elementos e parâmetros disponíveis são descritos em “Funções de utilizador programáveis” na página nº 105.

Tabela de referências de menu

Os menus seguintes aplicam-se ao calendário e aos programas.

Menu	Pág.	Descrição
2.2.1.n.3.24 Programa	183	Atribuir programas ao teclado seleccionado.
3.2.n.7 Programa	210	Atribuir programas ao grupo de utilizadores seleccionado.
4.2.n.8 Programa	233	Atribuir programas à área seleccionada.
5.1.n.7 Opções de zona horária	246	Configura as opções de programa para a porta seleccionada.
5.1.n.3.5.3 Sem ZH Req	252	Estender o acesso de saída para o leitor de saída seleccionado.
6.3.n.2 Programa	274	Atribuir programas ao acionamento seleccionado.
7 Calendário	275	Configura a execução automática de determinadas acções numa data e hora específicas.
8.2.7 Inspeção	292	Configura um lembrete de inspeção periódica.

Eventos

Registo

Todos os eventos são registados no registo do Advisor Advanced. O tamanho do registo é especificado em “Especificações” na página nº 37 do Capítulo 2 “Instalação”.

O registo pode ser visualizado utilizando “1.1 Ver registos” na página nº 148.

Nota: o registo de eventos obrigatórios limita o número de eventos repetidos a 3 eventos num ciclo de arme/desarme. Os eventos excessivos são armazenados no registo de eventos alargado.

Consulte também “Reportes de alarme” na página nº 100.

Programação

Os eventos Advisor Advanced podem também ser utilizados para a programação de funções do utilizador. Consulte “Filtros de condições” na página nº 87 para obter mais informações. Eventos e grupos de eventos, disponíveis para programação com filtros de condições, são indicados no Anexo A “Eventos do Advisor Advanced” na página nº 379.

Tabela de referências de menu

Os menus seguintes aplicam-se aos eventos.

Menu	Pág.	Descrição
1.1 Ver registos	148	Consultar os detalhes do alarme
1.2.5.2.3 Registo não testado	156	Se definido como Sim, as zonas não testadas durante o walk test são registadas no registo do sistema.
4.1.n.6.23 Registo	218	Determina se o evento da zona é registado no registo do sistema.
4.5.n.4 Foto por evrep	238	Permite que a câmara seja ativada por um evento de reporte selecionado.
5.1.n.6.5 A reportar	256	Determina quando os eventos de controlo de acesso são reportados.
6.1 Filtros de condição	267	Configura os filtros de condições ativados pelos eventos.
6.2.n.8 Limite log	273	Limitar o registo de eventos de ativação e restauro da saída seleccionada, para o ciclo de arme três por um.
8.6.5 Restauro de reporte	303	Determina se o evento de restauro é reportado à central recetora quando um utilizador reconhece um alarme.
8.7.6.8 Ligar msg CRA	307	Apresentar uma mensagem com um aviso para o utilizador chamar a central recetora quando um relatório tiver sido enviado.
8.7.6.9 Retardo Rep.	307	Ativa um atraso de 30 segundos antes do reporte de alarme exigido pelos regulamentos ACPO.

Menu	Pág.	Descrição
8.8.10 Reg. Anónimo	312	Definir um período de tempo após o qual os detalhes do utilizador são removidos de uma entrada de registo.
9.1 Central Receptora	316	Configurar as estações centrais e as opções de reporte.
9.2 Opções de eventos	327	Atribuir eventos às centrais recetoras e programar o atraso de reporte.

Testes e diagnósticos

O sistema Advisor Advanced apresenta uma série de funcionalidades de teste. Na sua maioria, estas estão disponíveis em “1.2 Testes ” na página nº 149.

Testes de entradas e detectores

Para testar entradas ou detectores individuais, utilize “1.2.1 Entradas teste” na página nº 149. Um estado de saída individual pode ser verificado em “1.2.1.7 Zona kOhm” na página nº 151.

Para verificar o estado de saídas sem fios, utilize “1.2.1.3 Test RF RSSI” na página nº 150 e “1.2.1.4 Diagnóstico RF” na página nº 150.

O alcance de câmaras PIR sem fios pode também ser verificado em “1.2.1.5 TstAlcance Cam” na página nº 151.

Se o detector possuir a funcionalidade de teste interno, utilize “1.2.1.8 Test Detector” na página nº 152 para configurar um autoteste, ou para executá-lo manualmente.

Teste os sensores de choque através de “1.2.2 Teste Choque” na página nº 153.

Saídas

Teste as saídas ou verifique o seu estado utilizando o menu “1.2.3 Outs e triggers” menu na página nº 153.

Walk test

O Walk Test é um teste de sistema realizado por um utilizador ou instalador. Para passar num teste, o utilizador ou instalador tem de passar pelos detectores para os activar. A intenção é verificar a funcionalidade do sistema de segurança.

A zona passa o teste ao comutar o seu estado de normal para activo e depois de activo para normal. No modo de Walk Test, cada mudança de estado da zona é assinalada pelo besouro do teclado ou por uma campainha interna.

O menu “1.2.5 Walk Test” na página nº 155 permite executar o teste manualmente (Walk Test de técnico), assim como definir condições quando o utilizador tem de executar o Walk Test, incluindo um Walk Test necessário antes de armar uma área (Walk Test de utilizador).

O menu permite também executar um walk test para uma zona única, bem como um walk test geral, que é exigido por um operador de central receptora para verificar todas as funções do sistema de alarme, incluindo arme e desarme, entrada e saída, tampers, etc.

Walk test de técnico

O Walk Test iniciado e executado pelo técnico de manutenção.

O Walk Test aplica-se a todas as zonas com a opção “4.1.n.6.11 Walk Test técnico” na página nº 216 activada.

Configure os parâmetros do teste utilizando o menu “1.2.5.1 Iniciar” na página nº 155.

Seguidamente, execute o Walk Test através de “1.2.5 Walk Test” na página nº 155.

Antes do início do walk test, é-lhe perguntado se o reporte às centrais receptoras deve ser activado.

```
Com reporte
>Sim<
```

Selecione Sim se todos os eventos correspondentes devem ser reportados à central receptora. Este incluem eventos de teste, eventos de walk test, e lista de zonas activadas. Se definido como Não, é enviado apenas um evento de resultado de Walk Test.

Nota: Se o reporte tiver sido inibido durante o início de sessão do instalador, o reporte do walk test é igualmente desactivado. Consulte “Aceder ao menu de programação do instalador” na página nº 134 para obter mais informações.

Em seguida, é-lhe solicitada a escolha entre walk test total e reduzido.

```
Âmbito Walkt.
>Total<
```

Estão disponíveis as seguintes opções:

- Total: Walk test padrão. São testadas todas as zonas adequadas.
- Reduzido: Walk test reduzido. Este teste está limitado apenas a zonas que não estiveram activas recentemente, durante as últimas 4 horas ou desde o último arme.

Nota: O período de tempo é programado em “1.2.5.2.9 Walk reduzido” na página nº 157.

Selecione um âmbito walk test e prima em Enter.

O comando Iniciar Walk Test inicia o Walk Test de técnico para as zonas que têm a opção Walk Test de técnico activada (consulte “4.1.n.6.11 Walk Test técnico” na página 216).

As áreas testadas precisam de ser desarmadas.

Nota: Se as zonas que geram alarmes independentemente do estado da área, por exemplo, tipo 24 h, estiverem incluídas no walk test, são suspensas durante o teste e não provocam um alarme. Contudo, a sua activação é reportada mesmo se o reporte for desactivado durante o início do teste.

Enquanto o teste está a ser executado, a lista de zonas não testadas é percorrida automaticamente. O LCD indica uma zona e a condição que tem de

ser efectuada. Por exemplo, o ecrã ilustrado a seguir indica que a zona 1 deve ser activada.

```
Zona 1
Requer Activ.
```

As zonas desaparecem da lista apresentada à medida que são testadas.

Quando todas as zonas são testadas com êxito, aparece a seguinte mensagem.

```
Walk Test OK
Prima ENTER
```

O teste é cancelado se a tecla Sair for premida. Também existe um limite máximo de tempo no teste, definido em “8.1.3.3 Walk Test” (consulte a página 285). O teste falha se este tempo expirar. Se o reset técnico falhar e a inibição de reporte não estiver activada quando aceder ao modo de programação, uma mensagem é enviada à central receptora a indicar que o teste falhou (consulte “Códigos de reporte utilizados no Advisor Advanced” na página nº 399).

Walk test de zona única

Pode também utilizar “1.2.5.3 UmaZona WT” na página nº 157 para realizar um Walk Test de zona única de acordo com as mesmas regras que o Walk Test de técnico descrito anteriormente.

Modo Walktest

Um modo de walk test especial permite a verificação de toda a funcionalidade do sistema de alarme. Neste modo, um técnico de manutenção ou um guarda devem realizar o maior número possível de acções no sistema de alarme operacional. Isto poderá incluir arme e desarme, entrada e saída, e activar todos os detectores e tampers. O sistema opera como habitualmente, enviando todos os eventos de alarme e de tamper para a central receptora, excepto que nenhuma das sirenes do sistema está activa.

Isto permite ao operador da central receptora analisar todos os alarmes recebidos e verificar se as funções apropriadas do sistema funcionam correctamente.

Walk Test active

O Walk Test activo permite testar o reporte de alarmes no caso de uma simulação de alarme confirmado (exigido pelo ACPO).

Selecione a zona A para alarme A, e a zona B para alarme B.

Primeiro active a zona A e depois a zona B.

O painel simula um alarme confirmado e envia todos os eventos de reporte aplicáveis para a central receptora.

Notas

- As zonas testadas devem ser de um dos tipos seguintes: 1. Alarme, 4. Incêndio, 5. Pânico, 6. 24H, 7. Tamper (Sabotagem), 13. Porta corta-fogo.
- As opções “4.1.n.6.11 Walk Test técnico” na página nº 216 relativas a estas zonas têm de ser activadas.
- Os privilégios de utilizador nesta área têm de permitir o Walk Test. Consulte “3.2 Grupos de utilizadores” na página nº 208 para obter mais informações.

Walk test de utilizador

Se o Walk Test de utilizador estiver configurado e activado, o utilizador deve realizar o Walk Test de utilizador antes de armar uma área. A frequência deste pedido é definida em “1.2.5.2.7 Frequência” na página nº 156. Se a opção “1.2.5.2.8 Necess. armar” na página nº 157 estiver activada, não é permitido armar uma área sem Walk Test de utilizador prévio.

Nota: para efeitos de Walk Test, o Advisor Advanced guarda a informação sobre qualquer activação de zona durante 4 horas. Por conseguinte, se uma zona tiver sido activada durante as últimas 4 horas antes do Walk Test, não é incluída na lista de zonas que têm de ser testadas. Se todas as zonas do Walk Test foram activadas durante este intervalo de tempo, o Walk Test não é solicitado.

Outros testes

Comunicação

Para configurar o teste de comunicação automático ou para executá-lo manualmente, utilize “1.2.6 Chamada de teste” na página nº 158..

Utilize o menu seguinte para diagnosticar caminhos de comunicação correctos (se disponíveis):

- IP: “1.2.7 Diagnóstico IP” na página nº 160
- GSM: “1.2.8 Diagnóst. GSM” na página nº 162

Bateria

Utilize “1.2.9 Teste da bateria” na página nº 164 para diagnosticar o estado da bateria do painel. O menu permite também configurar testes de bateria automáticos.

Teste de sessão de áudio

Utilize o menu “1.2.14 Listen-in” na página nº 169 para executar um teste de sessão de áudio de duas vias com outro número de telemóvel.

Consulte também Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123.

Tabela de referências de menu

Os menus seguintes aplicam-se aos testes.

Menu	Pág.	Descrição
1.2 Testes	149	Aceder a todas as funções de teste.
4.1.n.6.10 Soak test	216	Habilitar o modo soak test para a zona selecionada.
4.1.n.6.11 Walk Test técnico, 4.1.n.6.12 Walk Test utl	216	Permitir ao técnico e ao utilizador efetuar walk tests para a zona selecionada.
4.5.n.8 Foto Teste CRA	239	Obter uma imagem e enviá-la para uma central recetora selecionada.
8.1.4.3 Soak Test	287	Especifica o número de dias em que o soak test de uma zona está ativo.
8.8.6 Testar zonas	311	Define quais as entradas que devem estar acessíveis quando efetuar os testes de entrada.
9.3.n.11 Info módulos	344	Apresenta a versão de firmware do comunicador GSM, tipo de modem, etc.

Reportes de alarme

O reporte de alarmes é um procedimento para transmitir eventos de alarme ou outros eventos para a central receptora através de um comunicador ou outro dispositivo, e um conjunto de regras denominado protocolo.

As funcionalidades de reporte do Advisor Advanced são configuradas através do menu “9 Comunicação” na página nº 316 do Capítulo 5 “Referência de menu”.

Os códigos de reporte disponíveis para protocolos diferentes são indicados no Anexo B “Códigos de reporte utilizados no Advisor Advanced” na página nº 399.

Princípios de reportes de alarme

Consulte o Anexo B “Códigos de reporte utilizados no Advisor Advanced” na página nº 399 para ver uma lista de eventos que podem ser reportados às centrais receptoras.

Quando ocorre um novo evento, o sistema efectua algumas verificações antes de o mesmo ser reportado a centrais receptoras.

O evento está mapeado para alguma central receptora?

Cada evento do sistema Advisor Advanced tem definido um determinado conjunto de centrais receptoras às quais pode reportar. Isto é efectuado através do menu “9.2.1 Mapeamento CRA” na página nº 327.

Por exemplo, a central receptora 1 é o quartel dos bombeiros. Todos os eventos de incêndios podem então ser mapeados para CS 1. CS 3 é uma empresa de segurança que monitoriza alarmes anti-roubo. Os eventos de roubos, bem como os alarmes de tamper, são mapeados para ele.

Se um evento não estiver mapeado, não é reportado para nenhuma central.

Este evento já está a aguardar um reporte?

Se exactamente o mesmo evento (da mesma área e origem) já estiver a aguardar reporte, esse evento só será reportado uma vez.

Existem eventos restaurados?

Existem duas situações possíveis quando dois eventos consecutivos são ignorados durante o reporte:

- O novo evento é um evento restaurado de outro evento que já está a aguardar reporte.
- O novo evento é um evento cujo evento restaurado já está a aguardar reporte.

Se o primeiro evento complementar estiver configurado como um evento retardado no menu “9.2.3 Eventos retardados” na página nº 328, ambos os eventos são excluídos do reporte.

Por exemplo, o alarme anti-roubo (BA) da área 1 é um evento retardado, e o tempo de retardo é de 30 segundos. O evento está mapeado para a CS 1, bem como o evento anti-roubo restaurado (BR). Quando ocorre um alarme na área 1, o evento fica a aguardar reporte. Quando o utilizador confirma o alarme, ocorre o evento de restauro do roubo. Se o utilizador o fizer antes do limite de retardo de 30 segundos, nenhuma informação é enviada à central receptora 1.

Nota: os eventos não se excluem mutuamente se estiverem mapeados para diferentes centrais receptoras.

Este evento faz parte do reporte combinado OP/CL?

Se “9.1.n.9 Relatório OP/CL” na página nº 321 estiver definido como Combinado, apenas o desarme inicial da área (abertura) e o arme final da área (fecho) no grupo de áreas com o mesmo código de conta são reportados à central receptora. Os outros eventos de arme e desarme de área não são reportados.

Por exemplo, as instalações incluem as áreas 1, 2 e 4 (que têm o mesmo código de conta). O proprietário desarma as áreas 1, 2 e depois a 4 de manhã, e no fim do dia volta a armá-las pela mesma ordem. O evento é enviado para a central receptora apenas quando desarma a área 1 e arma a área 4.

Depois de satisfeitas todas as condições referidas acima, o evento fica a aguardar reporte. O possível atraso do reporte depende de factos como o evento poder ser um evento retardado, dos caminhos de comunicação que estão disponíveis e de quantos eventos com prioridade superior já se encontram a aguardar reporte.

Ordem dos reportes

Se existirem vários eventos a aguardar reporte, e várias centrais receptoras às quais reportar, são aplicados os seguintes princípios.

Ligar às centrais receptoras primárias

De entre todas as centrais receptoras primárias que necessitam de ser comunicadas devido a eventos existentes e respectivos mapeamentos, o sistema começa por estabelecer ligação a partir dos números de centrais receptoras mais pequenos para os maiores.

Por exemplo, se existirem eventos a reportar às centrais receptoras 1, 3 e 6, o sistema tenta primeiro contactar a CS 1.

Nota: a primeira tentativa de ligação é efectuada sempre duas vezes. O mesmo se aplica a centrais receptoras de backup.

Se a tentativa de comunicação falhar, o sistema tenta contactar CS 3 e depois CS 6. Se a ligação à CS 6 também não estiver disponível, o sistema começa novamente com a CS 1.

Se estiverem configurados os mesmos retardos e os mesmos números de tentativas de ligação, o Advisor Advanced tenta reportar às centrais receptoras pela ordem seguinte:

1, 1, 3, 3, 6, 6, 1, 3, 6, 1, 3, 6, etc.

Utilizar as centrais receptoras de backup

No caso de falhar o reporte à central receptora primária, o sistema tenta enviar o evento para a central receptora de backup aplicável. Por exemplo, se existirem as centrais receptoras primárias CS 1 e CS 4, e as centrais receptoras CS 2 e CS 3 (centrais de backup de CS 1), o Advisor Advanced tenta reportar às centrais receptoras pela ordem seguinte:

1, 1, 4, 4, 2, 2, 4, 3, 3, 4, 1, 4, 2, 4, 3, 4, 1, etc.

Nota: para manter a ordem de reporte transparente, programe sempre o mapeamento do evento para centrais receptoras de backup igual ao mapeamento para a central receptora primária.

Cuidado: A central recetora de backup aplica-se sempre à central anterior na lista. Tenha cuidado ao eliminar uma central recetora principal, que tem uma central recetora de backup. Se eliminar a central recetora principal CS 1 no exemplo acima, o painel de controlo irá tentar imediatamente comunicar com a central recetora de backup CS 2, porque a central recetora principal já não está acessível. Veja também “9.1.n.6 Modo” na página 318.

Reportar todos os eventos necessários à central receptora

Uma vez estabelecida a comunicação à central receptora, o sistema reporta todos os eventos activos que estão mapeados para esta central receptora.

Depois de todos os eventos necessários terem sido reportados com êxito à central receptora, o sistema fecha a comunicação e tenta contactar a próxima central receptora à qual os eventos activos precisam de ser reportados.

Prioridade de eventos

Na fila de eventos em espera para serem enviados para a CRA, os eventos com maior prioridade são transmitidos em primeiro lugar. Consulte a Tabela 33 na página nº 399 para saber os valores de prioridade de eventos.

Falha de comunicação (FTC)

Cada central receptora tem um valor “9.1.n.7 Repetir contagem”, conforme descrito na página nº 319. Quando o número de tentativas de comunicação mal sucedidas atinge este limite, o sistema pára de tentar reportar para esta central receptora, e gera uma falha FTC para esta central.

Nota: para o protocolo de Voz, existe a possibilidade de evitar a falha FTC utilizando a opção “9.1.n.8.2.1 Suprimir FTC” na página nº 320.

Na condição FTC, o sistema volta a tentar estabelecer a comunicação com a central receptora utilizando chamadas de teste configuradas no menu “1.2.6 Chamada de teste” descrito na página nº 158.

Nota: Se “1.2.6.n.5 Freq CT em FTC” na página nº 160 estiver definido como Sim, a chamada de teste é tentada todas as horas até ser restaurada a falha FTC.

Se surgirem novos eventos para esta central receptora, o sistema inicia novamente as tentativas de comunicação.

Se devido aos limites de tentativas não for possível ao painel enviar um evento a nenhuma das centrais receptoras para as quais está mapeado, é gerada uma falha FTC global.

Por exemplo, existe a central receptora CS 1 e as respectivas centrais receptoras de backup CS 2 e CS 3. O contador de tentativas está definido para 4. O Advisor Advanced tenta reportar às centrais receptoras pela ordem seguinte:

1, 1, 2, 2, 3, 3, 1, 2, 3, 1, <ocorre FTC 1>, 2, <ocorre FTC 2>, 3, <ocorre FTC 3>, <ocorre FTC Global>.

Quando ocorrer o FTC global, os eventos não reportados são eliminados da fila de espera de reportes.

Um evento que ocorra após o FTC global, reinicializa todos os contadores de reporte.

Áudio de duas vias

O áudio de duas vias permite ao operador da central recetora ouvir áudio ao vivo a partir das instalações protegidas no alarme e responder de volta.

Notas

- Apenas versões de firmware específicas são compatíveis com o áudio de duas vias.
- A verificação áudio dois-sentidos só se encontra disponível para o protocolo de reporte (X)SIA e caminhos de comunicação RTPC e GSM.

Nota: O correto envio de mensagens analógicas através do canal GSM, depende da qualidade da rede GSM, que altera frequentemente.

A sessão de áudio com a central recetora inicia-se quando um dos objetos com função listen-in configurada (zona, botões de comando ou teclado) gera um alarme. Quando a sessão de áudio é estabelecida, o dispositivo de áudio atribuído ao objeto em alarme é ligado em modo de escuta.

Durante a sessão de áudio, o operador da central recetora pode enviar comandos específicos utilizando códigos DTMF, se o a configuração do painel o permitir.

Para mais informações, consulte “Áudio de duas vias” na página nº 123.

Tabela de referências de menu

Os menus seguintes aplicam-se aos reportes de testes.

Menu	Pág.	Descrição
1.2.6 Chamada de teste	158	Define o intervalo de chamada de teste automático, e executa uma chamada de teste a pedido.
1.2.7 Diagnóstico IP	160	Ferramentas de diagnóstico para conectividade IP.
3.1.n.7 SMS e Voz	206	Menus de configuração para SMS e reporte por voz.
4.1.n.6.24 Reporte CRA	219	Determina se o evento da zona é reportado à central recetora.
4.1.n.6.38 Stop Reporte	222	Permite que a activação de uma zona de comutador de chave pare o reporte de voz.
4.5.n.3.m.3 Reporta como	238	Atribui um evento de reporte SIA ao filtro condicional da câmara seleccionada.
8.1.3.4 Rtd.rep.230VAC	285	Defini o tempo de atraso antes de uma falha na alimentação de corrente ser comunicada à central recetora.
8.4.3.1 Reporte BA	296	Se definido como Sim, em arme parcial, o sistema reporta à central recetora os alarmes de intrusão ativados durante o arme parcial.
8.6.5 Restauro de reporte	303	Reporta o evento de restauro à central recetora quando um utilizador reconhece um alarme.
8.7.6.8 Ligar msg CRA	307	Permite ao teclado apresentar uma mensagem com um aviso para o utilizador chamar a central recetora quando um alarme tiver sido enviado.
8.7.6.9 Retardo Rep.	307	Habilita um atraso de 30 segundos antes do reporte de alarme exigido pelos regulamentos ACPO.
9 Comunicação	316	Programar todas as opções de comunicação a nível do sistema.

Funções de utilizador programáveis

É possível programar as funções de utilizador que podem posteriormente ser activadas automaticamente ou manualmente. Por exemplo, é possível programar uma função de utilizador para arme de uma área ou comutação de uma saída, e definir de seguida um programa para a mesma.

Menu de programação

O menu de programação de funções é acessível a partir de vários menus onde são utilizadas funções de utilizadores programáveis.

A lista de funções permitidas pode variar consoante o menu.

Para programar uma função de utilizador:

```
1 Tipo
    >Nada<
```

Primeiro, escolha um tipo de função apropriado.

Nota: consoante a entrada do menu de utilizador, poderá ser necessário seleccionar primeiro um tipo de objecto, por exemplo Porta ou Área.

A seguir, configure os parâmetros da função.

Os parâmetros disponíveis dependem do tipo de função seleccionado. Para determinados tipos, os parâmetros estão desactivados.

Nota: Funções particulares requerem a introdução de código. Para desactivar, coloque em “não” o parâmetro “8.2.1 Aceit. necess”, se permitido. Consulte “Aceitação necessária” na página nº 134 para obter mais informações.

Consoante o método de activação, podem estar disponíveis os tipos de funções e parâmetros seguintes.

Tabela 18: Tipos de funções e parâmetros disponíveis

Tipo	Descrição	Parâmetros disponíveis
Nada	Nenhuma função é atribuída	Nenhum
Arme	Armar áreas [1][2]	1. Selecção de áreas 2. Selecção de grupos de áreas 3. Requisito código utilizador
Desarme	Desarmar áreas [1]	1. Selecção de áreas 2. Selecção de grupos de áreas
Trigger	Alterar o estado de um trigger	1. Nome de trigger 2. Alterar estado: limpar, armar ou comutar
Arme parcial 1	Arme parcial 1 para áreas [1][2]	1. Selecção de áreas 2. Requisito código utilizador

Tipo	Descrição	Parâmetros disponíveis
Arme parcial 2	Arme parcial 2 para áreas [1][2]	1. Selecção de áreas 2. Requisito código utilizador
Inibir	Inibir zonas [1][3]	Nenhum
Chamada de teste	Executar uma chamada de teste [3][4]	Nenhum
Ligação de PC	Estabelecer ligação ao PC [1][3]	Nenhum
Modo Técnico	Permitir serviço técnico [5]	Nenhum
Pânico	Activar alarme de pânico	Nenhum
Área CampPorta	Alterar o estado da funcionalidade de campanha na área	1. Selecção de áreas 2. Alteração de estado: limpar, accionar ou comutar
RAS CampPorta	Alterar o estado da funcionalidade de campanha no teclado	1. Selecção de teclado 2. Alteração de estado: limpar, accionar ou comutar
Arme s/T saída	Arme imediato (sem tempo de saída) [1]	1. Selecção de áreas 2. Selecção de grupos de áreas 3. Requisito código utilizador
Reset fogo	Reinicializar detectores de incêndio [1]	1. Selecção de áreas
Ver zonas ab.	Mostrar zonas abertas [1]	1. Requisito código utilizador
Alarme activo	Mostrar zonas em estado de alarme [1]	1. Requisito código utilizador
Falhas activas	Mostrar zonas em falha [1]	1. Requisito código utilizador
Memória de alarmes	Mostrar alarmes confirmados [1]	1. Requisito código utilizador
Alarmes p/ RCO	Mostrar alarmes não confirmados [1]	Nenhum
Controlo GU	Altera os privilégios de grupos de utilizadores	1. Identificação de GU 2 e superior – privilégios de grupo de utilizadores. Selecione um privilégio e depois altere-o. Consulte “3.2.n.6 Opções de GU” na página nº 210 para obter mais informações. Note que o tipo de grupo de utilizadores terá de permitir esta alteração. Consulte “3.2.n.2 Tipo de GU” na página nº 209 para obter mais informações.
Controlo RAS	Alterar opções do teclado	1. Identificação do teclado 2. Alterar estado: bloqueado ou desbloqueado
Walk test	Executar Walk Test [1]	1. Selecção de áreas

Tipo	Descrição	Parâmetros disponíveis
Teste de output	Testar saídas [1][4]	1. Selecção de saídas. Podem ser atribuídas 4 saídas. Estas saídas são activadas em simultâneo pelo período de tempo mais prolongado configurado em “8.1.2.1 Activação” na página nº 284. 2. Requisito código utilizador
Foto Teste CRA	Obter uma imagem e enviar para a central receptora	1. Câmara 2. Central receptora
Alarme de incêndio	Activar um alarme de incêndio	Nenhum
Alarme médico	Activar um alarme médico	Nenhum
Mostrar inibido	Mostrar zonas inibidas	Nenhum
Crédito GSM	Verificar crédito GSM	Nenhum
GU acesso área	Alterar o acesso de utilizadores a áreas	1 Identificação de GU 2 Selecção de áreas 3 Selecção de grupos de áreas
Proibir desarm	Desactivar desarme de área. Nota: Se o desarme for proibido, só é possível desarmar utilizando a Sessão do Downloader Comando e Controlo.	1 Selecção de áreas 2 Alterar estado: Ligado ou Desligado
Shunt	Permitir inibição nas áreas	1 Selecção de áreas 2 Alterar estado: Shunt, Unshunt, Comutar
Mostrar shunt	Mostrar shunt	Nenhum
Mostrar isoladas	Mostrar zonas, teclados e expansores inibidos	Nenhum
Desbloqueada	Desbloquear portas	1. Selecção de porta
RTE	Activar entrada de Pedido de saída para portas específicas	1. Selecção de porta
BaixaSegurança	Activar o modo de baixa segurança para portas específicas	1. Selecção de porta
Acesso Habil.	Activar o acesso às portas de um grupo de portas [6]	1. Selecção de grupos de portas

[1] Consoante as definições do sistema, a função poderá exigir o início de sessão de um utilizador com os privilégios aplicáveis. Consulte “2.2.1.n.3.12 Arme rápido” na página nº 181 para obter mais informações.

[2] O tempo de início de função de arme e arme parcial é o tempo em que o temporizador de aviso é iniciado. O tempo de aviso tem de ser considerado. Consulte “4.2.n.4.1 Tempo de aviso” na página nº 230 para obter mais informações.

[3] A função é uma entrada no menu de utilizador aplicável. Para mais informações, consulte o *Manual do Gestor do Advisor Advanced*.

[4] A função exige o início de sessão do supervisor ou do instalador.

[5] A função exige o início de sessão do supervisor.

[6] Cuidado: Esta função só deve ser executada numa janela de tempo com um tempo final especificado. Consulte também Capítulo 3 “Funções do sistema > Acções contrárias” na página nº 91.

As funções descritas podem ser activadas por qualquer um dos seguintes:

- Programa. Consulte “Calendário” na página nº 90 para obter mais informações.
- Tecla de função. Consulte “Teclas de funções” na página nº 65.
- Comando. Consulte “Programação de dispositivos sem fios” na página nº 110 para obter mais informações.

Tabela de referências de menu

Os menus seguintes aplicam-se a funções programáveis pelo utilizador.

Menu	Pág.	Descrição
2.2.1.n.3.13 Teclas Função	181	Atribuir uma função programável pelo utilizador a qualquer uma das teclas de funções disponíveis.
4.4.n.3 Botões	235	Atribuir uma função apropriada a um botão ou a uma combinação de botões.
7.2.n.5 Lista de Acções	276	Selecionar acções que têm de ser executadas pelo sistema de acordo com o programa seleccionado.

Arme automático

O sistema Advisor Advanced permite efectuar a configuração do arme automático. O sistema pode ser armado automaticamente através de programa.

As opções seguintes devem ser consideradas quando se pretende efectuar o arme automático.

- Utilizando o menu “7 Calendário” na página nº 275, criar uma acção com a função arme. Consulte também “Funções de utilizador programáveis” na página nº 105.
- Configure um programa apropriado utilizando o menu “7.2 Programas” na página nº 276.
- Activar ou desactivar a opção “4.2.n.5.2 AutoArmeSilenc” na página nº 231.
- Se necessário, definir a opção “4.2.n.5.2 Tentar Armar” na página nº 231.
Se Tentar Armar for permitido, configurar “8.4.8 AA tenta util” na página nº 299.
- Definir também a opção “4.2.n.4.1 Tempo de aviso” na página nº 230.
- Opcionalmente, definir a opção “8.4.7 AA tempo tent.” na página nº 298.

Tabela de referências de menu

Os menus seguintes aplicam-se ao arme automático.

Menu	Pág.	Descrição
4.2.n.4.1 Tempo de aviso	230	Período de tempo durante o qual o procedimento de arme automático pode ser adiado.
4.2.n.5.2 Tentar Armar	231	Define se os utilizadores podem adiar ou cancelar o arme automático.
4.2.n.5.2 AutoArmeSilenc	231	O besouro do teclado permanece silencioso durante o tempo de aviso.
7 Calendário	275	Configura um arme automático numa data e hora específicas.
8.4.7 AA tempo tent.	298	Define se e quando o sistema repete a tentativa de arme automático se o mesmo for impossibilitado por uma falha de sistema.
8.4.8 AA tenta util	299	Define um tempo de adiamento de arme automático para o utilizador normal.

Programação de dispositivos sem fios

Para adicionar um dispositivo sem fios, siga um dos procedimentos seguintes.

Aprendizagem de sensores sem fios

Existem dois modos para a aprendizagem de um dispositivo sem fios: o modo sequencial e o modo manual.

Modo sequencial

O modo sequencial permite a aprendizagem rápida de uma variedade de sensores sem fios.

Para a aprendizagem de sensores no modo sequencial:

1. Vá para o menu “4.1.0 Adicionar zona” descrito na página nº 211.

```
1>Expansor 1
2 Expansor 2
```

2. Seleccione a localização da zona.

```
Modo aprender
>Sequencial<
```

3. Seleccione Modo sequencial e prima Enter.

```
INFORMAÇÕES
Tamper RF 1
```

4. Active o dispositivo sem fios. Para mais informações sobre activação, consulte “Activação do dispositivo” na página nº 115.

Se ocorrer um erro, o teclado apresenta uma mensagem de erro e emite sete sinais sonoros.

Exemplo:

```
ERRO
RF duplicado
```

O erro pode ocorrer, por exemplo, ao tentar a aprendizagem de um dispositivo que já está programado no expansor sem fios.

Se o dispositivo estiver programado correctamente, o teclado emite dois sinais sonoros.

Se houver mais dispositivos sem fios a programar, e se as zonas consecutivas sem fios estiverem disponíveis no expansor sem fios, repita a activação de outro dispositivo sem fios.

```
INFORMAÇÕES
Tamper RF 2
```

Para parar o processo de aprendizagem e sair do menu, prima Sair.

Se as zonas seguintes já estiverem ocupadas no expansor sem fios, o processo de aprendizagem é dado por terminado.

Proceda com a configuração da zona.

Modo manual

O modo manual permite a aprendizagem e configuração de um sensor sem fios.

Para a aprendizagem de um sensor no modo manual:

1. Vá para o menu “4.1.0 Adicionar zona” descrito na página nº 211.

```
1>Expansor 1
2 Expansor 2
```

2. Seleccione a localização da zona.

```
Modo aprender
  >Manual<
```

3. Seleccione Modo manual e prima Enter.

```
Tamper RF 1
Prima # p/ ID
```

4. Active o dispositivo, ou prima Enter para introduzir manualmente a identificação do dispositivo sem fios. Para mais informações sobre activação, consulte “Activação do dispositivo” na página nº 115.

```
ID sensor
  > <
```

Nota: Não é suportada a aprendizagem de uma câmara PIR sem fios através da introdução do seu identificador.

O ID do sensor encontra-se impresso na etiqueta de código de barras localizada na caixa do sensor, no seguinte formato: “TX H<nnnnnnn>”. Por exemplo, “Tx H103EB2B” identifica um sensor com o ID 103EB2B. Ver também “4.1.n.7.1 ID sensor” na página nº 226 para mais informação sobre indentificação de sensor.

Se a entrada já tiver sido programada, será informado do facto por uma mensagem e sete sinais sonoros.

```
INFORMAÇÕES
RF existente
```

Seguidamente, é-lhe perguntado se deseja substituir o dispositivo sem fios programado.

```
Subst. Disp RF?
  >Não<
```

Nota: se o dispositivo programado tiver capacidade para duas entradas, o sistema pergunta se o dispositivo deve ocupar duas zonas. Consulte “Sensores RF de duas zonas” na página nº 114.

Se o dispositivo estiver programado correctamente, o teclado mostra uma mensagem informativa e emite um sinal sonoro.

```
INFORMAÇÕES  
RF aprendido
```

Seguidamente, é-lhe perguntado se deseja editar a nova zona.

```
Editar zona?  
>Não<
```

Selecione Sim e prima Enter para editar as definições de zona.

Caso contrário, é-lhe perguntado se deseja aprender outro dispositivo sem fios.

```
Zona seguinte?  
>Não<
```

Selecione Sim se precisar de configurar mais dispositivos. O procedimento será então repetido.

Nota: se o dispositivo sem fios aprendido for uma câmara PIR sem fios, ser-lhe-á também pedido que edite as definições da câmara criada.

```
Editar câmara?  
>Não<
```

Consulte “Utilizar câmaras” na página nº 117 para obter mais informações.

Aprendizagem de comandos

Para adicionar um comando, siga um dos procedimentos seguintes.

Modo sequencial

O modo sequencial permite a aprendizagem de uma variedade de comandos.

Para a aprendizagem de comandos no modo sequencial:

1. Vá para o menu “4.4.0 Adicionar comando” descrito na página nº 234.

```
1>Expansor 1  
2 Expansor 2
```

2. Selecione a localização da zona do comando.

```
Modo aprender  
>Sequencial<
```

3. Selecione Modo sequencial e prima Enter.

```
No. da entrada  
> <
```

4. Selecione um número de entrada.

```
INFORMAÇÕES  
Prog. comando 1.
```

5. Prima a sequência de teclas de programação para activar o comando. Para mais informações sobre activação, consulte “Activação do dispositivo” na página nº 115.

Se ocorrer um erro, o teclado apresenta uma mensagem de erro e emite sete sinais sonoros.

```
AVISO
ERRO
```

O erro pode ocorrer, por exemplo, ao tentar a aprendizagem de um comando que já está programado no expansor sem fios.

Se o comando estiver programado correctamente, o teclado mostra uma mensagem informativa e emite um sinal sonoro.

```
INFORMAÇÕES
Comand aprendido
```

Se houver mais comandos a programar, e se existirem entradas de comando disponíveis no expansor sem fios, repita a aprendizagem de outro comando.

```
INFORMAÇÕES
Prog. comando 2.
```

Para parar o processo de aprendizagem e sair do menu, prima Sair.

Proceda com a configuração do comando.

Modo manual

O modo manual permite a aprendizagem e configuração de um comando.

Para a aprendizagem de um comando no modo manual:

1. Vá para o menu “4.4.0 Adicionar comando” descrito na página nº 234.

```
1>Expansor 1
2 Expansor 2
```

2. Seleccione a localização da zona.

```
Modo aprender
  >Manual<
```

3. Seleccione Modo manual e prima Enter.

```
No. da entrada
  > <
```

4. Introduza o número de entrada.

Se a entrada estiver disponível, é-lhe pedido que active o dispositivo sem fios.

```
Prog. comando 1
Prima # p/ ID
```

5. Prima a sequência de teclas de programação para activar o comando, ou prima Enter para introduzir manualmente a identificação e o código de encriptação do comando. Para mais informações sobre activação, consulte “Activação do dispositivo” na página nº 115.

```
ID FOB  
> <
```

```
Inp. tecla FOB  
> <
```

Se a entrada já tiver sido programada, será informado do facto por uma mensagem e sete sinais sonoros.

```
INFORMAÇÕES  
Comando existe
```

Seguidamente, é-lhe perguntado se deseja substituir o comando programado.

```
Subst. Comando?  
>Não<
```

Se o comando estiver programado correctamente, o teclado mostra uma mensagem informativa e emite um sinal sonoro.

```
INFORMAÇÕES  
Comand aprendido
```

Seguidamente, é-lhe perguntado se deseja editar o novo comando.

```
Editar comando?  
>Não<
```

Selecione Sim e prima Enter para editar as definições do comando.

Caso contrário, é-lhe perguntado se deseja aprender outro comando.

```
Comand seguinte?  
>Não<
```

Selecione Sim se precisar de configurar mais comandos. O procedimento será então repetido.

Sensores RF de duas zonas

Determinados dispositivos RF, por exemplo, sensores de porta/janela e sensores de choque, possuem duas entradas no equipamento. Se estiverem activadas ambas as entradas no dispositivo, durante o processo de configuração o sistema pergunta se devem ser utilizadas duas zonas para reportar os estados destas entradas.

Nota: para que sejam visíveis duas zonas no processo de aprendizagem do dispositivo, este deve ter uma configuração correcta durante a activação. Consulte Tabela 19 abaixo para obter mais informações.

1 ou 2 zonas
>2<

Se for seleccionada uma zona, a funcionalidade desta zona depende da configuração do sensor. Consulte “4.1.n.7.5 Opções sensor” na página nº 227.

Se forem seleccionadas duas zonas, o dispositivo terá de ocupar duas zonas consecutivas.

Se a segunda zona já tiver sido programada, é apresentado um erro.

ERRO
Não é possível

Activação do dispositivo

Consoante o tipo de dispositivo, a activação da aprendizagem do mesmo pode variar. A Tabela 19 abaixo apresenta todos os dispositivos compatíveis e os respectivos métodos de activação.

Tabela 19: Activação da aprendizagem de dispositivos sem fios

Tipo de dispositivo	Activação de aprendizagem
Sensor de porta/janela	Activar um alarme de tamper abrindo a caixa. Notas - Para a programação de duas zonas no modo sequencial, a entrada de contacto externa deve encontrar-se no estado aberto. - Não é possível a programação de duas zonas no modo sequencial com a porta LoNa/sensor de janela. A segunda zona tem de ser adicionada manualmente.
Sensor de choque	Activar um alarme de tamper abrindo a caixa. Nota: Para a programação de duas zonas no modo sequencial, o contacto de lâminas deve ser activado e fechado com o ímane.
Detector de fumo	Activar um alarme de tamper removendo a cabeça do detector da base.
Câmara PIR	Active um alarme de tamper removendo a câmara PIR da sua placa de montagem.
Comando	<ol style="list-style-type: none"> 1. Prima rapidamente o botão de desbloqueio duas vezes, e depois prima continuamente até o LED de comando piscar 3 vezes. Solte imediatamente o botão depois de piscar pela terceira vez. 2. Prima rapidamente o botão de desbloqueio, e depois prima continuamente até o LED de comando piscar 2 vezes. Solte imediatamente o botão depois de piscar pela segunda vez. 3. Prima continuamente o botão de desbloqueio até a luz do touchpad piscar uma vez, e depois solte imediatamente o botão.

Para mais informações sobre a funcionalidade dos dispositivos, consulte um manual de dispositivos sem fios apropriado.

Tabela de referências de menu

Os menus seguintes aplicam-se aos dispositivos sem fios.

Menu	Pág.	Descrição
1.2.1.3 Test RF RSSI	150	Apresenta a indicação da força do sinal recebido (RSSI).
1.2.1.4 Diagnóstico RF	150	Apresenta o estado do dispositivo sem fios.
1.2.1.5 TstAlcance Cam	151	Verifica o sinal de receção da câmara PIR sem fios.
2.2.2 Dispositivos DGP	185	Configura os expansores sem fios.
3.1.n.4 Comandos	204	Configura os comandos de utilizador seleccionados.
4.1.n.7 Detalhes RF	225	Programa manualmente um dispositivo sem fios ou removê-lo do expansor sem fios.
4.4 Comandos	234	Configurar comandos.
4.5 Câmaras	237	Configura os módulos de câmara em câmaras PIR sem fios.

Utilizar câmaras

Uma câmara PIR sem fios é um detector PIR sem fios com uma câmara incorporada. A câmara pode ser programada para obter imagens no caso de activação de zonas associadas, filtros condicionais, bem como por activação manual ou pedidos remotos.

Após um alarme, as imagens associadas são enviadas para uma Central Receptora através de IP/GPRS. Também é possível visualizar imagens a partir de software de configuração.

Configuração

O sistema com um expansor de câmara PIR sem fios pode ter até 8 câmaras PIR sem fios programadas. Cada câmara pode ser activada no caso dos seguintes eventos:

- Activação de uma das 4 zonas atribuídas. As zonas são atribuídas no menu “4.5.n.2 Foto por zona” na página nº 237.

Neste caso, o tipo de evento de câmara depende do tipo de zona. Consulte “Tipos de eventos de câmara” abaixo.

Consulte também “Tipos de eventos de câmara” abaixo.

- Activação de um filtro de condições. O tipo de evento é definido para o filtro programado. Consulte “4.5 Câmaras” na página nº 237.
- Activação de um evento de relatórios normal. Consulte “4.5.n.4 Foto por evrep” na página nº 238.
- Comando de utilizador.
- Pedido remoto de software de configuração.

O número e a qualidade das imagens obtidas dependem do tipo de eventos de câmara.

Tipos de eventos de câmara

Estão disponíveis os seguintes tipos de eventos de câmara.

- Alarme de intrusão. Gerado por zonas de tipo Keybox, alarme, entrada/saída, acesso, 24 H e porta corta-fogo.
- Alarme de incêndio. Gerado por zonas de incêndio.
- Alarme de pânico. Gerado por zonas de pânico.
- Alarme médico. Gerado por zonas médicas.
- Alarme de tamper. Gerado por tamper de zonas.
- Falha. Gerado por zonas técnicas, de falha de transmissão, falha de bateria auxiliar e falha de rede auxiliar.
- Configur. tipo 1. Gerado por filtros condicionais deste tipo.
Os tipos são atribuídos a filtros condicionais em “4.5.n.3.m.2 Tipo de evento <n>” na página nº 238.

- Configur. tipo 2. Gerado por filtros condicionais deste tipo.

Os detalhes do tipo de evento estão descritos na Tabela 20 abaixo.

Tabela 20: Eventos da câmara e códigos de relatórios

Tipo de evento	Activado por tipo de zona [1]	Código SIA [2]
Alarme de intrusão	1. Alarme, 2. Entrada/Saída 1, 3. Acesso, 6. 24H, 13. Porta corta-fogo, 16. Key box, 18. Entrada/Saída 2	BA
Alarme de incêndio	4. Incêndio	FA
Alarme de pânico	5. Pânico	PA
Alarme médico	10. Médico	MA
Alarme de tamper	7. Tamper (Sabotagem)	TA
Falha	11. Técnico, 12. Falha via tx, 14. Flh.230VAC aux, 15. Falha bat.aux	UA
Configur. tipo 1	Não permitido [3]	Seleccionável [4]
Configur. tipo 2	Não permitido [3]	Seleccionável [4]

[1] As zonas de tipos particulares não activam a câmara. São 8. Terminador de saída, 9. Comutador, 17. Reset técnico. Quando uma zona atribuída estiver incluída num dos tipos descritos, será ignorada quando activada.

[2] Se a câmara tiver sido activada por um evento de relatório normal, não ocorre outro evento causado pela activação da câmara. Pode obter uma descrição detalhada dos códigos e dos valores de sub-evento em “Códigos de reporte utilizados no Advisor Advanced” on page 399.

[3] Os eventos de Person. Tipo apenas podem ser activados por filtros de condição.

[4] Consulte “4.5.n.3.m.3 Reporta como” na página nº 238 para obter mais detalhes.

Cada um destes tipos pode ser configurado em “2.2.2.n.4.9.1 Config. Imagem” na página nº 191.

Consoante o tipo de evento de câmara, a câmara pode ser programada para obter uma única imagem ou uma série de imagens, a resoluções baixas ou altas.

Como programar uma câmara:

1. Programe o expansor da câmara PIR sem fios. Consulte “Dispositivos” na página nº 67 para obter mais detalhes.
2. Programe uma câmara PIR sem fios como um detector PIR sem fios. Consulte “Programação de dispositivos sem fios” na página nº 110 para obter mais detalhes.

Se o detector for programado correctamente, a câmara aplicável será criada automaticamente. O número da câmara criada é igual ao número de zona do detector PIR sem fios.

3. Programe as opções da câmara. Consulte “4.5 Câmaras” na página nº 237.

4. Atribua zonas à câmara. Escolha até quatro zonas. A câmara será útil se o seu campo de visão abranger estas zonas ou possíveis vias de evasão de intrusos a partir daí. Consulte “4.5.n.2 Foto por zona” na página nº 237.

Por predefinição, a primeira zona atribuída é a zona do detector sem fios incorporado na câmara PIR sem fios configurada.

5. Se necessário, programe filtros de eventos condicionais que activem a câmara. Consulte “4.5 Câmaras” na página nº 237 para obter mais detalhes.
6. Se necessário, programe eventos de relatórios que activem a câmara. Consulte “4.5 Câmaras” na página nº 237 para obter mais detalhes.

Diagnóstico

Se necessário, utilize os menus seguintes para diagnóstico:

- “1.2.1.3 Test RF RSSI” na página nº 150
- “1.2.1.4 Diagnóstico RF” na página nº 150
- “1.2.1.5 TstAlcance Cam” na página nº 151

Tabela de referências de menu

Os menus seguintes aplicam-se às câmaras PIR sem fios.

Menu	Pág.	Descrição
1.2.1.3 Test RF RSSI	150	Apresenta a indicação da força do sinal recebido (RSSI).
1.2.1.4 Diagnóstico RF	150	Apresenta o estado do dispositivo sem fios.
1.2.1.5 TstAlcance Cam	151	Verifica o sinal de receção da câmara PIR sem fios.
2.2.2 Dispositivos DGP	185	Configura os expansores sem fios.
4.1.n.7 Detalhes RF	225	Programa manualmente um dispositivo sem fios ou removê-lo do expansor sem fios.
4.5 Câmaras	237	Configurar os módulos de câmara em câmaras PIR sem fios.
9.1 Central Receptora	316	Define as opções de transmissão das fotos.

Resolução de problemas

Consulte também Capítulo 7 “Resolução de problemas” na página nº 361.

Mensagem de câmara ocupada

A mensagem de câmara ocupada pode aparecer quando uma câmara ou um expansor sem fios não responder a um pedido por uma das seguintes operações estar actualmente em curso:

- Apagar a memória de imagens no expansor sem fios
- Efectuar o teste RSSI

- Efectuar um teste de diagnóstico RF
- Efectuar o teste de alcance
- Definição do modo da câmara (por exemplo, anular a definição do sistema)
- Obter imagens de acordo com outro pedido
- Efectuar o walk test
- Aprender a câmara
- Actualizar o estado actual (ocorre durante 2 a 3 s a cada 17 minutos)

Solução: repita o pedido após um atraso de alguns segundos.

Mensagem de erro da câmara

A mensagem de erro da câmara aparece devido a um dos seguintes estados:

- A processar outro pedido durante um período superior a 20 s (por exemplo, relatórios de imagens de um pedido anterior para esta câmara)
- Falhou a comunicação

Soluções:

- Repita o pedido após alguns minutos
- Verifique a fonte de alimentação
- Verifique a qualidade da comunicação

Consulte igualmente “Diagnóstico” na página nº 119.

Problemas na linha do receptor OH ao enviar mensagens MMS

O painel de controlo Advisor Advanced fornece uma opção de envio de imagens de câmaras PIR para um receptor Osborne-Hoffman NetRec, e de MMS para utilizadores em paralelo.

Quando o painel de controlo envia mensagens MMS, a mensagem de heartbeat é suspensa. Se este atraso for superior ao período de supervisão, por exemplo, devido ao envio de múltiplas mensagens MMS, o receptor gera uma falha.

Solução: o período de supervisão no receptor OH deve ser superior ao tempo que demora a enviar 10 imagens (VGA) e deve ser prolongado pelo período necessário para APN Switch. Este período é de aproximadamente 7 minutos. Note que condições fracas da rede GSM podem prolongar este período de tempo.

Reset técnico

Alguns eventos podem ser configurados de modo a ser necessário efectuar um reset técnico. O reset técnico pode ser efectuado de uma das seguintes maneiras:

- O técnico (instalador) executa um reset técnico a partir do menu Técnico. Consulte “8.2.4.13 Efectuar reset” na página 291.
- O utilizador introduz um código de reset.

No caso de ser necessário um reset técnico, é apresentado um código de técnico.

```
Reset téc.
Código:23353
```

Neste caso, o utilizador entra em contacto com o técnico (instalador) e fornece-lhe o código de técnico apresentado. Utilizando este código e o código do sistema definido no menu “8.2.4.12 Código sistema” na página nº 290, o instalador calcula um código de reset, que fornece ao utilizador. O utilizador introduz o código calculado e executa um reset técnico após iniciar sessão.

Nota: se o código do sistema não estiver definido, o reset técnico pelo utilizador não estará disponível.

- O reset é efectuado por uma activação do tipo de zona especial Reset Técnico (consulte “4.1.n.2 Tipo de zona” na página nº 213). Isto é utilizado em sistemas que utilizam transmissores RedCare, em que o operador da central receptora pode comutar uma saída que está ligada de volta ao painel para executar um reset técnico.

Tabela de referências de menu

Os menus seguintes aplicam-se ao reset técnico.

Menu	Pág.	Descrição
8.2.4 Reset técnico	289	Define as condições que requerem um reset técnico, efetuar o reset.

Desarme / ATM Temporizado

A ATM (caixa multibanco automática) tem uma funcionalidade de segurança adicional que inclui o seguinte:

- Desarme com código duplo. O utilizador da ATM deve inserir o código e depois inseri-lo novamente depois do período de retardo programado.

O retardo é definido em “8.9.1 Retardo” na página nº 314.

Após este retardo, aparece uma mensagem a pedir para o utilizador inserir novamente o código.

O utilizador deve pertencer a um grupo de utilizadores do tipo Desarme/ATM Temporizado. Consulte “3.2.n.2 Tipo de GU” na página nº 209 para obter mais informações.

- Desarme temporizado. A ATM é desarmada por um período de tempo programado. Este período é definido em “8.9.2 Tempo Desarme” na página nº 315.

O teclado apresenta o tempo de desarme restante.

```
Temp Rest 11 min
```

- Tempo alargado. O utilizador pode prolongar o tempo de desarme por um período de tempo adicional, se esse período for definido em “8.9.3 Tempo Desarme Estendido” na página 229 como maior que 0.

```
Temp Rest 11 min
* p/ temp estend
```

Prima * para prolongar o tempo de desarme. O tempo de desarme pode ser prolongado apenas uma vez.

Nota: a funcionalidade de Desarme/ATM Temporizado está disponível apenas nos teclados LCD.

Tabela de referências de menu

Os menus seguintes aplicam-se ao desarme temporizado.

Menu	Pág.	Descrição
8.9 DesarmTemp/ATM	314	Configura as opções de interface do ATM (caixa automática), por exemplo atraso de desarme e atraso de desarme estendido.

Áudio de duas vias

O áudio de duas vias permite ao operador da central recetora ouvir áudio ao vivo a partir das instalações protegidas em alarme e responder de volta.

Nota: apenas versões de firmware específicas são compatíveis com o áudio de duas vias.

Para o áudio de duas vias funcionar, é requerido o equipamento seguinte:

- Controlador de áudio de duas vias ATS1520 (instalado na caixa do painel de controlo)
- Dispositivos de áudio de duas vias ATS1521 satélite (instalados nas instalações protegidas)
- Módulo ATS7700 RTPC (instalado no interior da caixa do painel de controlo) ou módulo ATS73X0 Módulo GSM.

Nota: O correto envio de mensagens analógicas através do canal GSM, depende da qualidade da rede GSM, que altera frequentemente.

Consulte as fichas de instalação específicas para mais informações sobre a montagem e instalação.

Para ativar o áudio de duas vias:

- Instale dispositivos de áudio utilizando o menu “2.2.4 Dispositivos de áudio” na página nº 198.
- Configure a central recetora necessária e as definições DTMF no menu “9.1.n.10 Listen-in” na página nº 325.
- Configure as definições de zona no menu “4.1.n.8 Listen-in” na página nº 223.
- Configure as definições de comando no menu “4.4.n.5 Listen-in” na página nº 236.
- Configure as definições de teclado utilizando “2.2.1.n.5 Listen-in” na página nº 184.
- Defina o caminho de transmissão para PSTN utilizando “9.1.n.2 Via de transm” na página 317.
- Defina o protocolo de reporte para SIA ou XSIA no menu “9.1.n.3 Protocolo” na página 317.
- Selecione eventos para reporte áudio em “9.2.4 L-in Eventos” na página nº 328.

Sessão de áudio

A sessão de áudio com a central recetora inicia-se quando um dos objetos com função listen-in configurada (zona, botões de comando ou teclado) gera um evento. Quando a sessão de áudio é estabelecida, o dispositivo de áudio atribuído a este objeto é ligado em modo de escuta.

Os eventos seguintes não param a sessão ativa, mas ativam dispositivos de áudio consecutivos e adicionam-nos à lista a seguir. Podem existir até

32 microfones e 4 altifalantes na lista a seguir. A lista a seguir é limpa a cada ciclo de arme.

Durante a sessão de áudio, são silenciadas todas as sirenes; porém, os temporizadores de sirene apropriados não param. Todos os outros reportes por RTPC são colocados em espera até a sessão ter terminado.

No caso de um alarme de coação, todos os altifalantes são desativados; por isso, o modo de fala não tem efeito.

Controlo DTMF

Durante a sessão de áudio, o operador da central recetora pode enviar comandos específicos utilizando códigos DTMF, se a configuração do painel o permitir.

Estão disponíveis os seguintes tons DTMF: 1, 2, 3, 4, 5, 6, 7, 8, 9, *, 0, #, 99.

Utilizando o menu “9.1.n.10.3 Controlo DTMF” na página nº 326, pode atribuir comandos aos tons. Estão disponíveis os seguintes comandos:

- Desabilitado: nenhuma ação atribuída.
- Ouvir: comuta a sessão de áudio para o modo de escuta.
- Falar: comuta a sessão de áudio para o modo de fala.
- Sessão estendida: estende o tempo de sessão em 30 s.
- Terminar sessão: termina a sessão de áudio.
- Acionar os flags 1 a 4: aciona os flags 1 a 4 da central recetora.

Para permitir que o operador da central recetora comute estados de saída no painel de controlo para comando de equipamento externo, proceda do seguinte modo:

- Configure as saídas apropriadas ou funções programáveis pelo utilizador. Consulte também “Saídas” na página 79 e “Funções de utilizador programáveis” na página 105.
- Atribua códigos DTMF apropriados a eventos da central recetora. Utilize “9.1.n.10.3 Controlo DTMF” na página 326. Consulte também “Eventos do Advisor Advanced”, no Anexo A, na página 379.
- Se necessário, utilize “Filtros de condições”, descritos na página 87.

Menus específicos de áudio

Os menus seguintes são específicos para os painéis com a funcionalidade de áudio de duas vias.

Menu	Pág.	Descrição
1.2.14 Listen-in	169	Teste de sessão de audio duas-vias entre o sistema e o telefone
2.1.3 Dispositivos de áudio	174	Visualizar os dispositivos de áudio instalados
2.2.1.n.5 Listen-in	184	Configurar áudio de duas vias para o teclado selecionado
2.2.4 Dispositivos de áudio	198	Configurar dispositivos de áudio

Menu	Pág.	Descrição
4.1.n.8 Listen-in	223	Configurar áudio de duas vias para a zona selecionada
4.4.n.5 Listen-in	236	Configurar áudio de duas vias para o comando selecionado
9.1.n.10 Listen-in	325	Configurar áudio de duas vias para a central recetora selecionada
9.2.4 L-in Eventos	328	Seleciona eventos que ativam uma sessão de áudio de duas vias com uma central recetora.

UltraSync

UltraSync é uma solução de “cloud” segura, ligando dispositivos de alarme a aplicação remota através de um portal Web de Gestão, suportado por um modelo de serviço. A conectividade UltraSync pode ser ativada no painel (todas as variantes ATsx500A), na aplicação móvel Advisor Advanced (IOS/Android), e o software ATS8500.

O caminho de comunicação pode ser único ou duplo: através da ligação Ethernet incorporada e o comunicador GSM/GPRS (ATS73X0) ligado ao painel.

Os eventos podem ser transmitidos por notificações push para os dispositivos móveis, até um máximo de 16 utilizadores.

Nota: As notificações “push” só podem ser recebidas se o smartphone se encontrar ligado a quando do envio da mensagem, e a aplicação em execução. A cloud UltraSync não armazena as notificações após o envio para o serviço de notificações “push”, como tal não existe forma de assegurar que a notificação é entregue no smartphone, uma vez que depende somente da qualidade de ligação entre o smartphone e o serviço de notificações “push”.

Cuidado: quando o painel está registado na “cloud” UltraSync, todo o reporte de segurança da “cloud” é configurado remotamente a partir da “cloud”. Neste caso, as definições de código de cliente são desabilitadas para a central receptora.

O painel é identificado na “cloud” UltraSync pelo seu número de série único. O número de série é mostrado no ecrã “9.5.2 Número SID” descrito na página nº 349.

É necessário definir uma palavra-passe UltraSync para poder ligar o painel remotamente utilizando o Downloader ou a aplicação móvel através da “cloud” segura UltraSync.

Atenção: É necessária ligação a Internet para ativar a funcionalidade UltraSync. Assegure-se que os endereços de IP do painel e de DNS são válidos. Ver “Opções específicas do IP” na página nº 332, “Opções espec. de GSM/SMS/GPRS” na página nº 335, e “1.2.7 Diagnóstico IP” na página nº 160.

A ligação UltraSync utiliza o porta 443 e os seguintes endereços: at1.zerowire.com e at1.ultraconnect.com. Certifique-se de que o seu firewall permite.

Os endereços podem ser alterados no future. Contate o seu fornecedor para obter informação sobre quais os endereços que devem ser permitidos pelo firewall

Modelo de serviço

O serviço fornecido pela “cloud” segura UltraSync existe em dois modelos:

- Modelo de Serviço Básico
- Modelo de Serviço Portal

No Modelo de Serviço Básico, utiliza o número de série único na aplicação móvel e no Downloader para se ligar de modo fácil. Este modelo inclui mensagens push para smartphone. Os reportes de alarme têm de ser configurados pelo instalador para um recetor OH, utilizando um módulo Ethernet ou GSM para comunicação. Quando utilizar a ligação móvel, precisa de utilizar o seu próprio cartão SIM.

No Modelo de Serviço Portal, utiliza todas as funções do modelo Básico e, adicionalmente, pode obter acesso ao portal Web UltraSync. Este portal permite-lhe registar painéis para os ligar a uma central recetora à escolha e executar relatórios ou ver estatísticas de todos os seus painéis ligados. Como parte do modelo, um cartão SIM Carrier pode ser aplicado à conexão celular. Para obter acesso ao portal Web, precisa de solicitar o acesso através do escritório de vendas Carrier e assinar um formulário de pedido UltraSync.

Registo do painel na “cloud” UltraSync

O registo do painel na “cloud” UltraSync tem um custo mensal de serviço.

Um painel não registado não suporta cartões SIM UltraSync. A monitorização do caminho de comunicação UltraSync também não é suportada.

O portal Web e as funções de diagnóstico não estão disponíveis quando o painel está ligado à “cloud” UltraSync utilizando um cartão SIM de terceiros.

Cartão SIM UltraSync

O AT57320-SIM é um módulo AT57320 GSM com um cartão SIM UltraSync pré-instalado. Este módulo e o seu cartão SIM devem ser utilizados para a funcionalidade UltraSync apenas quando o painel está registado no portal UltraSync. *O registo do painel na “cloud” UltraSync tem um custo mensal de serviço.*

A Carrier reserva-se o direito de verificar se o cartão SIM Carrier é utilizado no modem correto. A utilização inadequada do modem ou do cartão SIM pode fazer com que o produto pare de operar com a infraestrutura UltraSync.

Nota: O cartão SIM UltraSync não suporta SMS, relatórios de voz, relatórios GPRS OH e áudio bidirecional.

Cuidado: Quando utilizar o cartão SIM UltraSync, certifique-se de que o nome do APN está vazio. Consulte “9.3.n.7.1 Nome APN” na página 342.

Configurar um painel de controlo a partir da aplicação móvel Advisor Advanced Pro

Consulte “Aplicação móvel” na página nº 129 para obter informações.

Criar um site num portal Web

Cada painel é representado como um site no portal Web. Para adicionar o seu site ao portal Web, proceda do seguinte modo:

1. Certifique-se que o painel está ligado à “cloud” segura através de Ethernet ou GPRS.
2. Inicie sessão no portal Web utilizando o endereço e as credenciais obtidas do fabricante.
3. Na lista de sites disponíveis (painéis), clique em Novo site.
4. Selecione a central recetora (definida pelo fabricante), ou selecione Self Monitoring.
5. Forneça o nome do seu site, que o identifica no portal Web.
6. Introduza a morada e contato da instalação, se necessário.
7. Introduza o número ID de série do seu painel, que se encontra na embalagem, ou no ecrã “9.5.2 Número SID” descrito na página nº 349.
8. Selecione o seu fuso horário.
9. Selecione o canal de reporte (VFNN).
10. Introduza o número da conta.

Nota: o portal Web permite que seja definido apenas um número de conta por painel.

11. Introduza o grau de serviço necessário.

O grau de serviço define o grau de segurança e o reporte do caminho de comunicação, que pode ser IP (Ethernet), celular (GPRS) ou duplo (reporte primário IP e reporte de backup celular).

12. Selecione o formato de reporte requerido pela central recetora.
13. Clique em Criar.

O seu site está agora criado.

Para a sua monitorização e controlo, consulte o manual do apropriado do portal Web.

Tabela de referências de menu

Os menus seguintes aplicam-se à funcionalidade UltraSync.

Menu	Pág.	Descrição
9.1.n.2 Via de transm	317	Define a comunicação da central recetora para a “cloud” UltraSync.
9.5 UltraSync	349	Configurar a comunicação UltraSync.

Aplicação móvel

A aplicação móvel Advisor Advanced Pro permite-lhe monitorizar e controlar o seu sistema de segurança Advisor Advanced através de TCP/IP utilizando um smartphone com o sistema operativo Android ou iOS.

Nota: o seu painel de controlo tem de ser ligado à Ethernet ou à internet (por exemplo, por ligação GPRS). Se o painel estiver ligado a um router doméstico, também têm de ser aplicadas as definições seguintes:

- Configure o reencaminhamento de portas no seu router doméstico
- Em vez de o ligar ao painel, ligue-o ao endereço IP do router ou ao nome DNS

Contacte o seu instalador para ativar a funcionalidade de controlo móvel no seu painel e para obter todos os detalhes de ligação.

Ligar ao painel através da nuvem UltraSync

Para se ligar ao painel a partir da aplicação móvel através do UltraSync, proceda do seguinte modo:

1. Execute a aplicação móvel Advisor Advanced Pro.
2. Defina o UltraSync como o canal de comunicação.
3. Introduza o número de série do seu painel no campo de número SID.
4. Introduza a palavra-passe UltraSync.
5. Introduza o nome do seu painel para identificação na aplicação móvel.
6. Toque em Seguinte.

Introduza o PIN do seu painel e selecione o modo de solicitação do PIN.

Nota: quando um utilizador tenta estabelecer ligação ao painel com um PIN incorreto, dez vezes, o início de sessão remoto é bloqueado durante 30 minutos.

Toque em Iniciar sessão ou Definir painel seguinte, se necessário.

Se a aplicação estiver a ser executada pela primeira vez, é solicitado o contrato de licença de utilizador final (EULA). Leia e aceite o contrato para começar a utilizar a aplicação e ligá-la ao painel.

Para mais informações, consulte o *manual de utilizador da aplicação móvel Advisor Advanced Pro* e a *ajuda online da aplicação móvel Advisor Advanced Pro*.

Tabela de referências de menu

Os menus seguintes aplicam-se à funcionalidade da aplicação móvel.

Menu	Pág.	Descrição
3 Gestão utlz	201	Adicionar, editar ou eliminar utilizadores e grupos de utilizadores.
4.5 Câmaras	237	Configura os módulos de câmara em câmaras PIR sem fios.
6 Outputs e filtros	267	Configura saídas.
9 Comunicação	316	Programa todas as opções de comunicação a nível do sistema.

Segurança dos dados do cartão

Os dados do cartão podem ser protegidos ao utilizar dispositivos de segurança (leitores ATS118X e os keypad ATS1136) com smart cards. Para proteger os dados, devem ser ativadas as funções seguintes:

- **Modo seguro:** Os dados do cartão enviados de um smart card para um dispositivo de segurança são protegidos pela encriptação AES.
- **Canal seguro:** Os dados enviados de um dispositivo de segurança para o painel de controlo através de bus de dados ATS são protegidos pela encriptação AES.

Modo seguro

No modo seguro, o cartão é identificado pelos dados encriptados e guardados no mesmo, e não pelo seu número de série. Os dados do cartão só poderão ser lidos se a chave segura programada no painel estiver correta.

O modo seguro é ativado no menu “8.8.11.1 Modo seguro” na página nº 312.

Nota: trata-se de uma definição para todo o sistema. Apenas os leitores ATS118X e os keypad ATS1136 com leitores suportam o modo seguro. Se a função estiver ativada, ela é aplicada automaticamente a estes dispositivos.

A chave segura é programada no menu “8.8.11.3 Chave App.” na página nº 312.

Nome da aplicação e ID do ficheiro

No modo seguro, o smart card do utilizador pode conter múltiplos dados para várias aplicações.

O painel de controlo, que concede o acesso ao utilizador com um cartão, é identificado como uma das aplicação e números de ficheiro da aplicação definidas neste cartão. O nome da aplicação do sistema é definido em “8.8.11.4 Nome App.” na página nº 312, o seu número de ficheiro é definido em “8.8.11.5 App.IDFicheiro” na página nº 313.

Podem existir até 32 ficheiros para cada aplicação. As ID de ficheiro de aplicação são números hexadecimais de 00 a 1F.

Pode utilizar um smart card noutros sistemas ou painéis de controlo utilizando nomes de aplicação diferentes e as ID do ficheiro. Por exemplo, é possível um cartão ter acesso a seis painéis de controlo ATS com as ID de ficheiro de 01 a 06 para a aplicação “555443”, que engloba os sistemas de segurança ATS.

Nota: cada ficheiro é encriptado com a sua própria chave de aplicação. Consulte também “8.8.11.3 Chave App.” na página nº 312.

Canal seguro

O canal seguro é utilizado para a comunicação entre dispositivos seguros e o painel de controlo através do bus de dados ATS. Se o canal seguro estiver ativado, os dados enviados são encriptados em AES.

Nota: trata-se de uma definição para todo o sistema. Apenas os leitores ATS118X e os keypad ATS1136 com leitores suportam o canal seguro. O canal seguro é ativado automaticamente se o dispositivo suportar esta funcionalidade. A chave de encriptação para o canal seguro é negociada entre o dispositivo e o painel de controlo e não está acessível aos utilizadores.

Cuidado: o seu bus de dados do sistema tem de estar fisicamente protegido contra o acesso não autorizado quando a chave de encriptação do canal seguro é redefinido, por exemplo, durante os seguintes processos:

- Instalação do sistema e colocação em serviço
- Predefinição do painel (consulte “1.7 Reinstalar” na página nº 173 e “8.8.11.8 Predefinição” na página nº 313)
- Arranque inicial (consulte “Arranque inicial” na página nº 142)
- O procedimento de recuperação (consulte “Procedimento de recuperação” na página nº 362)
- A redefinição da chave de comunicação (consulte “2.2.1.n.6 RstChave com.” na página nº 184)

Se um dispositivo existente for substituído por um novo, o novo dispositivo não conhece a chave de encriptação e, portanto, a comunicação entre o dispositivo e o painel não poderá ser estabelecida. Utilize o menu “2.2.1.n.6 RstChave com.” na página nº 184 para redefinir a encriptação, para que o painel e o dispositivo possam negociar uma nova chave de encriptação.

Cuidado: as chaves de encriptação apenas devem ser redefinidas ao substituir um dispositivo existente (por exemplo, com defeito) sem reconfigurá-lo. Esta operação utiliza a chave de encriptação predefinida. Apenas deve redefinir a chave de encriptação quando o sistema estiver totalmente protegido contra a intervenção física e o bus de dados protegido.

O mesmo se aplica ao predefinir o painel de controlo, se estiverem a ser utilizados dispositivos de canal seguro.

Cartão de configuração

Os dispositivos seguros, como leitores ATS118X e os keypad ATS1136 com leitores podem ser programados sequencialmente utilizando um cartão de configuração.

Para preparar o cartão de configuração, siga os passos seguintes:

1. Programar todas as definições de segurança do leitor, utilizando o menu “8.8.11 Secur. LEITOR” na página nº 312.
2. Programar o cartão de configuração com a mesma chave de configuração definida no painel de controlo.

Utilizar o menu “1.5 Cartão de configuração” na página nº 172 para suspender o polling de novos dispositivos por 30 minutos, o que irá permitir programar sequencialmente cada um deles.

Tabela de referências de menu

Os menus seguintes aplicam-se ao modo seguro e à funcionalidade de canal seguro.

Menu	Pág.	Descrição
1.5 Cartão de configuração	172	Suspender o polling de novos dispositivos para programação sequencial com um cartão de configuração.
2.2.1.n.3.8.7 Link a leitor	180	Ligar um leitor ao keypad selecionado.
2.2.1.n.6 RstChave com.	184	repor a encriptação entre o painel e o dispositivo.
8.8.11 Segur. LEITOR	312	Definições de segurança do leitor.

Capítulo 4

Programação

Resumo

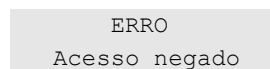
Este capítulo explica como utilizar o menu de programação do Advisor Advanced para programar o sistema.

Índice

- O menu do Advisor Advanced 134
 - Como estão organizadas as secções do menu neste manual 134
 - Disponibilidade de opções 134
 - Aceder ao menu de programação do instalador 134
 - Informações apresentadas no ecrã LCD 136
 - Editar as opções 137
 - Confirmação de alterações 139
 - Sair do menu 139
 - Disposição do teclado 139
- Acesso remoto 141
- Arranque inicial 142
 - Configuração automática 144

O menu do Advisor Advanced

Se tentar seleccionar uma opção não autorizada para o seu PIN (por exemplo, menus do utilizador), o ecrã mostra a mensagem:



ERRO
Acesso negado

Nota: se introduzir um código PIN incorrecto três vezes, o teclado é bloqueado durante 120 segundos.

Como estão organizadas as secções do menu neste manual

As entradas do menu estão numeradas no sistema Advisor Advanced. Este sistema de numeração também é utilizado neste manual, portanto a opção 1 de menu “Inibir zonas” é descrita na secção “1 Inibir zonas”.

O número do menu também corresponde à sequência de teclas que deve premir para aceder ao menu. Por exemplo, se desejar aceder ao menu 1.4 Walk Test, pode premir 1, 4 depois de se encontrar no menu de instalador.

Disponibilidade de opções

Poderão não estar disponíveis todas as opções descritas abaixo.

A disponibilidade das opções depende de um dos factores seguintes:

- Versão de firmware
- Modo do painel (por exemplo, modelo IP ou não IP)
- Expansões instaladas (por exemplo, expansor sem fios ou módulo de comunicação GSM)
- Variante de painel configurada durante o arranque inicial. Consulte “Arranque inicial” na página nº 142 para obter mais informações.

Aceder ao menu de programação do instalador

O sistema Advisor Advanced é programado a partir do menu de programação do instalador. Antes de aceder ao menu de programação, o administrador do sistema tem de desarmar as áreas que serão configuradas. Consoante as definições do sistema, o sistema poderá também solicitar que o utilizador abra a caixa do painel antes de configurar o sistema.

Aceitação necessária

O sistema pode ser configurado de forma a impedir que o instalador aceda a menus sem permissão do gestor. Isto é exigido, por exemplo, pelos regulamentos EN 50131. Isto é definido no menu “8.2.1 Aceit. necess” (consulte a página 288).

Código desafio necessário

O sistema pode ser configurado de forma a impedir que o instalador aceda a menus sem permissão do operador da central receptora. Neste caso, o instalador obtém um código de pedido de 10 dígitos apresentado no LCD quando acede ao menu. O utilizador tem de chamar a central receptora e comunicar este código de pedido ao operador. Seguidamente, o operador da central receptora gera um código de desafio exclusivo e fornece-o ao instalador. O instalador utiliza esse código de desafio para aceder aos menus de programação.

Este código é válido durante o período de tempo definido em “8.1.3.6 Manutenção em” na página nº 286. A opção é activada em “8.2.6 Código desafio” na página nº 292.

Seleção de áreas

Se a opção “8.8.13 Configuração no arme” descrita na página 314 estiver definida para Não, o sistema apenas pode ser programado depois de todas as áreas estarem desarmadas e colocadas no modo de serviço. Neste modo, não ocorrem alarmes e falhas.

Se a opção “8.8.13 Configuração no arme” estiver definida para Sim, é pedido ao instalador que escolha as áreas desarmadas, onde o modo de serviço estará ativado, ao entrar no menu de programação. A lista de seleção de áreas é igual à lista de áreas armadas/desarmadas. Consulte o *Guia do Utilizador do Advisor Advanced* para obter mais informações.

As áreas seleccionadas serão excluídas do funcionamento normal. Os utilizadores não conseguirão controlar estas áreas seleccionadas até o instalador sair do modo de programação.

Nota: A funcionalidade de acesso à porta não é afetada pelo modo de programação.

Como aceder ao menu de programação do instalador

1. Comece com este ecrã LCD:

```
Carrier F&S
TER 27 Mai 10:00
```

2. Se a opção “8.2.1 Aceit. necess” (consulte a página 288) estiver definida como Sim, primeiro tem de ser concedido acesso ao técnico pelo gestor. O gestor tem de iniciar sessão, activar a opção “Modo técnico”, e terminar sessão. Agora o instalador pode iniciar sessão dentro do período de tempo definido em “8.1.3.6 Manutenção em” na página nº 286.

3. Prima Menu. O ecrã apresenta:

```
Cartão/código
>_
```

4. Introduza o seu PIN e, em seguida, prima Enter.

Alternativamente, no caso de estar configurado um cartão, poderá apresentá-lo ao leitor.

5. Selecione as áreas em que o modo de serviço estará ativado e prima Enter. Consulte “Seleção de áreas” na página nº 135 para obter mais informações.

Aparece o ecrã seguinte:

```
Inib. reportes
      >Não<
```

6. Seleccione Sim se desejar inibir todos os reportes durante a programação do sistema. Os reportes incluem os relatórios para a central receptora assim como relatórios de eventos nos registos.
7. Prima Enter. O ecrã seguinte indica se os tampers estão inibidos e se as áreas estão desarmadas:

```
Inibir tampers
Desarmar áreas
```

8. Prima Enter novamente. Encontra-se agora no menu de programação. Aparece o ecrã seguinte:

```
1>Serviço
2 Disp.BUS
```

A partir deste ecrã pode agora:

Opção	Acção	Resultado
Alterar selecção	Prima Para cima ou Para baixo	Seleccionar a entrada de menu anterior ou seguinte
Aceder à entrada de menu	Introduza o número de entrada de menu, ou Prima Enter ou Direita para introduzir o seleccionado	Passar para uma entrada de menu específica
Mostrar ajuda	Prima Ajuda	É apresentada uma descrição da entrada de menu seleccionada (se disponível)
Sair da entrada de menu	Prima Esquerda ou Sair	Sair da entrada de menu

Agora pode seleccionar a opção de menu que deseja programar. Consulte “Mapa de programação” na página nº 429 para ver um diagrama de todas as entradas de menu disponíveis no menu de programação.

Informações apresentadas no ecrã LCD

O ecrã LCD do teclado tem duas linhas de caracteres.

Uma opção de programação ocupa ambas as linhas:

```
DGP número
      >_<
```

Um comando de menu ocupa geralmente uma linha. É mostrado a seguir dois comandos de um menu:

```
1>Disposit. RAS
2 Disposit. DGP
```

Certas entradas de menu ocupam o ecrã inteiro, e a linha “>>>” indica um submenu.

```
3>Config. RAS
      >>>
```

Editar as opções

Após seleccionar a opção de menu que deseja programar, a maioria das opções podem ser programadas utilizando o procedimento padrão descrito em “Como programar” abaixo.

Como programar

O método de programação depende das opções a programar. Algumas opções necessitam de um valor, enquanto que outras apenas necessitam de uma definição de Sim/Não.

Como programar valores

```
3 Tempo entrada
      >_<
```

- 1 a 0: Introduza a nova informação
- Enter: Confirmar a entrada
- Sair: Sair sem efectuar alterações

Como programar opções Sim/Não

```
01 Alarme zona
      >Sim<
```

- Teclas de seta Para cima e Para baixo: Alternar entre opções
- Enter: Confirmar a entrada

Como editar texto

```
1 Nome da área
>Área 1 <
```

As teclas 1 a 9 têm caracteres alfabéticos impressos por cima das mesmas. Para introduzir uma letra, prima a tecla o número de vezes relativo à posição da letra. Estão disponíveis tanto maiúsculas como minúsculas, assim como valores numéricos e espaços. Consulte Disposição do teclado na página 139.

- 1 a 0: Introduzir um carácter
- Para cima: Eliminar um carácter
- Para baixo: Retrocesso
- Esquerda e Direita: Mover o cursor
- Função, e depois Esquerda: eliminar texto para trás
- Função, e depois Direita: eliminar texto para a frente
- Enter: Confirmar a entrada
- Sair: Sair sem efectuar alterações

Como editar uma lista

```
5 Áreas
>12.4....<
```

- Para cima ou Para baixo: Alternar o valor por baixo do cursor
- 0: Incluir ou excluir todos os valores da lista
- Esquerda e Direita: Mover o cursor para um item específico
- Enter: Confirmar a entrada
- Sair: Sair sem efectuar alterações

Se o número de elementos da lista permitidos for maior que 16, os elementos da lista são agrupados, por exemplo:

```
01-10 Áreas
>12.4.....<
```

Neste caso, seleccione primeiro um grupo e depois edite o grupo seleccionado conforme descrito anteriormente.

Como editar um endereço host

```
Nome do Host
> <
```

Utilizando as mesmas regras conforme descrito em “Como editar texto” na página nº 137, introduza uma das seguintes opções:

- Um endereço IP como nnn.nnn.nnn.nnn. Por exemplo, 192.168.1.20.
Nota: Cada número IP, pode ser introduzido em formato decimal, octal ou hexadecimal. O formato Octal requer zero inicial, e o formato hexadecimal utiliza o prefixo 0x. Por exemplo, endereço decimal 192.168.1.20 é igual a 0300.0xA8.0x1.024.
- Um nome de Host como uma sequência de texto. Por exemplo, “carrier.com”. Neste caso, o servidor DNS tem de ser configurado em “9.3.n.6 Config.DNS” na página nº 333, e tem de estar disponível.

Confirmação de alterações

Se determinadas definições forem alteradas, o sistema solicita que confirme essas alterações quando sair do menu actual. Aparece o ecrã seguinte:

```
Aplicar conf.?
  >Não<
```

A alteração de outras definições que afectam a configuração do utilizador, tais como comprimento do PIN, método de coacção, etc., requer a reiniciação da base de dados de todos os utilizadores. Neste caso, é-lhe pedido para confirmar a remoção de todos os utilizadores.

```
Reset util.?
  >Não<
```

Se desejar manter as alterações, escolha “Sim” e prima Enter, caso contrário as alterações serão canceladas.

Sair do menu

Tem de confirmar a sua decisão de sair do sistema de menus. Aparece a mensagem aplicável. Escolha “Sim” e prima Enter para sair do menu.

```
Adeus?
  >Não<
```

Alternativamente, seleccione “Modo técnico”. Neste caso, o painel mantém-se no modo de serviço técnico enquanto o instalador termina sessão no teclado. Permite que o instalador inicie sessão noutra teclado sem sair do modo de programação.

Se existirem quaisquer falhas ou entradas abertas, as mesmas são apresentadas da mesma maneira que no menu “1.2.4 Estado painel” na página nº 154.

Disposição do teclado

Tabela 21: Disposição do teclado ATS111xA para introduzir texto

Tecla	Sequência de caracteres
1	a b c A B C 1
2	d e f D E F 2
3	g h i G H I 3
4	j k l J K L 4
5	m n o M N O 5
6	p q r P Q R 6
7	s t u S T U 7
8	v w x V W X 8

Tecla	Sequência de caracteres
9	y z Y Z 9
0	Espaço . , + - * % 0

Tabela 22: Disposição do teclado ATS113x para introduzir texto

Tecla	Sequência de caracteres
1	. , ` ? ! - & % * / _ < > @ 1
2	a b c A B C 2
3	d e f D E F 3
4	g h i G H I 4
5	j k l J K L 5
6	m n o M N O 6
7	p q r s P Q R S 7
8	t u v T U V 8
9	w x y z W X Y Z 9
0	Espaço 0

A disposição do teclado, assim como o texto do menu, depende do idioma programado para o utilizador actualmente em sessão.

A disposição poderá mudar consoante o contexto do valor editado. Por exemplo, ao editar números de telefone, os dígitos são introduzidos antes dos caracteres.

Acesso remoto

A programação do painel pode ser acedida remotamente através de software de configuração. Um acesso remoto pode ser conseguido por meio de conexão IP, GPRS, RTPC ou RDIS, dependendo da configuração e definições de hardware do painel disponíveis.

Nota: A conexão através de cabo USB não é uma conexão remota.

Por defeito, o menu é acessível remotamente com o mesmo PIN de instalação. O PIN de acesso remoto pode ser alterado, utilizando o menu “3.1.n.2.2 PIN Remoto” na página nº 202.

Cuidados

- Uma vez activado, o PIN remoto não pode ser desactivado nem alterado localmente, e o menu de PIN Remoto é desactivado.
- Se o comprimento de PIN for alterado (através de “8.7.4 Comprim. PIN” descrito na página nº 304) enquanto o PIN remoto estiver activado, o software de configuração não conseguirá voltar a ligar ao painel programado. Será necessário eliminar a configuração do painel no software e voltar a criar a mesma.

A configuração remota só é permitida se a opção “8.7.8.3 Acesso remoto” na página 308 estiver definida para Sempre ou Com assistência técnica. Se esta opção estiver definida para Com assistência técnica, é necessária uma autorização adicional. Consulte “O menu do Advisor Advanced” na página nº 134 para obter mais informações.

O supervisor está autorizado a configurar o painel remotamente apenas se a opção “8.7.8.2 Config. superv.” na página nº 308 o permitir.

Nota: quando um utilizador tenta estabelecer ligação com o painel com um PIN incorreto, três vezes, o início de sessão remoto é bloqueado durante 30 minutos.

Arranque inicial

Ao ligar o sistema pela primeira vez, este solicita que efectue uma instalação.

INFORMAÇÕES
Instal. neces

Cuidado: só é possível efectuar a instalação do sistema inicial a partir do teclado 1.

É necessário definir os valores predefinidos apropriados para este sistema em particular, antes de efectuar a programação. As seguintes definições podem ser definidas durante a instalação.

Tabela 23: Valores definidos durante a instalação

Opção	Descrição
1 Idioma painel	Define o idioma* dos menus do painel. Este idioma é utilizado para mensagens quando nenhum utilizador está em sessão. Após o início de sessão, o idioma muda para o idioma atribuído ao utilizador que iniciou sessão (definido pelo gestor do sistema).
2 Predefinições	Define valores predefinidos dependentes de aprovações*. Nota: Os valores predefinidos das opções de programação específicas podem depender desta seleção. Este manual mostra os valores predefinidos para os padrões EN Grau 3.
3 Hora e data	A data e a hora devem ser configuradas durante a instalação. Consulte também “8.1.1 Hora e data” na página nº 283.
4 UltraSync	Opções UltraSync. Consulte “UltraSync” na página nº 126 para obter mais informações.
1 Conectividade	Ativar ou desativar a ligação à “cloud” UltraSync. Consulte também “9.5.1 Conetividade” na página nº 349.
2 Password	A palavra-passe UltraSync é necessária para ligar o painel remotamente através da “cloud” UltraSync. Consulte também “9.5.3.1 Password cloud” na página nº 349.
5 Outras opc	
1 Método coacção	Método de coacção predefinido. Para mais informações, consulte o <i>Manual do Gestor do Advisor Advanced</i> . Consulte também “8.7.3 Método coacção” na página nº 304.
2 Comprim. PIN	Comprimento predefinido do PIN (permitido no intervalo de 4 a 10). Consulte “8.7.4 Comprim. PIN” na página nº 304 para obter mais informações.
3 Modo alt. PIN	Modo alteração de PIN. Consulte “PIN” na página 77, para obter mais informações sobre a utilização do PIN. Consulte também “8.7.5 Modo alt. PIN” na página nº 305.
6 Instalar	Executar o processo de instalação.

* Contacte o seu fornecedor para obter uma lista dos idiomas disponíveis e das versões aprovadas.

Defina as opções aplicáveis e execute a instalação. Em seguida, escolha OK e prima Enter.

De seguida, é solicitado que altere os PIN's de instalador e supervisor.

```
Alterar PIN
  Installer
```

Pressione Enter.

```
Novo PIN
>_
```

```
Vericar
>_
```

Permite ao novo PIN de instalador com o comprimento requerido, e pressione Enter. De seguida, digite novamente o PIN para verificação.

Se o PIN for alterado com sucesso, é visualizada a seguinte mensagem.

```
INFO
PIN alterado
```

Se o PIN digitado for mais pequeno que o requerido, ou não coincide com o PIN digitado anteriormente, é apresentada a mensagem de aviso

```
AVISO
PIN Errado
```

Se a confirmação do PIN falhar, é apresentada a mensagem de aviso, seguinte.

```
AVISO
PIN NÃO alterado
```

Repita os passos acima descritos para o PIN de supervisor.

```
Alterar PIN
  Supervisor
```

Nota: 1278 é o PIN predefinido para o instalador principal e 1122 é o PIN predefinido para um supervisor. se o comprimento do PIN estiver configurado para mais de 4 dígitos, são acrescentados zeros aos valores PIN predefinidos. Por exemplo, se o sistema estiver configurado para um PIN de 6 dígitos, o PIN do instalador principal é 127800.

Após a alteração de ambos os PIN's com sucesso, o painel continua o processo de instalação.

O ecrã mostra a percentagem completa do progresso da instalação.

Concluída a instalação, o painel é reiniciado.

Nota: Poderá alterar mais tarde a maioria destes valores utilizando o menu "8.7 Painel" consulte a página 304).

Consulte também "1.7 Reinstalar" na página nº 173.

Cuidado: depois de aplicar as predefinições do painel, reinicie o sistema desligando-o e voltando a ligá-lo.

Configuração automática

Durante o segundo arranque do sistema, o painel apresenta uma mensagem para activar uma configuração automática do sistema.

```
Auto Config?  
>Sim<
```

Seleccione Não e prima Enter para cancelar.

Seleccione Sim e prima Enter para executar o processo de configuração automática.

O sistema configura os elementos seguintes:

1 Teclados e expansores.

```
RAS 1-16 BUS1  
R-?-----
```

```
DGP 1-15 BUS1  
-?-----
```

```
Aud 1-16 BUS1  
-?-----
```

Os dispositivos bus são automaticamente configurados de maneira semelhante à configuração através do menu de dispositivos de visualização. Consulte “2.1 Mostrar dispositivos” na página nº 174 para obter mais informações.

2 Zonas.

As zonas são configuradas de acordo com o número de expansores internos e externos instalados, bem como o número de entradas físicas num estado que seja igual ao estado normal da zona.

Nota: o estado normal da zona depende do “2.2.2.n.4.5 Modo de input” na página nº 187 e do “8.6.1 Modo entrada” na página nº 302.

Concluída a configuração, é apresentado o número de elementos configurados.

```
Adicionado  
R:1 D:0 Z:8  
A:0
```

São apresentados os seguintes elementos: R – teclados remotos (ou RAS), D – expansores remotos (DGP), Z – zonas, A – dispositivos de áudio.

Cuidado: após a instalação e a configuração automática, acede automaticamente ao menu de programação. Da próxima vez, necessitará de autorização para entrar no menu.

Capítulo 5

Referência de menu

Resumo

Este capítulo contém a descrição de todas as entradas do menu de programação do painel de controlo Advisor Advanced.

Consulte “O menu do Advisor Advanced” na página nº 134 para obter mais informações sobre a organização do menu.

Índice

- 1 Serviço 148
 - Opções de teste 149
- 2 Disp.BUS 174
 - 2.1 Mostrar dispositivos 174
 - 2.2 Editar dispositivos 175
 - 2.2.1 Dispositivos RAS 175
 - Config. RAS 175
 - 2.2.2 Dispositivos DGP 185
 - Opções de expansores 185
 - Opções específicas sem fios 188
 - Opções específicas da câmara 191
 - Opções específicas do expansor de quatro portas 194
 - 2.2.3 Leit Exp CP/CE 197
 - Opções leitor 197
 - 2.2.4 Dispositivos de áudio 198
 - Opções de dispositivos de áudio 199
- 3 Gestão utlz 201
 - 3.1 Utilizadores 201
 - Opções comuns 201
 - Opções de telemóvel 206
 - Opções de acesso 207
 - 3.2 Grupos de utilizadores 208
 - Opções de grupos de utilizadores 208
- 4 Zonas e áreas 211
 - 4.1 Zonas 211
 - Opções de zona 211

Adicionar um sensor sem fios	212
Opções comuns	212
Opções de sensor de choque	225
Opções de sensores sem fios	225
4.2 Áreas	227
Opções de área	228
4.3 Grupos Área	233
Opções de grupos de áreas	234
4.4 Comandos	234
Opções de comandos	234
4.5 Câmaras	237
5 Menu Porta	241
5.1 Portas	241
Opções comuns de portas	241
Opções específicas de portas padrão	250
Opções específicas de portas inteligentes	251
5.2 Grupos portas	261
5.3 Regiões	263
5.4 Pisos	264
5.5 Grupos de pisos	265
6 Outputs e filtros	267
6.1 Filtros de condição	267
Definições de filtros	267
6.2 Outputs	269
Definições de saídas	269
6.3 Triggers	273
Definições de triggers	273
7 Calendário	275
7.1 Ver	275
7.2 Programas	276
Definições de programas	277
8 Sistema	283
8.1 Temporizadores	283
8.2 Opções de técnico	288
8.3 Menu e LCD	293
8.4 Opções de arme	295
8.5 Opções de acesso	299
8.6 Opções de zona	302
8.7 Painel	304
8.8 Outro	309
8.9 DesarmTemp/ATM	314
9 Comunicação	316
9.1 Central Receptora	316
Opções comuns	317
Opções específicas de RTPC e ISDN	322
Opções espec. de IP e GSM/GPRS	322
Opções específicas de fototransmissão	324

Opções específicas de GSM/Telefone	324
Opções de áudio específicas	325
Opções específicas de UltraSync	326
Opções específicas de VdS	327
9.2 Opções de eventos	327
9.3 Opções de via	328
Opções comuns	329
Opções específicas de PSTN	331
Opções específicas de ISDN	332
Opções específicas do IP	332
Opções espec. de GSM/SMS/GPRS	335
9.4 Ligação de PC	344
Opções comuns	345
Opções específicas de RTPC	347
Opções específicas de IP	348
Opções específicas de GSM	348
9.5 UltraSync	349

1 Serviço

```
1>Ver registos
2 Testes
```

O menu Serviço proporciona um instalador com opções de comissionamento e manutenção, como panorâmica geral do hardware, listas de registos, etc.

1.1 Ver registos

```
1>Tudo
2 Obrigatório
```

O menu Ver registos oferece uma maneira rápida e fácil de observar onde ocorreram alarmes. Esta informação é útil, se tiver reposito um alarme sem verificar inicialmente a sua causa.

É possível seleccionar um dos seguintes tipos de mensagens:

1. Tudo: Todos os eventos.
2. Obrigatório: Apenas eventos considerados obrigatórios pela norma EN 50131-1 (alarmes, arme/arme parcial/desarme, suspensão, sabotagem (tamper), falha, alteração de utilizador, reset técnico, etc.)
3. Não obrigatório: Eventos diferentes dos eventos obrigatórios acima referidos
4. Instalador: Eventos causados por um instalador (modo de programação, ligação PC, etc.)
5. Acesso: Eventos de acesso, tais como acesso concedido e acesso negado
6. Comunicador: Eventos de comunicação e de marcador

O ecrã mostra onde ocorreu o alarme.

```
1>Acesso conced
Utilizador 3
```

Agora pode:

- Percorrer a lista de alarmes. Premir Para cima ou Para baixo
- Visualizar detalhes. Prima Enter.

```
05Mai08 15:04:54
Teclado 1
```

Se houver outras informações, serão percorridas automaticamente.

- Sair do histórico. Permite sair do histórico de alarmes e voltar ao ecrã inicial. Prima Sair.

Opções de teste

1.2 Testes

```
1>Entradas teste
2 Teste Choque
```

O menu Testes dá acesso a todas as funções de teste.

1.2.1 Entradas teste

```
1>Teste de input
2 Qtd zona utiliz
```

Aceda ao menu Teste de entrada para testar as entradas.

1.2.1.1 Teste de input

```
0>Zona
1 Painel
```

Selecione a opção zona para introduzir o número de zona. Em alternativa, selecione primeiro a localização de entrada (painel, expansor interno ou externo) e em seguida introduza o número de entrada (física) desta localização.

São apresentados o número, nome e estado de entrada.

```
12>Armazém
Normal
```

Agora pode:

- Percorrer a lista de zonas. Premir Para cima ou Para baixo.
- Percorrer o estado de entrada, o tipo de zona e a localização de zona. Premir Esquerda ou Direita.

```
12>Armazém
Alarme
```

```
12>Armazém
Exp. painel 1.12
```

- Sair do teste de entrada. Prima Sair.

1.2.1.2 Qtd zona utiliz

```
Zonas Usadas
8/128
```

O menu Número de zonas usadas mostra os seguintes dados de sistema:

- Zonas usadas: número de zonas actualmente programadas.
- Capacidade de zonas: número máximo de zonas no sistema Advisor Advanced.

1.2.1.3 Test RF RSSI

```
1>Expansor 1
2 Expansor 5
```

Selecione primeiro a localização da entrada.

Notas

- São apresentados apenas os expansores RF existentes.
- A função não é suportada nos expansores sem fios ATS1235 com uma versão de firmware anterior a 1.20.

Introduza o número de entrada física desta localização. É apresentado o RSSI para a zona seleccionada.

```
Zona 1
-44dBm [IIII ]
```

Nota: no caso do ATS1235, o valor é actualizado automaticamente cada vez que a zona seleccionada é activada.

Se o detector sem fios estiver equipado com dois transmissores sem fios (LDR — Low Data Rate e HDR — High Data Rate), o ecrã acima mostra os dados LDR.

Prima Direita para alternar entre dados de receptor LDR e HDR, ou aguarde 2 segundos para o ecrã se deslocar automaticamente.

```
Zona 1
QI=50% [III ]
```

Para mais informações sobre a qualidade da comunicação, consulte o manual do expansor sem fios apropriado.

1.2.1.4 Diagnóstico RF

```
1>Expansor 1
2 Expansor 5
```

Selecione primeiro a localização da entrada.

Notas

- São apresentados apenas os expansores RF existentes.
- A função não é suportada nos expansores sem fios ATS1235 com uma versão de firmware anterior a 1.20.

Introduza o número de entrada física desta localização. É então apresentado o estado de RF, por exemplo:

```
Zona 1
LB D
```

O dispositivo pode reportar os seguintes estados:

- Estado de RF OK: O dispositivo RF funciona correctamente
- Sem dados: nenhuns dados recebidos do dispositivo RF
- LB: Falha de bateria fraca

- SS: Falha de supervisão curta
- LS: Alarme de supervisão longa
- D: Sensor de incêndio contaminado

1.2.1.5 TstAlcance Cam

```
17 Câmara 17
18 Câmara 18
```

O teste de alcance permite verificar a recepção de sinal da câmara PIR sem fios. Seleccione uma câmara para activar o teste de alcance.

```
Câmara 17
em tst alcance
```

Neste modo, as câmaras PIR sem fios seleccionadas mostram a qualidade da recepção com as cores de LED de alarme seguintes:

- Verde: Bom sinal
- Laranja: Sinal médio
- Vermelho: Sinal fraco

O LED segue o link da comunicação mais fraco de LDR e HDR.

Para mais informações sobre a qualidade da comunicação, consulte o manual do expansor da câmara PIR sem fios apropriado.

1.2.1.6 Dias inactivos

```
0>Reset tempos
>>>
```

A função de walk test invertido é executada observando todos os temporizadores de zonas inactivos e decidindo se um longo período de inactividade é causado por uma falha de detector.

O menu permite visualizar temporizadores de dias inactivos para cada dia, e repor todos os temporizadores de zona.

De cada vez que uma zona fica activa, o temporizador de dia inactivo é repostado para essa zona. O intervalo do temporizador é de 0 a 127 dias.

Prima 0 para repor todos os temporizadores de dia inactivos.

Escolha uma zona para ver o respectivo temporizador.

```
1>Zona 1
108
```

Consulte também “8.1.4.7 Dias Inactivos” na página nº 288.

1.2.1.7 Zona kOhm

```
1>Painel
2 Exp. zonas
```

O menu permite monitorizar resistências de zona.

Selecione primeiro a localização da entrada (painel ou expansor interno). Em seguida, introduza o número de entrada (física) desta localização.

É apresentada a resistência de zona.

```
Painel 1.1
      4.6kOhm
```

Os valores acima de 65 kΩ são considerados como estado aberto.

Pode agora percorrer a lista de entradas, premindo Cima ou Baixo.

Nota: Os expansores externos (DGP) não suportam esta funcionalidade.

1.2.1.8 Test Detector

```
1>Duração [seg.]
      10
```

A funcionalidade de teste de detectores permite testes remotos de detectores com um teste de entrada dedicado. O menu permite configurar parâmetros de teste de detector automático, ou executar o teste manualmente.

1.2.1.8.1 Duração [seg.]

```
1 Duração [seg.]
      >10<
```

A duração define o período de tempo durante o qual o sinal de teste está activo. O intervalo permitido é de 10 a 60 segundos.

1.2.1.8.2 Tempo teste

```
2 Tempo teste
      >00:00<
```

A hora a que o sistema activa um teste de detector automático.

O intervalo permitido é 00:00 a 23:59, com 00:00 igual a Desligado, significando que o teste automático está desactivado.

1.2.1.8.3 Teste qd Arme

```
3 Teste qd Arme
      >Desligado<
```

Define se um teste automático está activado ou não quando a área com o detector aplicável está armada.

1.2.1.8.4 Teste manual

```
4 Teste Manual
      >Cancelar<
```

Altere o valor para OK e prima Enter para activar o teste de detector manualmente.

1.2.1.9 Shunt Zonas

```
1>Shunt Zonas
   Shunt Off
```

O menu permite inibir zonas manualmente.

1.2.2 Teste Choque

```
1>Painel
2 Exp. zonas
```

Utilizando o menu Teste Choque, pode testar a sensibilidade do sensor de choque.

Selecione primeiro a localização da entrada (painel, expansor interno ou externo). Em seguida, introduza o número de entrada (física) desta localização.

É apresentado o estado da entrada.

```
Painel 1.1
   normal 0
```

Aplicar choques à estrutura. O menu indica o estado da entrada e o nível bruto do choque (para mais informações, consulte “4.1.n.7.2 Nível de impacto” na página 225).

A definição correcta para ataques brutos pode ser definida para o valor + 1, uma vez que um alarme só deve ser activado quando o ataque de teste for excedido.

1.2.3 Outs e triggers

```
1>Teste output
2 Est. Trigger
```

O menu Outs e triggers permite testar as saídas e verificar o estado dos triggers.

1.2.3.1 Teste de output

```
1>Outputs
2 LEDs de RAS
```

O Teste de saída permite verificar as saídas e os LEDs.

1.2.3.1.1 Outputs

Utilize o menu Saídas para testar as saídas do sistema.

Selecione primeiro a localização da saída (painel, expansor interno ou externo ou teclado). Em seguida, introduza o número de saída desta localização.

É apresentado o estado actual da saída.

```
Painel 1.1
   Desligado
```

Agora pode:

- Alternar o respectivo estado utilizando o botão Enter.
- Percorrer a lista de saídas. Premir Para cima ou Para baixo

- Sair do teste de saída. Após sair, a saída volta ao seu estado original. Prima Sair.

1.2.3.1.2 LEDs de RAS

```
1>Teclado 1
2 Teclado 2
```

Utilize o menu LEDs de Teclado para testar os LEDs do teclado e do leitor. Escolha o teclado e prima Enter.

Agora pode:

- Comutar todos os LEDs de teclado para o estado ligado ou desligado utilizando o botão Enter.
- Sair do teste de LEDs de teclado. Prima Sair para sair do teste e restaurar o estado dos LEDs.

1.2.3.2 Est. Trigger

```
1>Trigger 1
2 Trigger 2
```

O menu do estado do trigger permite alterar manualmente o estado dos flags dos triggers.

Selecione o trigger e depois escolha o flag aplicável. Em seguida, defina o estado requerido.

```
1>PROGRAMA
    Desligado
```

1.2.4 Estado painel

```
1>Zonas Abertas
2 Alarmes
```

O menu de estado do painel apresenta uma perspectiva geral de todos os estados de zonas anómalos, alarmes e falhas presentes no sistema.

Selecione o estado que pretende visualizar.

1.2.4.1 Zonas Abertas

```
INFORMAÇÕES
Zonas Abertas
```

```
2>Porta frente
    Tamper zona
```

Ver estados de zona anómalos.

Todos os itens são percorridos automaticamente. Prima Enter para sair.

1.2.4.2 Alarmes

```
INFORMAÇÕES
Sem alarmes
```

Ver alarmes activos. Prima Enter para sair.

1.2.4.3 Falhas

```
INFORMAÇÕES
Sem falhas
```

Ver falhas do sistema activas. Prima Enter para sair.

1.2.5 Walk Test

```
1>Iniciar
2 Opções
```

O menu Walk Test permite testar as zonas. A zona passa o teste ao comutar o seu estado de normal para activo e depois de activo para normal. No modo de Walk Test, cada mudança de estado da zona é assinalada pelo besouro do teclado ou por uma campainha interna.

Consulte também “Walk test” na página nº 95 do Capítulo 3 “Funções do sistema”.

1.2.5.1 Iniciar

Execute o Walk Test técnico.

Consulte “Walk test de técnico” na página nº 95 para obter mais informações.

1.2.5.2 Opções

```
1>Usar sir. int
Sim
```

O menu Opções permite configurar as seguintes opções de Walk Test.

1.2.5.2.1 Utilizar sirene interna

```
1 Usar sir. int
>Sim<
```

Se a opção Utilizar sirene interna estiver definida como Sim, cada activação de zona testada é assinalada pela sirene interna.

1.2.5.2.2 Utilizar besouros

```
2 Usa besouro?
>Não<
```

Se definido para Sim, cada activação de zona de teste é sinalizada pelo besouro do teclado.

1.2.5.2.3 Registo não testado

```
3 Reg. não test
  >Sim<
```

Se a opção Registo não testado estiver definida como Sim, as zonas não testadas são registadas no registo do sistema.

1.2.5.2.4 Tamper de zona

```
4 Tamper zona
  >Sim<
```

Se a opção Tamper de zona estiver definida como Sim, o tamper de zona é incluído no Walk Test.

1.2.5.2.5 Tamper de RAS/DGP

```
5 Tamper RAS/DGP
  >Não<
```

Se a opção de tamper Teclado/expansor estiver definida como Sim, os alarmes de tamper de teclados e expansores atribuídos a esta área têm também de ser testados.

1.2.5.2.6 Tamper de sirene

```
6 Tamper sirene
  >Não<
```

Se a opção Tamper de sirene estiver definida como Sim, os alarmes de sabotagem (tamper) das sirenes atribuídas a esta área também têm de ser testados.

1.2.5.2.7 Frequência

```
7 Frequência
  >Nunca<
```

A definição Frequência define quão frequentemente o utilizador tem de executar o Walk Test de utilizador antes de armar uma área. Estão disponíveis as seguintes opções:

- Nunca: Um Walk Test de utilizador não é necessário
- A cada arme: O utilizador deve executar o Walk Test antes de cada arme
- 1.º arme do dia: O utilizador deve executar o Walk Test antes do primeiro arme de cada dia
- 1.º arme da semana: O utilizador deve executar o Walk Test antes do primeiro arme de cada semana
- 1.º arme do mês: O utilizador deve executar o Walk Test antes do primeiro arme de cada mês

Nota: para efeitos de Walk Test, o Advisor Advanced guarda a informação sobre qualquer activação de zona durante 4 horas. Por conseguinte, se uma zona tiver sido activada durante as últimas 4 horas antes do Walk Test, não é incluída na lista de zonas que têm de ser testadas. Se todas as zonas do Walk Test foram activadas durante este intervalo de tempo, o Walk Test não é solicitado.

1.2.5.2.8 Necess. armar

8 Necess. armar
>Desligado<

Se a opção Necess. armar estiver definida como Ligado, é obrigatório o Walk Test de utilizador solicitado. A área não pode ser armada até aprovar o Walk Test.

1.2.5.2.9 Walk reduzido

9 Walk reduzido
>4h<

O período de walk test reduzido é um período de tempo antes de o walk teste reduzido iniciar, em que a activação de zona particular exclui esta zona da lista de zonas a ser testadas. Estão disponíveis as seguintes opções:

- 4 h: O walk test reduzido inclui apenas zonas que não estiveram activas nas últimas 4 horas.
- Arme/arme: O walk test reduzido inclui apenas zonas que não estiveram activas no último arme.

Consulte “1.2.5.1 Iniciar” na página nº 155 para obter mais informações sobre o walk test reduzido.

1.2.5.3 UmaZona WT

Com reporte
>Sim<

Antes do início do walk test, é-lhe perguntado se o reporte às centrais receptoras deve ser activado (consulte “1.2.5.1 Iniciar” na página nº 155 para mais informações).

Seleccione primeiro a localização da entrada (painel, expansor interno ou externo). Em seguida, introduza o número de entrada (física) desta localização.

Proceda com o walk test relativamente a esta zona em particular, tal como para todas as zonas num walk test standard. Consulte “1.2.5.1 Iniciar” na página nº 155.

1.2.5.4 Modo Walktest

4 Modo Walktest
>Não<

Um modo de walk test especial permite a verificação de toda a funcionalidade do sistema de alarme. Neste modo, um técnico de manutenção ou um guarda

devem realizar o maior número possível de acções no sistema de alarme operacional. Isto poderá incluir arme e desarme, entrada e saída, e activar todos os detectores e tampers. O sistema opera como habitualmente, enviando todos os eventos de alarme e de tamper para a central receptora, excepto que nenhuma das sirenes do sistema está activa.

Isto permite ao operador da central receptora analisar todos os alarmes recebidos e verificar se as funções apropriadas do sistema funcionam correctamente.

1.2.5.5 WT Activo

```
Zona A  
>>>
```

O Walk Test activo permite testar o reporte de alarmes no caso de uma simulação de alarme confirmado (exigido pelo ACPO).

Consulte “Walk Test active” na página nº 97 para obter mais informações.

1.2.6 Chamada de teste

```
1>CRA 1  
2 CRA 2
```

O menu Chamada de teste permite definir o intervalo de chamada de teste automático, e executar uma chamada de teste a pedido.

1.2.6.n Seleccionar a CRA

```
1>Modo Cham Test  
Off
```

Selecione a estação receptora para configurar as opções de chamada de teste.

1.2.6.n.1 Modo Cham Test

```
1 Modo Cham Test  
>Desligado<
```

Selecione o modo de chamada de teste. Estão disponíveis os seguintes modos:

- Desligado: A funcionalidade de chamada de teste automática está desactivada.
- Tempo: A chamada de teste automática é accionada todos os dias à hora programada em “1.2.6.n.2 T. Cham. teste” na página nº 159.
- Período: A chamada de teste automática é accionada uma vez à hora especificada em “1.2.6.n.2 T. Cham. teste” na página nº 159, e repete-se depois no intervalo programado em “1.2.6.n.3 Período” na página nº 159.

1.2.6.n.2 T. Cham. teste

2 T. Cham. teste
>00:35<

Se o “1.2.6.n.1 Modo Cham Test” na página nº 158 estiver definido como Tempo, o menu permite definir a hora do dia para chamadas de teste para a central receptora.

Se o “1.2.6.n.1 Modo Cham Test” na página nº 158 estiver definido como Período, o menu permite definir a hora do dia para a *primeira* chamada de teste para a central receptora. Uma vez definida a hora neste menu, o painel começa a enviar o relatório do RP do evento (teste automático/teste de chamada) para as centrais receptoras apropriadas. O evento é enviado periodicamente, sendo o período definido no menu “1.2.6.n.3 Período” abaixo.

Nota: se a opção “1.2.6.n.4 Expandir” abaixo estiver definida como Sim, o tempo real da chamada de teste pode variar consoante os outros eventos reportados à central receptora.

Esta hora de início é utilizada pelo painel quando ocorre um dos seguintes casos:

- O painel é reinicializado
- Uma das opções de chamada de teste é alterada pelo instalador

A hora da chamada de teste é configurada no formato de 24 h, como HH:MM.

1.2.6.n.3 Período

3 Período
> <

O menu Período define um intervalo para as chamadas de teste conforme descrito em “1.2.6.n.2 T. Cham. teste” acima.

O intervalo permitido é de 1 a 999 horas.

1.2.6.n.4 Expandir

4 Expandir
>Não<

A opção Expandir define se o intervalo de chamada de teste é contado a partir da chamada de teste anterior ou desde o último relatório de evento bem sucedido.

Se esta opção estiver definida como Sim, depois de um evento ser transmitido para a central receptora, o atraso da chamada de teste é expandido e a chamada de teste seguinte é adiada.

Se esta opção estiver definida como Não, a chamada de teste seguinte ocorre num período de chamada de teste após a chamada de teste anterior, independentemente de outros eventos reportados.

1.2.6.n.5 Freq CT em FTC

```
5 Freq CT em FTC
  >Não<
```

Se esta opção estiver definida como Sim, durante a falha de comunicação (FTC) o painel procura estabelecer a comunicação iniciando uma chamada de teste a cada hora. Caso contrário, a chamada de teste é ensaiada como habitualmente.

Cuidado: ativar esta função apenas para a central receptora primária.

1.2.6.n.6 Teste manual

```
A chamar CS 1...
  Pronto
```

A opção de chamada de teste manual permite testar o reporte da central receptora. Seleccione a central receptora. Agora o painel tenta estabelecer uma ligação com a central receptora seleccionada.

O estado da evolução da chamada é mostrado no ecrã.

1.2.6.n.7 RSSI em report

```
7 RSSI em report
  >Não<
```

Se a opção estiver definida como Ligado, os relatórios de chamada de teste (RP,RX) contêm o nível GSM RSSI como subevento.

1.2.7 Diagnóstico IP

```
1>ETH
  >>>
```

O menu Diagnóstico IP proporciona acesso às ferramentas de diagnóstico para a conectividade IP.

1.2.7.n Escolha interface

```
1>Estatística IP
  >>>
```

Escolha um interface para diagnóstico. Dependendo do firmware e hardware do painel, podem estar disponíveis os seguintes interfaces:

- ETH: Ethernet
- GPRS: GPRS via módulo GSM
- TDA74xx: Comunicador externo

1.2.7.n.1 Estatística IP

```
1>TX pacotes
5
```

O menu Estatísticas IP permite visualizar as estatísticas indicadas a seguir.

- 1 TX pacotes: Número de pacotes enviados
- 2 RX pacotes: Número de pacotes recebidos
- 3 Pacotes: O número de pacotes que são rejeitados pela firewall incorporada rejei. Para mais informações, consulte “9.3.n.8 Firewall” na página nº 334.
- 4 TX bytes: Número de bytes enviados
- 5 RX bytes: Número de bytes recebidos
- 6 Limpar estat?: Este comando apaga os dados descritos acima

1.2.7.n.2 Ping host

```
Nome do Host
> <
```

O comando Ping host permite enviar um ping para o endereço da rede especificado. Este comando é utilizado para verificar se o host especificado está presente e está acessível na rede a partir do painel.

Se o interface selecionado fornecer vários caminhos de comunicação, ser-lhe-á pedido que selecione um caminho, que deve ser utilizado para o ping.

```
1>ETH
2 GPRS
```

Nota: o comando de ping tem de ser aceitável pelo host remoto. Certifique-se de que as firewalls e routers do host permitem pedidos de ping e respostas. Isto aplica-se a todos os comandos de ping.

1.2.7.n.3 Ping PC

```
1>Ligação PC 1
-----
```

O comando Ping PC permite enviar um ping ao PC especificado se estiver configurado como uma ligação PC via IP. Esta função é idêntica à do menu “9.4 Ligação de PC”. Consulte “9.4.1.n.4.3 Ping host” na página nº 348 para obter mais informações. Consulte também “1.2.7.n.2 Ping host” acima.

1.2.7.n.4 Ping CRA

```
2>CRA 2
-----
```

O comando Ping CRA permite enviar um ping à central receptora especificada se estiver configurada como uma ligação à central receptora via IP. Esta função é idêntica à do menu “9.1 Central Receptora”. Consulte “9.1.n.4.3 Ping host” na página nº 322 para obter mais informações. Consulte também “1.2.7.n.2 Ping host” acima.

1.2.7.n.5 Estado NTP

```
5>Estado NTP
  Inactivo
```

O ecrã Estado NTP permite verificar o estado actual do servidor Network Time Protocol (Protocolo de tempo de rede) configurado. Os estados possíveis do servidor são indicados a seguir.

- Inactivo: O servidor NTP ainda não foi consultado. Este estado geralmente está presente depois de um reinício do painel ou da configuração do NTP.
- Desconhecido: A consulta foi enviada, mas ainda não foi recebida qualquer resposta do servidor NTP.
- Falha: Nenhuma resposta do servidor NTP.
- OK: O servidor NTP respondeu à consulta.
- Erro de link: Linha Ethernet defeituosa.

1.2.8 Diagnóst. GSM

```
1>Estado PIN
  Normal
```

O menu Diagnóstico GSM proporciona um acesso às ferramentas de diagnóstico para a conectividade GPRS e SMS.

1.2.8.1 Estado PIN

```
1>Estado PIN
  Normal
```

O Estado PIN é um ecrã informativo que permite verificar o estado de aceitação do PIN. O estado pode ser um dos seguintes:

- Normal: aceite pelo SIM.
- Desconhecido: o estado é desconhecido.
- Disp.1 tent.! o cartão SIM proporciona a última tentativa para o PIN correcto.
- Necessário PUK! o cartão SIM está bloqueado após três tentativas infrutíferas de introdução do PIN, até que seja fornecido o PUK.

Só pode desbloquear o cartão SIM inserindo-o num telemóvel vulgar e fornecendo o PUK. Não há possibilidade de introduzir o PUK no sistema Advisor Advanced.

1.2.8.3 GSM net.reg.

```
3>GSM net.reg.
  Rede doméstica
```

O estado do registo de rede GSM pode ser um dos seguintes:

- Inactivo: o comunicador não se registou na rede, e não está a procurar rede nem a ligar-se
- Rede doméstica: registado na rede doméstica
- A procurar: a procurar rede para se registar
- Reg. negado: o registo na rede foi recusado

- Desconhecido: estado do registo desconhecido
- Roaming: registado numa rede em roaming

1.2.8.4 GPRS net.reg.

```
4>GPRS net.reg.  
Rede doméstica
```

O estado de registo na rede GPRS pode ter os valores descritos em “1.2.8.3 GSM net.reg.” na página nº 162.

1.2.8.5 Estado GPRS

```
5>Estado GPRS  
Rede doméstica
```

O estado de rede GPRS pode ser um dos seguintes:

- Não disponível: funcionalidade GPRS não disponível.
- Sem rede: a funcionalidade GPRS encontra-se disponível, mas não existe rede (por exemplo, falta cartão SIM).
- Não efectuado: a funcionalidade GPRS encontra-se disponível, mas a ligação não foi estabelecida (parâmetros IP não atribuídos).
- Configurado: a funcionalidade GPRS encontra-se disponível e a ligação estabelecida.
- Parado: a funcionalidade GPRS encontra-se disponível, mas a ligação foi interrompida por ter expirado o tempo de desligado. Consulte “9.3.n.7.8 Tempo desligar” na página nº 343 para obter mais informações.
- Sem dados: erro desconhecido.

1.2.8.6 Nome da rede

```
6>Nome da rede  
MyGSM
```

O Nome da rede é o nome da rede GSM na qual o comunicador GSM está actualmente registado. Trata-se de uma informação apenas de leitura. O nome pode ser “desconhecido”, se o código da rede não for reconhecido pelo módulo de comunicação.

1.2.8.7 Código de rede

```
7>Código de rede
```

O código de rede é um número de identificação exclusivo da rede GSM na qual o comunicador GSM está actualmente registado.

1.2.8.8 RSSI

```
8>RSSI  
23 [IIII ]
```

O valor da indicação da intensidade do sinal recebido (RSSI - Received Signal Strength Indication) é uma informação de diagnóstico apenas de leitura.

Estão disponíveis os seguintes intervalos:

Tabela 24: Intervalos RSSI

RSSI	Nível de sinal	Indicador de barras	Descrição
0	<-112 dBm	[]	Sem sinal
1 a 7	-111 a -99 dBm	[I]	Sinal insuficiente
8 a 12	-97 a -89 dBm	[II]	Sinal medíocre
13 a 20	-87 a -73 dBm	[III]	Bom sinal
21 a 26	-71 a -61 dBm	[IIII]	Sinal excelente
27 a 31	>-60 dBm	[IIIIII]	Sinal excelente

Para uma transferência de dados precisa, recomendamos um valor RSSI superior a 16.

1.2.8.9 TX. Msg. 24h

```
1>Todos SMS
```

```
0
```

O menu TX. Msg 24h apresenta uma lista de todas as mensagens de SMS enviadas desde a meia-noite (00:00). Estão disponíveis os seguintes submenus.

1. Todos SMS: Todas as mensagens.
2. Reporte SMS: Mensagens de reporte.
3. SMS desc.: Mensagens de controlo por SMS do utilizador que não foram reconhecidas e portanto foram reencaminhadas para o Supervisor.

Nota: este contador só funciona se o reenvio de SMS se encontrar activo. Consulte “9.3.n.6.2 Reenvio de SMS” na página nº 340.

1.2.8.10 Estado da bateria

```
10>Estado Bat.
```

```
OK
```

O ecrã informativo mostra o estado da bateria do módulo GSM.

O estado da bateria deve ser OK. Se a bateria estiver avariada ou em falta, o estado da bateria é Falha.

1.2.9 Teste da bateria

```
1>Opções teste
```

```
2 Teste Bat. Man
```

Este menu permite realizar um teste manual da bateria, bem como configurar um teste automático das baterias no painel ou num expansor.

Notas

- Esta funcionalidade está disponível apenas em determinados dispositivos, por exemplo nos expansores ATS120xE.

- O teste de bateria só funciona se não houver nenhuma falha de rede.

1.2.9.1 Opções de teste

```
1>Painel
3 DGP
```

Utilize este menu para configurar um teste automático da bateria.

Em primeiro lugar, seleccione o painel ou um expansor para testar a bateria.

1.2.9.1.m Tipo de dispositivo

```
1>DGP 1
2>DGP 2
```

Seleccione o grupo de dispositivos apropriado.

1.2.9.1.m.n Dispositivo

```
1>Tempo de teste
10
```

Seleccione o dispositivo apropriado.

1.2.9.1.m.n.1 Tempo de teste

```
1 Tempo de Teste
> 10<
```

Defina a duração (em minutos) do teste de bateria.

A gama permitida situa-se entre 2 e 254.

1.2.9.1.m.n.2 Freq.TesteBat.

```
2 Freq.TesteBat.
>Desactivado<
```

Defina a frequência do teste de bateria. Estão disponíveis os seguintes valores:

- Desactivado
- Todos os dias úteis
- Todas as Segundas
- Primeira Segunda do mês
- Todos os dias

1.2.9.1.m.n.3 Tempo de início

```
3 Tempo Inicio
>00:00<
```

Defina a hora do dia em que o dispositivo realiza um teste automático da bateria.

1.2.9.2 Teste Bat. Man

```
1>Painel
3 DGP
```

O menu permite executar um teste manual à bateria do dispositivo.

1.2.9.2.m Tipo de dispositivo

```
1>DGP 1
2>DGP 2
```

Selecione o grupo de dispositivos apropriado.

1.2.9.2.m.n Dispositivo

```
1>Tempo de teste
2 Ini./Stop test
```

Selecione o dispositivo apropriado.

1.2.9.2.m.n.1 Tempo de teste

```
1 Tempo de teste
> 10<
```

Defina a duração (em minutos) dos testes de bateria.

A gama permitida situa-se entre 1 e 254.

1.2.9.2.m.n.2 Ini./Stop test

```
1>Iniciar teste?
>Sim<
```

Execute o teste de bateria.

A duração do teste é definida em “1.2.9.2.m.n.1 Tempo de teste” acima.

Se já estiver a ser executado um teste de bateria para este dispositivo, é-lhe pedido que interrompa este teste.

1.2.9.3 Bateria substituída

```
Confirma?
>Não<
```

Depois de substituir a bateria, o instalador deve confirmar esta acção utilizando o menu Bateria substituída.

Selecione Sim e prima Enter. A confirmação é apresentada durante 3 segundos.

```
INFORMAÇÕES
Bat.Confirmada
```

A substituição da bateria é registada no registo de eventos do painel de controlo.

1.2.10 Diag. Painel

```
1>Sistema V/A
2 Tensão Bateria
```

O diagnóstico do painel permite monitorizar dados eléctricos específicos, por exemplo, a corrente e a tensão.

1.2.10.1 Sistema V/A

```
Tensão Sistema:
13,8V
```

```
Corrente Sist.:
0,8A
```

Os ecrãs percorridos mostram a tensão e a corrente da fonte de alimentação do sistema.

1.2.10.2 Tensão Bateria

```
Tensão Bateria:
12,8V
```

O ecrã mostra a tensão da bateria.

1.2.11 Verificar cartão

```
Cartão
RAS 1
```

Utilize o menu para ler dados de um cartão de utilizador.

O cartão é indicado no ecrã do teclado da mesma forma que é feito quando se efectua a programação do cartão de utilizador (consulte “3.1.n.3.1 Atribuir cartão” na página nº 203).

Nota: o teclado ou a porta para a programação dos cartões de utilizador são seleccionados em “8.8.5 Aprende cartão”, na página nº 310.

Se o cartão é programado no sistema, é apresentada a informação do utilizador que o detém:

```
Utilizador 05
J.Smith
```

Caso contrário, se o cartão for desconhecido, o seu tipo e os seus dados são apresentados no mesmo formato que no registo de eventos.

```
CARTÃO/ETIQUETA
48.111.2.3.146.>
```

Passe outro cartão ou prima X para sair do menu.

1.2.12 Modo Demo

```
1-8 Modo Demo  
>1234....<
```

Active o modo de demonstração do Advisor Advanced.

Seleccione áreas nas quais o modo demo estará activo.

Neste modo o sistema funciona com as limitações seguintes:

- Todos os teclados atribuídos a áreas seleccionadas apresentam a mensagem seguinte:

```
MODO DEMO  
Activado
```

- Somente as zonas de acesso e entrada/saída se encontram operacionais.
- Não são reportados eventos obrigatórios a uma central receptora nem são registados no registo de eventos. A alternância para o modo de demonstração também não é reportada.

Consulte também “1.1 Ver registos” na página nº 148.

- O reset técnico é desactivado.
- O Walk Test é desactivado.
- As saídas de sirene interior e exterior são desactivadas.

O modo demo é cancelado:

- Automaticamente após 15 minutos
- Quando a opção é desligada
- Quando o sistema é reiniciada

O modo só pode ser activado através do teclado.

Nota: o modo demo só deve ser activado quando todas as áreas estiverem desarmadas.

1.2.13 Controlo porta

```
1>Porta aberta
```

O menu permite enviar um comando directo para uma porta específica.

- 1 Porta aberta: Abrir uma porta específica para um período configurado para esta porta. Consulte “5.1.n.5.1 Tempo de desbloqueio” na página nº 243.
- 2 Bloqueio porta: Bloquear uma porta específica.
- 3 Desbloq. porta: Desbloquear uma porta específica até o comando de bloqueio de porta ser enviado.
- 4 Desabil. porta: Desactivar uma porta específica. Isto faz com que seja negado o acesso a todos os utilizadores.
- 5 Habilita porta: Activar uma porta desactivada.

Seleccione um comando, seleccione uma porta na lista de portas e prima Enter.

1.2.14 Listen-in

```
1>N.º telefone
+88123456789
```

Utilizar o menu para testar uma sessão de áudio de duas vias entre o sistema e outro número de telemóvel.

Esta opção está disponível apenas para sistemas de áudio de duas vias. Consulte o Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123 para obter mais informações.

1.2.14.1 Número de telemóvel

```
1 N.º telemóvel
>+88123456789<
```

Digite um número de telefone para chamada de teste.

1.2.14.2 Chamada de teste

```
1>Chama teste
RTPC
```

Entre no menu para executar a sessão de teste de áudio de duas-vias.

Notas

- Esta chamada de teste está limitada apenas ao reporte de áudio. Não são enviados eventos.
- Só é possível testar um dispositivo de áudio de cada vez.

Primeiro, selecione um dos seguintes caminhos de comunicação:

- PSTN
- GSM/SMS/GPRS

Nota: O correto envio de mensagens analógicas através do canal GSM, depende da qualidade da rede GSM, que altera frequentemente.

```
1>Áudio 1
* Escuta
```

Selecione um dispositivo de áudio para testar. Um asterisco “*” assinala o dispositivo que está atualmente a ser testado.

O estado da sessão é apresentado na linha inferior. Pode ser um dos seguintes:

- Pronto: o dispositivo está pronto para ser testado.
- Linha ocupada: o número de telefone está ocupado.
- Marcação: marcação em curso.
- Escuta: a sessão de áudio está no modo de escuta.
- Fala: a sessão de áudio está no modo de fala.
- DTMF x: é recebido um tom DTMF específico. Note que o código DTMF é apresentado durante 3 segundos.

Para mais informações sobre os tons DTMF, consulte o Capítulo 3 “Funções do sistema > Controlo DTMF” na página nº 124.

Tanto o instalador como o operador CRA podem alternar entre o modo de escuta e de fala:

- Escuta: prima a tecla 1, ou DTMF 1
- Fala: prima a tecla 2, ou DTMF 2

Saia do menu para terminar a sessão de teste.

Nota: os dispositivos de áudio têm de ser configurados e o número de telemóvel tem de ser introduzido em “1.2.14.1 Número de telemóvel” na página nº 169 antes de efetuar a chamada de teste.

1.2.15 Teste notific

```
1>Notificação 1
2>Notificação 2
```

O menu permite-lhe enviar uma notificação de teste de push.

Selecione uma notificação para enviar um teste de notificação push para o destinatário selecionado.

É apresentado o resultado do teste.

```
Notificação
Sucesso envio
```

1.3 Info painel

```
1>Versão painel
2 Idioma painel
```

Os ecrãs de informação fornecem informações sobre o firmware do painel e configurações iniciais.

1.3.1 Versão do painel

```
ATS1000A 1.0
TR_008.008.0028
```

O menu Versão do painel permite visualizar a informação do número da versão do firmware do painel.

1.3.2 Idioma do painel

O ecrã mostra o conjunto de idiomas do painel durante a instalação.

Consulte “Arranque inicial” na página nº 142 para obter mais informações.

1.3.3 Predefinições

O ecrã mostra as predefinições do painel durante a instalação.

Consulte “Arranque inicial” na página nº 142 para obter mais informações.

1.3.4 Upgrade USB

Permite escrever ou ler o firmware ou a configuração do painel utilizando uma unidade flash USB.

1.3.4.1 Upgrade FW

Permite actualizar o firmware ou a configuração do painel com um ficheiro seleccionado da unidade flash USB.

1.3.4.2 Upload FW

Permite ler o firmware ou a configuração do painel e armazenar como um ficheiro .dfu na unidade flash USB.

1.3.5 Info Falha Sis

```
FlhSistem R 3
01JUN19 15:22:56
```

O menu permite-lhe ver as informações sobre a última falha crítica do sistema. As seguintes informações são exibidas: número de identificação exclusivo (UID) da falha, a respetiva data e hora. É apresentado um indicador de letra (R) se a falha tiver sido reportada ao serviço de suporte técnico.

1.3.6 Variante de HW

```
6>Variante de HW
HW predefinido
```

O display indica a versão de hardware do painel, predefinido ou VdS.

1.3.7 Modo CDC

```
7 Modo CDC
Padrão
```

O display mostra o modo do controlador de porta CDC4.

Para obter mais informações, consulte o *Manual de Instalação e Programação do Controlador de Porta CDC4*.

1.4 Isolar caixa

```
1>Isolar caixa
01'00
```

A opção Isolar caixa permite ligar um PC sem iniciar o alarme de tamper do painel. Os seguintes menus permitem definir o temporizador de isolamento e executar o processo de ligação.

Para ligar um cabo USB ao painel:

1. Certifique-se de que o valor definido em “1.4.1 Tempo t. painel” é suficiente para chegar até ao painel e abrir a tampa da caixa.

2. Ignorar abert painel utilizando o menu “1.4.2 Tamper painel” na página nº 172.

O tamper da central encontra-se agora isolado e o temporizador de tampa de painel inicia-se.

3. Abra a caixa do painel e ligue o cabo USB.

O temporizador é parado e o tamper do painel encontra-se isolado, enquanto a tampa permanecer aberta.

1.4.1 Tempo t. painel

```
1 Temp. T.painel
>01'00<
```

O Temporizador de abertura do painel define o tempo durante o qual a abert de painel é ignorada.

1.4.2 Tamper painel

```
2>Tamper painel
Sim
```

Aceda ao menu Tamper painel para ignorar a abert de painel. O temporizador de tamper da abert de painel inicia a contagem do tempo.

Se a abert de painel já tiver sido ignorada, ao aceder a este menu anula o bypass.

1.5 Cartão de configuração

```
5 Cartão config.
>Desativado<
```

O menu permite ao técnico de instalação ativar a programação do leitor por um cartão de configuração. Ao ativar o cartão de configuração, não é feito o polling de todos os dispositivos seguros adicionados por 30 minutos, para que o técnico de instalação possa configurar cada dispositivo utilizando o cartão de configuração. Quando a opção é desativada, é feito normalmente o polling de todos os dispositivos.

Consulte “Segurança dos dados do cartão > Cartão de configuração” na página nº 131 para obter mais informações.

1.6 Manutenção em

```
6 Manutenção em
Desactivado?
```

O menu Manutenção em permite desactivar a função de acesso do instalador antes de expirar o tempo de acesso (consulte “8.1.3.6 Manutenção em” na página nº 286).

Nota: esta opção só é válida se o instalador precisar de autorização do utilizador. Consulte “8.2.1 Aceit. necess” na página nº 288.

Utilize esta função após terminar a programação do painel. Para cancelar o tempo de acesso do instalador, navegue para este menu e prima Enter. A seguir, saia de sessão. Posteriormente, o início de sessão do instalador irá precisar de outra confirmação do utilizador.

Consulte também “8.2.1 Aceit. necess” na página nº 288.

1.7 Reinstalar

```
7 Reinstalar  
  >Cancelar<
```

O menu Reinstalar permite anular todas as definições e repetir a instalação inicial.

Cuidado

- Este comando elimina todas as definições de programação, incluindo os utilizadores.
- Quando o canal de segurança está a ser utilizado, utilize esta opção apenas se o seu bus de dados do sistema estiver fisicamente protegido contra o acesso não autorizado. Para mais informações, consulte Capítulo 3 “Funções do sistema > Canal seguro” na página nº 130.
- Depois de aplicar as predefinições do painel, reinicie o sistema desligando-o e voltando a ligá-lo.

Para mais informações, consulte “Arranque inicial” na página 142.

2 Disp.BUS

```
1>Mostrar disp  
2 Editar disp
```

O menu de dispositivos permite visualizar e configurar dispositivos bus: teclados (RAS), expansores (DGP), leitores e dispositivos de áudio.

Para mais informações sobre teclados e expansores, consulte Capítulo 3 “Funções do sistema > Dispositivos” na página nº 67.

Para mais informações sobre leitores, consulte “Controlo de acesso” na página nº 80.

Para informações sobre a numeração de dispositivos bus, consulte “Bus – enumeração” na página nº 67.

2.1 Mostrar dispositivos

```
1>Disposit. RAS  
2 Disposit. DGP
```

O menu de dispositivos remotos instalados mostra o estado de todos os teclados remotos ligados e vários expansores do sistema e locais e dispositivos de áudio.

Nota: O número máximo de dispositivos permitidos no databus é indicado em “Características gerais” na página nº 39.

Selecione um tipo de dispositivo a mostrar.

2.1.1 Disposit. RAS

2.1.2 Disposit. DGP

2.1.3 Dispositivos de áudio

```
RAS 1-8 BUS1  
R-?-----
```

A linha inferior apresenta uma lista dos estados do dispositivo; cada estado de dispositivo é indicado como um carácter, que pode ser um dos seguintes.

- ? : O dispositivo está actualmente a ser lido
- x : O dispositivo está offline ou não é suportado
- l : O dispositivo está configurado mas isolado
- R : O teclado está online e configurado (sujeito a polling)
- r : O teclado está online, mas não configurado (novo)
- D : O expansor está online e configurado (sujeito a polling)
- d : O expansor está online, mas não configurado (novo)
- A : o dispositivo de áudio está online e configurado (sujeito a polling)
- a : o dispositivo de áudio está online, mas não configurado (novo)
- M : O expansor do bus MI está online e configurado (sujeito a polling)
- m : O expansor do bus MI está online, mas não configurado (novo)

- c: O expansor do bus MI está online, mas o seu endereço está em conflito com outro expansor
- O: O comunicador IP/GPRS da série ATS7400 está online e configurado (sujeito a polling)
- —: Sem dispositivo

Nota: Para dispositivos de expansão (DGP) locais, seleccione primeiro o endereço do expansor e depois seleccione o tipo de dispositivo local.

Prima Sair para sair desta vista.

Prima Enter e depois seleccione OK para confirmar a nova configuração. Neste caso, todos os novos dispositivos são adicionados e os dispositivos em falta são removidos do sistema.

Nota: O segundo bus de sistema (BUS2) só está disponível ao utilizar o segundo módulo de extensão RS485 LAN. Consulte também “Dois databus do sistema” na página nº 25.

2.2 Editar dispositivos

```
1>Disposit. RAS
2 Disposit. DGP
```

Escolha o tipo de dispositivo que deseja configurar.

2.2.1 Dispositivos RAS

```
0>Adicionar RAS
1 RAS 1
```

Prima 0 para adicionar um teclado, ou um número para configurar um teclado existente.

Nota: O número máximo de dispositivos permitidos no databus é indicado em “Características gerais” na página nº 39.

Config. RAS

2.2.1.0 Adicionar RAS

```
RAS número
>_<
```

No menu Adicionar teclado, introduza o número para este novo teclado e prima Enter para confirmar ou Sair para sair sem adicionar um dispositivo.

Depois de o dispositivo ser adicionado, são apresentadas as opções de configuração do teclado.

2.2.1.n Seleccionar o teclado

Selecione o número do teclado a configurar.

2.2.1.n.1 Tipo de RAS

```
1>Tipo de RAS
   ATs1115
```

O ecrã do tipo de Teclado é um ecrã informativo. O tipo é definido pelo próprio teclado.

2.2.1.n.2 Endereço BUS

```
2>Endereço BUS
   BUS 1 ADDR 0
```

O endereço bus é um ecrã informativo que indica o endereço do bus definido por DIP switches ou programado no teclado.

Nota: se o keypad comunicar com o painel utilizando um canal seguro, ele é marcado pelo indicador “SC”, por exemplo: “SC BUS 1 ADDR 0”. Consulte também “Segurança dos dados do cartão” na página nº 130.

2.2.1.n.3 Configurações RAS

```
3>Config. RAS
   >>>
```

O menu Opções do teclado contém os menus indicados a seguir, que são necessários para configurar o teclado seleccionado.

Nota: as opções disponíveis dependem do tipo de teclado.

2.2.1.n.3.1 Nome RAS

```
1>Nome RAS
   RAS 1
```

Utilize a opção de nome do Teclado para introduzir um nome que identifique o teclado ao utilizador final.

Quando é criado um teclado, é-lhe atribuído o nome predefinido “Teclado<n>”, em que <n> é o número do teclado. Aceda a este menu para editar o nome actual.

Um nome de teclado pode ser constituído por 16 caracteres.

2.2.1.n.3.2 Tamper Área

```
2>Tamper Área
   Área 1
```

A opção Tamper Área determina que área recebe eventos de falha e tamper de teclado. Para alterar a área, seleccione a área e prima Enter.

2.2.1.n.3.3 Detetar tamper

```
3 Detetar tamper
  >Ligado<
```

Se estiver definido como Desligado, os alarmes de tamper não são reportados ao painel pelo teclado seleccionado.

2.2.1.n.3.4 Ver áreas

```
01-10>Ver áreas
  12.4.....
```

O menu Ver áreas permite especificar que área apresentará informação sobre este teclado sem autorização do utilizador. As áreas são apresentadas em forma de lista. Para alterar a selecção, prima Enter e seleccione as áreas apropriadas.

Nota: após uma autorização, a vista da área depende dos privilégios do utilizador e do estado do sistema.

Como seleccionar as áreas a visualizar

Consulte “Como editar uma lista” na página nº 138.

Notas

- Após alterar esta lista, o controlo das áreas seleccionadas é também activado (consulte “2.2.1.n.3.6 Áreas de controlo” abaixo).
- Não é possível seleccionar uma área para visualizar e controlar utilizando esta opção, se esta área estiver atribuída a uma porta. Para tal, utilize o menu “5.1.n.6.3 Controlo de Alarme” na página nº 244.

2.2.1.n.3.5 Ver GA

```
01-10>Ver GA
  12.4.....
```

Proporciona a mesma funcionalidade que em “2.2.1.n.3.4 Ver áreas” acima, mas para grupos de áreas.

Consulte também “Grupos Área” na página nº 55.

2.2.1.n.3.6 Áreas de controlo

```
6>Controlo áreas
  12.4.....
```

O menu Áreas de controlo permite seleccionar as áreas que podem ser controladas por este teclado. As áreas são apresentadas em forma de lista. Para alterar a selecção, prima Enter ou Direita e seleccione as áreas apropriadas.

Consulte também “2.2.1.n.3.4 Ver áreas” acima.

2.2.1.n.3.7 Controlar GA

```
01-10>Control.GA
12.4.....
```

Proporciona a mesma funcionalidade que em “2.2.1.n.3.6 Áreas de controlo” na página nº 177, mas para grupos de áreas.

Consulte também “Grupos Área” na página nº 55.

2.2.1.n.3.8 Opções de controlo

```
1>Cartão&PIN
Cartão ou PIN
```

O menu contém um conjunto de opções ligadas às funções de controlo do teclado seleccionado.

Consulte também “Teclas” na página nº 62.

2.2.1.n.3.8.1 Modo cartão e PIN

```
2 Cartão e PIN
>Apenas PIN<
```

A opção Modo Cartão e PIN permite seleccionar um dos seguintes métodos de controlo.

- Apenas PIN: Só é necessário o PIN para o arme e desarme de áreas
- Apenas cartão: Um só cartão desarma áreas
- Desarme Cartão e PIN: São necessários o Cartão e o PIN para o desarme de áreas
- Cartão e PIN sempre: São necessários o Cartão e o PIN para o arme ou desarme de áreas
- Cartão ou PIN: Para o arme ou desarme é necessário um PIN ou um cartão

2.2.1.n.3.8.2 Tempo Logoff

```
2 Tempo Logoff
>3<
```

Um período de tempo (em minutos) de inactividade do teclado antes de a sessão do utilizador ser terminada automaticamente.

O intervalo permitido é de 1 a 255 minutos. O valor predefinido é 3.

2.2.1.n.3.8.3 1 x arme/desarme

```
3 1xarme/desarme
>Desligado<
```

O arme/desarme com um único cartão define se o teclado seleccionado permite armar ou desarmar áreas com um único cartão. Estão disponíveis os seguintes valores:

- Desligado: Um cartão não causa nenhuma acção de arme ou desarme.
- Desarme: Um cartão desarma áreas.

- Arme-Desarme: Um cartão arma ou desarma áreas.
- GP1-Desarme/GP2-Desarme: Um cartão arma parcialmente ou desarma áreas.

2.2.1.n.3.8.4 3xCartão arma

```
4 3xcartão arma
  >Desligado<
```

O arme com a passagem de três vezes o cartão define se o teclado seleccionado permite armar áreas com a passagem de três vezes o cartão. Estão disponíveis os seguintes valores:

- Desligado: A passagem de três vezes do cartão não causa nenhuma acção.
- Arme: Passagem de três vezes do cartão.
- Arme parcial 1/Arme parcial 2: Passar três vezes o cartão arma parcialmente as áreas.

Notas

- Esta funcionalidade só funciona se as áreas puderem ser armadas com cartão. Consulte “2.2.1.n.3.8.1 Modo cartão e PIN” na página nº 178 para ver os modos disponíveis.
- Esta funcionalidade só está disponível se a opção “2.2.1.n.3.8.3 1 x arme/desarme” option descrita na página nº 178 não estiver configurada como Arme-Desarme.

2.2.1.n.3.8.5 Modo tecla/cartão

```
5 ModoTecla/Cart
  >Alarme&Acesso<
```

A opção define como o leitor de cartões trata as sequências de chaves em conflito que possam ser utilizadas para acesso às portas e controlo de alarmes (p. e., cartão + PIN + desligado num leitor de cartões sem LCD). Estão disponíveis os seguintes valores:

- Alarme&Acesso: a sequência de chaves em conflito abre a porta e define ou não define o sistema.
- Acesso: a sequência de chaves apenas abre a porta.

Nota: se a opção estiver definida como Acesso, a opção 2.2.1.n.3.8.3 1 x arme/desarme está indisponível.

Consulte também “Teclas”, na página nº 62.

2.2.1.n.3.8.6 BloqTampCódigo

```
6 BloqTampCódigo
  >Desligado<
```

Se a opção estiver ativada, o leitor de cartão e o keypad bloqueiam durante 120 s ao ser apresentado, três vezes, um cartão não autorizado.

Nota: a opção aplica-se apenas a cartões. Os PIN incorretos irão causar o bloqueio do keypad, independentemente do estado da opção.

2.2.1.n.3.8.7 Link a leitor

```
7 Link a leitor  
>Não config<
```

Utilize o menu para ligar o leitor ao keypad do LCD selecionado, para que a informação deste leitor seja apresentada no keypad e o leitor seja utilizado para autorização do utilizador.

2.2.1.n.3.9 Bloq. PIN ES

```
9 Bloq.PIN ES  
>Não<
```

Se a opção Bloq.PIN ES estiver definida como Sim, não é possível utilizar um PIN durante o tempo de entrada predefinido.

Nota: se o teclado estiver configurado como um leitor, utilizar esta opção não é permitido, e causa um aviso:

```
AVISO  
Verif CfgPorta
```

Neste caso, programe esta opção utilizando o menu “5.1 Portas > 5.1.n.6.3.4.3 Bloq.PIN ES” na página nº 246.

2.2.1.n.3.10 Isolar teclado

```
10 Isolar tecl>  
>Não<
```

Utilize a opção Isolar teclado para isolar eventos de falha de tamper no teclado seleccionado. No entanto, o teclado mantém-se funcional.

2.2.1.n.3.11 Besouro silenciado

```
11 Besouro silen  
>Nunca<
```

É possível desactivar o besouro do teclado para eventos específicos. Estão disponíveis as seguintes opções:

- Nunca: Besouro funciona normalmente. É impossível silenciar o besouro utilizando X + Controlo de volume esquerdo.
- Durante GP Sda: O besouro não é actuado em arme parcial. O controlo manual de volume está disponível sem limitações.
- Sempre: O besouro é desactivado. O controlo manual de volume está disponível sem limitações.
- Durante E/S: O besouro mantém-se silenciado durante o tempo de entrada e saída.

2.2.1.n.3.12 Arme rápido

```
12 Arme rápido
   >Desligado<
```

A opção de Arme rápido permite armar áreas sem ter que digitar código ou apresentar cartão. Se esta funcionalidade for activada, a instalação é armada após premir On, sem autorização de utilizador.

Estão disponíveis as seguintes opções:

- Desligado: Arme rápido desactivado
- Sem lista: Todas as áreas atribuídas ao teclado são armadas após premir a tecla On
- Com lista: Após premir On, o sistema solicita que escolha as áreas entre as que se encontram atribuídas ao teclado.

Esta opção afecta também o arme parcial.

2.2.1.n.3.13 Teclas Função

```
1>Tecla F1
2 Tecla F2
```

As teclas de funções permitem atribuir uma função programável pelo utilizador a qualquer uma das teclas de funções disponíveis. Consulte “Funções de utilizador programáveis” na página nº 105 para obter mais informações.

A disponibilidade das teclas de funções depende do tipo de teclado. Consulte também “2.2.1.n.1 Tipo de RAS” na página nº 176.

2.2.1.n.3.14 LED1 ind. área

```
14 LED1 ind.área
   >.....<
```

LED1 ind. área permite atribuir áreas ao LED 1 programável do teclado. O indicador fica verde quando todas as áreas atribuídas estiverem prontas para arme. Fica vermelho quando uma área está armada ou parcialmente armada. O indicador vermelho pisca quando existe um alarme numa área atribuída ao mesmo.

Nota: esta funcionalidade é diferente quando apenas uma área é atribuída a ambos os indicadores. Neste caso, a combinação de dois indicadores mostra outros dois estados desta área:

- LED 1 vermelho, LED 2 desligado: área em estado de arme parcial 1.
- LED 1 desligado, LED 2 vermelho: área em estado de arme parcial 2.

Esta indicação exige que o teclado seleccionado seja atribuído apenas a esta área em particular para visualização e controlo. Consulte “2.2.1.n.3.4 Ver áreas” na página nº 177 e “2.2.1.n.3.6 Áreas de controlo” na página nº 177.

2.2.1.n.3.15 LED2 ind. área

```
15 LED2 ind.área  
>.....<
```

Utilize LED2 ind. área para programar o indicador LED 2 tal como descrito em “2.2.1.n.3.14 LED1 ind. área” na página nº 181.

2.2.1.n.3.16 Ind. estado

```
16 Ind. estado  
>Lista<
```

A indicação do estado define o modo de apresentação da lista de estados de áreas. As opções seguintes poderão estar disponíveis consoante a variante do painel e o modelo do teclado:

- Lista: as áreas são apresentadas em forma de lista vertical com nomes e estados, o que requer percorrer.
- Símbolos: Todas as áreas são apresentadas num único ecrã. Só são apresentados números e estados de áreas.
- Lista GA: O mesmo que lista, mas para grupos de áreas.
- Símbolo GA: O mesmo que símbolo, mas para grupos de áreas.

Consulte o *Guia do Utilizador do Advisor Advanced* para obter mais informações sobre a selecção de áreas.

2.2.1.n.3.17 Ilumin. LCD

```
17 Ilumin. LCD  
>Sempre on<
```

A opção de retroiluminação do LCD define quando se acende a retroiluminação do ecrã do teclado. Estão disponíveis as seguintes opções:

- Sempre ligado: A retroiluminação do LCD nunca se desliga.
- Normal: A retroiluminação do LCD desliga-se após um tempo de inactividade específico.
- Excl. entrada: A retroiluminação do LCD está desligada durante o tempo de entrada, até ser premida uma tecla.

Nota: o tempo limite de retroiluminação depende do firmware específico do teclado.

2.2.1.n.3.18 REC no RAS

```
1>RAS 1  
2 RAS 2
```

A opção CONF no teclado permite seleccionar um teclado LCD adicional que apresenta uma mensagem de confirmação após o desarme do sistema utilizando o leitor ou teclado não LCD.

Nota: esta opção só está disponível em leitores de cartões e teclados não LCD.

Consulte também “4.1.n.6.26 REC no RAS” na página nº 219 para obter mais informações.

2.2.1.n.3.19 ES 1 Besouro

```
19 ES 1 Besouro
    >Sim<
```

Se a opção estiver definida como Sim, o besouro do teclado seleccionado está activo durante o tempo de entrada/saída 1.

Consulte “2. Entrada/Saída 1” na página nº 49 para obter mais informações.

2.2.1.n.3.20 ES 2 Besouro

```
20 ES 2 Besouro
    >Sim<
```

Se a opção estiver definida como Sim, o besouro do teclado seleccionado está activo durante o tempo de entrada/saída 2.

Consulte “18. Entrada/Saída 2” na página nº 51 para obter mais informações.

2.2.1.n.3.21 Teclas 1+3

```
21 Teclas 1+3
    >Sim<
```

Se a opção estiver definida como Sim, a combinação das teclas 1 e 3 permite activar um alarme de pânico.

Consulte o *Guia do Utilizador do Advisor Advanced* para obter mais informações.

Esta funcionalidade só se encontra disponível para teclados ATS113x.

2.2.1.n.3.22 RTE

```
22 RTE
    >Ligado<
```

Se a opção estiver definida como Ligado, o pedido para sair no input do teclado seleccionado está ativado.

2.2.1.n.3.23 Backlight

```
23 Backlight
    >Ligado<
```

Se a opção estiver definida como Ligado, a iluminação de fundo das teclas do teclado seleccionado está sempre ativa. Se estiver definida como Desligado, a iluminação de fundo acende-se apenas durante um curto período de tempo após premir uma tecla ou passar um cartão.

2.2.1.n.3.24 Programa

O menu de atalhos permite atribuir até dois programas ao elemento seleccionado.

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

2.2.1.n.4 Menu RAS

```
4>Menu RAS
    >>>
```

O menu teclado dá acesso ao menu de programação incorporado no teclado. Para mais informações, consulte o manual aplicável do teclado.

2.2.1.n.5 Listen-in

```
1>Modo de escuta
    Desativado
```

Utilize o menu para configurar o áudio de duas vias para o teclado selecionado. Esta opção está disponível apenas para sistemas de áudio de duas vias. Consulte o Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123 para obter mais informações.

2.2.1.n.5.1 Modo de escuta

```
1 Modo de escuta
    >Desativado<
```

Selecione um modo de escuta para o teclado selecionado. Estão disponíveis as seguintes opções:

- Desativado: sem áudio.
- Só escuta: o operador da central recetora apenas pode ouvir o áudio do dispositivo de áudio atribuído ao teclado.
- Escuta e fala: o operador pode ouvir o áudio ou falar utilizando o dispositivo de áudio atribuído.

2.2.1.n.5.2 Ligação áudio

```
0 Nada
1 Áudio 1
```

Atribua um dispositivo de áudio ao teclado selecionado.

2.2.1.n.6 RstChave com.

```
6 RstChave com.
    >Cancelar<
```

O menu permite redefinir uma chave de encriptação utilizada para a canal de comunicação seguro entre o dispositivo selecionado e o painel de controlo. Utilize este menu para recuperar o canal seguro em caso de substituição do dispositivo ou de falha de comunicação do bus do sistema.

Cuidado: Quando o canal de segurança está a ser utilizado, utilize esta opção apenas se o seu bus de dados do sistema estiver fisicamente protegido contra o acesso não autorizado.

Consulte Capítulo 3 “Funções do sistema > Canal seguro” na página nº 130 para obter mais informações.

2.2.1.n.6 Remover RAS

```
6 Remover RAS
  >Cancelar<
```

Para remover o teclado, prima Enter, seleccione OK e prima novamente Enter. O teclado é eliminado.

Nota: Antes de remover um teclado, deve remover primeiro as saídas ou filtros de condições ligados ao teclado.

2.2.2 Dispositivos DGP

```
0>Adicionar DGP
1 DGP 1
```

No menu Dispositivos de Expansor, prima 0 para adicionar um expansor, ou um número para configurar um expansor existente.

Nota: O número máximo de dispositivos permitidos no databus é indicado em “Características gerais” na página nº 39.

Opções de expansores

2.2.2.0 Adicionar DGP

```
DGP número
  >_<
```

No menu Adicionar expansor, introduza o número para este novo expansor e prima Enter para confirmar ou Sair para sair sem adicionar um dispositivo.

Depois de o dispositivo ser adicionado, são apresentadas as opções de configuração do expansor.

2.2.2.n Seleccionar expansor

Selecione o número do expansor a configurar.

2.2.2.n.1 Tipo de DGP

```
1>Tipo de DGP
  ATS1201
```

O ecrã do tipo de expansor é um ecrã informativo. O tipo é definido pelo expansor.

2.2.2.n.2 Endereço BUS

```
2>Endereço BUS
      01
```

O endereço bus é um ecrã informativo que fornece o endereço do DIP switch.

2.2.2.n.3 Entradas DGP

```
3>Entradas DGP
      113-128
```

Intervalo de expansão é um ecrã informativo. Apresenta o intervalo de zonas disponível para este expansor.

Nota: no caso dos dispositivos de 32 zonas, existem dois intervalos de zonas.

```
3>Entradas DGP
      113-128 353-368
```

Consulte “2.2.2.n.4.6 DGP modo” na página nº 190 para obter mais informações.

2.2.2.n.4 Configurações DGP

```
4>Config. DGP
      >>>
```

O menu de definições de expansão contém os menus indicados em baixo, os quais são necessários para configurar o expansor seleccionado.

Nota: as opções disponíveis dependem do tipo de expansor.

2.2.2.n.4.1 Nome DGP

```
1 Nome DGP
>DGP 1 <
```

Utilize a opção de nome do Expansor para introduzir um nome que identifique o expansor ao utilizador final.

Quando é criado um expansor, é-lhe atribuído o nome predefinido “Expansor <n>”, em que <n> é o endereço do expansor. Aceda a este menu para editar o nome actual.

Um nome de expansor pode ser constituído por 16 caracteres.

2.2.2.n.4.2 Tamper Área

```
2>Tamper Área
      Área 1
```

A opção Tamper Área determina que área recebe eventos de falha e tamper de expansor. Para alterar a área, prima Enter e seleccione a área.

2.2.2.n.4.3 Detetar tamper

```
3 Detetar tamper
  >Lig.<
```

Se a opção estiver desligada, a deteção de tamper do dispositivo estará desativada.

2.2.2.n.4.4 Isolar DGP

```
4 Isolar DGP
  >Não<
```

Utilize o comando Isolar expansor para isolar eventos de falha de tamper no expansor seleccionado. No entanto, o expansor mantém-se funcional.

2.2.2.n.4.5 Modo de input

```
5 Modo Input
  >Loop dupla<
```

A opção de modo de Input determina a configuração das entradas de zona do expansor. Esta configuração é semelhante ao modo de input de zona do painel, descrito em “8.6.1 Modo entrada” na página nº 302.

Consulte “Ligação das zonas” na página nº 25 para mais informações sobre a utilização de EOL.

2.2.2.n.4.6 EOL

```
6 EOL
  >4k7<
```

O menu de Resistência EOL permite definir o valor da resistência fim-de-linha das entradas de zona do expansor. Esta configuração é semelhante ao menu resistência fim de linha das zonas do painel, descrito em “8.6.2 Resistência EOL” na página nº 302.

Consulte “Ligação das zonas” na página nº 25 para mais informações sobre a utilização de EOL.

2.2.2.n.5 Menu DGP

```
5>Menu DGP
  >>>
```

O menu dá acesso ao menu de programação incorporado no expansor. Para mais informações, consulte o manual aplicável do expansor.

Nota: Este menu não está disponível nos expansores sem fios ATS1235 com a versão de firmware 1.20 e superior.

2.2.2.n.6 Remover DGP

```
0>Remover tudo
1 Remover zona
```

Utilize o comando Eliminar expansor para eliminar um expansor ou elementos específicos do sistema atribuídos ao mesmo, por exemplo, zonas ou saídas.

Consoante o tipo de expansor, poderão estar disponíveis as seguintes opções:

- 0 Remover tudo: Eliminar expansor e todos os elementos atribuídos ao mesmo.
- 1 Remover zona: Eliminar zonas atribuídas ao expansor selecionado.

```
465>Zona 465
466 Zona 466
```

A lista de zonas atribuídas é apresentada.

Selecione uma zona e prima Enter para eliminá-la.

```
Eliminar zona
>Cancelar<
```

Selecione OK e prima Enter para confirmar.

- 2 Remover comando: Eliminar comandos atribuídos ao expansor selecionado.
- 3 Remover saída: Eliminar saídas atribuídas ao expansor selecionado.

Se não estiverem atribuídos quaisquer elementos ao expansor selecionado, apenas poderá eliminar o próprio expansor.

```
Remover DGP
>Cancelar<
```

Selecione OK e prima Enter para confirmar. O expansor é eliminado.

Nota: antes de remover um expansor, deve eliminar quaisquer filtros de condições ligados ao expansor.

Opções específicas sem fios

2.2.2.n.4.4 Supervisão

```
1>Super. pequena
20
```

A supervisão é utilizada para desactivar o arme se o expansor sem fios não receber uma mensagem de supervisão de um sensor dentro do tempo de supervisão curta.

Uma função de supervisão programável verifica o estado dos dispositivos em campo. Os temporizadores de supervisão nos sensores são sujeitos a um ligeiro “dithering” para que as transmissões ocorram de forma aleatória, com o efeito de minimizar as colisões em instalações de maior dimensão.

Notas

- Comando de dois e quatro botões não transmitem sinais de supervisão
- O tempo de supervisão não pode ser definido para sensores individuais, mas apenas para expansores individuais sem fios

2.2.2.n.4.4.1 Super. pequena

```
1 Super. pequena
   >20<
```

A supervisão curta é utilizada para desactivar o arme se o expansor sem fios não receber uma mensagem de supervisão de um sensor dentro do tempo de supervisão curta.

O intervalo permitido é de 20 a 1920 minutos.

2.2.2.n.4.4.2 Super. longa

```
2 Super. longa
   >20<
```

A supervisão longa define uma condição de alarme no painel para um sensor cujo temporizador de supervisão expirou. Programe o tempo de supervisão de modo a controlar a frequência com que o expansor sem fios verifica se o sensor está em comunicação e no alcance do expansor sem fios.

O intervalo permitido é de 20 a 1920 minutos.

2.2.2.n.4.4.3 Super. fumo

```
3 Super. fumo
   >65<
```

A supervisão de fumo define uma condição de falha no painel quando um temporizador de supervisão de detector expira. Programe o tempo de supervisão de modo a controlar a frequência com que o expansor sem fios verifica se o sensor está em comunicação e no alcance do expansor sem fios.

O intervalo permitido é de 65 a 1920 minutos.

2.2.2.n.4.5 Sens. Recpt.

```
5 Sens. Recpt.
   >Normal<
```

Utilize o menu Sensibilidade do receptor para diminuir a sensibilidade do expansor sem fios. Mudar o valor de Normal para Baixo reduz a sensibilidade em 6 dB.

Depois de sair do modo de programação, a sensibilidade regressa ao valor normal.

2.2.2.n.4.6 DGP modo

```
6 DGP modo
  >16 zonas<
```

Escolha um dos modos seguintes para o expansor:

- 16 zonas: O expansor possui 16 zonas.
- 32 zonas: O expansor possui 32 zonas.

Notas

- O modo de 32 zonas só está disponível no expansor sem fios com a versão de firmware 1.20 ou superior.
- As zonas atribuídas às entradas 17-32 não são adjacentes às zonas atribuídas às entradas 1-16 do expansor. Por exemplo, as primeiras 16 zonas estão atribuídas às zonas de painel 113 a 128, e as entradas 17 a 32 estão atribuídas às zonas 353 a 368.

2.2.2.n.4.7 DGP versão

```
ATS1238.B008
```

O ecrã de versão do expansor é um ecrã informativo com os dados da versão do expansor.

2.2.2.n.4.8 Menu empaste

```
1>Empastelamento
  Activado
```

Utilize o menu para definir as opções de deteção de empastelamento.

2.2.2.n.4.8.1 Empastelamento

```
1 Empastelamento
  >Activado<
```

A opção de deteção de empastelamento deve ser definida como Sim se o expansor sem fios tiver de detectar e reportar tentativas de empastelamento da comunicação.

Uma condição de empastelamento ocorre se o empastelamento estiver presente em qualquer momento, durante um período de tempo superior ao definido em “2.2.2.n.4.8.2 Empast. segundos” na página nº 191. O limite de empastelamento requerido está definido em “2.2.2.n.4.8.3 Thresh Empast.” na página nº 191.

Nota: os menus mencionados acima estão disponíveis apenas para ATS1235 com a versão de firmware V1.20 e mais recentes. Em versões mais antigas, os valores são definidos utilizando o menu do expansor interno.

2.2.2.n.4.8.2 Empast. segundos

```
2 Empast. seg
  > <
```

O período de empastelamento pode ser configurado de 10 a 50 segundos. O valor predefinido é 30 segundos.

2.2.2.n.4.8.3 Thresh Empast.

```
3 Thresh Empast.
  > <
```

O limite de empastelamento pode ser configurado de 25,0 a 75,0%. O limite predefinido é 44,8%.

2.2.2.n.4.11 Cfg. Fab. DGP

```
11 Cfg. Fab. DGP
  >Não<
```

Repor as definições de fábrica do expansor sem fios.

Opções específicas da câmara

2.2.2.n.4.9 Opções Imagem

```
1>Config. Imagem
  >>>
```

Este menu é específico de sistemas com expansores de câmara PIR sem fios. Consulte “Utilizar câmaras” na página nº 117 para obter mais informações.

2.2.2.n.4.9.1 Config. Imagem

```
1>Conf. Alarme
  >>>
```

O menu permite configurar opções de gravação de fotos separadamente para os seguintes tipos de eventos de câmara:

- Alarmes de intrusão
- Alarmes de incêndio
- Alarmes de pânico
- Alarmes médicos
- Alarmes de tamper
- Falhas: Alarmes técnicos e falhas do dispositivo
- Configur. tipo 1: Tipo programável pelo utilizador 1
- Configur. tipo 2: Tipo programável pelo utilizador 2

Consulte também “Tipos de eventos de câmara” na página nº 117.

2.2.2.n.4.9.1.1 Conf. Alarme

1>Qtd imagens
1

Aceder ao menu BA Config. para configurar as definições de imagem para alarmes de intrusão.

2.2.2.n.4.9.1.1.1 Qtd imagens

1 Qtd imagens
>1<

Definir o número de imagens tiradas após ocorrer um evento do tipo seleccionado.

A gama permitida situa-se entre 1 e 30. O atraso entre imagens é definido em “2.2.2.n.4.9.1.1.2 Taxa de frames” abaixo.

2.2.2.n.4.9.1.1.2 Taxa de frames

2 Taxa de frames
>500 ms<

O menu define uma frequência de obtenção de imagens ao ocorrer um evento do tipo seleccionado.

O menu só está disponível se o valor de “2.2.2.n.4.9.1.1.1 Qtd imagens” acima for maior que 1.

Os valores permitidos são 500 ms, 1 s, 5 s, 15 s, 60 s.

2.2.2.n.4.9.1.1.3 Resolução Foto

3 Resolução Foto
>QVGA<

A opção define as resoluções de imagens obtidas ao ocorrer um evento do tipo seleccionado. Estão disponíveis as seguintes opções:

- QVGA: 320 x 240 pixéis
- VGA: 640 x 480 pixéis
- QVGA e VGA: Duas imagens de cada vez, uma de baixa resolução e outra de alta resolução.

2.2.2.n.4.9.1.2 Conf. incêndio

2.2.2.n.4.9.1.3 Conf. pânico

2.2.2.n.4.9.1.4 Conf. médico

2.2.2.n.4.9.1.5 Conf. tamper

2.2.2.n.4.9.1.6 Conf. falhas

Consulte “2.2.2.n.4.9.1.1 Conf. Alarme” acima.

2.2.2.n.4.9.1.7 Configur. tipo 1

2.2.2.n.4.9.1.8 Configur. tipo 2

Os tipos personalizados são utilizados com filtros de condições para activação da câmara.

Consulte “2.2.2.n.4.9.1.1 Conf. Alarme” na página nº 192.

2.2.2.n.4.9.2 Ver mem imagem

```
Imagens: 12
Livre: 123
```

```
Livre: 3,0 MB
Total: 4,0 MB
```

O ecrã informativo mostra o número de imagens actualmente armazenadas no expansor da câmara PIR sem fios, bem como a memória disponível.

2.2.2.n.4.9.3 AutoapagarImag

```
3 AutoapagarImag
>1 dia<
```

O valor define se as imagens guardadas no expansor da câmara PIR sem fios são apagadas automaticamente após um período de tempo determinado (em dias).

O intervalo permitido é de 1 a 120 dias. 0 ou Desligado significa que as imagens nunca são apagadas automaticamente. Os utilizadores devem controlar a memória disponível e remover as imagens manualmente.

2.2.2.n.4.9.4 Cont Total Foto

```
Cont Total Foto:
12
```

O contador total de fotografias mostra quantas fotografias foram armazenadas na memória flash do expansor da câmara PIR desde o início do seu funcionamento.

2.2.2.n.4.11 Apagar imagem

```
11 Apagar imagem
>Cancelar<
```

Selecione OK e prima Enter para remover todas as imagens armazenadas do expansor da câmara PIR sem fios.

Opções específicas do expansor de quatro portas

2.2.2.n.4.7 Módulos Output

```
7 Módulos Output
  >0<
```

Introduza o número de controladores de output incluídos no controlador de portas.

A gama permitida situa-se entre 0 e 32. 0 significa que não há nenhuma placa de saída programada. Note que existem quatro saídas do tipo colector aberto disponíveis no controlador de portas para uma placa de 4 relés.

2.2.2.n.4.8 Limite ContReg

```
8 Limite ContReg
  >65534<
```

Quando o número de utilizadores atinge este limite, o controlador de portas define um flag interno (limite de contagem de região) que pode ser utilizado na lógica de macros do controlador de portas. É possível activar eventos quando um determinado número de utilizadores se encontra numa região.

O intervalo permitido é de 0 a 65534.

Exemplos:

- Activar um sinal quando um parque de estacionamento está cheio.
- Definir áreas quando a última pessoa tiver abandonado a região, ou desarmar áreas quando a primeira pessoa entra na região.

2.2.2.n.4.9 Macro lógica

```
00>Adic. Macro
01 Macro 1
```

Utilize o menu para programar macros de controladores de portas.

Para mais informações sobre macros, consulte “Lógica de macros dos controladores de portas” na página nº 83.

2.2.2.n.4.9.0 Adicionar macro

Aceda à opção de menu Filtro de macros para adicionar uma macro. Se a macro for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Macro Adic.
```

É atribuído à nova macro o nome predefinido de “Macro N” e a macro é colocada no fim da lista de macros. Pode agora começar a editar os respectivos detalhes.

2.2.2.n.4.9.m Macro

Selecione uma macro existente a programar.

2.2.2.n.4.9.m.1 Nome de macro

```
1 Nome de macro
>Macro 1 <
```

O nome identifica a macro para o instalador, tornando as dependências de programação mais claras.

2.2.2.n.4.9.m.2 Fórmula

```
1>!Porta aberta>
2 OU
```

O menu Fórmula permite definir a fórmula da macro. Podem ser combinados 4 eventos numa fórmula.

2.2.2.n.4.9.m.2.x Seleccionar evento

Selecione o evento apropriado para o configurar.

```
1>Grupo
Porta
```

Para escolher um evento apropriado, tem de definir primeiro a origem do evento. A origem é definida por um grupo de objectos, e um objecto dentro deste grupo. Os grupos disponíveis são indicados no Anexo A, “Eventos do Advisor Advanced”, Tabela 32 na página nº 393.

Quando o grupo e o objecto (se disponível) estiverem seleccionados, selecione o evento apropriado. A selecção disponível depende da origem seleccionada. A lista completa de eventos com origens é apresentada no Anexo A “Eventos do Advisor Advanced”, Tabela 32 na página nº 393.

As seguintes funções estão disponíveis para o evento seleccionado:

1. Grupo: Seleccionar grupo
2. Input flag: Seleccionar um input flag do grupo acima
3. Item: Seleccionar um item para o input flag acima
4. Inversão: Inverter o evento seleccionado. Se invertido, é assinalado com um '!' na fórmula

Nota: eventos específicos só podem ser entradas, enquanto que alguns eventos podem ser utilizados apenas como saídas.

2.2.2.n.4.9.m.2.y Operador

Todos os eventos são unidos com operadores lógicos. Escolha o operador para o alterar. Os operadores válidos são AND (E) e OR (OU).

2.2.2.n.4.9.m.3 Macro Output

```
3 Macro Output
>>>
```

Configure a saída da macro seleccionada.

2.2.2.n.4.9.m.3.1 Função da Output

```
1 Função Output  
>Não temp.<
```

As funções de saída são descritas em “Lógica de macros dos controladores de portas” na página nº 83.

2.2.2.n.4.9.m.3.2 Duração

```
2 Duração [s]  
> <
```

Indique a duração da função de saída a partir do menu anterior.

As unidades são mostradas no título do menu. O intervalo permitido é de 1 a 255.

2.2.2.n.4.9.m.3.3 Activo

```
1>Grupo  
Porta
```

Selecione o evento de saída da mesma forma como configura o evento de entrada. Consulte “2.2.2.n.4.9.m.2.x Seleccionar evento” na página nº 195 para obter mais informações.

2.2.2.n.4.9.m.4 Apagar Macro

```
4 Apagar Macro  
>Cancelar<
```

Utilize o comando para remover uma macro do controlador de portas. Para remover a macro, seleccione OK e prima Enter.

2.2.2.n.4.10 Disp. Locais

O menu é igual a “2.2.3 Leit Exp CP/CE”, mas aplica-se apenas a leitores ligados ao bus local do controlador de portas seleccionado. Consulte “2.2.3 Leit Exp CP/CE” na página nº 197.

2.2.2.n.4.11 Versão Disp.

```
1250.0000.11MIUM
```

O ecrã informativo mostra a versão de firmware do controlador de porta.

2.2.2.n.4.12 Sincronizar

```
12 Sincronizar  
>Cancelar<
```

O menu permite-lhe sincronizar as definições do painel de controlo e do controlador de porta.

Selecione OK e prima Enter para sincronizar. Os dados seguintes serão enviados a partir do painel de controlo para o controlador de porta selecionado, dependendo do modelo: utilizadores, faixas horárias, definições.

O início do processo de sincronização é confirmado no display LCD.

```
INFORMAÇÕES
Sinc. Iniciado
```

2.2.3 Leit Exp CP/CE

```
0>Adicionar lei>
1 Leitor 1
```

Os teclados e leitores, ligados a um dos bus de controlador de portas locais, podem ser configurados como leitores de sistema inteligentes para disponibilizar funções de controlo de acesso.

Prima 0 para adicionar um leitor, ou um número para configurar um leitor existente.

Nota: o número máximo de dispositivos permitidos no databus é indicado em “Características gerais” na página nº 39.

Opções leitor

2.2.3.0 Adicionar leitor

```
Número leitor
      >_<
```

No menu Adicionar leitor, introduza o número para este novo leitor e prima Enter para confirmar ou Sair para sair sem adicionar um dispositivo.

Depois de o dispositivo ser adicionado, são apresentadas as opções de configuração do leitor.

2.2.3.n Seleccionar leitor

Selecione o número do leitor a configurar.

2.2.3.n.2 Endereço de leitor

```
2>End. de leitor
Exp: 1 ENDE: 0
```

O ecrã informativo que mostra o endereço do leitor. O endereço é definido por DIP switches ou programado no menu de teclado ou de leitor.

2.2.3.n.3 Opções leitor

```
1>Nome de leitor  
Leitor 1
```

O menu Opções do leitor contém os menus indicados a seguir, que são necessários para configurar o leitor seleccionado.

2.2.3.n.3.1 Nome de leitor

```
1>Nome de leitor  
>Leitor 1<
```

Utilize a opção Nome de leitor para introduzir um nome que identifique o leitor ao utilizador final.

Quando é criado um leitor, é-lhe atribuído o nome predefinido “Leitor <n>”, em que <n> é o número do leitor. Aceda a este menu para editar o nome actual.

Um nome de leitor pode ser constituído por 16 caracteres.

2.2.3.n.3.2 LCD

```
2 LCD  
>Sim<
```

A opção LCD determina se o leitor seleccionado tem LCD.

Nota: se o controlador de portas reconhecer o modelo do leitor seleccionado, este valor será só de leitura.

2.2.3.n.4 Menu de leitor

```
4>Menu de leitor  
>>>
```

O menu de leitor dá acesso ao menu de programação incorporado no leitor. Para mais informações, consulte o manual do dispositivo aplicável.

2.2.3.n.5 Apagar leitor

```
5 Apagar leitor  
>Cancelar<
```

Para remover o leitor, prima Enter, seleccione OK e prima novamente Enter. O leitor é eliminado.

2.2.4 Dispositivos de áudio

```
0>Adic. áudio  
1 Áudio 1
```

Prima 0 para adicionar um dispositivo de áudio, ou um número para configurar um dispositivo de áudio existente.

Nota: o número máximo de dispositivos de áudio permitidos é indicado em “Características gerais”, na página 39.

Opções de dispositivos de áudio

2.2.4.0 Adicionar áudio

```
Áudio número
      >_<
```

Introduza o número para o novo dispositivo de áudio e prima Enter para confirmar ou Sair para sair sem adicionar um dispositivo.

Depois de o dispositivo ter sido adicionado, são apresentadas as opções de configuração do dispositivo de áudio.

2.2.4.n Selecionar áudio

Selecione o número do dispositivo de áudio a configurar.

2.2.4.n.1 Tipo de áudio

```
1>Tipo áudio
      ATs1521
```

O tipo de dispositivo de áudio é um ecrã de informação. O tipo é definido pelo dispositivo.

2.2.4.n.2 Endereço áudio

```
2>End. áudio
      BUS: 1 END: 1
```

O endereço do dispositivo de áudio é um ecrã de informação que fornece o endereço do DIP switch.

2.2.4.n.3 Definições áudio

```
1>Nome áudio
      Áudio 1
```

O menu contém os menus apresentados em baixo, os quais são necessários para configurar o dispositivo de áudio selecionado.

2.2.4.n.3.1 Nome áudio

```
1 Nome áudio
>Áudio 1 <
```

Utilize a opção para introduzir um nome que identifique o dispositivo de áudio para o utilizador final.

Quando é criado um dispositivo de áudio, é-lhe atribuído o nome predefinido “Áudio<n>”, em que <n> é o endereço do dispositivo de áudio. Aceda a este menu para editar o nome atual.

Um nome de dispositivo de áudio pode ser constituído por 16 caracteres.

2.2.4.n.3.2 Tamper área

```
2>Tamper área
  Área 1
```

A opção Área de tamper determina que área recebe tamper de dispositivo e eventos de falha. Para alterá-la, prima Enter e selecione a área.

2.2.4.n.3.3 Isolar áudio

```
3 Isolar áudio
  >Não<
```

Utilize o comando para isolar ou retirar o isolamento dos eventos de falha de tamper no dispositivo selecionado. No entanto, o dispositivo permanece funcional quando isolado.

2.2.4.n.4 Apagar áudio

```
6 Apagar áudio
  >Cancelar<
```

Utilize o comando para remover um dispositivo de áudio. Prima Enter, selecione OK e prima Enter novamente. O dispositivo é eliminado.

3 Gestão utlz

```
1>Utilizadores
2 Grupos de utlz
```

Utilize o menu de utilizadores para adicionar, editar ou eliminar utilizadores do sistema Advisor Advanced. Este menu permite também editar grupos de utilizadores.

3.1 Utilizadores

```
0>Adicionar utlz
1 Instalador
```

O menu Utilizadores permite adicionar, eliminar e editar utilizadores do sistema.

Opções comuns

3.1.0 Adicionar utilizador

```
Modo Adicionar
  >Manual<
```

Aceda ao menu para adicionar utilizadores.

Selecione o modo manual ou sequencial para adicionar utilizadores.

No modo manual, é criado um utilizador no primeiro número não ocupado na lista de utilizadores. Se o utilizador for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Utlz adicion
```

Depois disto, pode começar a editar os detalhes do utilizador para o novo utilizador.

No modo sequencial, é-lhe solicitado que passe o novo cartão de utilizador.

```
Cartão
RAS 1
```

Passe o cartão no leitor ou porta programados nas opções do sistema. Para obter mais informações, consulte “8.8.5 Aprende cartão”, na página nº 310.

Se o cartão estiver válido e o utilizador for criado com êxito, aparece a seguinte mensagem:

```
Utilizador 13
Cartão atribuído
```

A seguir, é-lhe solicitado que passe outro cartão. Prima Cancelar para sair da programação sequencial de utilizador e ir para a configuração de utilizador.

Se o cartão já for usado, é apresentado o erro.

```
ERRO
Cartão em uso
```

3.1.n Seleccionar utlz

Selecione um utilizador para editar.

Podem ser configuradas as opções indicadas a seguir.

3.1.n.1 Nome de utlz

```
1 Nome de utlz
>Utilizador 6 <
```

Prima Enter para editar o nome ou prima Sair para sair.

O nome de utilizador predefinido é “Utilizador N”, em que N é o número do utilizador.

O nome pode ter no máximo de 16 caracteres.

3.1.n.2 PIN

```
1>Alterar PIN
>>>
```

O menu permite alterar o PIN do utilizador, bem como configurar o código de utilizador remoto.

3.1.n.2.1 Alterar PIN

```
2 Código PIN
*****
```

Altere o PIN de utilizador seleccionado.

Consulte “PIN” na página nº 77 para mais informações sobre a utilização do PIN.

3.1.n.2.2 PIN Remoto

```
1>Definir PIN
*****
```

O PIN remoto é um PIN para programar o painel através de uma ligação remota. Se o PIN remoto não estiver definido, o instalador utiliza o PIN local para iniciar sessão remotamente.

Nota: este submenu está disponível apenas para o instalador. Se permitido pela opção “8.7.8.2 Config. superv.” na página nº 308, o submenu também fica disponível para o supervisor.

Consulte “Acesso remoto” na página nº 141 para obter mais informações.

3.1.n.2.2.1 Definir PIN

```
1>Definir PIN
  >          <
```

Definir PIN remoto.

Para activar o PIN remoto, utilize “3.1.n.2.2.2 Permitir login” abaixo.

3.1.n.2.2.2 Permitir login

```
2>Permitir login
  >Sim<
```

Utilize o comando para activar o PIN remoto.

Cuidado: Uma vez activado, o PIN remoto não pode ser desactivado nem alterado localmente, e o menu de PIN Remoto é desactivado.

Consulte “3.1.n.2.2 PIN Remoto” na página nº 202 para obter mais informações.

3.1.n.3 Cartão utilizador

```
3>Atrib. cartão
  Cart. não atrib
```

O menu Cartão de utilizador permite atribuir ou eliminar um cartão de utilizador.

O conteúdo do menu depende de o cartão já ter sido atribuído ou não.

3.1.n.3.1 Atribuir cartão

Se o utilizador não tiver nenhum cartão atribuído, o menu permite introduzir um número de cartão de utilizador.

Prima Enter e apresente o cartão ao teclado no espaço de 10 segundos.

```
INFORMAÇÕES
  Cartão
```

Nota: Esta operação só é possível em teclados com leitores integrados. O teclado ou a porta para aprendizagem de cartões estão definidos nas opções do sistema. Para obter mais informações, consulte “8.8.5 Aprende cartão”, na página nº 310. Se estiver definido outro teclado ou porta para aprendizagem de cartões, esse mesmo nome é pedido, por exemplo:

```
Cartão
Teclado 3
```

Remover um cartão

Se o utilizador tiver um cartão atribuído, pode remover o cartão atribuído. Aparece o ecrã seguinte.

```
1>Remover cartão
  Cartão atrib
```

Prima Enter.

```
INFORMAÇÕES  
Cartão removido
```

O cartão foi removido do utilizador seleccionado.

3.1.n.4 Comandos

```
0>Adic.comando  
1 Com 1
```

Este menu permite ver todos os comandos programados para o utilizador seleccionado, seleccionar um comando existente ou criar um novo comando.

O conteúdo do menu é semelhante ao menu 4 Zonas e áreas > 4.4 Comandos descrito na página nº 234.

3.1.n.5 Idioma

```
5>Idioma  
PORTUGUES
```

O sistema Advisor Advanced pode apresentar os menus no idioma preferido de cada utilizador.

O idioma é alterado após a autorização do utilizador.

Para mais informações sobre os idiomas disponíveis, entre em contacto com o seu fornecedor.

3.1.n.6 Grupos utlz

```
1>Não config.  
2 Não config.
```

Utilize o menu Grupos de utilizadores para atribuir grupos de utilizadores ao utilizador seleccionado. Um utilizador pode ter até 8 grupos de utilizadores atribuídos. Os grupos de utilizadores definem as opções e áreas disponíveis aos utilizadores.

Para alterar uma atribuição de grupo de utilizadores, seleccione o campo aplicável.

Se o campo seleccionado estiver vazio (o grupo de utilizadores não está atribuído), é-lhe solicitado que seleccione um dos grupos de utilizadores disponíveis.

```
02>Supervisor G>  
03 Área 1
```

Selecione o grupo de utilizadores adequado a atribuir ao utilizador seleccionado.

Se o campo seleccionado já contiver um grupo de utilizadores atribuído, o ecrã passa para o menu “Alterar grupo de utilizadores”.

```
1>Alterar GU
  Grp.Utilizador 3
```

Agora pode efectuar uma das seguintes acções:

- Alterar o grupo atribuído: premir 1 ou Enter ou Direita para ir para a lista de grupos de utilizadores e seleccionar o grupo aplicável.
- Remover o grupo atribuído: premir 2 ou ir para a entrada de menu seguinte e premir Enter.

Nota: o grupo de utilizadores “grupo de instaladores” só pode ser atribuído ao instalador.

Para mais informações sobre grupos de utilizadores, consulte “3.2 Grupos de utilizadores” na página nº 208.

3.1.n.9 Seleccione Modo

```
9 Seleccione Mo>
  >Áreas<
```

Consoante a selecção, o utilizador opera em áreas ou grupos de áreas. Estão disponíveis as seguintes opções:

- Áreas. O utilizador só pode armar e desarmar áreas específicas. Este é o valor predefinido.
- Grupos Área. O utilizador só pode armar e desarmar grupos de áreas específicos.
- Tudo. O utilizador pode armar e desarmar áreas e grupos de áreas.

3.1.n.10 Remover utlz

Para remover um utilizador, seleccione o utilizador com o cursor, ou introduza o número de utilizador e aceda ao menu Remover utilizador.

O ecrã apresenta:

```
10 Remover utlz
  >Cancelar<
```

Seleccione OK e prima Enter. Isto remove o utilizador.

Repita o comando para eliminar outros utilizadores, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: só pode eliminar um utilizador se o seu grupo de utilizadores o autorizar a fazê-lo.

Opções de telemóvel

3.1.n.7 SMS e Voz

```
1>Tel.utilizador
    Nada
```

O menu SMS e Voz contém menus de configuração de reporte de SMS e de voz.

3.1.n.7.1 Telefone de utilizador

```
1 Tel.utilizador
> <
```

O menu Telefone de utilizador permite definir o número de telefone pessoal do utilizador.

Este número de telefone é utilizado se o tipo de destino do reporte GSM for definido para Utilizador ou Grupo de utilizadores. Consulte “9.1.n.4.1 Tipo” na página nº 325.

Este número de telefone também identifica um remetente de um comando SMS. Para mais informações, consulte o *Guia de Referência do Controlo por SMS do Advisor Advanced*.

3.1.n.7.2 Reporte de SMS

```
2 Reporte SMS
    Desligado
```

O menu Reporte SMS permite activar ou desactivar o reporte SMS do utilizador seleccionado. O reporte pode apresentar um dos seguintes estados:

- Sempre: o reporte está activado
- Desligado: o reporte está desactivado
- Off até rearme: O reporte está temporariamente desactivado até ao próximo arme do sistema

Esta opção é editável apenas se o utilizador pertencer a um grupo de utilizadores que tem o privilégio de reporte SMS activado. Consulte “3.2.n.6 Opções de GU” na página nº 210 para obter mais informações.

3.1.n.7.3 Controlo SMS

```
3 Controlo SMS
    Desactivar
```

O menu Controlo SMS permite activar ou desactivar o controlo por SMS para o utilizador seleccionado.

Esta opção só pode ser alterada se o utilizador pertencer a um grupo de utilizadores que tenha o privilégio de reporte SMS activado. Consulte “3.2.n.6 Opções de GU” na página nº 210 para obter mais informações.

Nota: o controlo por SMS de um utilizador é desactivado após 10 tentativas de execução de um comando SMS não autorizado. Para mais informações, consulte o *Guia de referência do Controlo por SMS do Advisor Advanced*.

Opções de acesso

3.1.n.8 Opções acesso

```
1>Grp. Portas
  Não utilizado
```

Utilize o menu para configurar as opções de controlo de acesso para o utilizador seleccionado.

3.1.n.8.1 Grupo de portas

```
1 Grp. Portas
  >Não utilizado<
```

Atribua um grupo de portas ao utilizador seleccionado.

Consulte Capítulo 3 “Funções do sistema > Grupos de portas” na página nº 81 para mais informações sobre grupos de portas.

3.1.N.8.2 Grupo de pisos

```
2 Grupo de pisos
  >Não utilizado<
```

Atribua um grupo de pisos ao utilizador seleccionado.

Consulte o Capítulo 3 “Funções do sistema > Grupos de pisos” na página nº 81 para obter mais informações sobre grupos de pisos.

3.1.n.8.3 Seguir

```
3 Seguir
  >Não<
```

Se definido como Sim, todos os eventos de acesso relacionados com este utilizador serão enviados de controladores de portas para o painel e armazenados no respectivo registo, para que o operador do painel o possa seguir.

3.1.n.8.4 Com Privilégio

```
4 Com Privilégio
  >Não<
```

Se definido como Sim, este utilizador pode anular a funcionalidade de anti-passback e obter acesso a regiões que deveriam ser restritas para um utilizador normal devido às limitações de anti-passback.

3.1.n.8.5 Estender acesso

```
5 Est. Acesso  
>Não<
```

Se estiver definido para Sim, o utilizador selecionado terá um tempo de desbloqueio de porta alargado e um tempo de desvio concedido após a leitura de um cartão válido ou da introdução do PIN. O tempo estendido é definido separadamente para cada porta. Consulte “5.1.n.5.2 Tempo alargado” na página nº 243.

3.1.n.8.6 TipoUtilAcesso

```
6 TipoUtilAcesso  
>Normal<
```

Define o tipo de utilizador para maior segurança.

- Normal: Funcionamento normal.
- Dois Cartões: Requer que sejam apresentados dois cartões ou códigos de utilizador válidos para executar quaisquer funções de controlo de acesso ou alarme.
- Vigilante: O cartão ou código de utilizador só pode executar funções quando utilizado juntamente com um cartão ou código de visitante.
- Visitante: Requer um cartão ou código de um utilizador de tipo Vigilante.
- Util. Alta Seg: só quando é alcançado o número exigido de utilizadores deste tipo dentro de uma região de alta segurança é que os utilizadores normais também podem permanecer na região. Consulte “Alta segurança” na página nº 83 para obter mais informações.

3.2 Grupos de utilizadores

```
0>Adicionar GU  
1 Grupo instal.
```

O bloco de programação Grupos de utilizadores é utilizado para registar informação acerca de grupos de utilizadores.

Opções de grupos de utilizadores

3.2.0 Adicionar GU

Aceda ao menu para adicionar um grupo de utilizadores. Se o grupo de utilizadores for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES  
GU adicionado
```

É atribuído ao novo grupo de utilizadores o nome predefinido de “GU N” e é colocado no fim da lista de grupos de utilizadores. Agora o utilizador pode começar a editar os detalhes do grupo de utilizadores para o novo grupo de utilizadores.

3.2.n Seleccionar GU

Para editar um grupo de utilizadores, seleccione primeiro o grupo de utilizadores pretendido.

Podem ser configuradas as opções indicadas a seguir.

3.2.n.1 Nome

```
1 Nome GU
>Grp.Utilizador>
```

Utilize a opção Nome GU para definir o nome do grupo de utilizadores. Prima Enter para editar o nome ou prima Sair para sair.

O nome do grupo de utilizadores pode ter no máximo 16 caracteres.

3.2.n.2 Tipo de GU

```
2 Tipo de GU
>Arme total<
```

Selecione um tipo do grupo de utilizadores seleccionado.

Para uma descrição detalhada dos tipos de grupos de utilizadores e tipos de grupos de utilizadores disponíveis, consulte “Tipos de grupos de utilizadores” na página nº 72.

3.2.n.3 Áreas GU

```
01-10>Áreas GU
1.....
```

A opção Áreas do grupo de utilizadores define as áreas que o utilizador pode controlar.

3.2.n.4 GU GA

```
01-10>GU GA
1.....
```

A opção de grupo de áreas de GU define quais os grupos de áreas que o utilizador pode controlar.

3.2.n.5 Filtro GU

```
5>Filtro GU
Não utilizado
```

Quando utilizar um filtro, os direitos do utilizador definidos pelo grupo de utilizadores dependem do estado deste filtro.

Para mais informações sobre filtros de condições, consulte “6.1 Filtros de condição” na página nº 267.

3.2.n.6 Opções de GU

```
6>Opções de GU
  >>>
```

As Opções de grupo de utilizadores definem os direitos de acesso do utilizador às diferentes opções. Podem ser configuradas as opções indicadas a seguir.

As opções disponíveis são indicadas em “Opções de grupos de utilizadores” na página nº 75.

3.2.n.7 Programa

Selecione programas para o grupo de utilizadores seleccionado.

O menu de atalhos permite atribuir até dois programas a cada um dos elementos seguintes:

- 1 Privilégios
- 2 Acesso área

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

3.2.n.8 Remover GU

Para remover um grupo de utilizadores, selecione o grupo de utilizadores com o cursor, ou introduza o número do grupo de utilizadores e aceda ao menu Eliminar GU.

O ecrã apresenta:

```
8 Remover GU
  >Cancelar<
```

Selecione OK e prima Enter. Isto remove o grupo de utilizadores.

Repita o comando para eliminar outros utilizadores, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: não é possível eliminar um grupo de utilizadores se ao mesmo estiverem atribuídos utilizadores, acções ou centrais receptoras.

4 Zonas e áreas

```
1>Menu Zona
2 Áreas
```

Na secção de programação de Zonas e Áreas são programados todos os parâmetros de zona, comando e área.

Cuidado: Selecione o esquema de numeração pretendida antes de programar as zonas. Ver “8.7.9 Esquema Objeto” na página nº 308 para mais informações

4.1 Zonas

```
0>Adicionar zona
1 Zona 1
```

Este menu permite ver todas as zonas programadas, seleccionar uma zona existente ou criar uma nova zona.

Cada zona pode ser uma entrada física no painel de controlo, um expansor ou um expansor plug-in, ou um dispositivo sem fios programado no expansor sem fios.

Opções de zona

4.1.0 Adicionar zona

```
0>Zona
1 Painel
```

Utilize o menu Adicionar zona para adicionar uma nova zona. Ao adicionar uma zona, seleccione uma das opções seguintes:

- 0 Zona: Adicionar uma zona atribuída à entrada de sistema específica.
- 1 Painel: Adicionar uma zona atribuída à entrada de painel específica.
- 2 Exp. Painel: Adicionar uma zona atribuída à entrada de expansor de painel específica.
- 3 DGP: Adicionar uma zona atribuída à entrada específica de um expansor. Seleccionar primeiro um expansor.

Se o expansor seleccionado suportar tanto zonas com e sem fios, ser-lhe-á solicitado para seleccionar a opção apropriada.

```
Disp. sensor
>Sem fios<
```

Para zona com fios, seleccione uma entrada no expansor.

Para dispositivos sem fios, consulte “Adicionar um sensor sem fios” na página nº 212.

- 4 Auto-detectar: Adicionar uma zona atribuída à primeira entrada de sistema não utilizada.

Consulte “Endereçamento de zonas, saídas e portas” na página nº 33 para ver endereçamentos de zona disponíveis.

Se a zona seleccionada já existir, aparece um aviso.

Se a zona for criada com êxito, o ecrã passa para o menu “4.1.n.1 Nome da zona”.

Adicionar um sensor sem fios

Se o expansor seleccionado for um expansor sem fios, adicionar zonas resulta na aprendizagem do sensor sem fios pelo expansor sem fios.

A aprendizagem de sensores sem fios é descrita em “Programação de dispositivos sem fios” na página nº 110.

Se o dispositivo for uma câmara PIR sem fios, será também criada uma câmara correspondente na base de dados de câmaras. Consulte “Utilizar câmaras” na página nº 117.

4.1.n Seleccionar zona

```
1>Nome da zona
   Zona 1
```

Selecione uma zona existente a programar.

Selecione uma zona a programar.

Nota: as opções específicas deste menu diferem relativamente a sensores diferentes. Para ver opções específicas, consulte:

- “Opções de sensor de choque” na página nº 225
- “Opções de sensores sem fios” na página nº 225

Opções comuns

4.1.n.1 Nome da zona

```
1 Nome da zona
>Zona 1 <
```

Utilize a opção Nome da zona para definir um nome de zona. O nome da zona identifica ao utilizador final a zona para reportes de alarme ou para apresentar o estado ou as mensagens de erro. Sem um nome próprio, o utilizador final não poderia resolver problemas que tivessem origem numa determinada zona.

Quando uma zona é criada, é-lhe atribuído o nome predefinido “Zona n”.

Aceda a este menu para editar o nome actual.

Um nome de zona pode ser constituído por 30 caracteres.

4.1.n.2 Tipo de zona

```
1>Tipo de zona
  Alarme
```

Utilize o menu Tipo de zona para definir o tipo de zona de uma zona específica. O tipo de zona determina exactamente como a zona funciona em determinadas circunstâncias. Cada tipo de zona tem um comportamento diferente.

Notas

- As opções de zona disponíveis dependem do tipo de zona.
- O tipo de zona para um dispositivo sem fios é definido inicialmente pelo tipo de dispositivo durante a aprendizagem do dispositivo. Por exemplo, a zona com botão de pânico é definida por predefinição com o tipo “Pânico”.

Em “Tipos de zonas” são apresentados todos os tipos de zona e as respectivas opções (consulte a página 49).

4.1.n.3 Isolado

```
3 Isolado
  >Não<
```

O menu Isolado menu permite isolar ou retirar o isolamento da zona seleccionada.

4.1.n.4 Localiz. zona

```
4>Localiz. zona
  Painel 1.1
```

O campo Localização da zona informa qual a entrada física à qual está ligada a zona.

4.1.n.5 Zona áreas

```
5>Zona áreas
  12.....
```

A zona necessita de uma área para poder enviar informações de alarme à central receptora, e para poder reinicializar quando ocorre um alarme. Utilize o menu Áreas para atribuir a área à zona que tem de gerar o alarme quando a zona é activada e o estado da área (armada ou desarmada) satisfaz os requisitos do tipo de zona.

No caso de serem seleccionadas várias áreas, o alarme refere-se à área com o menor número atribuído. O alarme ocorre consoante o tipo de zona e apenas se todas as áreas atribuídas estiverem armadas.

A função da zona depende do tipo de zona seleccionado durante a programação.

O ecrã apresenta uma lista das áreas às quais a zona está atribuída. Por exemplo, o ecrã anterior indica que a zona está atribuída às áreas 1 e 2.

4.1.n.6 Opções de zona

```
6>Opções de zona
    >>>
```

O menu Opções de zona contém todas as definições de zona. Essas definições são descritas em baixo.

Nota: poderão não estar disponíveis todas as opções. As opções disponíveis dependem do tipo de zona (consulte “Tipos de zonas” na página 49).

4.1.n.6.1 Inibir

```
1 Inibir
    >Sim<
```

Se a opção Inibir estiver definida como Sim, esta zona pode ser inibida pelo utilizador.

4.1.n.6.2 Isolar

```
2 Isolar
    >Sim<
```

Se a opção Isolar estiver definida como Sim, esta zona pode ser isolada pelos utilizadores.

4.1.n.6.3 Excl. em ArP1

```
3 Excl. em ArP1
    >Não<
```

Quando uma zona está programada para arme parcial (a opção Excluído em arme parcial está definida como Sim), é excluída quando a área atribuída é armada parcialmente. As condições normais de desarme, se relevantes, continuam a ser monitorizadas (tamper, anti-máscara, etc). Se a opção Excluído em arme parcial estiver definida como Não, a zona é armada nos dois modos, arme parcial e arme total.

Existem dois armas parciais, ArP1 e ArP2.

4.1.n.6.4 Excl. em ArP2

Consulte “4.1.n.6.3 Excl. em ArP1” acima.

4.1.n.6.5 Duplo impulso

```
5 Duplo impulso
    >Não<
```

Se a opção Duplo impulso estiver definida como Sim, a zona necessita que dois parâmetros estejam presentes para gerar um alarme. Se a zona ficar activa e se normalmente accionaria um alarme, a zona necessita de permanecer activa durante o tempo de abertura programado de Duplo impulso (consulte “8.1.4.2 Abertura duplo impulso” na página nº 286) ou a zona tem de voltar para

o normal e accionar novamente dentro do intervalo de Duplo impulso (consulte “8.1.4.1 Intervalo duplo impulso” na página nº 286).

Nota: se a opção estiver activa, a opção “4.1.n.6.30 Mantida abert” na página nº 221 não estará disponível.

4.1.n.6.6 Swinger shunt

```
6 Swinger shunt
  >Não<
```

Se a opção Swinger shunt estiver definida como Sim, o número de alarmes a partir desta zona está limitado ao número definido em “8.6.4 Swinger shunt” (consulte a página 303) para um ciclo de arme/desarme.

4.1.n.6.7 Anti-Mask

```
7 Anti-Mask
  >Sim<
```

Quando a opção Anti-Mask estiver definida como Sim, a janela de alarme inferior, nominalmente a meio do módulo EOL, é monitorizada para uma condição de máscara de detector.

Consulte “Ligação das zonas” na página nº 25 para obter mais informações.

4.1.n.6.8 Empar. zona

```
8 Empar.zona
  >Não<
```

Se a opção Empar. de zona estiver definida para Sim, esta zona só é considerada activa quando estão activas duas entradas: a atribuída (n) e a que se encontra a seguir à atribuída (n+1).

A zona atribuída à entrada a seguir (n+1) tem de existir no sistema. Este alarme de zona não é registado se ambas as zonas atribuídas á mesma área.

Nota: não é possível utilizar esta opção na zona atribuída à entrada com o último número.

Somente zonas de um tipo específico é podem ser emparelhadas. Ver Tabela 12 na página nº 52 para mais informação.

4.1.n.6.9 Campainha

```
9 Campainha
  >Desligado<
```

Se a opção Campainha estiver definida como Ligado, a zona pode ser desligada e, consoante a definição em “8.8.2 Campainha” (consulte a página 310), pode activar um breve sinal:

- Nos besouros de teclado de todos os teclados atribuídos às áreas relacionadas
- Na sirene interna atribuída às áreas relacionadas

4.1.n.6.10 Soak test

```
10 Soak test
    >Não<
```

A zona pode ser armada no modo Soak test, o que é útil para efeitos de diagnóstico. Uma zona em soak test não gera alarmes no sistema mas a sua activação é registada. Esta zona não é verificada durante o arme.

Nota: Se esta opção for ativada numa zona de entrada/saída, a funcionalidade de entrada/saída é desabilitada e os temporizadores de entrada/saída não são ativados.

4.1.n.6.11 Walk Test técnico

```
11 Walk Test téc
    >Não<
```

Se a opção Walk Test técnico estiver definida para Sim, a zona é incluída no Walk Test de técnico. Para mais informações, consulte “1.2.5 Walk Test” na página 155.

4.1.n.6.12 Walk Test utl

```
12 Walk Test utl
    >Sim<
```

Se a opção Walk Test do utilizador estiver definida para Sim, a zona é incluída no Walk Test do utilizador. Para mais informações, consulte “1.2.5 Walk Test” na página 155.

4.1.n.6.13 Sensor choque

```
13 Sensor choque
    >Não<
```

A opção Sensor de choque activa a funcionalidade de sensor de choque. Se esta opção estiver definida como Sim, a zona opera de acordo com as definições configuradas em “4.1.n.7 Sensor Choque” (consulte a página 225).

Apenas as primeiras oito entradas do painel de controlo e as primeiras oito do expansor de entrada suportam esta opção.

4.1.n.6.14 Prolongar EE

```
14 Prolongar EE
    >Não<
```

Se a opção Prolongar EE estiver definida como Sim, a activação da zona prolonga o tempo de entrada relativamente ao valor definido por “4.2.n.4.2 Tempo pré-alarm” na página nº 230.

Nota: após expirar o tempo limite da temporização de entrada, é activado o alarme local.

4.1.n.6.15 Porta final

```
15 Porta final
    >Não<
```

Quando a opção Porta final está definida como Sim, a zona tem a funcionalidade de saída terminal. Se a zona estiver activada durante o tempo de saída, a temporização de saída é terminada depois de expirar o atraso do arme final (consulte “8.1.3.5 Rtd.arme final” na página nº 286) e a área é armada.

4.1.n.6.16 Chave latch

```
16 Chave latch
    >Não<
```

Se a opção Chave latch estiver definida como Sim, a entrada da zona do comutador de chave está em latch. Se o estado da zona for activo, a área é armada. Se a zona mudar para normal, a área é desarmada.

Se estiver definida como Não, a entrada precisa que ambos os estados alternem entre arme e desarme (comutador de chave de impulso).

4.1.n.6.17 Arme por chave

```
17 Arme chave
    >Desligado<
```

A opção Arme por chave define a zona como um comutador de chave do arme da área. Estão disponíveis as seguintes opções:

- Desligado: o arme da área não é afectado pela zona.
- Arme parcial por chave: a zona é um comutador de chave do arme parcial da área.
- Arme total por chave: a zona é um comutador de chave do arme total da área.

4.1.n.6.18 Desarme por chave

```
18 Desarme chave
    >Não<
```

Se a opção Desarme por chave estiver definida como Sim, a zona é um comutador de chave que desarma uma área.

4.1.n.6.19 Arme total técnico

```
19 Arme tot. téc
    >Não<
```

A opção define como os alarmes técnicos são mostrados quando a área está armada:

- Não: Os alarmes técnicos nesta zona estão desativados. Não estão indicados nem reportados.
- Aviso: Os alarmes técnicos são indicados como falhas.

- **Alarme:** Os alarmes técnicos fazem com que o LED de falha acenda e a flag de da zona em alarme seja ativada

Se definidos como Aviso ou Alarme, os alarmes técnicos são reportados com os eventos listados na Tabela 25 na página nº 220.

4.1.n.6.20 Desarme técnico

```
20 Desarme téc
    >Não<
```

A opção define como os alarmes técnicos são mostrados quando a área está desarmada:

- **Não:** Os alarmes técnicos nesta zona estão desativados. Não estão indicados nem reportados.
- **Aviso:** Os alarmes técnicos são indicados como falhas.
- **Alarme:** Os alarmes técnicos fazem com que o LED de falha acenda e a flag de da zona em alarme seja ativada

Se definidos como Aviso ou Alarme, os alarmes técnicos são reportados com os eventos listados na Tabela 25 na página nº 220

4.1.n.6.21 Arme parcial técnico

```
21 Arme parc.téc
    >Não<
```

A opção define a forma como os alarmes técnicos são mostrados quando a área está parcialmente armada:

- **Não:** Os alarmes técnicos nesta zona estão desativados. Não estão indicados nem reportados.
- **Aviso:** Os alarmes técnicos são indicados como falhas.
- **Alarme:** Os alarmes técnicos fazem com que o LED de falha acenda e a flag de da zona em alarme seja ativada.

Se definidos como Aviso ou Alarme, os alarmes técnicos são reportados com os eventos listados na Tabela 25 na página nº 220.

4.1.n.6.22 RAS LCD

```
22 RAS LCD
    >Não<
```

Se a opção LCD de Teclado estiver definida como Sim, quando a zona é activada o nome da zona é apresentado no LCD de teclado de todos os teclados relacionados com a área.

4.1.n.6.23 Registo

```
23 Registo
    >Não<
```

A opção Registo determina se o evento da zona é registado no registo do sistema.

4.1.n.6.24 Reporte CRA

```
24 Reporte CRA
  >Não<
```

A opção Reporte CRA determina se o evento da zona é reportado à central receptora.

4.1.n.6.25 Temp. Retardo

```
25 Temp. Retardo
  >Não<
```

Se a opção Temporizador de retardo estiver definida como Sim, é activado um temporizador de retardo para esta zona. O temporizador de retardo é definido em “8.1.4.4 Retardo de input” (consulte a página 287).

4.1.n.6.26 REC no RAS

```
26 REC no RAS
  >RAS 1<
```

As opções confirmadas estão disponíveis para o tipo de zona de comutador de chave. Permitem definir um teclado onde um utilizador específico inicia sessão automaticamente. Isto faz com que as informações de falha e alarme sejam apresentadas instantaneamente no teclado seleccionado.

A sessão CONF abre-se durante 2 minutos. Durante este período de tempo pode reconhecer o alarme no teclado programado.

Nota: “4.1.n.6.27 REC p/ Utiliz” abaixo deve também ser definido para que a funcionalidade de confirmação funcione.

4.1.n.6.27 REC p/ Utiliz

```
27 REC p/ Utiliz
  >Utilizador 3<
```

A opção define o utilizador que inicia sessão automaticamente quando a zona seleccionada causa um alarme.

Nota: “4.1.n.6.26 REC no RAS” acima deve também ser definido para que a funcionalidade de confirmação funcione.

Consulte “4.1.n.6.26 REC no RAS” acima para obter mais informações.

Consulte também “2.2.1.n.3.18 REC no RAS” na página nº 182.

4.1.n.6.28 Sensor tipo

```
28 Sensor tipo
  >Temp. baixa<
```

Os eventos reportados por uma zona técnica dependem do tipo de sensor ligado. A opção Tipo de sensor indica o tipo de sensor e quais os eventos que deve reportar. Estão disponíveis os seguintes tipos de sensor:

- Detector de temperatura baixa

- Detector de gás
- Detector de temperatura alta
- Detector de inundação
- Fogo
- Genérico

Tabela 25 abaixo indica eventos que podem ser reportados para cada tipo de sensor.

Tabela 25: Tipos de sensor e eventos reportados

Tipo de sensor	Código	Alarme	Restaurar alarme	Bypass	Unbypass	Supervisão longa	Restauro de supervisão
Temp. baixa	SIA	ZA	ZR	ZB	ZU	ZS	ZJ
	CID	E152	R152	E570	R570	E381	R381
Gás	SIA	GA	GR	GB	GU	GS	GJ
	CID	E151	R151	E570	R570	E381	R381
Temp. alta	SIA	KA	KR	KB	KU	KS	KJ
	CID	E158	R158	E570	R570	E381	R381
Inundação	SIA	WA	WR	WB	WU	WS	WJ
	CID	E154	R154	E570	R570	E381	R381
Fogo	SIA	FA	FR	FB	FU	FT	FJ
	CID	E110	R110	E570	R570	E373	R373
Módulo ext.	SIA	ET	ER	UB	UU	ZS	ZJ
	CID	E333	R333	E570	R570	E381	R381
	VdS	0x30	0xB0	0x51	0xD1	0x30	0xB0
Tamper do módulo ext.	SIA	ES	EJ	UB	UU	ZS	ZJ
	CID	E341	R341	E570	R570	E381	R381
	VdS	0x23	0xA3	0x51	0xD1	0x30	0xB0
Genérico	SIA	UA	UR	UB	UU	ZS	ZJ
	CID	E140	R140	E570	R570	E381	R381

Consulte também “Códigos de reporte utilizados no Advisor Advanced” on page 399.

4.1.n.6.29 Zona virtual

```
1>Saídas
2 RAS
```

O menu permite mapear a zona seleccionada para uma saída existente ou para um teclado.

Se não for definida uma saída ou um teclado, o estado da zona segue o estado da entrada física atribuída.

- Se for seleccionada uma saída, a zona transforma-se numa zona virtual que está activa quando a saída seleccionada está activa. Neste caso, a entrada física não tem qualquer efeito sobre a zona.
- Se for seleccionado um teclado a zona transforma-se numa zona virtual, que está activa quando o teclado seleccionado tem um pedido para sair do estado (RTE) activo.

Consulte também “Saídas” na página nº 79.

4.1.n.6.30 Mantida abert

```
30 Mantida abert
    >Não<
```

O menu define se esta zona gera um alarme de “zona aberta demasiado tempo” se for mantida aberta durante um período de tempo superior ao período definido.

O período para manter aberto é definido em “8.1.4.6 Tempo Manter Aberto” na página nº 287.

Nota: se a opção estiver activa, a opção “4.1.n.6.5 Duplo impulso” na página nº 214 não estará disponível.

4.1.n.6.31 ES verif arme

```
31 ES verif arme
    >Não<
```

Se definido para sim, a zona de entrada/saída ou de acesso deve estar em estado normal aquando do arme da área. Caso contrário, o utilizador não tem autorização para armar as instalações até o problema estar resolvido.

A opção apenas está disponível para zonas de tipo entrada/saída e acesso.

4.1.n.6.32 Alarme em AP1

```
32 Alarme em AP1
    >Não<
```

Se a opção estiver definida como sim, a zona de entrada/saída torna-se uma zona de alarme durante o arme parcial 1.

Notas

- A opção apenas está disponível para zonas de tipo entrada/saída. Consulte também “Tipos de zonas” na página nº 49.
- A zona deve ser incluída no arme parcial 1. Consulte “4.1.n.6.3 Excl. em ArP1” na página nº 214.
- A funcionalidade da zona não se altera se a mesma zona pertencer a uma área em estado de alarme total.

4.1.n.6.33 Alarme em AP2

O mesmo que “4.1.n.6.32 Alarme em AP1” acima, mas para arme parcial 2.

4.1.n.6.34 Reportar como

```
34 Reportar como  
>Pânico (PA)<
```

Define como o alarme de pânico é reportado às estações centrais.

- Reportar como pânico: É reportado o evento PA.
- Reportar como coacção: É reportado o evento HA.

Para mais informações, consulte “Códigos de reporte utilizados no Advisor Advanced” on page 399.

Notas

- Esta opção apenas está disponível para zonas de tipo pânico. Consulte também “Tipos de zonas” na página nº 49.
- A opção apenas está disponível quando o modo de pânico está definido para Silencioso. Caso contrário, o alarme de pânico é sempre reportado como evento PA. Consulte “8.8.1 Modo de pânico” na página nº 309.

4.1.n.6.35 Auto Teste

```
35 Auto Teste  
>Sim<
```

Se a opção estiver definida como Sim, o detector é testado automaticamente quando auto teste está activo. Consulte também “1.2.1.8 Test Detector” na página nº 152.

4.1.n.6.36 Shunt

```
36 Shunt  
>Sim<
```

Se a opção estiver definida como Sim, a zona pode ser isolada.

Consulte “Inibição de zonas” na página nº 60 para mais informações.

4.1.n.6.37 Ver isolados

```
37 Ver isolados  
>Ligado<
```

Se a opção estiver definida como Ligado, os utilizadores são avisados sobre esta zona estar isolada ao tentar armar ou desarmar a área apropriada.

4.1.n.6.38 Stop Reporte

```
38 Stop Reporte  
>Não<
```

Se a opção estiver definida como Sim, a activação de zona interrompe o reporte por voz, se estiver activo.

Esta opção só está disponível para zonas de tipo comutador de chave.

4.1.n.6.39 Limitar relatórios

```
39 Limita relat.
  >Desligado<
```

Se a opção estiver definida como Ligado, o reporte da zona é limitado com a janela de tempo definida em “8.6.6 Limitar relatórios” na página nº 303.

4.1.n.8 Listen-in

```
1>Modo escuta
  Desativado
```

Utilize o menu para configurar o áudio de duas vias para a zona selecionada.

Esta opção está disponível apenas para sistemas de áudio de duas vias. Consulte o Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123 para obter mais informações.

4.1.n.8.1 Modo de escuta

```
1 Modo de escuta
  >Desativado<
```

Selecione um modo de escuta para a zona selecionada. Estão disponíveis as seguintes opções:

- Desativado: sem áudio.
- Só escuta: o operador da central recetora apenas pode ouvir o áudio do dispositivo de áudio atribuído à zona.
- Escuta e fala: o operador pode ouvir o áudio ou falar utilizando o dispositivo de áudio atribuído.

4.1.n.8.2 Link áudio

```
0 Nada
1 Áudio 1
```

Atribui um dispositivo de áudio à zona selecionada.

4.1.n.8 Copiar e Adic

```
1>Copia par. de
  >>>
```

Utilize o menu Copiar para copiar parâmetros de zonas.

Estão disponíveis os seguintes métodos de cópia:

4.1.n.8.1 Copia par. de

```
Zona 1
Zona 2
```

Utilize o menu Parâmetros de zona para importar todos os parâmetros de zona de uma zona específica para a zona seleccionada.

Escolha a zona cujos parâmetros devem ser copiados para a zona seleccionada e prima Enter.

```
INFORMAÇÕES
Cópia ok
```

São copiadas todas as definições com excepção do descritivo.

4.1.n.8.2 Atribuir bloco

```
Input início
>>>
```

Utilize o menu Bloq atrib para copiar todos os parâmetros de zona seleccionados para um intervalo de entradas, criando as zonas apropriadas.

Selecione um início e um fim para o intervalo de entradas de dispositivo.

O sistema cria ou modifica as zonas existentes com parâmetros equivalentes à zona seleccionada (excepto nomes predefinidos).

Nota: a cópia de parâmetros de zona não copia um dispositivo sem fios. O dispositivo deve ser programado em separado. Consulte “4.1.n.7 Detalhes RF” na página nº 225 para obter mais informações.

4.1.n.9 Mover zona

```
04>Não utilizado
09 Não utilizado
```

Permite mover a zona seleccionada para outro número de zona disponível.

Esta opção só está disponível num esquema flexível de numeração de zonas. Consulte “8.7.9 Esquema Objeto” na página nº 308 para obter mais informações.

Consulte também “Endereçamento de zonas, saídas e portas” na página nº 33.

4.1.n.10 Remover zona

```
10 Remover zona
>Cancelar<
```

Utilize o comando Remover zona para remover uma zona do sistema. Para remover a zona, selecione OK e prima Enter. A zona é eliminada.

Notas: no caso de um dispositivo sem fios, o dispositivo é também removido da base dados do expansor sem fios.

Cuidado: se a zona estiver atribuída a um dispositivo RF de duas zonas, ambas as zonas serão eliminadas. Consulte “Sensores RF de duas zonas” na página nº 114 para obter mais informações.

Opções de sensor de choque

4.1.n.7 Sensor Choque

```
7>Sensor choque
  >>>
```

As opções de impacto e impulso são válidas se a funcionalidade “4.1.n.6.13 Sensor choque” (consulte a página 216) para esta zona estiver definida como Sim.

4.1.n.7.1 Número de impulsos

```
1>Número impulso
  0
```

Defina o número de impulsos dentro de um intervalo de tempo que activará a zona.

São aplicáveis os seguintes valores:

- 1 a 9: número de impulsos no espaço de 30 segundos que activa a zona. Apenas 1 por segundo é levado em conta.
- 0: a funcionalidade de contagem fica desactivada.

4.1.n.7.2 Nível de impacto

```
2>Nível impacto
  0
```

Utilize a opção Nível de impacto para definir o nível para um único impulso activar a zona. São aplicáveis os seguintes valores:

- 1 a 9: Nível de impacto em que 1 significa alta sensibilidade e 9 baixa sensibilidade
- 0: o Nível de impacto está desactivado

O Nível de impacto pode ser verificado no menu “1.2.2 Teste Choque” (consulte a página 153).

Opções de sensores sem fios

4.1.n.7 Detalhes RF

```
1>ID sensor
  10EBA9E
```

O menu Detalhes de RF permite programar um dispositivo sem fios manualmente, ou removê-lo do expansor sem fios.

Nota: este menu só está disponível no expansor sem fios ATS1235 com a versão de firmware 1.20 ou superior, que está online.

4.1.n.7.1 ID sensor

```
1>ID sensor
  10EBA9E
```

O ecrã permite ver a ID do sensor.

Nota: os primeiros dois dígitos do identificador do sensor definem também o tipo de sensor. Consulte a Tabela 26 abaixo.

4.1.n.7.2 Tipo de sensor

```
2>Tipo sensor
  DWS
```

O ecrã permite ver o tipo de sensor. Estão disponíveis os seguintes tipos de sensor:

Tabela 26: Tipos de sensores sem fios

Tipo	Descrição	ID
Repetidor	Repetidor de sinal sem fios	0A*
CO	Sensor de monóxido de carbono	0D*
SPJ	Sensor de porta/janela	10*
Sensor fumo	Sensor de fumo	11*
PIR	Detector de infra-vermelhos passivo	12*
Botão Pânico 2 B	Sensor de pânico de 2 botões	14*
Choque	Sensor de choque	18*
Sensor acústico	Sensor de som de vidro partido	1A*
Sensor da câmara PIR	Câmara PIR sem fios	23*

4.1.n.7.3 Modo sensor

```
3>Modo sensor
  Simple
```

O ecrã informativo permite ver se o sensor funciona em modo de duas zonas. Estão disponíveis os seguintes valores:

- Singular: Sensor de zona individual.
- Multi-zona (Master) : A zona seleccionada é a primeira zona de um sensor de duas zonas.
- Multi-zona (Slave) : A zona seleccionada é a segunda zona de um sensor de duas zonas.

Consulte “Sensores RF de duas zonas” na página nº 114 para obter mais informações.

4.1.n.7.4 Supervisão

```
4 Supervisão
  >Desligado<
```

Activa ou desactiva a supervisão do dispositivo sem fios. A supervisão de todos os tipos fica activa. Consulte “2.2.2.n.4.4 Supervisão” na página nº 188 para obter mais informações.

4.1.n.7.5 Opções sensor

```
5 Opções sensor
  >Ignorar alarme<
```

As opções de sensor dependem do tipo de dispositivo sem fios.

Para mais informações sobre as opções disponíveis, consulte um manual de dispositivo RF.

Poderão estar disponíveis as seguintes opções:

Tabela 27: Opções de sensores sem fios

Opção	Tipo de sensor	Descrição
Reed e contacto	Sensor de porta/janela	Reportar alarmes de ambas as origens
Contacto	Sensor de porta/janela	Ignorar alarmes de lâminas
Reed e choque	Sensor de choque	Reportar alarmes de ambas as origens
Sensor choque	Sensor de choque	Ignorar alarmes de lâminas
Reed	Sensor de porta/janela, sensor de choque	Reportar apenas alarmes de lâminas
Aviso tamper	Sensor de fumo	Controlar alarmes de tamper de caixa
Ignorar tamper	Sensor de fumo	Ignorar alarmes de tamper de caixa

4.1.n.7.6 Remover disp RF

```
Remover disp RF?
  >Cancelar<
```

Selecione OK e prima Enter para remover o dispositivo sem fios da base de dados do expansor sem fios.

4.2 Áreas

```
1>Área 1
2 Área 2
```

O menu Áreas permite-lhe configurar áreas.

Consulte “Áreas” na página nº 55 do Capítulo 3 “Funções do sistema” para obter mais informações.

Cada área pode ser programada com um número de opções, como o nome da área, tempos de entrada e saída, etc. Antes de continuar, seleccione a área a programar.

Opções de área

4.2.n Seleccionar área

```
1>Nome da área
   Área 1
```

Seleccione uma área a programar.

4.2.n.1 Nome da área

```
1 Nome da área
>Área 1 <
```

Cada área pode ser programada com um nome para identificar a área.

Utilize o ecrã Nome da área para introduzir e editar o nome da área. O nome da câmara pode conter um máximo de 30 caracteres.

4.2.n.2 Tempo de saída

```
2>Tempo saída 1
   15
```

Cada área possui os seus próprios temporizadores de saída. Os temporizadores de saída permitem que os utilizadores que armam uma área deixem as instalações sem gerar um alarme (utilizando zonas de acesso ou de entrada/saída). Apenas depois de expirarem os tempos de saída poderá ocorrer um alarme.

Cada área pode ser programada com dois tempos de saída, um para o tipo de zona de entrada/saída 1 e outro para a zona de entrada/saída 2. Seleccione um temporizador apropriado e defina o tempo.

Os temporizadores de saída podem ser programados de 0 a 255 segundos. 0 significa que o temporizador não está activado e a área é armada imediatamente. 255 significa que o temporizador permanece activo e necessita de uma funcionalidade de saída terminal (consulte “4.1.n.2 Tipo de zona” na página nº 213) ou uma zona com a opção Porta final (consulte “4.1.n.6.15 Porta final” na página nº 217) para terminar.

4.2.n.2.1 Tempo de saída 1

4.2.n.2.2 Tempo de saída 2

Configure temporizadores de saída para os tipos de zona entrada/saída 1 e entrada/saída 2. Consulte “4.2.n.2 Tempo de saída” acima para obter mais informações sobre a programação de temporizador de saída.

4.2.n.2.3 GP Tempo de saída 1

4.2.n.2.4 GP Tempo de saída 2

Configure temporizadores de saída de arme parcial para os tipos de zona entrada/saída 1 e entrada/saída 2.

Os temporizadores de saída de arme parcial são configurados da mesma forma que os temporizadores de saída de arme total. Consulte “4.2.n.2 Tempo de saída” na página nº 228 para obter mais informações sobre a programação de temporizador de saída.

Nota: se forem atribuídas zonas a mais de uma área, é utilizado o tempo de saída mais longo. Consulte “4 Zonas e áreas” na página nº 211.

4.2.n.2.5 TempoSaída Rem

```
5 TempoSaída Rem
    > <
```

O temporizador é utilizado caso exista um arme remoto iniciado pelo software de configuração, gestão ou por uma aplicação móvel. A ativação de qualquer zona, incluindo as zonas de entrada/saída e de acesso, durante o tempo de saída remoto, gera uma falha de E/E.

Se o valor estiver definido para 0, é utilizado o tempo de saída programado em “4.2.n.2.1 Tempo de saída 1” na página nº 228.

4.2.n.3 Tempo de entrada

```
3>T. entrada 1
    15
```

Cada área possui o seu próprio temporizador de entrada. Ao entrar nas instalações através de uma zona de entrada/saída, inicia-se o tempo de entrada. Um utilizador pode desarmar a área enquanto o tempo de entrada está a decorrer sem gerar um alarme, desde que as zonas de entrada/saída ou zonas de acesso estejam activadas.

Nota: o tempo de entrada pode ser prolongado para zonas de entrada específicas. Consulte “4.2.n.4.2 Tempo pré-alarm” na página nº 230 para obter mais informações.

Cada área pode ser programada com dois tempos de entrada, um para o tipo de zona de entrada/saída 1 e outro para a zona de entrada/saída 2. Seleccione um temporizador apropriado e defina o tempo.

Os temporizadores de entrada podem ser programados de 0 a 255 segundos. 0 significa que o temporizador não está activado e o alarme é imediatamente activado ao entrar nas instalações armadas. 255 ou superior significa que o tempo é infinito.

Nota: se forem atribuídas zonas a mais de uma área, são utilizados os tempos de entrada e saída mais longos. Consulte “4 Zonas e áreas” na página nº 211.

4.2.n.3.1 Tempo de entrada 1

4.2.n.3.2 Tempo de entrada 2

Configure temporizadores de entrada para os tipos de zona entrada/saída 1 e entrada/saída 2. Consulte “4.2.n.3 Tempo de entrada” na página nº 229 para obter mais informações sobre a programação de temporizador de entrada.

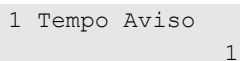
4.2.n.3.3 GP Tempo entrada 1

4.2.n.3.4 GP Tempo entrada 2

Configure temporizadores de entrada de arme parcial para os tipos de zona entrada/saída 1 e entrada/saída 2.

Os temporizadores de entrada de arme parcial são configurados da mesma forma que os temporizadores de entrada de arme total. Consulte “4.2.n.3 Tempo de entrada” na página nº 229 para obter mais informações sobre a programação de temporizador de entrada.

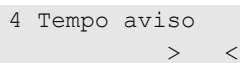
4.2.n.4 Outros Tempos



1 Tempo Aviso
1

O menu agrupa temporizadores de áreas adicionais. Consulte os submenus abaixo para mais informações.

4.2.n.4.1 Tempo de aviso



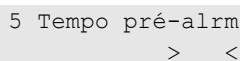
4 Tempo aviso
> <

Tempo de aviso é o período do tempo durante o qual o procedimento de arme pode ser adiado. Após expirar o tempo de aviso o sistema é armado.

O adiar de arme deve ser permitido em “4.2.n.5.2 Tentar Armar” na página nº 231.

O temporizador de aviso pode ser programado de 1 a 15 minutos.

4.2.n.4.2 Tempo pré-alarm



5 Tempo pré-alm
> <

Cada área possui o seu próprio temporizador de pré-alarme. Quando um alarme é accionado, gera apenas um alarme local, e o temporizador de pré-alarme é iniciado. Se o alarme local não for confirmado durante o tempo de pré-alarme, o alarme é reportado.

Nota: a zona de entrada tem de ter activada a opção “4.1.n.6.14 Prolongar EE” descrita na página nº 216.

Utilize o ecrã Tempo pré-alm para definir o tempo de pré-alarme para a área. Cada área pode ser programada com um tempo de pré-alarme.

Os temporizadores de pré-alarme podem ser programados de 0 a 255 segundos.

Nota: se forem atribuídas zonas a mais de uma área, é utilizado o tempo de pré-alarme mais longo. Consulte “4 Zonas e áreas” na página nº 211.

4.2.n.4.3 Retardo Desarme

```
3 Retardo Desar>
  > <
```

Defina um retardo para desarme autorizado (em minutos). O intervalo permitido é 1 a 30 min. 0 significa que não é aplicado nenhum retardo. Consulte “Desarme retardado” na página nº 58 para obter mais informações.

4.2.n.5 Opç.arm/desarm

```
1>Alm. Entrada
  Retardado
```

O menu agrupa as seguintes opções de arme.

4.2.n.5.1 Alarmes de entrada

```
1 Alm.Entrada
  >Retardado<
```

A opção de alarmes de entrada define se a falha de entrada é reportada de imediato. São aplicáveis os seguintes valores:

- Retardado: o alarme activa-se 30 s após o fim do tempo de entrada.
- Imediato: o alarme é activado de imediato.

4.2.n.5.2 Tentar Armar

```
2 Tentar Armar
  >Desligado<
```

A opção de tentativa de arme automático define se os utilizadores podem adiar ou cancelar o arme automático. Se esta opção estiver definida como Ligado, pode adiar o arme automático durante o tempo de aviso (consulte “4.2.n.4.1 Tempo de aviso” na página nº 230). Se o arme automático foi adiado por um utilizador normal, o sistema irá tentar armar novamente após o período de tempo definido em “8.4.8 AA tenta util” na página nº 299.

Nota: os utilizadores com privilégios (Instalador e Supervisor) podem escolher o tempo de adiamento durante o tempo de aviso.

4.2.n.5.2 AutoArmeSilenc

```
9 AutoArmeSilenc
  >Desligado<
```

Se o arme silencioso estiver definido como ligado, o besouro do teclado permanece desactivado durante o “4.2.n.4.1 Tempo de aviso” descrito na página nº 230.

4.2.n.5.4 Desarme Duplo

```
4 Desarme Duplo
  >Desligado<
```

Se a opção estiver definida como Sim, é necessária a autorização de dois utilizadores válidos para desarmar a área.

Nota: os utilizadores devem autorizar no mesmo teclado.

Cuidado: antes de ligar esta opção, ou de aplicar predefinições que têm esta opção activada, adicione pelo menos um utilizador, caso contrário irá perder o acesso ao menu de programação. Consulte também “Procedimento de recuperação” na página nº 362 do Capítulo 7 “Resolução de problemas”.

4.2.n.5.5 Confirmar alarme

```
5 Confirma alarm
  >Após desarme<
```

A opção define quando um alarme pode ser confirmado por um utilizador. Estão disponíveis os seguintes valores:

- Após desarme: Um alarme só pode ser confirmado quando a área estiver desarmada.
- Sem desarmar: Um alarme pode ser confirmado quando a área estiver armada ou desarmada.

Consulte o *Guia do Utilizador do Advisor Advanced ATsx500A* para obter mais informações sobre a confirmação do alarme.

4.2.n.6 Hierarquia

```
6 Hierarquia
  >Desligado<
```

Defina uma hierarquia para a área seleccionada. A hierarquia da área pode ter um valor de 1 (mais alto) a 3 (mais baixo). Hierarquia 0 significa que a funcionalidade está desligada e que esta área funciona sem restrições.

Consulte “Hierarquia das áreas” na página nº 55 para obter mais informações.

4.2.n.7 Limites

```
1>Limite Inibir
  128
```

Limita o número de elementos do sistema que podem ser isolados ou inibidos de uma vez.

Os intervalos permitidos dependem da variante do painel. Consulte “Características gerais” na página nº 39 do Capítulo 2 “Instalação”.

Consulte também “Inibir e isolar” na página nº 60.

4.2.n.7.1 Limite Inibição

```
1 Limite Inibir
  > <
```

O número máximo de elementos do sistema que podem ser inibidos de uma vez.

4.2.n.7.2 Limite Isolamento

```
2 Limite Isolar
  > <
```

O número máximo de elementos do sistema que podem ser isolados de uma vez.

4.2.n.7.3 Limite de Shunt

```
3 Limite Shunt
  > <
```

O número máximo de elementos do sistema que podem ser inibidos de uma vez.

4.2.n.8 Programa

Selecione programas para a área seleccionada.

O menu de atalhos permite atribuir até dois programas a cada um dos elementos seguintes:

- 1 Arme
- 2 Shunt
- 3 Proibir desarm
- 4 Área CampPorta

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

4.3 Grupos Área

```
1>GA 1
2 GA 2
```

O menu de grupos de áreas permite atribuir áreas a grupos de áreas.

Nota: a disponibilidade dos grupos de áreas depende da variante do painel de controlo. Consulte “Especificações” na página nº 37 no Capítulo 2 “Instalação”.

Consulte também “Grupos Área” na página nº 55.

Opções de grupos de áreas

4.3.n Seleccionar GA

```
1>Nome  
GA 1
```

Selecione um grupo de áreas a programar.

4.3.n.1 Nome GA

```
1 Nome  
>GA 1 <
```

Cada grupo de áreas pode ser programado com um nome para identificar a área.

Utilize o ecrã Nome de grupos de áreas para introduzir ou editar o nome do grupo de áreas. O nome do grupo de áreas pode conter um máximo de 16 caracteres.

4.3.n.2 Áreas

```
01-10 Áreas  
.....
```

Atribua áreas ao grupo de áreas seleccionado.

4.4 Comandos

```
0>Adic.comando  
1 Comando 1
```

Este menu permite ver todos os comandos programados, seleccionar um comando existente ou criar um novo comando.

Opções de comandos

4.4.0 Adicionar comando

Para adicionar um comando, siga um dos procedimentos descritos em “Programação de dispositivos sem fios” na página nº 110.

4.4.n Comando

```
1>Nome comando  
Comando 1
```

Selecione um comando existente a programar.

4.4.n.1 Nome comando

```
1 Nome comando
>Comando 1 <
```

Utilize a opção Nome do comando para definir um nome de comando. O nome do comando identifica ao utilizador final o comando para reportes de alarme ou para apresentar o estado ou as mensagens de erro.

Quando é criado um comando, é-lhe atribuído o nome predefinido “Comando Ex.y”, em que <x> é o número do expansor e <y> é o número de entrada do expansor. Por exemplo, o nome predefinido de comando “Comando Ex.y” é dado ao comando atribuído à entrada 8 do expansor 2.

Um nome de comando pode ser constituído por 16 caracteres.

4.4.n.2 Util Atribuído

```
2>Util Atribuído
Utilizador 1
```

Atribua um utilizador existente ao comando seleccionado.

Nota: um utilizador pode ter alguns comandos atribuídos. No entanto, um comando pode ser atribuído apenas a um utilizador.

4.4.n.3 Botões

```
1>Botão 1
2 Botão 2
```

Utilize o menu Botões para atribuir uma função apropriada a um botão ou a uma combinação de botões.

Tabela 28 abaixo mostra os botões e combinações disponíveis.

Tabela 28: Botões de comando e combinações

Botões	Função
Botão 1	Armar todas as áreas
Botão 2	Desarmar todas as áreas
Botão 3	Arme parcial 1 de todas as áreas
Botão 4	Alternar trigger 99
Botões 1 + 2	—
Botões 1 + 3	—
Botões 1 + 4	—
Botões 2 + 3	—
Botões 2 + 4	—
Botões 3 + 4	—

4.4.n.3.1 Seleccionar botão

```
1>Função  
    >>>
```

Selecione um botão para atribuir uma função de utilizador ao mesmo. Consulte “Funções de utilizador programáveis” na página nº 105 para obter mais informações.

4.4.n.4 Detalhes RF

```
1>ID sensor  
    14232C1
```

O menu Dispositivo de RF permite programar um dispositivo sem fios manualmente, ou removê-lo do expansor sem fios.

4.4.n.4.1 ID sensor

```
1>ID sensor  
    14232C1
```

O ecrã permite ver a ID do sensor.

4.4.n.4.2 Remover disp RF

```
Remover disp RF?  
    >Cancelar<
```

Selecione OK e prima Enter para remover o dispositivo sem fios da base de dados do expansor sem fios.

4.4.n.5 Listen-in

```
1>Modo escuta  
    Desativado
```

Utilize o menu para configurar o áudio de duas vias para o comando selecionado.

Esta opção está disponível apenas para sistemas de áudio de duas vias. Consulte o Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123 para obter mais informações.

4.4.n.5.1 Modo de escuta

```
1 Modo escuta  
    >Desativado<
```

Selecione um modo de escuta para o comando selecionado. Estão disponíveis as seguintes opções:

- Desativado: sem áudio.
- Só escuta: o operador da central recetora apenas pode ouvir o áudio do dispositivo de áudio atribuído ao comando.

- Escuta e fala: o operador pode ouvir o áudio ou falar utilizando o dispositivo de áudio atribuído.

4.4.n.5.2 Link áudio

```
0 Nada
1 Áudio 1
```

Atribua um dispositivo de áudio ao comando selecionado.

4.4.n.6 Remover

```
Remove comando?
  >Cancelar<
```

Utilize o comando Remover comando para remover um comando do sistema. Selecione OK e prima Enter. O comando é eliminado do painel e da base de dados do expansor.

4.5 Câmaras

```
17>Câmara 17
18 Câmara 18
```

O menu permite configurar módulos de câmara em câmaras PIR sem fios.

Para mais informações sobre câmaras, consulte também “Utilizar câmaras” na página nº 117.

4.5.n Seleccionar câmara

```
1>Nome Câmara
  Câmara 17
```

Seleccionar uma câmara adequada a configurar.

4.5.n.1 Nome Câmara

```
1 Nome Câmara
  >Câmara 17 <
```

Introduzir o nome da câmara.

4.5.n.2 Foto por zona

```
1>Zona 17
2 Zona 2
```

Escolha 1 a 4 zonas que accionem a câmara quando activas.

Por predefinição, a primeira zona atribuída é a zona com detector PIR desta câmara PIR sem fios.

Escolha uma posição à qual atribuir uma zona, ou uma zona existente para removê-la da lista de zonas associada.

4.5.n.3 Foto p/ filtro

```
1>Filtro 1
    >>>
```

Além das zonas indicadas em “4.5.n.2 Foto por zona” na página nº 237, podem existir até dois filtros de condições que também accionam a câmara.

4.5.n.3.m Seleccionar o filtro

```
1>Filtro 1
    Não utilizado
```

Selecione um de dois filtros para configurar.

4.5.n.3.m.1 Fechar o filtro

```
00>Não utilizado
01 Sir. interior
```

Selecione um filtro que activa a câmara seleccionada.

4.5.n.3.m.2 Tipo de evento <n>

```
2 Evento tipo 1
    >Intrusão<
```

Defina um tipo do filtro de condições seleccionado em “4.5.n.3.m Seleccionar o filtro” acima.

Os tipos de filtro disponíveis estão descritos em “Tipos de eventos de câmara” na página nº 117.

4.5.n.3.m.3 Reporta como

```
3 Reporta como
    >Não utilizado<
```

Se o filtro possuir uma person. tipo, é necessário atribuir um evento de relatório, que ocorre quando o filtro fica activo.

Notas

- Depois de sair deste menu, o evento é mostrado como um código de relatório no formato SIA.
- Apenas estão disponíveis eventos de relatório particulares.

4.5.n.4 Foto por evrep

```
1>Evento rep. 1
    Não utilizado
```

A câmara também pode ser activada por um evento de relatório seleccionado.

4.5.n.4.m Seleccionar evento

```
1 Evento rep. 1
>Não utilizado<
```

Selecione um de dois eventos de relatório para configurar.

Selecione um evento que activa a câmara seleccionada.

Notas

- Depois de sair deste menu, o evento é mostrado como um código de relatório no formato SIA.
- Apenas estão disponíveis eventos de relatório particulares.

4.5.n.5 Isolado

```
5 Isolado
>Não<
```

Quando a câmara é isolada, não obtém imagens. Além disso, as imagens não podem ser enviadas para o painel.

4.5.n.6 Max. fotos 24h

```
6 Max. Fotos 24h
>Infinito<
```

O número máximo de pedidos de imagens define quantos alarmes podem activar a câmara durante um período 24 horas de estado armado ou desarmado.

O contador é repostado quando a área altera o seu estado de arme.

O intervalo permitido é 1 a 400, ou 0 (infinito), o que significa um número ilimitado de alarmes.

Se atingir o limite, os pedidos de imagem seguintes são recusados pelo sistema e é registado um evento apropriado no registo.

4.5.n.7 Imagens Remotas

```
7 Imagens Remot>
>Sim<
```

Se for activado o accionamento remoto de imagens, é possível obter uma imagem remotamente utilizando software de configuração.

4.5.n.8 Foto Teste CRA

```
1>CRA 1
-----
```

O comando permite obter uma imagem e enviá-la para uma Central Receptora especificada.

Escolha uma Central Receptora e envie a imagem.

Chamar CRA 1...
A transmitir

O estado actual de transmissão de imagem é mostrado na linha inferior do ecrã.

5 Menu Porta

```
1>Portas
2 Grupos portas
```

Utilize o menu Porta para adicionar, editar ou eliminar portas, grupos de portas e regiões do sistema Advisor Advanced.

5.1 Portas

```
0>Adic. Porta
1 Porta 1
```

Utilize o menu Porta para adicionar, editar ou eliminar portas.

O menu permite configurar portas de ambos os tipos, padrão e inteligente.

Nota: determinadas opções deste menu são específicas para diferentes tipos de porta. Para ver opções específicas, consulte:

- “Opções específicas de portas padrão” na página nº 250
- “Opções específicas de portas inteligentes” na página nº 251

Opções comuns de portas

5.1.0 Adic. Porta

```
0>Porta
1 Painel
```

Aceda à opção de menu Adicionar porta para adicionar uma porta.

Escolha uma das localizações seguintes:

- 0: Porta. Adicione uma porta indicando o endereço de sistema dessa porta. Se o endereço for válido, o painel apresentará a localização física da porta para confirmar.

```
Exp 3.2
      >OK<
```

Selecione OK para confirmar ou Cancelar para sair, e prima Enter.

- 1: Painel. Adicione uma porta padrão indicando o respectivo número no painel de controlo
- 2: Exp CP/CE. Adicione uma porta inteligente seleccionando o controlador de portas, e introduzindo um número da porta nesse controlador de portas.

Se a porta for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Porta adicionada
```

É atribuído à nova porta o nome predefinido de “Porta N” e a porta é colocada no fim da lista de portas. Agora o utilizador pode começar a editar os detalhes da porta para a nova porta.

Para o endereçamento predefinido de leitores, zonas de portas e saídas de bloqueio, consulte, “Endereçamento de zonas, saídas e portas” na página nº 33 no Capítulo 2 “Instalação”.

5.1.n Seleccionar porta

Selecione uma porta a editar.

Podem ser visualizadas ou configuradas as opções seguintes.

5.1.n.1 Nome da Porta

```
1 Nome da Porta
   >Porta 1<
```

Prima Enter para editar o nome ou prima Sair para sair.

O nome de porta predefinido é “Porta N”, em que N é o número da porta.

O nome pode ter um máximo de 16 caracteres.

5.1.n.2 Localização de Porta

```
2> Local. Porta
   Exp 3.2
```

O ecrã só de leitura que mostra a localização física da porta seleccionada.

A localização da porta é mostrada no mesmo formato que a localização da zona. Consulte “4.1.n.4 Localiz. zona” na página nº 213.

5.1.n.3 Leitores de porta

```
1>Ent Leitor
   Leitor 1
```

O menu permite atribuir leitores de entrada (ENT) e saída (SAÍ) à porta seleccionada.

Nota: as portas padrão só podem possuir um leitor de ENTRADA e um leitor de SAÍDA. Os leitores de porta adicionais só podem ser atribuídos a uma porta inteligente. Para opções relacionadas com portas inteligentes, consulte “Opções específicas de portas inteligentes” na página nº 251.

Os submenus seguintes estão disponíveis para todas as portas:

- 1 Ent Leitor: Seleccionar um leitor de entrada
- 2 Saí Leitor: Seleccionar um leitor de saída

Os submenus seguintes estão disponíveis apenas para portas inteligentes:

- 3 Ent Leitor 2: Seleccionar um leitor de entrada adicional
- 4 Saí Leitor 2: Seleccionar um leitor de saída adicional

5.1.n.4 Output Porta

```
0>Não utilizado
17 Output 17
```

Selecione a saída de desbloqueio de porta.

Para portas inteligentes, a saída deve situar-se no intervalo correcto de saídas de controladores de portas.

É também possível seleccionar uma saída que não possa ser controlada directamente a partir do sistema Advisor Advanced. Consulte “8.5.2.1 Mapear relés” na página nº 301 para obter mais informações.

Não é possível seleccionar saídas que já estejam atribuídas a Porta forçada, Aviso, DOTL ou outras saídas.

Recomenda-se a utilização de uma das primeiras quatro saídas de controlador de portas para o desbloqueio de porta.

5.1.n.5 Tempos de portas

```
1>Tempo Desbloq.
>>>
```

Utilize o menu para configurar vários temporizadores para a porta seleccionada.

Nota: para portas padrão, o valor do temporizador é definido em minutos e segundos no formato mm’ss, por exemplo: 01’30.

No caso das portas inteligentes, utilize duas opções colocadas como submenus:

1. Tempo: Defina o valor de tempo entre 0 e 127.
2. Resolução: Defina as unidades (segundos ou minutos) para o valor de tempo acima.

5.1.n.5.1 Tempo de desbloqueio

```
1>Hora
0
```

Programo o tempo (valor e unidades) para a porta desbloquear quando o utilizador introduz um cartão ou PIN válido no leitor de porta.

5.1.n.5.2 Tempo alargado

```
1>Hora
0
```

Programo o tempo (valor e unidades) para a porta desbloquear quando o utilizador, com a opção “Estender acesso” activada, apresenta um cartão ou PIN válido no leitor de porta. Consulte também “3.1.n.8.5 Estender acesso” na página nº 208.

5.1.n.6 Opções de porta

```
1 Zonas porta
  >>>
```

O menu contém várias opções para a porta seleccionada.

Para opções relacionadas com portas inteligentes, consulte “Opções específicas de portas inteligentes” na página nº 251.

5.1.n.6.1 Zona de porta

```
1 Zona de porta
  Não utilizado
```

Utilize o menu para atribuir as zonas requeridas à porta seleccionada.

No caso de uma porta padrão, só pode haver uma zona de porta que indica a abertura de porta.

Nota: não é possível atribuir uma zona a uma função específica de porta se essa zona já estiver a ser utilizada para outra função de porta. São apresentadas apenas as zonas não atribuídas.

5.1.n.6.1.1 Zona de porta

```
0>Não utilizado
17 Zona 17
```

Selecione uma zona com contacto de porta para a porta seleccionada.

5.1.n.6.3 Controlo de Alarme

```
1>Áreas porta
  >>>
```

Defina as opções de controlo de alarme para a porta seleccionada.

5.1.n.6.3.1 Áreas de porta

```
1>Áreas porta
123456789012345>
```

Selecione áreas de porta.

No caso de uma porta inteligente, as áreas aqui especificadas são utilizadas para o seguinte:

- Os LEDs de leitor, se a opção “5.1.n.3.5.5 Opções de LEDs” descrita na página nº 252 for seleccionada para mostrar o estado da área.
- “5.1.n.6.3.4.1 Negar acesso” quando definido (descrito na página nº 246).
- A opção “5.1.n.6.4.3 Desb.qd Armado” na página nº 256 quando estiver definida como Sim para leitores de entrada.

Embora as áreas *não* sejam utilizadas para controlo de áreas, o controlador de portas *tem* de identificar o estado dessas áreas para saber se deve enviar um comando de arme ou desarme para o painel de controlo. Isto sucede *apenas* ao utilizar cartões sozinhos para arme/desarme, por exemplo, controlo de alarme na

1ª ou 3ª passagem do cartão. Lembre-se de que o grupo de utilizadores determina as áreas que podem ser armadas ou desarmadas por um utilizador, não as áreas aqui indicadas. Consulte também “Grupos de utilizadores” na página nº 72.

Consulte “Como editar uma lista” na página nº 138 para obter mais informações sobre a selecção de áreas.

Nota: “2.2.1.n.3.4 Ver áreas” na página nº 177 e “2.2.1.n.3.6 Áreas de controlo” na página nº 177 não estão disponíveis para teclados configurados como leitores de porta.

5.1.n.6.3.2 Grp Área Porta

```
2>Grp Área Porta
123456789012345>
```

Selecione grupos de áreas de portas do mesmo modo que as áreas em “5.1.n.6.3.1 Áreas de porta” na página nº 244.

5.1.n.6.3.3 Quando desarmado

```
1>Baixa Seguran.
      Não
```

Definir a funcionalidade de porta quando as áreas atribuídas estão desarmadas.

5.1.n.6.3.3.1 Baixa Segurança

```
1 Baixa Seguran.
      >Não<
```

Se definido como Sim, a porta funciona em modo de baixa segurança quando todas as áreas de portas estão desarmadas, o que significa que a autorização do utilizador é alterada de Cartão e PIN para Cartão ou PIN.

5.1.n.6.3.3.2 Desbloquear Porta

```
2 Desbloq. Porta
      >Não<
```

Se definido como Sim, a porta é desbloqueada quando todas as áreas de portas estão desarmadas.

5.1.n.6.3.4 Quando armado

```
1>Negar acesso
      Não
```

Definir a funcionalidade de porta quando as áreas atribuídas estão armadas.

5.1.n.6.3.4.1 Negar acesso

```
1> Negar acesso
   >Não<
```

Se definido como Sim, o acesso de porta é negado incondicionalmente quando alguma das áreas de portas está armada.

5.1.n.6.3.4.2 Bloquear porta

```
2 Bloq. porta
   >Não<
```

Se definido como Sim, a porta é bloqueada quando todas as áreas de portas estão armadas.

5.1.n.6.3.4.3 Bloq.PIN ES

```
3 Bloq.PIN ES
   >Não<
```

Se a opção Bloq.PIN ES estiver definida como Sim, não é possível utilizar um PIN durante o tempo de entrada.

A opção é igual e “2.2.1 Dispositivos RAS > 2.2.1.n.3.9 Bloq. PIN ES” na página nº 180.

5.1.n.6.4 Opções RTE

```
1 Usar RTE
   >>>
```

Configure as opções da funcionalidade RTE (Pedido de saída).

5.1.n.6.4.1 Usar RTE

```
1>RTE ENTRADA
2>RTE SAÍDA
```

Especifique se a entrada de pedido de saída está activada no leitor.

Em primeiro lugar, seleccione o leitor de entrada ou de saída aplicável. A seguir, defina Sim ou Não para configurar a opção para o leitor especificado.

Para opções relacionadas com portas inteligentes, consulte “Opções específicas de portas inteligentes” na página nº 251.

5.1.n.7 Opções de zona horária

```
1>Porta desbloq.
   >>>
```

O menu permite configurar opções de programa para a porta seleccionada.

5.1.n.7.1 Porta desbloqueada

```
1>Programa
    >>>
```

Configure as opções de programa para o desbloqueio de porta.

5.1.n.7.1.1 Programa

Selecione programas para o desbloqueio de porta.

O menu de atalhos permite atribuir até dois programas ao elemento selecionado.

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

5.1.n.8 Opções de Shunt

```
1>Zonas
    >>>
```

Utilize o menu para configurar opções de shunt de porta para a porta.

Consulte também “Shunt de porta” na página nº 82 no Capítulo 3 “Funções do sistema” para ver uma descrição da funcionalidade de shunt (inibição).

Para opções específicas das portas padrão, consulte “Opções específicas de portas padrão” na página nº 250. Para opções relacionadas com portas inteligentes, consulte “Opções específicas de portas inteligentes” na página nº 251.

5.1.n.8.2 Tempo shunt

```
1>Tempo Shunt
    >>>
```

O menu permite configurar temporizadores atribuídos ao shunt de porta.

Estão disponíveis as seguintes opções:

- 1 Tempo: Defina o valor de tempo entre 0 e 127.
- 2 Resolução: Defina as unidades (segundos ou minutos) para o valor de tempo acima.

5.1.n.8.2.1 Tempo Shunt

```
1>Hora
    0
```

O tempo (valor e unidades) para o shunt (inibição) da zona de porta.

5.1.n.8.2.2 Temp alargado

```
1>Hora
```

```
0
```

O temporizador de shunt alargado, que é aplicado caso o utilizador tenha a opção de tempo alargado activada. Consulte “3.1.n.8.5 Estender acesso” na página nº 208 para obter mais informações.

5.1.n.8.2.3 Aviso Shunt

```
1>Tempo
```

```
0
```

O tempo de aviso é o período de tempo do aviso de shunt de porta antes de expirar o tempo de shunt (ou o tempo de shunt alargado).

Podem ser utilizados flags de eventos de aviso aplicáveis, activos durante este período de tempo, para a função programável pelo utilizador. Consulte também “Funções de utilizador programáveis” na página nº 105, “Inibição de zonas” na página nº 60.

5.1.n.8.3 Tipo de shunt

```
1>Shunting
```

```
Shunting zona
```

O menu contém parâmetros que definem o efeito do shunt.

Para opções específicas das portas padrão, consulte “Opções específicas de portas padrão” na página nº 250.

5.1.n.8.3.1 Shunting

```
1 Shunting
```

```
>Zone shunting<
```

A opção define o objecto do shunt. Estão disponíveis as seguintes opções:

- Sem shunting. A porta não é inibida.
- Shunting zona. A porta é inibida. Gera um alarme padrão, baseado nas definições de tipo de zona, se deixada aberta mais tempo do que o tempo de shunt programado. Consulte “5.1.n.8.2.1 Tempo Shunt” na página nº 247.
- ShuntZona&DOTL. A porta é inibida e gera um alarme DOTL (Door Open Too Long - porta aberta demasiado tempo) se for deixada aberta para além do tempo de shunt programado. Permite que Porta forçada e DOTL sejam reportados em números de zona separados, conforme programado em “5.1.n.6.5.4 Porta forçada” na página nº 257 e “5.1.n.6.5.5 DOTL” na página nº 257.

Nota: esta opção está disponível apenas para portas inteligentes.

- AutoShunt&DOTL. Se a área atribuída à porta estiver desarmada, o shunt da porta inicia-se quando a zona de porta estiver activa (sem necessidade de código ou cartão). O alarme DOTL (Door Open Too Long - porta aberta

demasiado tempo) é gerado se for deixada aberta para além do tempo de shunt programado. Porta forçada e DOTL são reportados em números de zona separados, como acima.

Nota: esta opção está disponível apenas para portas inteligentes.

5.1.n.8.5 Até porta fech

```
5 Até porta fech
  >Não<
```

Se definido como Sim, as zonas de shunt de porta mantêm-se inibidas enquanto a porta estiver aberta.

5.1.n.8.6 CancelApósFech

```
6 CancelApósFech
  >Não<
```

Por razões de segurança, poderá ser necessário limitar o período de shunt tanto quanto possível. Se a opção estiver definida como Sim, as zonas de shunt de porta são inibidas até a porta se fechar. Não é possível abrir novamente a porta durante o tempo de shunt, uma vez que tal gera um alarme (existe sempre um tempo de “debounce” de aproximadamente 2 segundos).

5.1.n.10 Mover Porta

```
5> Não utilizado
6> Não utilizado
```

O menu permite mover a porta seleccionada para outra localização física. A nova localização deve ser uma localização não utilizada.

Se a porta for movida com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Porta movida
```

Nota: o nome da porta só é alterado se estiver predefinido; por exemplo, Porta 5 passa a Porta 17. Se a porta tiver um nome personalizado, este não se altera.

Esta opção só está disponível num esquema flexível de numeração. Consulte “8.7.9 Esquema Objeto” na página nº 308 para obter mais informações.

Consulte também “Endereçamento de zonas, saídas e portas” na página nº 33.

5.1.n.11 Desabilitar porta

```
Desabil. porta
  Sim
```

O comando permite-lhe desativar ou ativar a porta seleccionada.

Quando uma porta é desativada, o acesso a esta porta é negado e não são permitidos quaisquer comandos de controlo da porta.

5.1.n.11 Apagar porta

```
12 Apagar porta  
>Cancelar<
```

Utilize o comando Eliminar porta para remover a porta do sistema. Para remover a porta, seleccione OK e prima Enter. A porta é eliminada.

Opções específicas de portas padrão

5.1.n.8.3.2 Shunt activo

```
2 Shunt activo  
>Sempre<
```

Permite seleccionar um estado do sistema quando o shunt de porta é activado.

- Sempre: o shunt de porta é activado em todos os estados do sistema.
- Arme: o shunt de porta é activado apenas se as áreas com a porta seleccionada estiverem armadas.
- Desarme: o shunt de porta é activado apenas se as áreas com a porta seleccionada estiverem desarmadas ou parcialmente armadas.

5.1.n.8.4 Indicação

```
1>Porta aberta  
Não
```

O menu permite configurar opções de indicação de eventos de controlo de acesso específicos.

5.1.n.8.4.1 Porta aberta

```
1 Porta aberta  
>Não<
```

Se a opção for definida como Sim, o teclado emite um sinal intermitente quando a porta fica aberta para além do tempo permitido pelo temporizador de shunt (ou temporizador de shunt alargado).

5.1.n.8.7 ES Shunt

```
7 ES Shunt  
>Não<
```

Se o shunt de entrada/saída estiver definido como E/S 1 ou E/S 2, a zona inibida transforma-se numa zona de entrada/saída, e o shunt de porta inicia o temporizador de entrada/saída 1 (ou temporizador de entrada/saída 2).

5.1.n.8.8 Início shunt

```
8 Início Shunt
>Acesso conced.<
```

A opção define o momento em que o shunt da porta inicia.

- **Acesso concedido:** O shunt da porta inicia quando o acesso à porta é concedido.
- **Porta aberta:** O shunt da porta inicia após ser concedido o acesso à porta e a porta abre (a zona é ativada).

Opções específicas de portas inteligentes

5.1.n.3.5 Opções de leitores

```
>Cartão e PIN
>>>
```

Utilize o menu para configurar leitores da porta seleccionada.

5.1.n.3.5.1 Cartão e PIN

```
1>Ent Leitor
Não
```

Especifique qual o método requerido para abrir a porta a partir do leitor seleccionado.

- **Sim:** Desbloqueia a porta apresentando um cartão válido ao leitor e introduzindo um PIN através do teclado do leitor.
- **Não:** Desbloqueia a porta apresentando um cartão válido ao leitor ou introduzindo um PIN válido através do teclado do leitor.

A opção é configurada separadamente para cada leitor de porta. Depois de seleccionar a opção, escolha o leitor aplicável e defina o valor da opção.

5.1.n.3.5.2 Dois cartões

```
1>Ent Leitor
Não
```

Define se são necessários dois cartões ou PINs de utilizador para obter acesso. Se definido como Sim, dois utilizadores diferentes terão de apresentar o respectivo cartão e/ou PIN dentro do tempo programado para poder desbloquear a porta.

O tempo é definido em “8.5.1.2 Dois cartões” na página nº 300.

A opção é configurada separadamente para cada leitor de porta. Depois de seleccionar a opção, escolha o leitor aplicável e defina o valor da opção.

5.1.n.3.5.3 Sem ZH Req

```
1>Saí Leitor
      Não
```

Esta opção estende o acesso de saída para o leitor de saída seleccionado.

- Sim: O utilizador tem acesso à porta a partir do lado do leitor de saída mesmo que o respectivo programa já tenha expirado. No entanto, terá de ter um qualquer programa atribuído a si para a porta no seu grupo de portas, já que os utilizadores sem programa não têm acesso à porta.
- Não: É necessário um programa válido para o utilizador poder sair.

A opção é configurada separadamente para cada leitor de saída de porta. Depois de seleccionar a opção, escolha o leitor aplicável e defina o valor da opção.

5.1.n.3.5.4 Formato do cartão

```
4 Formato cartão
>Wiegand 27 bit<
```

Defina o formato de dados do leitor e cartão, chave ou token a ser utilizado.

- Wiegand 27 bit
- Tecom ASP 27 bit
- K 32 bit
- Wiegand 26 bit (ID=16, FC=8)
- Indala ASC 27 bit
- Indala ASC 26 bit
- Wiegand 32 bit
- C 36 bit
- ATS Wiegand 23 bit
- MagSwipe - formato Aritech
- Magswipe - formato Midas

5.1.n.3.5.5 Opções de LEDs

```
5 Opções LEDs
>Porta bloq.<
```

Especifique o estado indicado pelos LED do leitor (apenas aplicável para leitores de controlador de portas ligados à interface Wiegand).

- Porta bloq. O LED 1 está ligado quando a porta está bloqueada.
- Porta desbloq. O LED 1 está ligado quando a porta está desbloqueada.
- Área armada. O LED 1 indica se a área atribuída à porta está armada. Se estiver atribuída mais de uma área, todas as áreas atribuídas à porta têm de ser armadas antes de o LED mudar de estado.
- Área desarmada. O LED 1 indica se a área atribuída à porta está desarmada. Se estiver atribuída mais de uma área, todas as áreas atribuídas à porta têm de ser desarmadas antes de o LED mudar de estado.

- Área Arm/Desar. Os leitores com controlo duplo de LED indicam área desarmada e armada com diferentes cores de LED.
- Válido/anulado. Os leitores com controlo duplo de LED indicam utilizador válido ou anulado com diferentes cores de LED.
- LEDs Desab. Sem controlo de LED.

Nota: nos leitores com controlo duplo de LED, o LED 2 pode também ser programado para indicar outras condições utilizando a programação de lógica de macros de controladores de portas. Consulte “Lógica de macros dos controladores de portas” na página nº 83.

Consulte também “5.1.n.6.3.1 Áreas de porta” na página nº 244.

5.1.n.3.5.6 Time&Attendance

```
6 Time&Attendan>
  >Não<
```

Se definido como Sim, o leitor funciona como um leitor de tempo e participação. Faz com que os eventos de acesso de utilizador ocorridos neste leitor sejam enviados do controlador de portas para o painel de controlo e possam ser utilizados para controlo da participação do utilizador.

5.1.n.3.5.7 Desabilitar coacção

```
7 Desab.Coação
  >Não<
```

Esta opção é utilizada para desactivar o funcionamento dos códigos de coacção. Se definido como Sim, nenhuma função de coacção estará disponível nesta porta.

5.1.n.6.1.2 Segunda zona

```
0>Não
17 Zona 17
```

O controlador de portas permite que o sistema monitorize dois contactos de porta para uma porta inteligente individual. Seleccione uma segunda zona com contacto de porta para a porta seleccionada. Se existir apenas um contacto de porta, seleccione Não.

Consulte também “5.1.n.6.1.1 Zona de porta” na página nº 244.

5.1.n.6.1.3 Zona DOTL

```
0>Não utilizado
17 Zona 17
```

Especifique a zona que reporta a condição de alarme DOTL (Door Open Too Long - porta aberta demasiado tempo) para a porta seleccionada.

Nota: o reporte de DOTL tem de ser activado nas opções de Shunt. Consulte “5.1.n.6.5.5 DOTL” na página nº 257.

5.1.n.6.2 Porta desbloqueada

```
1>Até fechar
      Não
```

O menu contém várias opções para o processo de desbloqueio da porta seleccionada.

5.1.n.6.2.1 Até fechar

```
1 Até fechar
      >Não<
```

Esta opção determina quando a porta irá voltar a bloquear utilizando o retardo de re-bloqueio.

- Sim: O bloqueio de porta não voltará a bloquear até a porta estar fechada. Isto é utilizado nos casos em que o mecanismo de bloqueio, quando bloqueado, impede o fecho da porta.
- Não: O bloqueio de porta voltará a bloquear (após o tempo de desbloqueio expirar, etc) independentemente de a porta estar aberta ou fechada.

5.1.n.6.2.2 Até abrir

```
2 Até abrir
      >Não<
```

Por motivos de segurança, a porta pode voltar a bloquear no momento em que se abre. A porta fica desbloqueada até ser aberta, e o retardo de porta é desactivado depois de a porta se abrir.

A porta permanece desbloqueada durante o tempo de desbloqueio, ou a porta fica fechada, obedecendo ao período de tempo mais longo. Consulte também “5.1.n.5.1 Tempo de desbloqueio” na página nº 243.

5.1.n.6.2.3 Bloq/Dbloq Imp

```
3 Bloq/Dbloq Imp
      >Não<
```

Esta função é utilizada apenas em fechos electrónicos especiais que requerem que dois relés separados sejam pulsados em alturas diferentes para abrir, e duas zonas separadas para monitorização. Se esta função estiver definida como Sim, a abertura de fecho por bloqueio normal está desactivada. Esta opção deve ser *sempre* definida como Não, salvo especificação contrária.

A funcionalidade é descrita detalhadamente em Capítulo 3 “Funções do sistema > Impulso bloqueio e des” na página nº 84.

5.1.n.6.3.5 Grupo de utilizadores

```
1>Grupo instal.
2 Grupo superv.
```

Selecione um grupo de utilizadores para a porta seleccionada.

Consulte “Grupos de utilizadores” na página nº 72 para obter mais informações.

5.1.n.6.3.6 Tipo Controlo

```
6 Tipo Controlo
>Sem Controlo<
```

Especifique o tipo de controlo de alarme que está disponível para a porta seleccionada.

- **Sem Controlo:** O leitor não possui controlo de alarme. Não é possível armar ou desarmar áreas utilizando os leitores.
- **Na1Passagem:** A apresentação de um cartão válido num leitor de porta desarma as áreas do grupo de utilizadores na primeira passagem. Passar o cartão três vezes arma as áreas.
- **Na3Passagem:** A apresentação de um cartão válido três vezes arma ou desarma as áreas do grupo de utilizadores.
- **Sempre on:** A apresentação de um cartão válido no leitor de entrada desarma as áreas do grupo de utilizadores. A apresentação de um cartão válido no leitor de saída arma as áreas do grupo de utilizadores.

5.1.n.6.3.7 Se PIN arma

```
1>Negar acesso
      Não
```

Configurar o funcionamento da porta se a área é armada utilizando um PIN.

5.1.n.6.3.7.1 Negar acesso

```
1>Negar acesso
      Não
```

Se definido como Sim, o acesso à porta é negado se as áreas tiverem sido armadas utilizando um PIN.

5.1.n.6.4.2 Zona RTE

```
0>Não utilizado
19 Zona 19
```

Selecione uma zona que opere como uma entrada RTE para uma porta inteligente.

Nota: não é possível escolher uma zona que já seja utilizada no controlador de portas (por exemplo, zona de porta ou DOTL, etc.)

Consulte também “5.1.n.6.4 Opções RTE” na página nº 246.

5.1.n.6.4.3 Desb.qd Armado

```
1>Ent Leitor  
2 Saí Leitor
```

Especifique se a funcionalidade RTE é desactivada se alguma das áreas de portas estiver armada.

Em primeiro lugar, seleccione o leitor de entrada ou de saída aplicável. A seguir, defina Sim ou Não para configurar a opção para o leitor especificado.

5.1.n.6.4.4 Controlo RTE

```
4 Controlo RTE  
>AbertTempPorta<
```

Define o funcionamento do botão de pedido de saída.

- AbertTempPorta. Quando o botão RTE é premido, a porta fica desbloqueada durante o tempo de desbloqueio programado. Consulte “5.1.n.5.1 Tempo de desbloqueio” na página nº 243.
- Manter Porta Aberta. Permite que a porta seja mantida desbloqueada enquanto o botão RTE estiver premido ou durante o tempo de desbloqueio programado, obedecendo ao período de tempo mais longo.
- Só Shunt. Quando o botão RTE é premido a zona é inibida, mas não é concedido acesso.

5.1.n.6.5 A reportar

```
1>Fech. & Bloq.  
Não
```

Determina quando os eventos de controlo de acesso são reportados.

5.1.n.6.5.1 Fech. & Bloq.

```
1 Fech. & Bloq.  
>Não<
```

Se definido como Sim, a porta é reportada quando fechada e bloqueada (comando de bloqueio enviado e estado da zona normal).

Nota: não existe nenhum evento especificado no painel de controlo. Esta função só pode ser utilizada em conjunto com as opções seguintes.

5.1.n.6.5.2 AbDbl como Dbl

```
2 AbDbl como Dbl  
>Não<
```

Se definido com Sim, a porta é reportada como desbloqueada se estiver aberta e desbloqueada.

5.1.n.6.5.3 Abertura/fecho

```
3 Abertura/fecho
  >Não<
```

Se definido como Sim, a abertura ou o fecho da porta são reportados. Caso contrário, não é efetuado qualquer reporte a menos que ocorra um alarme (consoante o tipo de zona).

5.1.n.6.5.4 Porta forçada

```
4 Porta forçada
  >Não<
```

Se definido como Sim, é reportada a abertura da porta sem um cartão válido, PIN ou pedido de saída.

5.1.n.6.5.5 DOTL

```
5 DOTL
  >Não<
```

Reporte quando a porta fica aberta demasiado tempo. Se definido como Sim e se a zona atribuída à porta estiver no estado DOTL (por exemplo, ainda aberta após expirar o temporizador de shunt), é reportado o evento DOTL.

5.1.n.6.5.6 RTE

```
6 RTE
  >Não<
```

Se definido como Sim, é reportada a activação de pedido de saída da zona.

5.1.n.6.6 Interbloqueio

```
6 Interbloqueio
1234567890123456
```

Este menu estipula os números de zona no controlador de portas que impedem o acesso simultâneo às portas. Os números têm de ser números de zona no mesmo controlador de portas.

Para interbloquear com uma porta noutra controlador de portas, um contacto dessa porta tem de estar ligado por cabo a uma zona de substituição no primeiro controlador de portas, e vice-versa. Neste caso, se uma zona estiver a ser utilizada para interbloqueio, e se nenhuma porta no controlador de portas tiver essa zona como seu “contacto de porta”, então o controlador de portas introduz automaticamente um retardo de 2 segundos antes da abertura da porta. Isto permite ter em conta os tempos de estabilização dos controladores de portas. É conveniente lembrar que este retardo de 2 segundos ocorre apenas quando uma zona está a ser utilizada para interbloqueio, e que essa zona vem de outra porta não presente neste controlador de portas.

Para activar ou desactivar o interbloqueio, alterne um número de zona local.

5.1.n.7.1.2 Após entrada

```
2 Após entrada
  >Não<
```

Selecione se a acção de ignorar entra imediatamente em vigor assim que o programa se inicia, ou após a entrada de um utilizador.

- Sim: Antes de o programa desbloquear a porta, o utilizador tem de entrar na área.
- Não: O desbloqueio automático inicia-se à hora de início do programa.

Consulte também “5.1.n.7.1 Porta desbloqueada” na página nº 247.

5.1.n.7.2 Baixa Segurança

```
1>ZH Baixa Seg.
  Não utilizado
```

Utilize o menu para configurar a funcionalidade de baixa segurança da porta. O modo de baixa segurança da porta significa que a autorização do utilizador é alterada de Cartão e PIN para Cartão *ou* PIN.

Estão disponíveis os submenus seguintes:

- 1 Programa. Selecione programas para a funcionalidade de baixa segurança.
O menu de atalhos permite atribuir até dois programas ao elemento seleccionado.
Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.
- 2 L.ENT INIB PIN. Se definido como Sim, o leitor de entrada está no modo de baixa segurança se o programa acima estiver activo.
- 3 L.SAI INIB PIN, etc.

A funcionalidade é configurada separadamente para cada leitor de porta. Depois de seleccionar a opção, escolha o leitor aplicável e defina o valor da opção.

5.1.n.7.3 Zona Horária RTE

```
1>ZH RTE
  Não utilizado
```

Selecione programas para a entrada de pedido de saída.

O menu de atalhos permite atribuir até dois programas ao elemento seleccionado.

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

5.1.n.8.1 Zonas

```
1 Zonas
1234567890123456
```

Selecione zonas que têm de ser inibidas na abertura de porta.

Para activar ou desactivar o shunt, alterne um número de zona local.

Consulte também “5.1.n.8 Opções de Shunt” na página nº 247.

5.1.n.8.4 Indicação

```
2>Output DOTL
Não utilizado
```

O menu permite atribuir saídas de controladores de portas para indicação de eventos de controlo de acesso específicos.

5.1.n.8.4.2 Output DOTL

```
00>Não utilizado
19 Output 17
```

Selecione uma saída no controlador de portas para indicar o alarme DOTL (Door Open Too Long - porta aberta demasiado tempo).

5.1.n.8.4.3 Output de aviso

```
00>Não utilizado
20 Output 17
```

Selecione uma saída no controlador de portas para indicar o aviso antes de expirar o tempo de shunt ou o tempo alargado de shunt. Consulte também “5.1.n.8.2 Tempo shunt” na página nº 247.

5.1.n.8.4.4 Porta forçada

```
00>Não utilizado
19 Output 17
```

Selecione uma saída no controlador de portas para indicar que a porta foi forçada (aberta sem a devida autorização).

5.1.n.9 Regiões & AP

```
1>Regiões
>>>
```

O menu contém opções de porta ligadas ao controlo de regiões e anti-passback.

5.1.n.9.1 Regiões

```
1>Ent Leitor
>>>
```

Utilize o menu para atribuir regiões a leitores.

Em primeiro lugar, seleccione o leitor aplicável. A seguir, escolha uma região à qual o leitor pertence.

```
0>Adic. região
1 Exterior
```

A lista de regiões permite adicionar uma nova região. O menu Adicionar região é igual ao menu em “5.3 Regiões” descrito na página nº 263.

Consulte Capítulo 3 “Funções do sistema > Regiões” na página nº 82 para obter mais informações.

5.1.n.9.2 Anti-passback

```
2 Anti-passback
  >Sem AP<
```

Controla o funcionamento da porta se for utilizado um cartão ou PIN para tentar entrar na região à qual o utilizador está atribuído actualmente. Estão disponíveis as seguintes opções:

- Sem AP: Sem controlo de passback.
- Soft Anti-PB: Um cartão ou PIN válido abre a porta quando utilizado para entrar na região pela segunda vez sem sair primeiro, mas é gerado um relatório.
- Hard Anti-PB: Um cartão ou PIN válido *não* abre a porta quando utilizado para entrar na região pela segunda vez sem sair primeiro. Tentar fazê-lo gera um relatório.
- Regiões AP: Um cartão ou PIN válido *não* abre a porta quando utilizado para sair de uma região diferente da região em que se entrou anteriormente. Por exemplo, se o utilizador tiver entrado na região 2 a partir da região 1, será negada a sua tentativa de entrada na região 1 a partir da região 0. Tentar fazê-lo gera um relatório.

Consulte Capítulo 3 “Funções do sistema > Anti-passback” na página nº 82 para obter mais informações.

5.1.n.9.3 Inib Reg 1 Utl

```
1>Ent Leitor
  >>>
```

Para utilizadores na região 1 (na maioria das ocasiões é “exterior”), está disponível uma função especial de segurança para dar acesso apenas através de outra região. Se a opção estiver definida como Sim, será negado o acesso a qualquer utilizador na região 1. Para aceder, em primeiro lugar o utilizador tem de estar noutra região.

A funcionalidade é configurada separadamente para cada leitor de porta. Depois de seleccionar a opção, escolha o leitor aplicável e defina o valor da opção.

5.1.n.9.4 Opções HSU

```
1>Req nr HSU
```

```
0
```

O menu contém opções de alta segurança.

Consulte Capítulo 3 “Funções do sistema > Alta segurança” na página nº 83 para obter mais informações.

5.1.n.9.4.1 Req nr HSU

```
1 Req nr HSU
```

```
>0<
```

O valor define quantos utilizadores de alta segurança (HSUs) têm de estar presentes na região atribuída à porta seleccionada.

5.1.n.9.4.2 Temp pré-aviso

```
2 Temp pré-aviso
```

```
> <
```

O valor define o tempo (em segundos) do temporizador de pré-aviso. Quando existe um número insuficiente de utilizadores de alta segurança numa região de alta segurança, inicia-se um temporizador de pré-aviso e, quando este expira, é emitido um alarme e activa-se a saída de alarme.

5.1.n.9.4.3 AS Out Alarme

```
00>Não utilizado
```

```
19 Output 17
```

Selecione uma saída no controlador de portas para indicar um alarme de anti-passback ou de alta segurança.

5.2 Grupos portas

```
0>Adic Grp Port>
```

```
1 Grp. Portas 1
```

Os grupos de portas definem quando um utilizador pode ter acesso a portas específicas.

Consulte Capítulo 3 “Funções do sistema > Grupos de portas” na página nº 81 para obter mais informações.

5.2.0 Adic Grp Portas

Aceda ao menu para adicionar um grupo de portas. Se o grupo de portas for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
```

```
Grp.Portas Adic
```

É atribuído ao novo grupo de portas o nome predefinido de “Grp. Portas N” e a porta é colocada no fim da lista de portas.

5.2.n Grupo de portas

```
1>Nome Grp.Port>  
  Grp. Portas 2
```

Selecione um grupo de portas a programar.

5.2.n.1 Nome Grp. Portas

```
1 Nome Grp.Port>  
>Grp. Portas 2 <
```

Cada grupo de portas pode ser programado com um nome que o identifique. Utilize o ecrã Nome Grp. Portas para introduzir ou alterar o nome do grupo de portas. O nome pode ter um máximo de 16 caracteres.

5.2.n.2 Porta GrpPorta

```
0>Adic. Porta  
-----
```

Programa o acesso de utilizador para o grupo de portas seleccionado.

Para configurar um grupo de portas:

1. Adicione uma porta ao grupo, se necessário. O programa predefinido (Sempre) é automaticamente atribuído a cada porta adicionada.
2. Selecione uma porta à qual um utilizador com o grupo de portas atribuído possa ter acesso.
3. Atribua até dois programas que definam quando é que os utilizadores com esse grupo de portas têm acesso a essa porta.

O menu de atalhos permite atribuir até dois programas ao elemento seleccionado.

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

4. Repita para todas as portas específicas deste grupo de portas.

5.2.n.3 Apaga Grp Portas

Para remover um grupo de portas, selecione o grupo de portas com o cursor, ou introduza o número do grupo de portas e aceda ao menu Apagar Grupo de Portas.

O ecrã apresenta:

```
2 Apaga Grp Por>  
  >Cancelar<
```

Selecione OK e prima Enter. Esta acção elimina o grupo de portas.

Repita o comando para eliminar outros grupos de portas, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: não é possível apagar um grupo de portas a menos que o seu grupo de utilizadores o autorize a fazê-lo.

5.3 Regiões

```
0>Adic. região
1 Exterior
```

Configure regiões.

Consulte Capítulo 3 “Funções do sistema > Regiões” na página nº 82 para obter mais informações.

5.3.0 Adicionar região

Aceda ao menu para adicionar uma região. Se a região for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Região Adic.
```

A primeira região recebe o nome de “Exterior”, enquanto que às regiões seguintes é atribuído o nome “Região 2”, “Região 3”, etc.

5.3.n Seleccionar região

```
1>Nome de Região
Região 2
```

Selecione uma região a programar.

5.3.n.1 Nome de Região

```
1 Nome de Região
>Região 2 <
```

Cada região, com excepção da região 1 “Exterior”, pode ser programada com um nome que a identifique.

Utilize o ecrã Nome de Região para introduzir ou alterar o nome da região. O nome pode ter um máximo de 16 caracteres.

5.3.n.2 Apagar região

Para remover uma região, selecione a região com o cursor, ou introduza o número da região e aceda ao menu Apagar região.

O ecrã apresenta:

```
2 Apagar região
>Cancelar<
```

Selecione OK e prima Enter. Esta acção elimina a região.

Repita o comando para eliminar outras regiões, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: não é possível eliminar a região 1.

5.4 Pisos

```
0>Adic. piso
1 Piso 1
```

Utilize o menu Piso para adicionar, editar ou eliminar pisos.

5.4.0 Adic. piso

Aceda à opção de menu Adicionar piso para adicionar um piso.

Se o piso for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Piso adic.
```

O novo piso recebe o nome predefinido de “Piso N” e é colocado no final da lista de pisos. Pode agora começar a editar os detalhes do piso para o novo piso.

5.4.n Selecionar piso

Selecione um piso a editar.

Podem ser visualizadas ou configuradas as opções seguintes.

5.4.n.1 Nome do piso

```
1 Nome do piso
   >Piso 1<
```

Prima Enter para editar o nome ou prima Limpar para sair.

O nome predefinido do piso é “Piso N”, em que N é o número do piso.

O nome pode ter até 30 caracteres.

5.4.n.2 Eliminar piso

Para remover um piso, selecione um piso com o cursor ou introduzindo o número do piso, em seguida aceda ao menu Eliminar piso.

O ecrã apresenta:

```
2 Eliminar piso
   >Cancelar<
```

Selecione OK e prima Enter. Esta ação elimina o piso.

Repita o comando para eliminar outros pisos, ou prima Limpar para sair e voltar ao nível superior de menu.

5.5 Grupos de pisos

```
0>Adic. Grp piso
1 Grp piso 1
```

Os grupos de pisos definem quando um utilizador pode ter acesso a pisos específicos.

Consulte o Capítulo 3 “Funções do sistema > Grupos de pisos” na página nº 81 para obter mais informações.

5.5.0 Adic. grupos de pisos

Aceda ao menu para adicionar um grupo de pisos. Se o grupo de pisos for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Adic. Grp Piso
```

O novo grupo de pisos recebe o nome predefinido de “Grupo de pisos N” e é colocado no final da lista de pisos.

5.5.n Selecionar grupo de pisos

```
1>Nome Grupo Pi>
   Grp piso 2
```

Selecione um grupo de pisos a programar.

5.5.n.1 Nome grupo piso

```
1 Nome Grp. Pis>
>Grp piso 2 <
```

Cada grupo de pisos pode ser programado com um nome que o identifique.

Utilize o ecrã do nome do Grp. Pisos para introduzir ou alterar o nome do grupo de pisos. O nome pode conter até 30 caracteres.

5.5.n.2 Pisos Grp Pisos

```
0>Adic. piso
-----
```

Programa o acesso de utilizador para o grupo de pisos selecionado.

Para configurar um grupo de pisos:

1. Adicione um piso ao grupo, se necessário. O horário predefinido (Sempre) é automaticamente atribuído a cada piso adicionado.
2. Selecione um piso ao qual um utilizador com o grupo de pisos atribuído possa ter acesso.
3. Atribua um horário que defina quando é que os utilizadores com este grupo de pisos têm acesso a este piso.

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

4. Repita para todos os grupos específicos para este grupo de pisos.

5.5.n.3 Eliminar Grp Pisos

Para remover um grupo de pisos, selecione um grupo de pisos com o cursor, ou introduza o número do grupo de pisos e aceda ao menu Eliminar grupo de pisos.

O ecrã apresenta:

```
2 Apaga Grp Piso
  >Cancelar<
```

Selecione OK e prima Enter. Esta ação elimina o grupo de pisos.

Repita o comando para eliminar outros grupos de pisos, ou prima Limpar para sair e voltar ao nível superior de menu.

Nota: não é possível eliminar um grupo de pisos a menos que o seu grupo de utilizadores o autorize a fazê-lo.

6 Outputs e filtros

```
1>Filtros cond
2 Outputs
```

Nesta secção de programação são programadas as saídas, filtros e triggers (accionadores). Podem ser activadas as saídas do painel ou do expansor, bem como os triggers do sistema.

6.1 Filtros de condição

```
0>Adic. filtro
1 Sir. interior
```

Um filtro de condição é uma avaliação e um algoritmo de tomada de decisão. Existem 64 filtros pré-programados.

Definições de filtros

6.1.0 Adicionar filtro

Aceda à opção de menu Adicionar filtro para adicionar um filtro de condições. Se o filtro for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Filtro adic
```

É atribuído ao novo filtro o nome predefinido de “Filtro N” e é colocado no fim da lista de filtros de condições. Pode agora começar a editar os respectivos detalhes.

6.1.n Seleccionar filtro

Selecione um filtro existente a programar.

6.1.n.1 Nome do filtro

```
1 Nome do filtro
>Filtro 52 <
```

O nome identifica o filtro para o instalador, tornando as dependências de programação mais claras.

6.1.n.2 Fórmula

```
0>Adic. evento
-----
```

O menu Fórmula permite a definição da fórmula do filtro. Podem ser combinados até 4 eventos numa fórmula.

6.1.n.2.0 Adicionar evento

```
0>Adic. evento
1 Sistema.0.1
```

Utilize o comando Adic. evento para adicionar um operando à fórmula actual. Prima Adic. evento para adicionar o operando.

Esta entrada de menu não está disponível se a fórmula já contiver 4 eventos.

Os passos seguintes dependem se seleccionar um evento ou um operador para a fórmula.

6.1.n.2.x Seleccionar evento

Selecione o evento apropriado para o configurar.

```
1>Grupo
Sistema
```

Para escolher um evento apropriado, tem de definir primeiro a origem do evento. A origem é definida por um grupo de objectos, e um objecto dentro deste grupo. Os grupos disponíveis são indicados em Anexo A “Eventos do Advisor Advanced” na página nº 379.

Quando o grupo e o objecto (se disponível) estiverem seleccionados, seleccione o evento apropriado. A selecção disponível depende da origem seleccionada. Uma lista completa de eventos com origens é apresentada no Anexo A “Eventos do Advisor Advanced” on page 379.

As seguintes funções estão disponíveis para o evento seleccionado:

1. Grupo: Seleccionar grupo
2. Elemento: Seleccionar um elemento (ou todos os elementos) do grupo acima
3. Evento: Seleccionar um evento para o elemento acima
4. Inverter: Inverte o evento seleccionado. Se invertido, é assinalado com um '!' na fórmula
5. Remover evento: Remover o evento seleccionado

6.1.n.2.y Seleccionar operador

Todos os eventos são juntados com operadores lógicos. Escolha o operador para o alterar. Os operadores válidos são AND (E), OR (OU) e XOR (OU exclusivo).

6.1.n.3 Inverter

```
3 Inverter
>Não<
```

A opção Inverter especifica se a saída de filtro de condição está invertida.

6.1.n.4 Remover filtro

```
4 Remover filtro
  >Cancelar<
```

Utilize o ecrã para remover um filtro de condições do sistema. Para remover o filtro, seleccione OK e prima Enter novamente. O filtro é eliminado.

6.2 Outputs

```
0>Adic. Output
1 Sir. interior
```

O menu Saídas permite ver todas as saídas programadas, seleccionar uma saída existente ou criar uma nova saída.

Definições de saídas

6.2.0 Adicionar output

```
1>Painel
2 Exp. Outputs
```

Quando adicionar uma nova saída, utilize o menu Adic. saída para seleccionar se a saída se localiza na PCI do painel, no expansor de saída, no expansor remoto ou no teclado. Consulte “Endereçamento de zonas, saídas e portas” na página nº 33 para ver endereçamentos de saída disponíveis.

Se a saída seleccionada já existir, aparece um aviso.

Se a saída for criada com êxito, o ecrã passa para o menu “6.2.n.1 Nome da output”.

6.2.n Seleccionar saída

Selecione o número apropriado da saída existente a programar. Existem 200 saídas programáveis no sistema.

6.2.n.1 Nome da output

```
1 Nome da output
  >Output P1.6 <
```

Utilize o ecrã Nome da saída para criar ou editar o nome da saída. O nome identifica a saída ao utilizador final quando uma saída é activada.

Quando uma saída é criada, é-lhe atribuído o nome predefinido “Saída Xy.z”, em que X define o tipo de dispositivo, <y> é o número do dispositivo e <z> é um número de saída do dispositivo. O tipo de dispositivo <X> pode ser um dos seguintes:

- P: painel
- O: módulo de expansão de saída
- R: Teclado

- E: Expansor

Por exemplo, o nome predefinido de saída “Saída E3.7” é dado à saída atribuída à saída física 7 do Expansor 3.

6.2.n.2 Localização da output

```
2>Loc. de Output  
Painel 1.6
```

A localização de saída é um campo só de leitura que é a identificação física de uma saída, no formato “<dispositivo> <y>.<z>”, em que <dispositivo> pode ser um painel, um expansor ou um teclado, <y> é o endereço do dispositivo e <z> é o número da saída.

6.2.n.3 Inverter

```
3 Inverter  
>Não<
```

A opção Inverter saída determina se a saída está invertida.

6.2.n.4 Iniciar filtro

```
00>Não utilizado  
01 Sir. interior
```

Utilize o menu Filtro de início para especificar um filtro de condições que irá activar uma saída. O comportamento da saída depende do modo de activação de saída, descrito em “6.2.n.6 Modo” abaixo.

6.2.n.5 Parar filtro

```
00>Não utilizado  
01 Sir. interior
```

Utilize o menu Filtro parar para especificar um filtro de condição opcional que desactiva a saída.

6.2.n.6 Modo

```
6>Modo  
Seguir
```

Encontram-se disponíveis os seguintes modos:

- Seguir: o estado da saída é igual ao estado do filtro de condição de início, a menos que o filtro de condição stop se torne válido.

O início da activação de saída depende do retardo programado em “6.2.n.7.1 Tempo retardo” na página nº 272.

Se o retardo for programado como 0, a saída é activada imediatamente. Caso contrário, a saída é activada apenas após o filtro de condição de início ter estado activo pelo tempo programado.

Quando o filtro de condição parar é activado, a saída fica imediatamente passiva.

- Um Impulso: activar o filtro de condição de início acciona o temporizador de retardo definido em “6.2.n.7.1 Tempo retardo” na página nº 272. Após o fim do tempo, a saída activa-se durante o tempo definido em “6.2.n.7.2 Tempo activo” na página nº 272, e depois desliga-se.

Se o filtro de condição parar estiver configurado, a sua activação desactiva a saída e efectua reset a ambos os temporizadores.

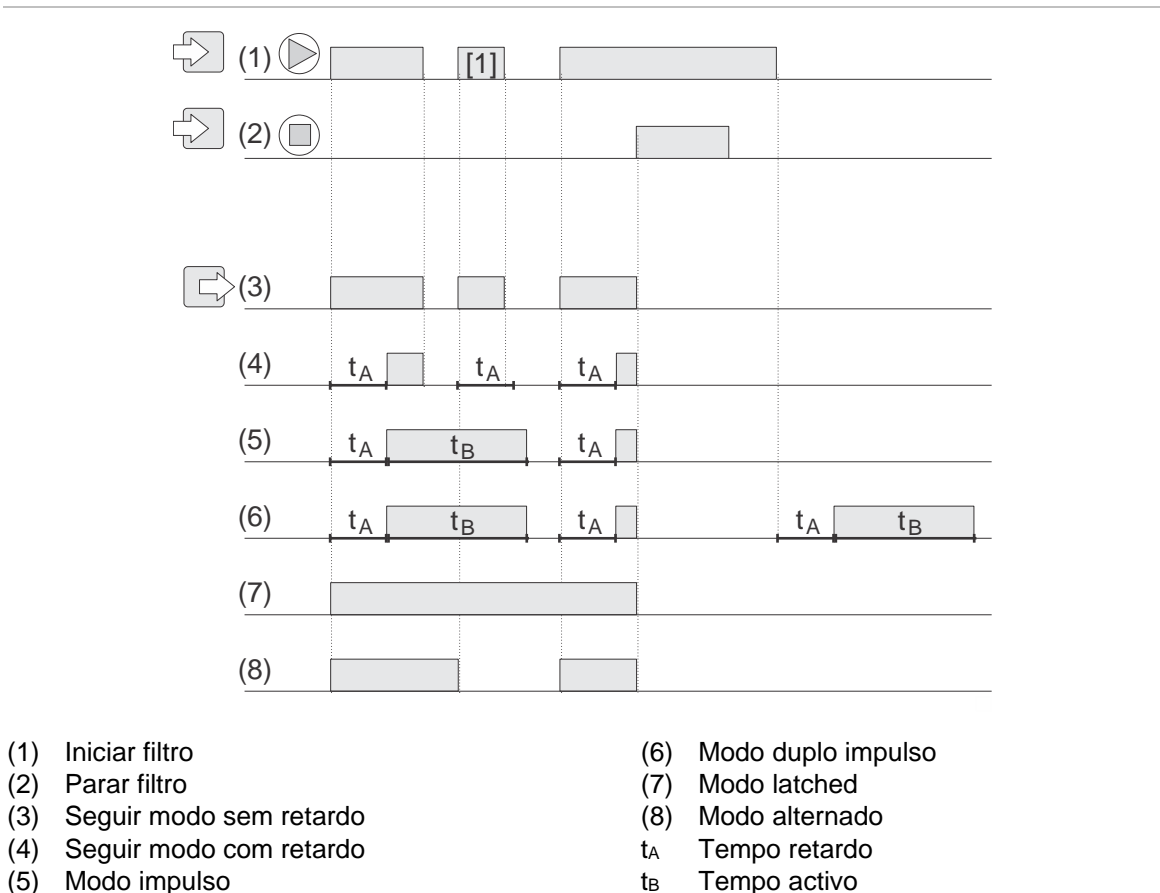
- Duplo Impulso: semelhante a Um Impulso, com excepção de que a temporização de retardo é activada por qualquer alteração do filtro de condição de início, activado e desactivado.
- Latched: Uma activação do filtro de condição de início comuta a saída para ligado. A saída só pode ser desactivada pela activação do filtro de condição parar.

Se o filtro de condição parar não estiver configurado, a saída irá permanecer sempre activa.

- Comutado: uma única activação do filtro de condição de início comuta o estado da saída para o oposto.

Figura 26 abaixo ilustra vários exemplos dos modos de activação de saída descritos.

Figura 26: Exemplos de modos de activação de saída



Nota: o tempo activado t_B é equivalente ao retardo programado se a opção 6.2.n.7.3 Novo trigger estiver definida como Não. Caso contrário, o temporizador é reiniciado quando o filtro de início se activa [1] e o tempo de activação é prolongado. Consulte “6.2.n.7.3 Novo trigger” abaixo para obter mais informações.

6.2.n.7 Parâmetros

```
7>Tempo retardo
  00:00'00
```

Defina os parâmetros aplicáveis para as funções acima descritas.

6.2.n.7.1 Tempo retardo

```
1 Tempo retardo
  >00:00'00<
```

O tempo de retardo define o tempo entre a activação da condição e a ligação da saída. Os valores permitidos situam-se entre 00:00'00 e 12:00'00. 00:00'00 significa que a saída é activada sem retardo.

6.2.n.7.2 Tempo activo

```
2 Tempo activo
  >00:00'01<
```

Tempo activo define o tempo de activação de uma saída. Os valores permitidos situam-se entre 00:00'01 e 12:00'00.

Esta opção só se encontra disponível se o modo Um Impulso ou Duplo Impulso se encontrar seleccionado em “6.2.n.6 Modo” na página nº 270.

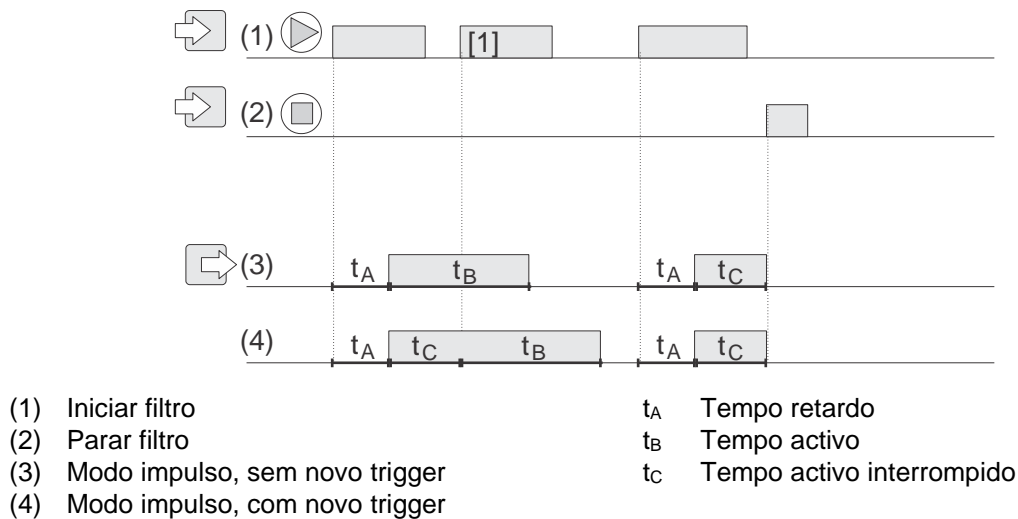
6.2.n.7.3 Novo trigger

```
3 Novo trigger
  >Não<
```

Nota: a opção Novo trigger só é válida para saídas em modo de Um Impulso e Duplo Impulso.

Se esta opção estiver definida como Sim, o temporizador de activação é reiniciado quando a condição de início volta a ficar válida durante o estado de activação, pelo que o tempo de activação é prolongado. A Figura 27 na página nº 273 mostra o reaccionamento da saída quando o filtro de início é reactivado [1].

Figura 27: Exemplos de saídas



6.2.n.8 Limite log

```
8 Limite log
   ctivado<
```

Se a opção Limite log estiver definida como Activado, só 3 pares de eventos de activação (abertura) e restauro (ou fecho) provenientes de uma única saída são registados no registo durante um ciclo de arme/desarme.

6.2.n.9 Remove output

```
9 Remove output
   >Cancelar<
```

Utilize o ecrã Remove output para remover uma saída do sistema. Para remover a saída, seleccione OK e prima Enter novamente. A saída é eliminada.

6.3 Triggers

```
0>Adicionar Trig
1 Trigger 1
```

O menu Triggers permite configurar triggers (accionadores) do sistema.

Definições de triggers

6.3.0 Adicionar Trig

Aceda ao menu para adicionar um trigger. Se o trigger for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Trigger adic.
```

É atribuído ao novo trigger o nome predefinido de “Trigger N” e é colocado no fim da lista de triggers. Agora o utilizador pode começar a editar os detalhes do novo trigger.

6.3.n Seleccionar trigger

```
1>Nome trigger
   Trigger 1
```

Selecione um trigger a configurar.

6.3.n.1 Nome trigger

```
1 Nome trigger
>Trigger 1 <
```

Cada trigger pode ser programado com um nome que o identifique.

Utilize o ecrã Nome trigger para introduzir ou editar o nome do trigger. O nome do trigger pode ser composto por até 16 caracteres.

6.3.n.2 Programa

Selecione programas para o trigger.

O menu de atalhos permite atribuir até dois programas ao elemento seleccionado.

Consulte “Menu de atalhos de programa” na página nº 91 para obter mais informações.

6.3.n.3 Apagar trigger

Para remover um trigger, selecione o trigger com o cursor, ou introduza o número do trigger e aceda ao menu Apagar trigger.

O ecrã apresenta:

```
3 Apagar trigger
   >Cancelar<
```

Selecione OK e prima Enter. Esta acção elimina o trigger.

Repita o comando para eliminar outros triggers, ou prima Sair para sair e voltar ao nível superior de menu.

7 Calendário

```
1>Ver
2 Programas
```

O calendário permite configurar a execução automática de determinadas acções numa data e hora específicas. As definições do painel podem ser automaticamente ajustadas de acordo com programas.

Consulte “Calendário” na página nº 90 no Capítulo 3 “Funções do sistema” para ver a descrição detalhada da funcionalidade.

7.1 Ver

```
1>10-03-2016
2 11-03-2016
```

Utilize o menu Ver para ver as acções e acções contrárias planeadas para o dia específico.

É possível desactivar uma acção planeada para o dia actual. Para tal, seleccione uma acção e alterne entre Ligado e Desligado.

7.1.n Data

```
1>Auto arme
2 Por objeto
```

Selecione ou introduza uma data para ver acções planeadas, ou para alterar o seu estado, e prima Enter.

7.1.n.1 Auto Arme

```
0>Todas áreas
>>>
```

Aceda ao menu para ver todas as acções de arme automático, em particular as áreas planeadas para o dia seleccionado.

Selecione Todas área, ou escolha a área aplicável.

7.1.n.2 Por objeto

```
1>Área
2 RAS
```

Aceda ao menu para ver todas as acções planeadas no dia seleccionado para objectos específicos.

Selecione o nome ou o tipo do objecto. Os objectos disponíveis são descritos em “Funções de utilizador programáveis” na página nº 105.

7.1.n.3 Dia Especial

```
1>Tipo de Dia
   Dia Normal
```

Aceda ao menu para configurar o dia seleccionado como um dia especial.

Para mais informações, consulte Capítulo 3 “Funções do sistema > Dias especiais nos programas” na página nº 91.

7.1.n.3.1 Tipo de Dia

```
1 Tipo de Dia
   >Dia Normal<
```

Escolha um tipo para o dia seleccionado:

- Dia Normal: Um dia normal. Uma janela de tempo de dia especial não é válida.
- Feriado, Dia especial 2, etc.: O dia é um dos dias especiais definidos em “7.2.n.6 Dias especiais” na página nº 280.

7.1.n.3.2 Recorrente

```
2 Recorrente
   >Sim<
```

Se definido como Sim, o dia especial repete-se todos os anos. Caso contrário, é válido apenas uma vez na data definida.

7.1.n.3.3 Até à data

```
3 Até à data
   >10.03.2016<
```

Se a data de fim estiver definida, o objecto de dia especial irá abranger um período de tempo desde o dia seleccionado até à data de fim definida no menu Até à data.

Nota: Um período de tempo substitui outros dias especiais no caso de coincidência.

7.2 Programas

```
0>Adic Z.Horária
1 Programa 1
```

Cada acção de painel executada automaticamente pode obedecer a até dois programas. Utilize o menu Programas para adicionar e alterar programas.

O número máximo de programas no sistema é indicado em “Características gerais” na página nº 39.

Para mais informações sobre programas, consulte “Programas” na página nº 90 no Capítulo 3 “Funções do sistema”.

Definições de programas

7.2.0 Adicionar Zona Horária

Aceda ao menu para adicionar um programa. Se o programa for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Adic Z.Horária
```

É atribuído ao novo programa o nome predefinido de “Programa N” e o programa é colocado no fim da lista de programas. Agora o utilizador pode começar a editar os detalhes do programa para o novo programa.

7.2.n Seleccionar programa

```
1>Nome
Programa 1
```

Selecione um programa a configurar.

7.2.n.1 Nome de programa

```
1 Nome
>Programa 1 <
```

A cada programa pode ser atribuído um nome para identificação.

Utilize o ecrã Nome de programa para introduzir ou editar o nome do programa. O nome do programa pode conter até 16 caracteres.

7.2.n.2 Activo

```
2 Activo
>Não<
```

Se estiver definido como Sim, o programa está actualmente activo.

7.2.n.3 Data

```
1>Data inicio
01.01.2016
```

Introduza as datas seguintes:

- 1 Data inicio: A data de início do programa.
- 2 Data fim: A data de fim do programa. Note que esta data não pode ser anterior à data de início.

7.2.n.4 Hora

```
0>Adc JanelaTemp
1 Jan. tempo 1
```

Defina janelas de tempo em que o programa é activado.

7.2.n.4.0 Adc JanelaTemp

Aceda ao menu para adicionar uma janela de tempo. Se a janela de tempo for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
JTempo Adic
```

É atribuído à nova janela de tempo o nome predefinido de “Janela de tempo N” e a janela de tempo é colocada no fim da lista de acções. Agora o utilizador pode começar a editar os detalhes da acção para a nova acção.

Cuidado: as janelas de tempo não devem coincidir.

7.2.n.4.m Janela de tempo

```
1>Tempo inicio
      00:00
```

Selecione uma janela de tempo a programar.

7.2.n.4.m.1 Tempo inicio

```
1 Tempo inicio
      >00:00<
```

Introduza a hora no formato de 24 horas HH:MM, quando a janela de tempo seleccionada é iniciada.

Nota: o valor 24:00 significa que a janela de tempo não está configurada.

7.2.n.4.m.2 Tempo fim

```
2 Tempo fim
      >00:00<
```

Introduza a hora no formato de 24 horas HH:MM, quando a janela de tempo seleccionada termina. O valor 00:00 significa que a hora de fim não está definida e, conseqüentemente, a acção contrária não será executada. Consulte Capítulo 3 “Funções do sistema > Acções contrárias” na página nº 91 para obter mais informações.

7.2.n.4.m.3 Dias da semana

```
Dias da semana
      >M.WT...<
```

Selecione os dias da semana quando a janela de tempo seleccionada está activa.

Se não for seleccionado nenhum dia da semana, o programa só será válido no primeiro e no último dia (programa não recorrente). Neste caso, só poderá ser utilizada uma janela de tempo. Consulte também Capítulo 3 “Funções do sistema > Programas” na página nº 90.

7.2.n.4.m.4 Apagar JT

Para remover uma janela de tempo, seleccione uma janela de tempo com o cursor, ou introduza o número da janela de tempo e aceda ao menu Apagar JT.

O ecrã apresenta:

```
4 Apagar JT
  >Cancelar<
```

Selecione OK e prima Enter. Esta acção remove a janela de tempo.

Repita o comando para eliminar outras janelas de tempo, ou prima Sair para sair e voltar ao nível superior de menu.

7.2.n.5 Lista de Acções

```
0>Adicionar Acç>
1 Acção 1
```

Selecione acções que têm de ser executadas pelo sistema de acordo com o programa seleccionado.

Cada acção pode ser programada com várias opções. Antes de avançar, seleccione a acção a programar.

O número máximo de acções para cada programa é indicado em “Características gerais” na página nº 39.

7.2.n.5.0 Adicionar Acção

Aceda ao menu para adicionar uma acção. Se a acção for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Acção adic.
```

É atribuído à nova acção o nome predefinido de “Acção N” e a acção é colocada no fim da lista de acções. Agora o utilizador pode começar a editar os detalhes de acção para a nova acção.

7.2.n.5.m Seleccionar acção

```
1>Nome
  Acção 1
```

Selecione a acção a programar.

7.2.n.5.m.1 Nome acção

```
1 Nome
>Acção 1 <
```

Cada acção pode ser programada atribuindo-lhe um nome que a identifique.

Utilize o ecrã Nome acção para introduzir ou editar o nome da acção. O nome da acção pode conter até 16 caracteres.

7.2.n.5.m.2 Tipo de Objeto

7.2.n.5.m.3 Função

7.2.n.5.m.4 Parâmetros

As funções e parâmetros disponíveis são descritos em “Funções de utilizador programáveis” na página nº 105.

7.2.n.5.m.5 Apagar Acção

Para remover uma acção, seleccione a acção com o cursor, ou introduza o número da acção e aceda ao menu Apagar Acção.

O ecrã apresenta:

```
5 Apagar acção
  >Cancelar<
```

Selecione OK e prima Enter. Isto remove a acção.

Repita o comando para eliminar outras acções, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: não pode eliminar uma acção, a menos que o seu grupo de utilizadores o autorize a fazê-lo.

7.2.n.6 Dias especiais

```
0>Adic Dia Espe.
1 Feriado
```

Configure dias especiais associados a este programa.

O número máximo de dias especiais para cada programa é indicado em “Características gerais” na página nº 39.

7.2.n.6.0 Adicionar dia especial

Aceda ao menu para adicionar um dia especial. Se o dia especial for criado com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
DiaEspAdici.
```

O primeiro dia especial recebe o nome predefinido “Feriado”, enquanto que aos dias especiais seguintes são atribuídos os nomes “Dia especial 2”, “Dia especial 3”, etc.

7.2.n.6.m Dia especial

```
1>Nome
  Feriado
```

Selecione um dia especial a programar.

7.2.n.6.m.1 Nome de Dia Especial

```
1 Nome
>Feriado <
```

Cada dia especial pode ser programado com um nome que o identifique.

Utilize o ecrã Nome de Dia Especial para introduzir ou editar o nome do dia especial. O nome do dia especial pode conter até 16 caracteres.

Nota: os nomes de dia especial são comuns em todos os programas.

7.2.n.6.m.2 Tempo inicio

```
1 Tempo inicio
>00:00<
```

Introduza a hora no formato de 24 horas HH:MM, quando a janela de tempo do dia especial seleccionado é iniciada.

7.2.n.6.m.3 Tempo fim

```
1 Tempo inicio
>00:00<
```

Introduza a hora no formato de 24 horas HH:MM, quando a janela de tempo do dia especial seleccionado termina.

7.2.n.6.m.4 Apagar dia especial

Para remover um dia especial, seleccione um dia especial com o cursor, ou introduza o número do dia especial e aceda ao menu Apagar dia especial.

O ecrã apresenta:

```
5 Apaga Dia Esp.
>Cancelar<
```

Selecione OK e prima Enter. Esta acção remove o dia especial.

Repita o comando para eliminar outros dias especiais, ou prima Sair para sair e voltar ao nível superior de menu.

7.2.n.7 Filtro

```
00>Não utilizado
01 Sir. interior
```

Atribua um filtro de condições adicional ao programa.

Se o filtro for desactivado, o programa será desactivado. Se não for atribuído nenhum filtro de condições, o programa será executado incondicionalmente.

Consulte “6.1 Filtros de condição” na página nº 267 para obter mais informações.

7.2.n.8 Apagar Zona Horária

Para remover um programa, seleccione o programa com o cursor, ou introduza o número do programa e aceda ao menu Apagar Zona Horária.

O ecrã apresenta:

```
8 Apagar FH  
>Cancelar<
```

Selecione OK e prima Enter. Esta acção remove o programa.

Repita o comando para eliminar outros programas, ou prima Sair para sair e voltar ao nível superior de menu.

8 Sistema

```
1>Temporizadores
2 Opções técnico
```

Utilize o menu Sistema para programar as opções globais do sistema, incluindo temporizadores.

8.1 Temporizadores

```
1>Hora&data
2 Sirenes
```

Utilize o menu Temporizadores para programar todos os temporizadores do sistema nesta secção.

Notas

- Os temporizadores são precisos a ± 1 do valor introduzido. Assim, um temporizador programado para 20 segundos, termina entre os 19 e os 21 segundos. Por conseguinte, evite utilizar valores de 1 segundo ou 1 minuto.
- Se um temporizador estiver ajustado para 0, não é utilizado.

8.1.1 Hora e data

```
1>Zona horária
      UTC+1
```

O menu Hora e data permite definir a hora e a data do sistema, bem como configurar o horário de verão.

Estão disponíveis as seguintes opções:

- 1 Zona horária: A zona horária do sistema.
- 2 Data: O formato da data é DD/MM/AAAA.
- 3 Hora: O formato da hora é 24 horas.
- 4 Mês iníc. HV: O mês de início do horário de verão.
- 5 Sem. iníc. HV: A semana de início do horário de verão. As opções disponíveis são: 1ª semana, 2ª semana, 3ª semana, 4ª semana, última semana.
- 6 Mês fim HV: Conforme exposto acima.
- 7 Sem. fim HV: Conforme exposto acima.
- 8 Correção: Permite a configuração da correção da hora, se necessário.
 - 8.1 Tempo/7dias: Este submenu permite definir a correção da hora que é efectuada a cada 7 dias de trabalho no painel. O valor máximo é de 5 min. e 40 segs. O valor positivo significa que o relógio está definido para a frente, negativo – para trás.

Durante a alteração de hora de Verão, a hora avança sempre no domingo às 2:00 e recuar às 3:00.

Nota: Consulte “Nota de hora de Verão” na página nº 91 para obter informações sobre a alteração de hora de Verão em acções programadas.

8.1.2 Sirenes

```
1>Activação
2 Retardo
```

O menu de opções de sirenes permite programar temporizadores aplicáveis a sirenes internas e externas.

Seleccione se deseja alterar a hora da activação ou o retardo da sirene.

8.1.2.1 Activação

```
1>Sir. interior
00:03'00
```

O menu Activação permite definir a hora de activação da sirene interna e externa.

8.1.2.1.1 Sirene interior

8.1.2.1.2 Sirene exterior

Introduza a hora de activação da sirene interna e externa. O formato do tempo é hh:mm:ss. O intervalo permitido é de 00:00'00 a 06:00'00. O valor 00:00'00 significa que a sirene não é activada. O valor 06:00'00 é igual a tempo infinito (a sirene fica activa até desactivada ou reinicializada).

8.1.2.1.3 Interior F/P/M

8.1.2.1.4 Exterior F/P/M

Introduza a hora de activação para a sirene interna/externa no caso de alarmes de fogo, pânico e médicos. O formato do tempo é hh:mm:ss. O intervalo permitido é de 00:00'00 a 06:00'00. O valor 00:00'00 significa que a sirene não é activada. O valor 06:00'00 é igual a tempo infinito (a sirene fica activa até desactivada ou reinicializada).

8.1.2.2 Retardo

```
1>Sir. interna
00:00'00
```

O menu Tempo de retardo permite definir o tempo de retardo antes que uma sirene interna ou externa seja activada.

8.1.2.2.1 Sirene interna

8.1.2.2.2 Sirene externa

Introduza o tempo de retardo da sirene interna/externa. O formato do tempo é hh:mm:ss. O intervalo permitido é de 00:00'00 a 06:00'00.

Cuidado: numa condição de desarme, o retardo da sirene interna é ignorado e a sirene é imediatamente activada.

8.1.3 Sistema

O menu Sistema permite configurar todos os temporizadores programáveis do sistema.

8.1.3.1 Screensaver

```
1 Screensaver
   >00'30<
```

O retardo de Screensaver é um retardo antes de o visor armado ser activado no LCD do teclado quando entra no estado de inactividade. O formato do tempo é mm:ss. O intervalo permitido é de 00'00 a 10'00.

8.1.3.2 Cartão e PIN

```
2 Cartão e PIN
   >00'10<
```

O menu Cartão e PIN permite definir o tempo máximo de retardo entre a apresentação do cartão e a introdução do PIN (o valor predefinido é 10 segundos). O formato do tempo é mm:ss. O intervalo permitido é de 00'00 a 05'00.

8.1.3.3 Walk Test

```
3 Walk Test
   00'00
```

A opção do menu Tempo de Walk Test define o tempo máximo para o Walk Test (0 a 30 minutos). Um valor de 00'00 significa sem limite; neste caso, o Walk Test é terminado pelo utilizador, ou quando concluído com êxito. Para mais informações, consulte “1.2.5 Walk Test” na página 158.

8.1.3.4 Rtd.rep.230VAC

```
4 Rtd.rep.230VAC
   >00:00'00<
```

A opção Rtd.rep.230VAC define o tempo de retardo (0 a 4 horas) antes de uma falha de rede ser comunicada à central receptora. Introduza o valor “0” para um reporte imediato.

8.1.3.5 Rtd.armed final

```
5 Rtd.armed final
  > <
```

A opção Rtd.armed final define o tempo de retardo entre a conclusão do armed de uma área por um terminador de saída ou o armed final da porta e a área a ser armada. O período permite que os dispositivos ligados a entradas voltem para o estado normal. O intervalo permitido é de 0 a 255 segundos.

8.1.3.6 Manutenção em

```
6 Manutenção em
  >00:01'00<
```

O menu Manutenção em permite configurar o tempo de acesso do técnico quando concedido por um utilizador (consulte “8.2.1 Aceit. necess” na página 288). Este tempo inicia-se quando o utilizador activa a opção “Acesso instal”. Durante este tempo, o instalador pode aceder ao menu do instalador e armar ou desarmar o sistema.

Nota: Qualquer sistema armado ou desarmado cancelará o instalador a tempo.

Quando o instalador se encontra no menu do instalador, este tempo não tem qualquer efeito no tempo que o instalador se pode manter em sessão.

O intervalo permitido é de 00 h 01 min a 11 h 59 min. Um valor de 12 h 00 min é equivalente a um acesso infinito.

8.1.4 Zonas

```
1>Int.dpl.impls
  10'00
```

O Menu de temporizador de zona permite configurar todos os temporizadores de zona programáveis.

8.1.4.1 Intervalo duplo impulso

```
1 Int.dpl.impls
  >00'00<
```

Se activado para uma determinada zona, o Intervalo duplo impulso especifica o tempo máximo permitido entre dois impulsos que regista um alarme. Se este valor estiver definido como 0, não é determinada uma condição de alarme pelo intervalo entre dois impulsos, mas unicamente pelo tempo de abertura de duplo impulso. O intervalo permitido é de 0 a 15 minutos.

8.1.4.2 Abertura duplo impulso

```
2 Abr.dpl.impls
  >00'05<
```

Se activado para uma determinada zona, a abertura duplo impulso especifica o tempo durante o qual a zona poderá permanecer activa. Se a zona

permanecer activa depois de excedido este tempo, é gerado um alarme sem esperar por uma segunda activação.

O formato do tempo é mm'ss. O intervalo permitido é de 00'00 a 15'00.

8.1.4.3 Soak Test

```
3 Soak Test
  > <
```

A opção Soak Test define o número de dias que o Soak Test de uma zona está activo. O intervalo permitido é de 0 a 30 dias.

O Soak Test é activado assim que a opção de zona Soak Test de uma zona (consulte “4.1.n.6.10 Soak test” na página 216) for definido como Sim. Durante o período de Soak Test a zona não acciona alarmes.

8.1.4.4 Retardo de input

```
4 Retardo input
  > <
```

O valor Retardo de input representa o retardo entre uma entrada e a activação da zona apropriada. O intervalo permitido é de 0 a 255 segundos.

8.1.4.5 Tempo key box

```
5 Tempo key box
  > <
```

O Tempo key box prolonga o tempo de saída. Imediatamente após expirar o temporizador de saída, o temporizador key box inicia-se para uma duração de tempo definida. Antes de expirar este temporizador, a zona tem de ser fechada. Se não estiver fechada, é accionado novamente um alarme completo, mesmo se o trigger anterior tiver sido também um alarme. Durante o funcionamento do temporizador de saída e do temporizador key box, as aberturas e os fechos não são registados e não originam um alarme.

O intervalo permitido é de 0 a 99 minutos.

8.1.4.6 Tempo Manter Aberto

```
6 T Manter Abert
  >00:00'00<
```

As opções definem o período de tempo para manter aberto, após o qual a zona gera um sinalizador de “aberto demasiado tempo”, que pode ser usado para a programação do filtro.

Consulte “4.1.n.6.30 Mantida abert” na página nº 221.

8.1.4.7 Dias Inactivos

```
7 Dias Inactivos
  > <
```

Se uma zona estiver inactiva por um período de tempo superior ao tempo programado neste menu (em dias), é activado um evento de dias inactivos apropriado para a zona.

O intervalo permitido é 0 a 127, com 0 a desactivar o temporizador relativo à zona.

Os temporizadores de dias inactivos da zona podem ser visualizados e repostos utilizando o menu “1.2.1.6 Dias inactivos” descrito na página nº 151.

8.2 Opções de técnico

```
1>Aceit. necess
  Sim
```

As Opções de técnico são opções que se aplicam a funções de manutenção e de instalação.

8.2.1 Aceit. necess

```
1 Aceit. necess
  >Sim<
```

Se a opção Aceitação necessária estiver definida como Sim, é necessário que um utilizador conceda ao instalador acesso ao menu de programação. Para mais informações sobre a opção Instalador, consulte o *Guia do Utilizador do Advisor Advanced*.

8.2.2 Tamper necessário

```
2 Tamper necess
  >Não<
```

Se a opção Tamper necessário estiver definida como Sim, o instalador tem de abrir a caixa do painel (iniciando o alarme de sabotagem) para poder aceder ao menu de programação.

8.2.3 Bloqueio técnico

```
3 Bloqueio Téc
  >Desactivado<
```

Se a opção Bloqueio técnico estiver definida como Activado, já não é possível aceder ao modo de programação durante o arranque utilizando o código predefinido do instalador (jumper T1 definido durante o arranque).

Cuidado: se esta opção estiver activada, é impossível executar o procedimento de recuperação do sistema. Consulte “Procedimento de recuperação” na página nº 362 para obter mais informações.

8.2.4 Reset técnico

1 >Alarme
Não

O menu Reset técnico permite definir que condições necessitam de um reset técnico, e permite também efectuar esse reset.

8.2.4.1 Alarme

1 Alarme
>Não<

Se a opção Alarme estiver definida como Sim, a área na qual ocorreu o alarme não pode ser armada até que seja efectuado um reset técnico, desde que o reset técnico impeça o arme (consulte “8.4.1 Pront.Armar”, na página 295).

Esta opção é ignorada no caso de estar activada a confirmação de alarme AB. Para mais informações, consulte “8.2.4.4 Confir. alarme” abaixo.

8.2.4.2 Tamper

2 Tamper
>Não<

Se a opção Tamper estiver definida como Sim, os alarmes de sabotagem (tamper) requerem um reset técnico.

8.2.4.3 Pânico

3 Pânico
>Não<

Se a opção Pânico estiver definida como Sim, os alarmes de pânico requerem um reset técnico.

8.2.4.4 Confir. alarme

4 Confir.alarme
>Desligado<

O menu Confirmação do alarme define qual o alarme AB que requer um reset técnico. As opções disponíveis são ALARME-A, ALARME-B ou Desligado (desactivado). Esta opção só funciona quando a confirmação de alarme AB está activada.

8.2.4.5 Falha de bateria

5 Falha bateria
>Desligado<

Se a opção Falha de bateria estiver definida como Sim, as falhas de bateria requerem um reset técnico.

8.2.4.6 Fusível aux

```
6 Fusível aux
  >Desligado<
```

Se a opção Fusível aux estiver definida como Sim, as falhas de fusível auxiliar requerem um reset técnico.

8.2.4.7 Falha 230VAC

```
7 Falha 230VAC
  >Desligado<
```

Se a opção Falha 230VAC estiver definida como Sim, as falhas de fornecimento de corrente requerem um reset técnico.

8.2.4.8 Falha de sirene

```
8 Falha sirene
  >Desligado<
```

Se a opção Falha de sirene estiver definida como Sim, as falhas de sirene requerem um reset técnico.

8.2.4.9 Falha interlig

```
9 Falha interl>
  >Desligado<
```

Se a opção Falha de interligação estiver definida como Sim, as falhas de interconexão requerem um reset técnico.

8.2.4.10 Reset auto

```
10 Reset auto
  >Desligado<
```

Se a opção de Reset automático estiver definida como Sim, o reset técnico é executado automaticamente quando o instalador inicia sessão.

8.2.4.11 Disp p/ srv

```
11 Disp p/ srv
  >Desligado<
```

Se a opção Disp p/ srv estiver definida como Sim, não é emitido um pedido de reset técnico enquanto o instalador tiver autorização de acesso ao sistema.

Nota: esta opção só é válida se o instalador precisar de autorização do utilizador. Consulte “8.2.1 Aceit. necess” na página nº 288.

8.2.4.12 Código sistema

```
12 Código siste>
  > <
```

O menu Código sistema permite definir o código do sistema para o reset técnico. O código pode ter até 5 caracteres.

O valor predefinido 0 significa que o código não está definido. Neste caso, a geração remota de código de reset está desactivada.

Se o código estiver definido, o seu valor e o valor do código do técnico são utilizados para gerar o código de reset. Consulte “Reset técnico” na página nº 121 para obter mais informações.

8.2.4.13 Efectuar reset

```
13 Efectuar res>
    >Cancelar<
```

O comando Efectuar reset é utilizado para executar o reset técnico.

8.2.4.14 Configurar texto

```
14 Config. texto
    >                <
```

Utilize configurar texto para programar um pedido exibido quando é necessário um reset técnico.

Se Configurar texto não estiver definido, o pedido padrão será apresentado como descrito em “Reset técnico” na página nº 121.

Caso contrário, os pedidos serão os seguintes, dependendo da apresentação de código do utilizador ou da mensagem de aviso:

```
<config. texto>
Código:23353
```

```
AVISO
<config. texto>
```

Consulte “Reset técnico” na página nº 121 para obter mais informações.

8.2.5 Manutenção em

```
5 Manutenção em
  Desactivar?
```

O menu Manutenção em permite desactivar a função de acesso do instalador antes de expirar o tempo de acesso (consulte “8.1.3.6 Manutenção em” na página nº 286).

Nota: esta opção só é válida se o instalador precisar de autorização do utilizador. Consulte “8.2.1 Aceit. necess” na página nº 288.

Utilize esta função após terminar a programação do painel. Para cancelar o tempo de acesso do instalador, navegue para este menu e prima Enter. A seguir, saia de sessão. Posteriormente, o início de sessão do instalador irá precisar de outra confirmação do utilizador.

Consulte também “Aceitação necessária” na página nº 134.

8.2.6 Código desafio

```
6 Código desafio
   Não
```

Utilize este menu para activar a funcionalidade de código desafio. Consulte “Código desafio necessário” na página nº 135 para obter mais informações.

Cuidado: uma vez activada, esta opção não pode ser desactivada pelas definições de software.

8.2.7 Inspeção

```
1>Data
   31.12.2099
```

Configure um lembrete de inspecção periódica.

8.2.7.1 Data

```
1 Data
   >31.12.2099<
```

Introduza a data da próxima inspecção.

8.2.7.2 Msg. personal

```
2 Msg. personal
   >Nec.inspecção<
```

Introduza a mensagem do lembrete de inspecção.

8.2.8 Grp instalador

```
1>Muitos instal.
   Desativar
```

O menu contém as opções que configuram o grupo de utilizadores dos instaladores.

8.2.8.1 Muitos instaladores

```
1 Muitos instal.
   >Desativar<
```

Se a opção estiver definida para Ativar, o sistema pode conter mais de um utilizador instalador.

Nota: A opção só pode ser desativada depois de todos os instaladores adicionais serem removidos da base de dados do painel.

8.2.8.2 SW de gestão

```
2 SW de gestão
  >Desativar<
```

Se a opção estiver ativada, é possível editar os instaladores a partir de um teclado, o software de configuração (ATS85xx) e remotamente através do software de gestão (ATS8600).

Se a opção estiver desativada, a edição dos instaladores só é possível a partir de um teclado e do software de configuração (ATS85xx).

Nota: A opção só está disponível se “8.2.8.1 Muitos instaladores” na página nº 292 estiver definido para Ativar.

Cuidado: Se a opção estiver ativada, deverá ter cuidado ao escrever os dados de utilizador do software de gestão para o painel de controlo. Não substitua os instaladores ativos.

8.3 Menu e LCD

```
1>Modo Scr saver
  Sempre
```

O menu Menu e LCD contém opções que podem ser definidas para LCDs e menus.

8.3.1 Modo Screensaver

```
1 Modo Scr saver
  >Sempre<
```

Se o Modo Screensaver estiver definido como Ligado, o visor armado é activado passado o tempo de inactividade programado. O tempo limite para o visor armado é programado em “8.1.3.1 Screensaver” (consulte a página 285).

O visor armado é desactivado ao executar qualquer acção que requeira uma autorização com um badge ou código de utilizador válido.

É possível seleccionar uma das seguintes opções de visor armado:

1. Desligado: O visor armado está desactivado.
2. Se armado: O visor armado só é activado quando a área estiver armada. Não aparece a informação do estado no LCD do teclado e LEDs (excepto o LED de corrente eléctrica e mensagem de alerta).
3. Sempre: O visor armado é sempre activado. Não aparece a informação do estado no LCD do teclado e LEDs (excepto o LED de corrente eléctrica e mensagem de alerta).
4. Sem código: O visor armado é sempre activado. Nenhum LED de área se acende.

Nota: este modo também permite desactivar o visor armado premindo a tecla Limpar.

8.3.2 Msg personalizada

```
2 Msg. personal  
>Carrier F&S <
```

O menu Mensagem personalizada permite definir uma mensagem de boas-vindas no teclado.

São registados 16 caracteres de texto personalizado que aparece na linha superior do LCD dos teclados em vez do texto predefinido. Os caracteres incluem números, espaços e pontuação.

8.3.3 Lista de alarmes

```
3 Lista alarmes  
>Desactivado<
```

A opção define a forma como os alarmes e falhas de zona podem ser visualizados no LCD por um utilizador sem sessão iniciada.

A opção define se os alarmes e falhas de zona são visíveis a um utilizador sem sessão iniciada.

- Desactivado: os alarmes e falhas de zona não são mostrados.
- Activado: a opção Lista alarmes permite ao utilizador fazer listas de entradas activas e de falhas, assim como de alarmes.

Consulte “Teclas” na página nº 62.

- Imediato: além da opção de lista de alarmes, os alarmes e falhas são mostrados imediatamente.

Nota: Os alarmes e as falhas não são visualizados se o screensaver estiver activo. Ver “8.3.1 Modo Screensaver” na página nº 293 para obter mais informações.

8.3.4 Indicar falhas

```
4 Indicar falhas  
>Sempre<
```

A opção define quando as falhas são indicadas nos LEDs. Estão disponíveis as seguintes opções:

- Sempre: As falhas são sempre mostradas.
- No arme: As falhas só são apresentadas durante uma tentativa de definição do sistema.

8.3.5 Ver tempo ES

```
5 Ver tempo ES
  >Desligado<
```

A opção define se os temporizadores de entrada e de saída são apresentados durante o arme e o desarme do sistema.

Nota: O temporizador de entrada/saída apropriado é apresentado num keypad apenas se a opção besouro de entrada/saída estiver ativada para este keypad. Consulte “2.2.1.n.3.19 ES 1 Besouro” na página nº 183 e “2.2.1.n.3.20 ES 2 Besouro” na página nº 183 para obter mais informações.

8.4 Opções de arme

```
1>Op.Pront.Armarm
2 Inib. inclusão
```

As opções do menu Opções de arme definem as condições de arme.

8.4.1 Pront.Armarm

```
01>Alarme zona
      Sim
```

O menu Opções Pronto a Armar define as condições que podem impedir o arme. Se uma das condições indicadas a seguir tiver esta opção definida como Sim, o respectivo estado afecta o estado “Pronto a Armar”. O sistema não permite armar áreas se qualquer uma das condições for verdadeira.

Para condições relativas a áreas, a condição é testada para essas áreas. Por exemplo, a Zona 5 atribuída à área 1 apenas afecta o arme da área 1.

Estão disponíveis as seguintes opções:

- 1 Alarme de zona: Zona activa
- 2 Pânico de zona: Dispositivo de suspensão activo
- 3 Zona AM: Estado de Anti-Mask/falha na entrada
- 4 Falha de zona: Falha de detector de intrusão
- 5 Tamper de zona: Tamper na zona
- 6 Falha de interconexão: Um erro crítico causado por um problema de comunicação entre componentes do painel interno
- 7 Falha 230VAC: Falha da rede eléctrica, incluindo falha exterior
- 8 Falha de bateria: Falha da bateria, incluindo falha exterior
- 9 FTC (Falha em comunicar): O reporte de alarmes não conseguiu entregar eventos
- 10 Falha de sirene: Falha de saída de sirene
- 11 Zona técnica: Estado de zona técnica
- 12 Falha de RAS: Uma falha reportada pelo teclado
- 13 Falha de DGP: Uma falha reportada pelo expansor remoto
- 14 Falha nas comunicações: Todos os caminhos de transmissão estão desligados (sem comunicação)
- 15 Reset técnico: Requisito de reset técnico

- 16 Alarmes em espera: Alarmes não confirmados
- 17 Falha de áudio: uma falha reportada pelo dispositivo de áudio

8.4.2 Inibir inclusão

```
01>Pânico zona
  Nivel acesso 2
```

O menu define as condições que um utilizador com um nível de acesso específico tem autorização para inibir. Se uma das condições indicadas a seguir tiver esta opção definida como Nível Acesso 2 ou Nível Acesso 3, um utilizador com este nível de acesso pode inibi-la utilizando um menu de inibir ou durante o arme.

Estão disponíveis as seguintes opções:

- 1 Pânico de zona: Dispositivo de suspensão activo
- 2 Anti-Mask de zona: Estado de Anti-Mask/falha na entrada
- 3 Falha de zona: Falha de detector de intrusão
- 4 Tamper de zona: Tamper na zona
- 5 Falha de interconexão: Um erro crítico causado por um problema de comunicação entre componentes do painel interno
- 6 Falha 230VAC: Falha da rede eléctrica, incluindo falha exterior
- 7 Falha da bateria: Falha da bateria, incluindo falha exterior
- 8 FTC (Falha em comunicar): Falharam as tentativas de reporte
- 9 Falha sirene: Falha de saída de sirene
- 10 Zona técnica: Estado de zona técnica
- 11 Falha de RAS: Uma falha reportada pelo teclado
- 12 Falha de DGP: Uma falha reportada pelo expansor remoto
- 13 Falha nas comunicações: Todos os caminhos de transmissão estão desligados (sem comunicação)
- 14 Reset técnico: Requisito de reset técnico
- 15 Falha de áudio: uma falha reportada pelo dispositivo de áudio

8.4.3 Arme parcial

```
1>Reporte BA
  Sim
```

O menu Arme parcial permite configurar as opções de arme parcial.

8.4.3.1 Reporte BA

```
1 Reporte BA
  >Sim<
```

Se a opção Reporte BA estiver definida como Sim, no arme parcial o sistema reporta à central receptora os alarmes anti-roubo activados durante o arme parcial.

8.4.3.2 Acesso para ES

```
2 Acesso para ES
  >Não<
```

Se a opção Acesso para Entrada/Saída estiver definida como Sim, as zonas de acesso tornam-se zonas de entrada/saída durante o arme parcial. Os utilizadores presentes nas instalações activarão então o temporizador de entrada, ficando cientes que a área está armada e que é necessário um procedimento de desarme.

8.4.3.3 EE arme total

```
3 EE Arme total
  >Não<
```

Se a opção estiver definida para Sim e o utilizador sair das instalações durante o tempo de saída de arme parcial (que provoca a activação da zona de entrada/saída), o estado de arme parcial muda para arme total.

Nota: A funcionalidade apenas funciona se existir tempo de saída definido para arme parcial. Isso significa que o tempo de saída da área definido da área em “4.2.n.2 Tempo de saída” na página nº 228 deve ser superior a 0.

8.4.3.4 Nome AP1

8.4.3.5 Nome AP2

```
4 Nome AP1
  > <
```

Utilize estes menus para alterar os nomes por defeito “Arme Parcial 1” e “Arme Parcial 2”. O campo vazio significa que será o nome por defeito.

Ver *Manual de Utilizador Advisor Advanced* para mais informações sobre o arme parcial.

8.4.4 Arme forçado

```
4 Arme forçado
  >Desligado<
```

A opção Arme forçado activa a funcionalidade de arme forçado. As opções de arme forçado são indicadas a seguir.

Arme forçado é uma opção em que as zonas activas podem ser automaticamente inibidas ao armar uma área.

Nota: esta opção deve ser utilizada com precaução. Os utilizadores poderão não saber quais são as zonas que estão inibidas.

8.4.5 Op. arme forçado

```
5 Op. arme forç  
>Inibir até DS<
```

O menu Opções de arme forçado define quando é possível o arme forçado. Estão disponíveis as seguintes opções:

- Inibido até desarmar: A zona está inibida até a área ser desarmada.
- Inibir saída: A zona está inibida até expirar o tempo de saída.
- Inibir fecho: A zona está inibida até o seu estado mudar para normal.

8.4.6 Alarmes em espera

```
6 Alarmes espera  
>Activado<
```

O menu define quais os alarmes que podem impedir o arme do sistema. Estão disponíveis as seguintes opções:

- Ativar. Se estiver definido para Ativar, a opção Alarmes pendentes requer que todos os alarmes sejam confirmados.
- Ativar EN 50131. O valor é igual a Ativar, mas todas as falhas e tampers também têm de ser reconhecidos.

O nível de utilizador para os utilizadores que têm permissão para confirmar depende das predefinições do painel. Consulte “Arranque inicial” na página 142 para obter mais informações.

Quando desactivada, não é necessária a confirmação dos alarmes. Durante o desarme ou rearme da área, o alarme é confirmado automaticamente. No entanto, cada alarme e falha é mostrado 3 vezes no ecrã do teclado.

8.4.7 AA tempo tent.

```
7 AA tempo tent.  
>15 minutos<
```

A tentativa de arme automático em falha de sistema define se e quando o sistema repete a tentativa de arme automático se uma falha de sistema impossibilitou o arme automático. Estão disponíveis as seguintes opções:

- Desligado
- 15 minutos
- 30 minutos
- 1 hora
- 2 horas
- 3 horas
- 4 horas

Consulte “Arme automático” na página nº 109 para obter mais informações.

8.4.8 AA tenta util

```
7 AA tenta util
  >15 minutos<
```

A opção de tempo de arme automático do utilizador define um tempo de adiamento de arme automático para o utilizador normal. Estão disponíveis as seguintes opções:

- Desactivado (o adiamento do arme automático não é permitido)
- 15 minutos
- 30 minutos
- 1 hora
- 2 horas
- 3 horas
- 4 horas

Consulte “Arme automático” na página nº 109 para obter mais informações.

O utilizador terá de possuir o privilégio de arme total para poder adiar o arme automático. Consulte “3.2.n.6 Opções de GU” na página nº 210 para obter mais informações.

8.4.9 Falha de saída

```
9 Falha de saída
  >Alarme<
```

O menu define o que acontece se a zona de entrada/saída ainda estiver ativa quando expira o tempo de saída. Estão disponíveis as seguintes opções:

- Alame: A falha de erro de saída é gerada e o sistema permanece desarmado.
- Entrada: O sistema encontra-se armado e o temporizador de entrada é iniciado de imediato.

8.4.10 Relt.Falha ES

```
10 Relt.Falha ES
  Falha EE
```

A opção define como a falha de saída de entrada/saída ou da zona de acesso é reportada à Central Recetora.

- Falha EE: Só são reportadas as falhas de entrada/saída.
- Falha EE + Alarme: São reportados dois eventos, a Falha EE e o Alarme de intrusão.

8.5 Opções de acesso

```
1>Temp. acesso
2 Opções de DGP
```

O menu contém várias opções de controlo de acesso.

8.5.1 Temporizadores acesso

```
>Cartão p/ PIN  
127
```

O menu contém definições de temporizadores de acesso.

Nota: todos os temporizadores são programados em segundos. Os intervalos permitidos são de 0 a 127 segundos.

8.5.1.1 Cartão p/ PIN

```
1 Cartão p/ PIN  
> <
```

Esta definição só se aplica quando um utilizador tem de apresentar um cartão e introduzir um PIN para obter acesso.

O tempo Cartão p/ PIN é o tempo permitido entre a apresentação de um cartão válido a um leitor de porta e a introdução de um PIN válido através do teclado. Se o PIN não for introduzido antes de o tempo expirar, o utilizador terá de repetir a função de abertura de porta.

8.5.1.2 Dois cartões

```
2 Dois cartões  
> <
```

Esta definição só é aplicável quando dois utilizadores têm de apresentar o seu cartão ou PIN para abrir uma porta, ou quando um utilizador é identificado como visitante ou vigilante e tem de estar acompanhado.

O tempo de dois cartões é o tempo permitido entre a apresentação do cartão ou introdução do PIN do primeiro utilizador e a apresentação do cartão ou introdução do PIN do segundo utilizador. Se o segundo cartão/PIN não for apresentado antes de o tempo expirar, a função de abertura de porta terá de ser repetida.

8.5.1.3 Multip Cartões

```
3 Multip Cartões  
> <
```

Esta definição só se aplica nos casos em que a porta foi programada para que a apresentação de um cartão por três vezes possa armar/desarmar o sistema e o utilizador tem autorização para armar/desarmar.

O Tempo multi-cartões é o tempo permitido entre a primeira apresentação do cartão e a terceira apresentação do cartão. Se o cartão não for apresentado três vezes antes de o tempo expirar, o utilizador terá de iniciar novamente a função.

8.5.1.4 Rtd rebloqueio

```
4 Rtd rebloqueio
  > <
```

Esta definição só se aplica quando a porta foi programada de modo que o retardo de desbloqueio não volte a bloquear até depois de a porta estar fechada.

Esta função é disponibilizada para fechaduras de tipo anti-alavanca e fechaduras magnéticas, etc, quando a porta tem de estar fechada antes de o relé de desbloqueio bloquear a porta.

O tempo de retardo de rebloqueio é o tempo entre o fecho da porta e a desactivação do relé de desbloqueio (rebloqueio). Isto permite um tempo de estabilização para garantir que os mecanismos de bloqueio estão alinhados.

8.5.2 Opções de DGP

```
1>Mapear relés
  127
```

O menu contém definições de controladores de portas.

8.5.2.1 Mapear relés

```
1 Mapear relés
  >Não<
```

Define se as saídas de desbloqueio de controlador de portas podem ser controladas como saídas padrão.

- Sim: As saídas de desbloqueio de porta podem ser controladas pelo painel de controlo como suas saídas.
- Não: As saídas de desbloqueio de porta só podem se activadas pelo controlador de portas ao utilizar o menu de utilizador de desbloqueio de porta, ou ao apresentar um cartão válido.

8.5.2.2 Mapear LED's Painel

```
2 Map LED Painel
  >Não<
```

Quando esta opção está definida como Sim, os LEDs nos leitores de porta ligados ao controlador de portas representarão o mesmo estado que os LEDs nos teclados ligados directamente ao painel.

8.5.3 Usa 27bitTecom

```
3 Usa 27bitTecom
  >Sim<
```

Quando a opção está definida para Sim, as credenciais de 27 bits apresentados nos leitores de bus de dados do sistema do painel serão identificados utilizando o cálculo do formato Tecom de 27 bits. Isto permite-lhe

utilizar credenciais compatíveis com os painéis de controlo ATS Master, bem como com os controladores de porta ATS125x e CDC4.

8.6 Opções de zona

```
1>Modo entrada
   Loop dupla
```

O menu Opções de zona define opções de entradas de zona.

8.6.1 Modo entrada

```
1 Modo entrada
  >Loop dupla<
```

A opção de modo de entrada determina a configuração das entradas de zona do painel. Podem ser configurados os seguintes valores:

- **Simple NO:** Em modo zona simples o painel só detecta alarme na zona. Em modo simples o estado normal depende do valor EOL. Se este valor for configurado como “Sem EOL” em “8.6.2 Resistência EOL” abaixo, o estado normal para zona Simple NO é aberto.
- **Simple NC:** Semelhante a Simple NO acima, mas se EOL for desactivado em “8.6.2 Resistência EOL” abaixo, o estado normal para a zona é o curto.
- **Loop dupla:** Para a loop dupla funcionar, cada zona necessita de duas ou três resistências EOL (fim de linha). Isto permite que o painel detecte vários estados de zona, incluindo alarme, tamper, máscara, etc, consoante o tipo de ligação e o valor de EOL definido em “8.6.2 Resistência EOL” abaixo. Consulte “Ligação das zonas” na página nº 25 para mais informações sobre a utilização de EOL.

No modo de loop dupla, o estado de circuito aberto ou curto origina tamper de zona.

Trata-se de uma definição apenas para painel. Para informações sobre expansores, consulte “2.2.2.n.4.5 Modo de input” na página nº 187.

8.6.2 Resistência EOL

```
2 EOL
   >4k7<
```

O menu permite definir valores da resistência de fim de linha. Para diferentes modos de entrada, podem estar disponíveis os valores seguintes: 1k0, 1k5, 2k, 2k2, 2k2+4k7, 3k3, 3k74, 4k7, 5k6, 6k8, 8k2, 10k, Sem EOL.

Nota: os valores de EOL disponíveis dependem da opção “8.6.1 Modo entrada” acima.

Consulte “Ligação das zonas” na página nº 25 para mais informações sobre a utilização de EOL.

Trata-se de uma definição apenas para painel. Para informações sobre expansores, consulte “2.2.2.n.4.6 EOL” na página nº 187.

8.6.3 Tamper Sir EOL

```
3 Tamper Sir EOL
  >4k7<
```

O menu EOL de tamper sirene permite definir o valor de uma resistência de fim de linha (EOL) para a sirene. Os valores de disponibilidade são descritos em “8.6.2 Resistência EOL” na página nº 302.

8.6.4 Swinger shunt

```
4 Swinger shunt
  > <
```

O valor do Swinger shunt define o número de alarmes de uma zona até ser inibida. O valor predefinido é 2; o valor máximo é 4.

Esta zona deve ter a opção “4.1.n.6.6 Swinger shunt” activada (consulte a página 215).

8.6.5 Restauro de reporte

```
5 Restauro Rep.
  >Não<
```

Se a opção de restauro de reporte estiver definida como “em RCO”, o evento de restauro é reportado à central receptora quando um utilizador reconhece um alarme, ou quando a zona volta ao estado normal.

8.6.6 Limitar relatórios

```
6 Limita relat.
  >120<
```

A opção é o tempo de inatividade (em segundos), que tem de decorrer após um alarme antes de o próximo alarme da mesma zona ser reportado à central recetora. Este tempo permite-lhe limitar o reporte de múltiplos alarmes a partir da mesma zona.

Nota: os alarmes a partir da mesma zona que ocorrem durante este tempo não são reportados, mas os eventos são guardados no registo. Cada novo alarme a partir desta zona reinicia o temporizador.

O intervalo permitido é 0 a 255 s. O valor predefinido é 120 s; 0 indica que o limite está desativado.

Consulte também “4.1.n.6.39 Limitar relatórios” na página nº 223.

8.7 Painel

```
1>Nome do painel
   Painel
```

O menu Painel permite alterar os valores definidos durante a instalação do sistema. Consulte também “Arranque inicial” na página 142.

Se determinadas definições forem alteradas neste menu, o sistema pede-lhe para confirmar essas alterações quando tentar sair do menu. Consulte “Confirmação de alterações” na página 139.

8.7.1 Nome do painel

```
1 Nome do painel
>Painel <
```

O menu Nome do painel permite alterar o nome do painel.

8.7.2 Idioma do painel

```
2 Idioma painel
   >PORTUGUES<
```

O menu Idioma do painel permite alterar o idioma do painel.

Cuidado: Alterações às opções de autorização seguintes causarão a eliminação de todos os PINs de utilizador e a definição de dois PINs padrão de dois utilizadores predefinidos. Consulte também “Arranque inicial” na página nº 142 e “Utilizadores predefinidos” na página nº 69.

8.7.3 Método coacção

```
3 Método coacção
   >Desactivado<
```

O menu Método de coacção permite alterar o método de introdução da coacção.

Nota: Se o Controlador da Porta CDC4 estiver ligado ao painel, a opção será só de leitura e o seu valor só pode ser alterado durante a instalação do painel. Consulte “Arranque inicial” na página 142 para obter mais informações.

Consulte o *Guia do Utilizador do Advisor Advanced* para obter mais informações sobre os métodos de coacção disponíveis.

8.7.4 Comprim. PIN

```
4 Comprim. PIN
   > <
```

O menu Comprimento do PIN permite alterar o comprimento do PIN. Para mais informações sobre PINs, consulte “3.1.n.2.1 Alterar PIN” na página nº 202.

Cuidado: Se o comprimento de PIN for alterado com o PIN remoto definido, o software de configuração não conseguirá voltar a conectar o painel com os dados programados. Consulte “3.1.n.2.2 PIN Remoto” na página nº 202 para obter mais informações.

8.7.5 Modo alt. PIN

```
5 Modo alt. PIN
>Configuráveis<
```

A opção Modo alteração de PIN permite escolher o modo apropriado de alteração do PIN. Consulte “PIN” na página nº 77, para obter mais informações sobre a utilização do PIN.

8.7.6 Confir. alarme

```
1>Modo AB
>>>
```

O menu Confirmação de alarme permite definir várias opções ligadas à verificação de alarmes.

8.7.6.1 Modo AB

```
1>Área 1
Desligado
```

A opção Modo AB permite a funcionalidade de confirmação de alarme AB para determinadas áreas. Quando definido como Ligado, o primeiro alarme é reportado como um alarme anti-roubo vulgar (Alarme A). Uma segunda entrada tem de gerar um alarme dentro de um determinado tempo para reportar um alarme confirmado (Alarme B), desde que o primeiro alarme na área não tenha ocorrido numa zona de entrada/saída.

O modo de verificação é programável por área.

8.7.6.2 Tempo AB

```
1>Tempo Alarm AB
1
```

O menu permite configurar o retardo máximo entre os alarmes A e B.

8.7.6.2.1 Tempo Alarm AB

```
1 Tempo Alarm AB
> <
```

O tempo máximo (0 a 255 minutos) que o sistema permite para que um segundo alarme de intrusão ocorra para reportar um alarme confirmado.

Se o segundo alarme ocorrer dentro deste tempo, é reportado como um alarme confirmado (Alarme B). Quando o tempo de AB expirar, qualquer novo alarme é novamente um alarme não confirmado (Alarme A). Se a zona que criou o alarme A inicial ainda estiver activa, é inibida.

8.7.6.2 Tempo Holdup AB

```
2 Tempo Holdup >
  > <
```

O tempo máximo (8 a 20 horas) que o sistema permite para que um segundo alarme de suspensão ocorra para reportar um alarme confirmado.

Consulte também “8.7.6.2.1 Tempo Alarm AB” na página nº 305.

8.7.6.3 Confirma.Sist

```
3 Confirma.Sist
  >Não<
```

A opção Confirmação do sistema define se a confirmação do alarme AB funciona apenas em áreas separadas, ou se permite uma validade a nível de todo o sistema. Se esta opção estiver definida como Sim, um alarme A de uma área pode ser confirmado por um alarme B de outra área. Caso contrário, o alarme A só pode ser confirmado por um alarme B da mesma área.

8.7.6.4 Confirmação EE

```
4 Confirmação EE
  >Não<
```

A opção Confirmação EE configura a confirmação de alarme AB durante o tempo de entrada.

Se a opção estiver definida como Sim, a confirmação de alarme é suspensa durante o tempo de entrada. Se não estiver presente nenhum alarme B, todos os alarmes durante o tempo de entrada são alarmes A. Quando o tempo de entrada expirar, a confirmação de alarme é activada. Contudo: as zonas de entrada/saída e zonas de acesso não podem gerar alarmes B.

Se esta opção estiver definida como Não, o início do temporizador de entrada desactiva qualquer confirmação de alarme até que a área esteja armada novamente.

8.7.6.5 EE inibido

```
5 EE inibido
  >Entrada/Saída<
```

A opção EE inibido define a funcionalidade da zona de acesso na área (se disponível) quando uma zona de entrada/saída (EE) é inibida no fim do tempo AB (função auto-inibir). São permitidos os seguintes valores:

- Entrada/Saída: uma zona de acesso actua como uma zona de entrada/saída, se a zona de entrada/saída estiver inibida.
- Acesso: uma zona de acesso não altera a sua funcionalidade e origina um alarme quando activado enquanto nenhum temporizador EE estiver em funcionamento.

8.7.6.6 Confirmação TA

```
6 Confirmação TA
  >Não<
```

Se a opção Confirmação TA estiver definida como Sim, o alarme de sabotagem (tamper) (TA) pode reportar um alarme anti-roubo (BA), e vice-versa.

8.7.6.7 Sirenes

```
1 Área 1
  >ALARME-A<
```

O menu Sirenes menu permite seleccionar por área quando a sirene é activada: no Alarme A ou no Alarme B.

Nota: a opção Alarme B só é válida se o modo AB estiver activado. Consulte “8.7.6.1 Modo AB” na página nº 305.

8.7.6.8 Ligar msg CRA

```
8 Ligar msg CRA
  >Não<
```

Se a opção Ligar para mensagem da central receptora estiver definida como Sim, em caso de alarme, o teclado apresenta uma mensagem com um aviso para o utilizador ligar para a central receptora quando um reporte tiver sido enviado.

8.7.6.9 Retardo Rep.

```
9 Retardo Rep.
  >Sim<
```

Activar um retardo de 30 segundos antes do reporte de alarme exigido pelos regulamentos ACPO.

8.7.7 Desarme Fácil

```
8 Desarme Fácil
  >Sim<
```

Se activado, pode desarmar instalações introduzindo um PIN ou passando um cartão válido sem premir outras teclas.

Nota: se a opção estiver definida para Sim, a opção de Apenas PIN para acesso à porta não é suportada. Consulte também “2.2.1.n.3.8.1 Modo cartão e PIN” na página 178.

8.7.8 Opções remoto

```
1>Config. Remota
  Sim
```

Defina as opções de configuração remota.

Consulte “Acesso remoto” na página nº 141 para obter mais informações.

8.7.8.1 Config. Remota

```
1 Config. Remota  
>Sim<
```

Se a opção estiver definida como Sim, os operadores remotos podem alterar os PINs e números de telefone de utilizadores quando as áreas estão armadas. Se definido como Não, os PINs e números de telefone de utilizadores só poderão ser alterados pelos operadores remotos quando todas as áreas estiverem desarmadas.

8.7.8.2 Config. superv.

```
2 Config. superv  
Sim
```

Se a opção estiver definida como Sim, o supervisor está autorizado a configurar o painel remotamente.

8.7.8.3 Acesso remoto

```
3 Acesso remoto  
>Qd ServiçoEm<
```

A opção define quando é que a configuração remota do sistema é permitida.

Estão disponíveis as seguintes opções:

- Nunca: O sistema não pode ser configurado remotamente.
- Sempre: O sistema pode ser configurado remotamente.
- Qd ServiçoEm: O sistema pode ser configurado remotamente apenas quando a função Assistência técnica está ativa.

8.7.9 Esquema Objeto

```
9 Esquema Objeto  
>Clássico<
```

Escolha um dos esquemas de numeração de objectos (zona, entrada, saída e porta) seguintes:

- Clássico. No esquema de numeração clássico, os identificadores de objecto predefinidos dependem da localização física das entradas ou saídas, por exemplo: Zona 1 é atribuída à entrada localizada no Painel 1.1, Zona 18 é atribuída à entrada localizada no Expansor 1.2.
- Flexível. No esquema de numeração flexível, os identificadores predefinidos são independentes. Ao adicionar um novo objecto, este é criado na primeira posição disponível da base de dados, independentemente da localização física específica da entrada ou saída.

Ao tentar alternar o esquema, é apresentada a confirmação.

Advertências

- A alteração do esquema de numeração requer a reinicialização do sistema. Posteriormente, os valores de eventos de reporte alterarão os números dos objectos de acordo com a nova numeração.
- Depois de alterar o esquema de clássico para flexível, todas as dependências de objecto programadas (por exemplo, filtros de condições, câmaras, etc.) ficarão indisponíveis. Os parâmetros aplicáveis serão definidos como “Não existe” em vez de objectos programados anteriormente até o esquema voltar a ser alterado.

Consulte também “Endereçamento de zonas, saídas e portas” na página nº 33 no Capítulo 2 “Instalação”.

8.8 Outro

```
1>Modo de pânico
  Silencioso
```

O menu PA e outros permite configurar o modo de alarme de pânico, o campainha, as opções de besouro, etc.

8.8.1 Modo de pânico

```
1 Modo de pânico
  >Silencioso<
```

O modo de pânico pode ser um dos seguintes.

- **Silencioso:** O alarme de pânico está silencioso (sem ativação de alarme sonoro). Até que o primeiro alarme de pânico seja restaurado, os subsequentes alarmes sem ser de pânico também são silenciosos.
Neste modo, a indicação de LED e LCD para o alarme de pânico também está desativada.
- **Al Pan silencioso:** O alarme de pânico está silencioso (sem ativação de alarme sonoro). Os alarmes subsequentes são audíveis.
- **Al Pan Sil sem eAl Son:** O alarme de pânico está silencioso (sem ativação de alarme sonoro). Até que o primeiro alarme de pânico seja restaurado, os subsequentes alarmes sem ser de pânico são audíveis só que os alarmes sonoros externos não são ativados.
- **Al Pan Sil sem Al Son:** O alarme de pânico está silencioso (sem ativação de alarme sonoro). Até que o primeiro alarme de pânico seja restaurado, os subsequentes alarmes sem ser de pânico são audíveis só que os alarmes sonoros não são ativados.
- **Audível:** O alarme de pânico é normal (com activação de sirene)
- **Alarme audível em caso de falha de linha:** O alarme de pânico é apenas audível se uma falha de linha (LF) ou uma falha de comunicação (FTC) estiver presente

8.8.2 Campanha

```
1>Campanha ArP
    Não
```

O menu Campanha permite definir as opções de campanha.

8.8.2.1 Campanha ArP

```
1 Campanha ArP
    >Não<
```

A opção Campanha em arme parcial define se a opção campanha está activa quando a área está em modo de arme parcial.

8.8.2.2 Campanha auto

```
2 Campanha auto
    >Sim<
```

Se a opção Campanha latched estiver definida como Sim, desactivar o campanha afecta apenas a funcionalidade de campanha até à próxima vez que a área for desarmada. Caso contrário, deverá ser activada manualmente.

8.8.3 TampSist áreas

```
3 TampSist áreas
    >12345678<
```

A opção Tamper áreas de sistema permite atribuir tampers do sistema e falhas às áreas especificadas. Tem de ser seleccionada pelo menos uma área.

8.8.4 Reactiv sirene

```
4 Reactiv sirene
    >Não<
```

Se existirem vários alarmes e a opção Reactivação de sirene estiver definida como Sim, a sirene externa é activada de cada vez que ocorre um alarme. Caso contrário, a sirene externa só é activada após o primeiro alarme.

8.8.5 Aprende cartão

```
1>Tec. aprender
2 Porta aprender
```

Selecione um keypad ou uma porta para a aprendizagem de cartões de utilizador. Consulte também “3.1.n.3 Cartão utilizador” na página nº 203.

8.8.5.1 Tec. aprender

```
1>RAS 1
2 RAS 2
```

Selecione um keypad para a aprendizagem de cartões de utilizador.

8.8.5.2 Porta aprender

```
1>Porta 1
2 Porta 2
```

Selecione uma porta para a aprendizagem de cartões de utilizador.

8.8.6 Testar zonas

```
6 Testar zonas
   >Tudo<
```

A opção Testar zonas define as entradas que devem estar acessíveis ao efectuar testes de entradas, conforme descrito em “1.2.1 Entradas teste” na página nº 149. Estão disponíveis as seguintes opções:

- Tudo: todas as entradas são visíveis.
- Se usado: Só são visíveis as entradas atribuídas às zonas existentes.

8.8.7 Modo besouro

```
7 Modo besouro
   >Contínuo<
```

O menu Modo besouro define a forma como o besouro funciona durante o tempo de saída. Estão disponíveis as seguintes opções:

- Contínuo: O besouro do teclado emite um sinal sonoro contínuo que muda para intermitente durante uma actividade de entrada/saída ou de acesso a zona.
- Intermitente: O besouro do teclado emite um sinal sonoro contínuo que muda para intermitente 10 segundos antes de expirar o tempo de saída.

8.8.8 Saída de mon. 3HC

```
8 Saída mon.3HC
   >Activado<
```

A 3ª opção saída de alta corrente monitorizada define se a saída de alta corrente 3 é ou não monitorizada.

O modo de saída 3 depende do modelo de painel. Consulte “Saídas” na página nº 32 para obter mais informações.

8.8.9 Nr. de cartão

```
9 Nr. de cartão
   >Básico<
```

Selecione a forma como o número do cartão é representado no painel de controlo.

- Básico. O número do cartão é representado no formato Advisor Advanced padrão.
- Titan. O número do cartão é representado no formato Titan estendido.

8.8.10 Reg. Anónimo

```
10 Reg. Anónimo
    > <
```

O menu permite definir um período de tempo após o qual os detalhes do utilizador são removidos de uma entrada de registo.

O intervalo permitido é 0 a 60 dias; 0 indica que a funcionalidade está desactivada. O valor predefinido é 0.

8.8.11 Segur. LEITOR

```
1>Modo seguro
    Ligado
```

O menu contém várias definições de modo seguro para dispositivos de segurança (keypad e leitores) no sistema de alarme.

Consulte Capítulo 3 “Funções do sistema > Segurança dos dados do cartão” na página nº 130 para obter mais informações.

8.8.11.1 Modo seguro

```
1 Modo seguro
    >Ligado<
```

Se definido como Ligado, os leitores de cartões funcionam no modo seguro. Neste modo, o utilizador do cartão é identificado pelos dados do smart card e não pelo número de série do cartão. Consulte também “Modo seguro” na página nº 130.

8.8.11.2 Chave Config.

```
2 Chave Config.
    > <
```

O menu permite definir a chave de encriptação do cartão de configuração.

A chave é composta por 16 números hexadecimais de dois dígitos (00 a FF).

Consulte “Segurança dos dados do cartão > Cartão de configuração” na página nº 131 para obter mais informações.

8.8.11.3 Chave App.

```
3 Chave App.
    > <
```

O menu permite definir a chave de encriptação do smart card.

A chave é composta por 16 números hexadecimais de dois dígitos (00 a FF).

8.8.11.4 Nome App.

```
4 Nome App.
    > <
```

O menu permite-lhe definir o nome da aplicação para os dados do smart card.

O nome é composto por 3 números hexadecimais de dois dígitos (00 a FF).
O valor predefinido é “55 54 43”.

Consulte “Nome da aplicação e ID do ficheiro” na página nº 130 para obter mais informações.

8.8.11.5 App.IDFicheiro

```
5 App.IDFicheiro
  > <
```

O menu permite-lhe alterar o número do ficheiro para a aplicação selecionada em “8.8.11.4 Nome App.” na página nº 312.

Consulte “Nome da aplicação e ID do ficheiro” na página nº 130 para obter mais informações.

8.8.11.6 ChaveResetTamp

```
6 ChaveResetTamp
  >Ligado<
```

Se a opção estiver definida como Ligado, todas as chaves de encriptação serão apagadas da memória do leitor quando ocorrer um alarme de tamper neste leitor.

Cuidado: se as chaves forem apagadas, o leitor terá de ser reinstalado.

8.8.11.7 Limit Bit Cart

```
7 Limit Bit Cart
  > <
```

A opção define se o comprimento do número do cartão é limitado. Estão disponíveis os seguintes valores:

- Sem limite: O comprimento do número do cartão não é limitado (valor padrão).
- 48 bits: O comprimento do número do cartão é limitado a 48 bits.

A opção só está disponível se o modo seguro estiver Desligado. É utilizado para retrocompatibilidade com modelos de leitores mais antigos.

8.8.11.8 Predefinição

```
8 Predefinição
  >Cancelar<
```

O menu permite restaurar todas as definições de modo seguro para os valores predefinidos.

Selecione OK e prima Enter para restaurar as predefinições do modo seguro.

Nota: após os valores terem sido restaurados, defina os seus próprios valores para proteger o seu sistema.

8.8.12 RAS LEDLaranja

```
12 RAS LEDLaran>  
>Falha<
```

O menu permite-lhe configurar a funcionalidade do LED do meio cor de laranja nos leitores e teclados semLCD. Estão disponíveis as seguintes opções:

- TdsZonasNormal: O LED do meio cor de laranja num teclado ou leitor sem LCD, fica aceso quando todas as zonas nas áreas atribuídas estão no estado normal.
- Falha: O LED cor de laranja está aceso em caso de falha do sistema.

8.8.13 Configuração no arme

```
13 ConfigEmArme  
>Não<
```

Se estiver definido para Sim, o sistema pode ser programado sem o desarmar.

Se definido para Não, o sistema tem de ser desarmado antes de poder configurá-lo.

Consulte também “Seleção de áreas” na página nº 135.

8.8.14 Reporte sirene

```
14 Reporte sire>  
>Falha (YA)<
```

A opção define a forma como a falha de sirene é reportada à central recetora. Estão disponíveis os seguintes valores:

- Falha (YA): A falha de sirene é reportada como uma falha
- Tamper (TA): A falha de sirene é reportada como um alarme de tamper

8.9 DesarmTemp/ATM

```
1>Retardo  
0
```

O menu permite configurar a interface da ATM (caixa multibanco automática).

8.9.1 Retardo

```
1 Retardo  
> <
```

O valor da opção é o tempo entre a primeira e a segunda introdução do código de utilizador da ATM. No final do período de retardo programado, o utilizador da ATM verá uma mensagem para inserir novamente o código.

O intervalo permitido é de 0 a 15 minutos. 0 significa que o código de utilizador da ATM pode ser inserido duas vezes sem qualquer retardo. O valor predefinido é 0.

8.9.2 Tempo Desarme

```
2 Tempo Desarme  
  > <
```

O tempo de desarme máximo permitido da ATM. O intervalo permitido é de 1 a 255 minutos.

8.9.3 Temp DesarmEst

```
Temp DesarmEst  
  > <
```

O tempo de desarme estendido máximo permitido da ATM. O intervalo permitido é de 0 a 255 minutos.

Nota: o utilizador pode prolongar o tempo de desarme apenas uma vez.

8.9.4 T.AvisoDesarme

```
4 T.AvisoDesarme  
  > <
```

O tempo de aviso é o tempo antes de terminar o tempo da ATM, quando é emitido um sinal de aviso.

O intervalo permitido é de 1 a 14 minutos, e o valor predefinido é 10 minutos.

9 Comunicação

```
1>Central Recept  
2 Opções eventos
```

O menu Comunicação é utilizado para programar opções de comunicação em todo o sistema.

9.1 Central Receptora

```
01>CRA 1  
02 CRA 2
```

O sistema Advisor Advanced permite programar até 16 centrais receptoras.

9.1.0 Adicionar CRA

Aceda ao menu para adicionar uma central receptora.

Se a central receptora for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES  
CRA adicionada
```

É atribuído à nova central receptora o nome predefinido de “CRA N” e é colocada no fim da lista de centrais receptoras.

Agora o utilizador pode começar a editar os detalhes da central receptora para a nova central receptora.

9.1.n Seleccionar a CRA

```
01>Nome CRA  
CRA 1
```

Selecione uma central receptora a programar.

Nota: as opções específicas deste menu diferem relativamente aos caminhos de transmissão específicos. Para ver opções específicas, consulte:

- “Opções específicas de RTPC e ISDN” na página nº 322
- “Opções espec. de IP e GSM/GPRS” na página nº 322
- “Opções específicas de fototransmissão” na página nº 324
- “Opções específicas de GSM/Telefone” na página nº 324
- “Opções de áudio específicas” na página nº 325
- “Opções específicas de UltraSync” na página nº 326
- “Opções específicas de VdS” na página nº 327

Opções comuns

9.1.n.1 Nome CRA

```
1 Nome CRA
>CRA 1 <
```

Utilize o ecrã Nome CRA para introduzir ou alterar o nome da central receptora. O nome da central receptora pode ser constituído por 16 caracteres.

9.1.n.2 Via de transm

```
1>RTPC
4 IP
```

O via de transmissao define o tipo de ligação para reportar alarmes à central receptora. Os caminhos podem ser definidos no menu “9.3 Opções de via” na página 328.

9.1.n.3 Protocolo

```
3 Protocolo
>(X)SIA<
```

Escolha o protocolo de comunicação aplicável.

Consoante as definições em “9.1.n.2 Via de transm” acima, podem estar disponíveis os seguintes protocolos:

- SIA
- (X)SIA
- VOZ
- CID
- OH+SIA
- OH+XSIA
- OH+CID
- TEXTO SMS
- SMS+CID
- SMS+SIA
- SMS+XSIA
- VOZ+SMS
- SMS+MMS
- OHPHOTO+CID
- OHPHOTO+SIA
- OHPHOTO+XSIA
- PHOTO+XSIA

O menu não está disponível para o caminho de comunicação UltraSync. Consulte “UltraSync” na página nº 126 para obter mais informações.

9.1.n.5 Contas

1>Área 1
Nada

Os números de conta identificam os reportes de sistemas de alarme às centrais receptoras. Os números de conta têm entre 4 e 6 dígitos (consoante o tipo de protocolo). Se configurado para Nenhum, o reporte da área seleccionada é desactivado.

Nota: quando se utilizam reportes de voz, são utilizados códigos de conta para identificar se os alarmes de uma área devem ser reportados. O código da conta não é transmitido.

Caso várias áreas tenham os mesmos números de conta, e se a opção “9.1.n.9 Relatório OP/CL” na página nº 321 estiver definida como Sim, é realizada uma operação especial para reportes SIA/XSIA de abertura/fecho, consoante a definição de modificação de área (consulte “9.1.n.8.1 XSIA”, na página 319).

- Modificação de área desligado: o fecho é reportado quando todas as áreas com o mesmo número de conta tiverem sido armadas. É reportada a última área a ser armada. A primeira a desarmar envia o sinal de abertura à área a abrir.
- Modificação de área ligada: os sinais de abertura e de fecho são reportados separadamente. A Modificação de área é utilizada para identificar a área correcta.

Nota: Eventos do sistema, assim como eventos da Área 1, são sempre reportados utilizando a Conta 1.

O menu não está disponível para o caminho de comunicação UltraSync. Consulte “UltraSync” na página nº 126 para obter mais informações.

9.1.n.5.m Selec. área

1 Área 1
> <

Defina números de conta para cada área.

9.1.n.6 Modo

6 Modo
>CRA Primária<

Estão disponíveis os seguintes modos para CRA:

- CRA primária: A central receptora primária deve receber incondicionalmente todos os eventos endereçados.
- CRA de backup: a central receptora pode ser uma central receptora de backup da central receptora anterior na lista de centrais receptoras (consulte “9.1 Central Receptora” na página nº 316). Isto significa que o painel só

reporta para esta central receptora se falhar o reporte para a central receptora primária.

Por exemplo, se CS 1 e CS 2 forem centrais receptoras primárias, e CS 3 e CS 4 forem centrais receptoras de backup, significa que a CS 1 não tem backup, CS 3 é uma central receptora de backup da CS 2, e CS 4 é uma central receptora de backup da central receptora 3.

Consulte “Princípios de reportes de alarme” na página nº 100 para obter mais informações.

9.1.n.7 Repetir contagem

```
7 Rep. contagem
    14<
```

O valor de Repetir contagem é o número de tentativas para efectuar uma chamada com êxito para a central receptora. Se o limite for alcançado, é gerada uma falha de comunicação (FTC).

O contador é repostado a zeros quando ocorre um novo evento em condição de FTC global. Consulte “Falha de comunicação (FTC)” na página nº 102 para obter mais informações.

O valor varia entre 0 e 14. O valor predefinido é 14.

9.1.n.8 Opç. protocolo

```
1> (X) SIA
2 VOZ
```

É possível personalizar os parâmetros do protocolo de comunicação utilizando o menu Opç. protocolo.

O menu não está disponível para o caminho de comunicação UltraSync. Consulte “UltraSync” na página nº 126 para obter mais informações.

9.1.n.8.1 XSIA

```
1>Modific. área
    Desligado
```

O menu XSIA permite definir as opções dos protocolos SIA e XSIA.

9.1.n.8.1.1 Modific. área

```
1 Modific. área
    >Desligado<
```

Se a opção Modificação de área estiver definida como Sim, a modificação de área é adicionada aos reportes SIA e XSIA. Isto permite enviar eventos de várias áreas utilizando o mesmo código de conta. Consulte também “9.1.n.5 Contas” na página 318.

9.1.n.8.1.2 Caract. nome

```
2 Caract. nome
   >16<
```

O valor de caracteres do nome define o comprimento das cadeias de nome utilizadas nos reportes XSIA.

Os valores permitidos são 16 e 30.

9.1.n.8.1.3 No. do evento

```
3 No. do evento
   >3 dígitos<
```

O valor de número do evento define o comprimento do campo do subevento (utilizador ou ponto).

Os valores permitidos são 2, 3 e 4 dígitos.

9.1.n.8.1.4 Codific.subev

```
4 Codific.subev
   >Decimal<
```

O valor de codificação de subeventos define se o número do subevento é reportado à central receptora em formato hexadecimal (hex) ou decimal.

9.1.n.8.1.5 Freq. SIA

```
5 Frequência SIA
   >Camp<
```

O menu Frequência SIA permite seleccionar uma de duas normas para comunicação de modem relativas às frequências de transmissão/recepção utilizadas pelo transmissor/receptor.

Esta opção permite seleccionar entre CCITT e BELL.

9.1.n.8.2 VOZ

```
1>Suprimir FTC
   Não
```

O menu VOZ permite configurar as opções de reporte de voz apresentadas a seguir.

9.1.n.8.2.1 Suprimir FTC

```
1 Suprimir FTC
   >Não<
```

Se a opção Suprimir FTC estiver definida como Sim, nenhuma falha FTC é activada para esta central receptora quando é utilizado o protocolo de voz.

Nota: se estiver a utilizar o módulo de voz ATS7200E, esta opção deve estar definida para Sim.

9.1.n.8.2.2 Sem confirmação

```
2 Sem REC
  >Não<
```

Se a opção Sem confirmação estiver definida como Sim, o destinatário de uma mensagem de voz não necessita de acusar a recepção da mensagem.

Caso contrário, tem de acusar a recepção premindo uma tecla do telefone, utilizando o modo de marcação por tons. O painel tenta retransmitir a mensagem até esta ser confirmada.

Nota: o módulo de voz AT57200E não suporta a função de reconhecimento de utilizador. se estiver a utilizar o AT57200E, esta opção deve estar definida como Sim.

9.1.n.9 Relatório OP/CL

```
9 Relat. OP/CL
  >Separado<
```

A opção Relatório OP/CL define se a abertura e fecho são reportados para todas as áreas com o mesmo código de conta, ou para cada uma delas separadamente. Estão disponíveis as seguintes opções:

- **Combinado:** quando todas as áreas com o mesmo código de conta são armadas, é reportado um fecho utilizando a área e o utilizador que a armou. É reportada uma abertura apenas quando a primeira das áreas com o mesmo código de conta é desarmada.
- **Separado:** é reportado um fecho e uma abertura para cada uma das áreas com o mesmo código de conta. A modificação da área indica a área em questão (consulte “9.1.n.8.1.1 Modific. área” na página nº 319).

Nota: quando o protocolo (X)SIA é seleccionado, os reportes separados apenas funcionam quando está activada a modificação de área SIA.

Consulte “9.1.n.5 Contas” na página nº 318 para obter mais informações.

O menu não está disponível para o caminho de comunicação UltraSync. Consulte “UltraSync” na página nº 126 para obter mais informações.

9.1.n.11 Apagar CRA

Para remover uma central receptora, seleccione a central receptora com o cursor, ou introduza o número da central receptora e aceda ao menu Apagar CRA.

O ecrã apresenta:

```
11 Apagar CRA
  >Cancelar<
```

Selecione OK e prima Enter. Isto remove a central receptora.

Repita o comando para eliminar outras centrais receptoras, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: não pode apagar uma central receptora, a menos que o seu grupo de utilizadores o autorize a fazê-lo.

Opções específicas de RTPC e ISDN

9.1.n.4 Telefone

```
4 Telefone
> <
```

Todas as centrais receptoras reportam para um número de telefone. O número de telefone pode conter até 20 dígitos. Estão disponíveis os seguintes caracteres especiais:

- P: pausa (3 s).
- T: a aguardar o sinal de marcação.

Nota: para introduzir um carácter, prima duas vezes a tecla correspondente.

Opções espec. de IP e GSM/GPRS

9.1.n.4 2. IP/Destino

```
1>Tipo
    Telef.
```

O menu de destino contém a configuração do receptor de reporte.

9.1.n.4.1 Nome dest

```
1 Nome destino
> <
```

Todas as centrais receptoras reportam para um endereço IP.

Um nome de destino pode ser um endereço IP numérico ou um endereço de domínio alfabético. Consulte também “Como editar um endereço host” na página nº 138.

9.1.n.4.2 Port destino

```
2 Port destino
> <
```

A porta de destino é utilizada para reportar ao host seleccionado em “9.1.n.4.1 Nome dest” acima.

9.1.n.4.3 Ping host

```
Pinging...
Tx/Rx: 2/2
```

O comando Ping host permite enviar um ping para a central receptora especificada. Este comando é utilizado para verificar se a central receptora está presente e se está acessível na rede a partir do painel.

O valor Tx/Rx indica o número de pacotes enviados e recebidos.

Nota: a estação de controlo pode ser configurada para não responder a pedidos de ping, portanto esta funcionalidade poderá não funcionar com todos os endereços IP de centrais receptoras. Para testar o caminho de comunicação, utilize o menu “1.2.7.n.2 Ping host” descrito na página nº 161 para enviar um ping a outro host.

9.1.n.8.3 OH2000

```
1>Versão
   OH V1.9.3
```

O menu OH2000 permite configurar algumas opções do protocolo OH2000 descritas a seguir.

9.1.n.8.3.1 Versão

```
1 Versão
   >OH V1.9.3<
```

Podem ser utilizadas para comunicação com o receptor Osborne-Hoffmans as seguintes versões do protocolo OH 2000:

- OH V1.9.3
- OH V2
- OH V3
- OH V3.1
- OH V4

Nota: A seleção da versão OH só está disponível se as seguintes opções estiverem definidas:

- 9.1.n.2 Via de transm: IP ou GSM/GPRS
- 9.1.n.3 Protocolo: OH+CID, OH+SIA, OH+XSIA, OHPHOTO+CID, OHPHOTO+SIA, OHPHOTO+XSIA

Para mais detalhes, consulte o manual do receptor apropriado.

9.1.n.8.3.2 Tempo de Heartbeat

```
2 Temp Heartbeat
   >00:00'01<
```

O Tempo de Heartbeat define a frequência com que o painel envia uma mensagem de presença (heartbeat) para a central receptora. O intervalo para este valor varia entre uma vez por segundo (00:00'01) e uma vez por dia (23:59'59). O valor máximo 23:59'59 significa que a funcionalidade heartbeat está desactivada.

9.1.n.8.3.3 Recetora nr.

```
3 Recetora nr.  
>0001<
```

Um identificador de receptor utilizado nas centrais receptoras com múltiplos receptores. O valor permitido é um número hexadecimal de 0001 a FFFF.

9.1.n.8.3.4 Linha nr.

```
4 Recetora nr.  
>0001<
```

Um identificador de linha utilizado nas centrais receptoras com múltiplas linhas receptoras. O valor permitido é um número hexadecimal de 0001 a FFFF.

9.1.n.8.3.5 Freq. tempo HB

```
5 Freq. tempo HB  
>00:01'00<
```

Se a comunicação com a CRA primária falhar, o tempo de heartbeat de CRA de backup é alterada de normal para frequente.

Consulte também “9.1.n.8.3.2 Tempo de Heartbeat” na página nº 323.

Opções específicas de fototransmissão

Além de “Opções espec. de IP e GSM/GPRS” descrito na página nº 322, é necessário definir as opções abaixo.

9.1.n.4.4 Encriptação

```
4 Encriptação  
>Não<
```

Se a opção Encriptação estiver definida como Sim, as imagens são enviadas encriptadas com o algoritmo AES.

9.1.n.4.5 Port dest vid

```
5 Port dest vid  
>9000<
```

A porta de destino é utilizada para enviar as imagens para um host configurado em “9.1.n.4.1 Nome dest” na página nº 322.

Opções específicas de GSM/Telefone

9.1.n.4 Destino

```
1>Tipo  
Telef.
```

O menu de destino contém a configuração do receptor de reporte.

9.1.n.4.1 Tipo

```
1 Tipo
  >Telefone<
```

O submenu Tipo define quem recebe os reportes dirigidos à central receptora especificada:

- **Telefone:** o reporte é enviado para um número de telefone especificado. O menu “9.1.n.4.2 Telefone/Utilizador/GU” abaixo configura este número de telefone.
- **Utilizador:** o reporte é enviado para um número de telefone especificado do utilizador. Este utilizador é seleccionado através do menu “9.1.n.4.2 Telefone/Utilizador/GU” abaixo.
- **Grupo de utilizadores:** o reporte é enviado para todos os utilizadores que pertencem ao grupo de utilizadores que é definido através do “9.1.n.4.2 Telefone/Utilizador/GU” abaixo.

Os reportes de utilizador e de grupo de utilizadores necessitam do seguinte:

- Os utilizadores devem ter os seus números de telefone definidos em “3.1.n.7.1 Telefone de utilizador” na página nº 206.
- Os reportes por SMS devem estar activados para estes utilizadores. Consulte “3.1.n.7.2 Reporte de SMS” na página nº 206.
- Pelo menos um dos grupos de utilizadores deve permitir que estes utilizadores recebam reportes por SMS. Consulte “3.2.n.6 Opções de GU” na página nº 210).

9.1.n.4.2 Telefone/Utilizador/GU

```
2 Telefone
  > <
```

Este menu depende do valor de Tipo que foi definido para o destinatário dos reportes. Consulte o menu “9.1.n.4.1 Tipo” acima para ver a descrição dos parâmetros.

Opções de áudio específicas

Estas opções estão disponíveis apenas para sistemas de áudio de duas vias. Consulte o Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123 para obter mais informações.

9.1.n.10 Listen-in

```
1>Activado
  Não
```

O menu permite-lhe configurar o áudio de duas vias para a central recetora seleccionada.

9.1.n.10.1 Activado

```
1 Activado
   >Não<
```

Se definido como Sim, o áudio de duas vias é ativado quando reporta à central recetora selecionada.

9.1.n.10.2 Tempo

```
2 Tempo
   >120<
```

A opção configura a duração máxima (em segundos) da sessão de áudio de duas vias. Após este tempo, a sessão termina automaticamente.

O intervalo permitido é 0 a 255 s; 0 indica que a sessão não inicia.

O tempo pode ser estendido utilizando o tom DTMF.

9.1.n.10.3 Controlo DTMF

```
1>DTMF 1
   Desativado
```

O menu permite-lhe configurar comandos DTMF que são utilizados pelo operador da central recetora para controlar a sessão de áudio de duas vias.

Primeiro, selecione o tom DTMF desejado a partir da lista. A seguir, atribua um comando ao tom selecionado.

Os tons e comandos disponíveis estão listados no Capítulo 3 “Funções do sistema > Controlo DTMF” na página nº 124.

Opções específicas de UltraSync

9.1.n.4 Número do canal

```
4>Nr. canal
   1
```

Os ecrãs de informação contêm o número do canal utilizado para a ligação à “cloud” UltraSync. O canal está configurado no portal Web UltraSync. Este configura definições como o formato de reporte, o número de conta e o tempo de polling.

Cuidado: quando o painel está registado na “cloud” UltraSync, todo o reporte de segurança da “cloud” é configurado remotamente a partir da “cloud”.

Consulte o Capítulo 3 “Funções do sistema > UltraSync” na página nº 126 para obter mais informações sobre a ligação à nuvem.

Opções específicas de VdS

9.1.n.8.4 VdS

```
1>Versão
    VdS 2465
```

O menu contém várias opções de relatório VdS descritas em baixo.

9.1.n.8.4.1 Versão

```
1 Versão
    >VdS 2465<
```

Selecione uma das versões do protocolo VdS suportadas no painel de controlo.

9.1.n.8.4.2 Nr.Chave Enc.

```
2 Nr.Chave Enc.
    > <
```

Selecione o número da chave de encriptação para a encriptação do protocolo VdS.

O número é usado para identificação na estação central.

0 significa que não foi aplicada encriptação.

9.1.n.8.4.3 Valor Chave Enc.

```
3 Valor Chave E>
    >0000000000000000<
```

Defina o valor para a chave de encriptação selecionada utilizada para encriptação do protocolo VdS.

9.2 Opções de eventos

```
1>Mapeamento CRA
2 Mapeamento voz
```

O menu Opções de eventos contém as opções dos eventos.

Para mais detalhes sobre reportes de eventos, consulte “Princípios de reportes de alarme” na página nº 100.

9.2.1 Mapeamento CRA

```
01>AN Reportar >
    >1234.....<
```

O menu Mapeamento CRA permite mapear eventos de reporte para as centrais receptoras específicas.

A lista de eventos é apresentada em Anexo A “Eventos do Advisor Advanced” na página 379.

9.2.2 Mapeamento voz

```
01>AN Número da>  
0
```

O menu Mapeamento de voz permite atribuir uma determinada mensagem de voz (0 a 14) a cada evento do sistema. 0 significa que nenhuma mensagem está atribuída.

A lista de eventos é apresentada no Anexo A “Eventos do Advisor Advanced” na página 379.

9.2.3 Eventos retardados

```
00>Temp. Retardo  
0
```

O menu Eventos retardados permite definir um retardo para determinados eventos.

A primeira entrada do menu, 0 Temp. Retardo, permite definir o retardo de reporte global entre 0 e 250 seg.

As entradas de menu seguintes representam os eventos particulares. Se a opção estiver definida como Ligado, o retardo é aplicado.

```
01>AN Retardado  
Desligado
```

Para a lista de eventos, consulte o Anexo A “Eventos do Advisor Advanced” na página 379.

9.2.4 L-in Eventos

```
001>AN L-in  
Desligado
```

O menu permite-lhe seleccionar eventos que ativam uma sessão de áudio de duas vias com uma central recetora.

Para ver a lista de eventos, consulte “Eventos do Advisor Advanced” no Anexo A, na página 379.

Consulte o Capítulo 3 “Funções do sistema > Áudio de duas vias” na página nº 123 para obter mais informações.

9.3 Opções de via

```
1>RTPC  
4 IP
```

O menu Opções de via permite configurar as opções dos caminhos de transmissão disponíveis.

9.3.n Seleccionar via

```
1>Nome via
      RTPC
```

Selecione o caminho de transmissão apropriado para configurar as respectivas opções.

Os caminhos de transmissão disponíveis dependem da configuração do sistema. Por predefinição, estão disponíveis os seguintes caminhos de transmissão:

- IP

Consoante a configuração do hardware, poderão também estar disponíveis os seguintes caminhos de transmissão:

- RTPC
- ISDN
- GSM
- TDA74xx
- UltraSync

Nota: as opções específicas deste menu diferem relativamente aos caminhos de transmissão específicos. Para ver opções específicas, consulte:

- “Opções específicas de PSTN” na página nº 331
- “Opções específicas de ISDN” na página nº 332
- “Opções específicas do IP” na página nº 332
- “Opções espec. de GSM/SMS/GPRS” na página nº 335

Opções comuns

9.3.n.1 Nome

```
1 Nome via
      >RTPC<
```

Utilize o ecrã Nome via para introduzir ou alterar o nome do caminho de transmissão. O nome pode ser constituído por até 16 caracteres.

9.3.n.2 Falha de linha

```
2 Falha de linha
      >Sempre<
```

Se a opção Falha de linha estiver definida como Sempre, a linha é testada relativamente a falhas de linha. Se estiver presente uma falha de linha, é gerada uma falha no sistema.

Se a falha de linha for configurado como “Se usado”, a linha é testada somente se o caminho for utilizado para comunicação para qualquer central receptora, e o código de cliente para esta central for configurado.

Nota: as opções seguintes deste menu diferem relativamente aos caminhos de transmissão específicos.

9.3.n.3 Retardo FL

```
3 Retardo FL
  >0<
```

O retardo de falha de linha define o período de tempo após o qual o caminho da falha é reportado à central recetora. Se a falha for restaurada antes de expirar este período de tempo, a falha não é reportada.

O intervalo permitido é de 0 a 255 segundos.

9.3.n.4 Menu DGP

```
4 Menu DGP
  >>>
```

Comunicadores específicos têm os seus menus internos. Aceda ao menu Expansor para definir as opções de comunicador interno.

O conteúdo do menu depende do equipamento.

9.3.n.8 Config. Toque

```
1 N.º de toques
2 OmiteChamada1
```

O menu contém opções de configuração de número de toques.

Nota: esta opção não está disponível para ligação IP.

9.3.n.8.1 N.º de toques

```
7 No. de toques
  > <
```

O ecrã Número de toques permite introduzir o número de toques antes de atender uma chamada recebida. O intervalo permitido é de 1 a 15. O número mais elevado é igual a infinito, pelo que as chamadas recebidas nunca são atendidas.

9.3.n.8.2 OmiteChamada1

```
2 OmiteChamada1
  >Não<
```

Utilize esta opção ao partilhar uma linha telefónica com outro equipamento (por exemplo, um fax ou um gravador de chamadas) que atenda automaticamente chamadas a entrar.

Se definido como Sim, o painel desliga após o número de toques programado em “9.3.n.8.1 N.º de toques” acima, e atende imediatamente a segunda chamada a entrar recebida no espaço de 30 segundos após a primeira chamada.

Se definido como Não, o painel atende após o número de toques programado em “9.3.n.8.1 N.º de toques”.

9.3.n.9 Encriptação

9 Encriptação
>Não<

Se a opção Encriptação estiver definida como Sim, a comunicação é encriptada com o algoritmo AES.

A chave da encriptação é definida utilizando o menu “9.4.3 Código de encriptação” na página nº 347.

Nota: a ligação de IP está sempre encriptada. Uma comunicação USB não utiliza encriptação.

Opções específicas de PSTN

9.3.n.4 Via de transm

3 Via transm
RTPC

A opção Via de transmissão é um campo só de leitura que identifica o método de comunicação utilizado para este caminho de transmissão.

9.3.n.5 Tom de chamada

5 Tom de chamada
>Predefinido<

O menu Tom de chamada permite escolher o tom de marcação apropriado para caminhos RTPC.

Pode seleccionar uma das seguintes opções de tom de marcação:

- Nenhum
- Predefinido (CTR21)
- Reino Unido
- Outro (Países Baixos)

9.3.n.6 Marcação

6 Marcação
>DTMF<

O menu Marcação permite seleccionar o modo de marcação RTPC: impulsos ou tons (DTMF).

Opções específicas de ISDN

9.3.n.6 Ponto a Ponto

```
6 Ponto a Ponto
  >Não<
```

A opção deve ser definida como Sim se o comunicador RDIS utiliza comunicação ponto a ponto, caso contrário deve ser definida como Não.

Contacte o seu fornecedor RDIS para obter mais informações sobre o serviço.

9.3.n.7 MSN

```
7 MSN
```

A opção MSN permite introduzir o número MSN ISDN.

Opções específicas do IP

9.3.n.4 Via de transm

```
4 Via transm
  ETHERNET
```

A opção Via de transmissão é um campo só de leitura que identifica o método de comunicação utilizado para este caminho de transmissão.

9.3.n.5 Config. IP

```
1>Config. IP
  Dinâmico
```

O menu Config IP permite configurar o endereço IP do painel.

Neste menu são configuráveis as seguintes opções.

9.3.n.5.1 Config. IP

```
1 Config. IP
  >Dinâmico<
```

Se a opção Config. IP estiver definida como Dinâmico, o DHCP está activado. Se este valor for Estático, tem de configurar as outras opções deste menu que são descritas a seguir.

9.3.n.5.2 Endereço IP

```
2 Endereço IP
  >000.000.000.00>
```

Se o DHCP estiver desactivado, terá de definir o endereço IP antes de utilizar a comunicação IP. Se o DHCP estiver activado no menu “9.3.n.5.1 Config. IP” acima, este valor indica o endereço IP dinâmico que é atribuído pelo servidor DHCP e que não pode ser alterado.

9.3.n.5.3 Subnet mask

```
3 Subnet mask
>255.255.255.00>
```

Se o DHCP estiver desactivado, tem de definir a máscara de subrede IP do painel antes de utilizar o protocolo de comunicação OH 2000. Se o DHCP estiver activado no menu “9.3.n.5.1 Config. IP” na página nº 332, este valor indica a máscara de subrede IP dinâmica, que não pode ser alterada.

9.3.n.5.4 Gateway

```
4 Gateway
>000.000.000.00>
```

Se o DHCP estiver desactivado, tem de definir o endereço IP da gateway antes de utilizar o protocolo de comunicação OH 2000 numa WAN. Se o DHCP estiver activado no menu “9.3.n.5.1 Config. IP” na página nº 332, este valor indica o endereço gateway dinâmico, que não pode ser alterado.

9.3.n.6 Config.DNS

```
1>Config.DNS
  Estático
```

Se utilizar nomes de domínio para os reportes Ethernet, o servidor DNS tem de ser configurado.

Neste menu são configuráveis as seguintes opções.

9.3.n.6.1 Config.DNS

```
1 Config.DNS
  >Estático<
```

Se a configuração do IP no menu “9.3.n.5 Config. IP” na página nº 332 estiver definida como Dinâmico (DHCP está activado), pode definir a opção de configuração do DNS para Estático, para substituir a configuração automática do DNS pelo servidor DHCP. Defina o endereço DNS no menu a seguir. Se esta opção for definida como Dinâmico, o DHCP é utilizado para obter o endereço IP do DNS.

Se o DHCP estiver desactivado, este menu não está disponível.

9.3.n.6.2 Servidor DNS

```
2 Servidor DNS
>000.000.000.00<
```

O menu Servidor DNS permite definir o endereço DNS se este for diferente do endereço fornecido pelo servidor DHCP, ou se DHCP estiver desactivado no menu “9.3.n.5.1 Config. IP” na página nº 332.

9.3.n.7 Config. NTP

```
1>Config. NTP
  Estático
```

O menu Config. NTP é utilizado para configurar o servidor NTP (Network Time Protocol - Protocolo de tempo de rede).

Neste menu são configuráveis as seguintes opções.

9.3.n.7.1 Config. NTP

```
1 Config. NTP
  >Estático<
```

Se a configuração do IP no menu “9.3.n.5 Config. IP” na página nº 332 estiver definida como Dinâmico (DHCP está activado), pode definir a opção de configuração do NTP para Estático, para substituir a configuração automática do NTP pelo servidor DHCP. Defina o endereço NTP no menu a seguir. Se esta opção for definida como Dinâmico, o DHCP é utilizado para obter o endereço IP do NTP.

Se o DHCP estiver desactivado, este menu não estará disponível.

9.3.n.7.2 Servidor NTP

```
2 Servidor NTP
>000.000.000.00<
```

O menu Servidor NTP permite definir o endereço NTP se este for diferente do endereço fornecido pelo servidor DHCP, ou se DHCP estiver desactivado no menu “9.3.n.5.1 Config. IP” na página nº 332.

9.3.n.8 Firewall

```
1>Firewall
  Ligado
```

O menu Firewall é utilizado para configurar a firewall incorporada. A firewall permite apenas comunicações de hosts que estão configurados como ligações de PC apropriadas em “9.4.1.n.4 IP/Destino” na página nº 348.

Neste menu são configuráveis as seguintes opções.

9.3.n.8.1 Firewall

```
1 Firewall
  >Ligado<
```

Utilize o menu Firewall para activar (Ligado) ou desactivar (Desligado) a firewall incorporada.

9.3.n.8.2 Resposta PING

```
2 Resposta PING
  >Não<
```

A opção Resposta PING define se a firewall permite responder a pedidos de ping. Se esta opção estiver definida como Não, os pedidos de ping não são respondidos.

9.3.n.10 Endereço MAC

```
10>Endereço MAC
  0051DB3D7E73
```

O endereço MAC do controlador Ethernet é um valor só de leitura.

9.3.n.11 Foto max. 24h

```
11 Foto max. 24h
  > <
```

Pode limitar o número máximo de imagens enviadas via GPRS ou IP para utilizadores, durante um período de 24-horas.

Se o limite for alcançado, os futuros pedidos de imagens são negados pelo sistema, sendo registado na memória o evento apropriado.

Não existe limite de imagens se este valor for colocado a 0.

9.3.n.12 WAN LF

```
12 WAN LF
  >Ligado<
```

Se a opção estiver definida para Ligado, a comunicação IP WAN com UltraSync é testada. Se existir uma falha de linha, é gerada uma falha WAN no sistema.

Opções espec. de GSM/SMS/GPRS

9.3.n.4 Via transm

```
4 Via transm
  ETHERNET
```

A opção Via de transmissão é um campo só de leitura que identifica o método de comunicação utilizado para este caminho de transmissão.

9.3.n.5 Config. GSM

```
1>PIN cartão SIM
  0000
```

O menu Config. GSM permite configurar o controlo e reporte GSM.

Notas

- Antes de utilizar o cartão SIM no sistema, insira-o num telemóvel e veja se é válido, verifique o crédito e envie uma mensagem SMS de teste.
- Antes de substituir o cartão SIM, apague o número do centro de SMS. Caso contrário, o sistema irá substituir o número predefinido do centro SMS no novo cartão por este número. Consulte “9.3.n.6.1 N. Centro SMS” na página nº 340 para obter mais informações.

9.3.n.5.1 PIN cartão SIM

```
1 PIN cartão SIM
   >0000<
```

O menu PIN cartão SIM permite configurar o PIN do cartão SIM.

Este menu também pode mostrar as seguintes mensagens:

- Necessário PUK!
- Disp.1 tent.!

Para uma explicação mais detalhada destas mensagens, consulte “1.2.8.1 Estado PIN” na página nº 162.

Este menu não tem qualquer funcionalidade se o PIN não for necessário para este cartão SIM.

9.3.n.5.2 Redes

```
1>Seleccção rede
   Automático
```

O menu Redes permite configurar as definições de rede GSM.

9.3.n.5.2.1 Seleccção rede

```
1 Seleccção rede
   >Automático<
```

O menu Seleccção rede permite definir a rede GSM de preferência. Introduza o código numérico da rede GSM. Se o código não for introduzido, a rede é escolhida automaticamente.

9.3.n.5.2.2 Selec. só rede

```
2 Selec. só rede
   >Não<
```

Se a opção Selec. só rede estiver definida como Sim, apenas a rede seleccionada em “9.3.n.5.2.1 Seleccção rede” acima é autorizada para a comunicação. De outra forma, se a rede configurada não estiver disponível, o sistema seleccionará automaticamente outra rede.

9.3.n.5.2.3 Procurar rede

```
0>Nova proc.rede
1 * MyGSM
```

O menu Procurar rede apresenta uma lista de todas as redes disponíveis. Também permite forçar outra procura.

A lista contém os nomes das redes GSM, os quais são precedidos por uma das seguintes marcas que definem a disponibilidade da rede:

- *: A rede está actualmente ligada.
- +: A rede é permitida para ligação.
- -: A rede é proibida para ligação.

Se o nome da rede for desconhecido (não reconhecido pelo comunicador GSM), o código da rede entre parênteses rectos é indicado em vez do nome, por exemplo, "+ [20999]".

9.3.n.5.2.3.0 Nova proc.rede

```
A procurar
Aguarde
```

O comando Nova proc.rede efectua uma procura de rede GSM.

A procura poderá demorar uns minutos. Pode cancelar a procura premindo Sair.

9.3.n.5.2.3.m Selec.uma rede

```
1>Nome da rede
MyGSM
```

Seleccione uma rede para ver mais opções.

9.3.n.5.2.3.m.1 Nome da rede

```
1>Nome da rede
MyGSM
```

O Nome da rede é o nome da rede GSM. Para mais informações, consulte "1.2.8.6 Nome da rede" na página nº 163.

9.3.n.5.2.3.m.2 Código de rede

```
2>Código de rede
21999
```

O Código de rede é o código exclusivo da rede GSM. Para mais informações, consulte "1.2.8.7 Código de rede" na página nº 163.

9.3.n.5.2.3.m.3 Disponibilidade

```
3>Disponibilidad
Ligado
```

Os valores de disponibilidade são descritos em "9.3.n.5.2.3 Procurar rede" acima.

9.3.n.5.2.3.m.4 RSSI

```
4>RSSI
-35 dBm [IIII ]
```

O valor da indicação da intensidade do sinal recebido (RSSI - Received Signal Strength Indication) é uma informação de diagnóstico. Para mais informações, consulte “1.2.8.8 RSSI” na página nº 163.

9.3.n.5.2.3.m.5 Usar esta rede

```
5>Usar esta rede
-----
```

Aceda ao menu Usar esta rede para estabelecer ligação à rede GSM seleccionada. Isto substitui a rede seleccionada em “9.3.n.5.2.1 Selecção rede” na página nº 336.

9.3.n.5.3 Crédito

```
1>Verificar já
>>>
```

O menu Crédito permite configurar e efectuar a verificação da conta GSM.

9.3.n.5.3.1 Verificar já

```
1>Verificar já
>>>
```

O menu Verificar já permite verificar manualmente a sua conta GSM. Quando recebido, o estado da conta é apresentado no ecrã LCD.

Para que isto seja possível, a verificação do crédito tem de ser configurada nos menus descritos a seguir.

9.3.n.5.3.2 Verificar modo

```
2 Verificar modo
>Normal<
```

Dependendo da rede GSM, o crédito pode ser verificado de diferentes formas. Estão disponíveis os seguintes modos:

- Normal: o crédito é verificado quando o operador é contactado, utilizando o código de pedido. Este modo é utilizado pela maioria dos operadores.
- Mensagem SMS: o crédito é verificado através do envio de uma mensagem SMS pré-definida, para o número descrito em “9.3.n.5.3.3 Verificar no.” na página nº 339.

9.3.n.5.3.3 Verificar no.

```
3 Verificar no.
  >+48600000000<
```

O numero de verificação é um contacto para onde são enviadas as mensagens SMS de verificação de crédito, se este modo tiver sido seleccionado no menu “9.3.n.5.3.2 Verificar modo” na página nº 338.

9.3.n.5.3.4 Pedir código

```
4 Pedir código
  > <
```

O código para a verificação da conta tem de ser configurado neste menu. Pode introduzir números, bem como os caracteres “*” e “#” (por exemplo, *101#). Contacte o seu operador GSM para saber como verificar a sua conta.

9.3.n.5.3.5 Verif. período

```
5 Verif. período
  > <
```

O valor de Verif. período (em dias) define a frequência com que o sistema verifica automaticamente a sua conta.

Nota: quando o sistema efectua uma verificação automática da conta, a resposta é tratada como um SMS de uma origem não autorizada e, por conseguinte, é reencaminhada para o supervisor. Certifique-se de que a opção “9.3.n.6.2 Reenvio de SMS” na página nº 340 está activada, caso contrário a resposta do estado da conta perde-se.

9.3.n.5.3.6 Verif. tempo

```
6 Verif. tempo
  >12:00<
```

O valor Verif. tempo é a hora do dia no formato de 24 h em que o sistema efectua a verificação automática da conta descrita em “9.3.n.5.3.5 Verif. período” acima.

9.3.n.5.4 Det.Empast.

```
1>Det.Empast.
  Desligado
```

O menu permite configurar os parâmetros de detecção de empastelamento do GSM.

9.3.n.5.4.1 Det.Empast.

```
1 Det.Empast.
  >Desligado<
```

Se definido como Ligado, o painel emite um alarme de tamper quando é detectado o empastelamento do GSM.

Nota: o marcador deve suportar a funcionalidade de detecção de empastelamento. A detecção é suportada no marcador GSM AT57310 com a versão de firmware V01.08 ou posterior.

9.3.n.5.4.2 Thresh.Empast.

```
2 Thresh.Empast.  
>20<
```

Configure o limiar para reporte de detecção de empastelamento. O intervalo permitido é de 1 (-111 dBm) a 31 (-51 dBm). O valor predefinido é 20 (-73 dBm).

9.3.n.6 Config. SMS

```
1>N. Centro SMS  
Nada
```

O menu Config. SMS permite alterar várias definições SMS.

9.3.n.6.1 N. Centro SMS

```
1 N. Centro SMS  
> <
```

O N. Centro SMS é o número de acesso ao serviço SMS.

Se este valor estiver vazio, o sistema utiliza o número predefinido armazenado no cartão SIM. Utilize este menu para introduzir um número diferente do número predefinido do fornecedor.

Cuidado: apague este número antes de substituir o cartão SIM. Caso contrário, o sistema irá substituir o número predefinido do centro SMS no novo cartão por este número.

9.3.n.6.2 Reenvio de SMS

```
0>Desligado  
-----
```

O menu Reenvio SMS permite escolher o número de telefone para o qual todas as mensagens não reconhecidas são reencaminhadas (geralmente o telefone do supervisor ou do administrador). Também pode desactivar o reencaminhamento de SMS com este menu.

A lista contém apenas os utilizadores que:

- Possuem os privilégios aplicáveis para receber mensagens SMS (consulte “3.2.n.6 Opções de GU” na página nº 210)
- Têm os seus números de telefone configurados (consulte “3.1.n.7.1 Telefone de utilizador” na página nº 206)

9.3.n.6.3 Máx. Msg 24h

```
3 Máx Msg 24h
  > <
```

Pode limitar o número máximo de mensagens SMS enviadas a utilizadores durante um período de 24 horas. Se esse limite for alcançado, as mensagens adicionais recebidas são ignoradas pelo sistema.

Os reportes SMS e os comandos SMS não reconhecidos têm dois contadores separados. No entanto, o limite máximo definido neste menu é o mesmo para ambos os contadores.

Se este valor for definido como 0, não há limite de mensagens.

9.3.n.6.4 Cabeçalho SMS

```
4 Cabeçalho SMS
  > <
```

O Cabeçalho SMS identifica o sistema Advisor Advanced. Está incluído no princípio de cada mensagem de texto SMS enviada pelo sistema, se o formato dos reportes estiver definido como texto SMS. Consulte “9.1.n.3 Protocolo” na página nº 317.

9.3.n.6.5 PIN Util. Req

```
5 PIN Util.Req
  >Não<
```

Se a opção PIN Util. Req estiver definida como Sim, terá de iniciar todas as mensagens de controlo por SMS com o seu PIN, caso contrário o comando será rejeitado. Para mais informações, consulte o *Guia de Referência do Controlo por SMS do Advisor Advanced*.

9.3.n.6.6 Ext.Caracteres

```
6 Ext.Caracteres
  >Não<
```

A opção Ext.Caracteres (UCS2) tem influência nas mensagens SMS enviadas pelo sistema Advisor Advanced ao utilizador. Esta opção tem de ser definida como Sim para se poder ler respostas e reportes SMS com caracteres especiais e nacionais que excedem o conjunto de caracteres GSM padrão GSM3.38.

Notas

- O conjunto de caracteres alargado é utilizado apenas se não for possível enviar a mensagem utilizando o conjunto de caracteres padrão.
- Os telemóveis mais antigos poderão não apresentar correctamente as mensagens que utilizam o conjunto de caracteres alargado.

9.3.n.7 Config. GPRS

```
1 Nome APN
    Nada
```

O menu de configuração de GPRS permite alterar várias definições de GPRS.

9.3.n.7.1 Nome APN

```
1 Nome APN
> <
```

O nome do ponto de acesso (APN) é um identificador de rede configurável utilizado pelo dispositivo móvel quando liga a uma operadora GSM. Deve ser especificado pelo fornecedor de GPRS.

9.3.n.7.2 Nome de utilizador

```
2 Nome Utiliza.
> <
```

O nome de utilizador deve ser especificado pelo fornecedor de GPRS.

9.3.n.7.3 Password

```
3 Password
> <
```

A password de utilizador deve ser especificada pelo fornecedor de GPRS.

Nota: os menus de configuração GPRS seguintes são iguais ao menu de configuração IP, excepto que só se aplicam a ligação IP via caminho GPRS.

9.3.n.7.4 Config. IP

Consulte “9.3.n.5 Config. IP” na página nº 332.

9.3.n.7.5 Config. DNS

Consulte “9.3.n.6 Config.DNS” na página nº 333.

9.3.n.7.6 Firewall

Consulte “9.3.n.8 Firewall” na página nº 334.

9.3.n.7.7 Falha de linha

```
8 Falha de linha
    >Não<
```

Se a opção de Falha de linha estiver configurada como SIM, a linha é verificada para detectar falhas de linha. Se estiver presente uma falha de linha, é gerada uma falha no sistema.

9.3.n.7.8 Tempo desligar

```
9 Tempo desligar
  >02:00<
```

A ligação é automaticamente encerrada quando não são enviados dados durante o tempo de desligar. A ligação é reinicializada quando necessário.

O tempo mínimo de desligamento é de 5 minutos. Se o tempo for definido como 23:59 ou mais, muda para infinito. Neste caso a ligação nunca é encerrada.

Cuidado: se o sistema receber pedidos de um PC a entrar através de GPRS, o tempo de desligamento deve ser definido como infinito para que a ligação se mantenha sempre aberta.

Nota: A opção não é utilizada quando a ligação UltraSync se encontra habilitada.

9.3.n.7.9 Max. Fotos 24h

Consulte “9.3.n.11 Foto max. 24h” na página nº 335.

9.3.n.10 Configuração de MMS

```
1>MMS center
  Nenhum
```

O menu permite configurar várias definições de MMS.

Nota: contacte o seu fornecedor de GSM para obter informações sobre todas as definições deste menu.

9.3.n.10.1 MMS Center

```
1 MMS center
  > <
```

O número de central de MMS é o endereço do serviço de MMS.

9.3.n.10.2 APN

Consulte “9.3.n.7.1 Nome APN” na página nº 342 para obter mais informações.

9.3.n.10.3 Nome de utlz

Consulte “9.3.n.7.2 Nome de utilizador” na página nº 342 para obter mais informações.

9.3.n.10.3 Password

Consulte “9.3.n.7.3 Password” na página nº 342 para obter mais informações.

9.3.n.10.5 Proxy

```
5 Proxy
  > <
```

Introduza o endereço de servidor proxy MMS.

9.3.n.10.6 Porta proxy

```
6 Porto MMS  
> <
```

Introduza o número de porta de servidor proxy do servidor proxy configurado em “9.3.n.10.5 Proxy” na página nº 343.

9.3.n.10.7 Máx MMS 24h

```
7 Máx MMS 24h  
> <
```

Pode limitar o número máximo de MMS enviados a utilizadores através de GPRS durante um período de 24 horas.

Se o limite for alcançado, o sistema recusará mais pedidos de MMS e será registado um evento apropriado no registo.

Nota: esta definição afecta apenas um ciclo de arme/desarme. Quando uma área muda de estado, por exemplo, se estiver a ser definida, o contador é repostado.

Não existe um limite de MMS se este valor for definido como 0.

9.3.n.11 Info módulos

```
1>Versão módulo  
731000V01
```

Os ecrãs informativos contêm a versão de firmware do comunicador GSM, tipo de modem, etc.

9.4 Ligação de PC

```
1>Ligações  
>>>
```

Uma ligação de PC pode ser utilizada para:

- Upload / download (U/D)
- Gestão
- Controlo à distância

O menu Ligação de PC permite definir os parâmetros de ligação do PC.

9.4.1 Ligações

```
0>Adic.Ligação >  
1 Ligação PC 1
```

É possível definir até 16 ligações de PC diferentes.

9.4.1.0 Adic. ligação PC

Aceda ao menu para adicionar uma ligação de PC. Se a ligação de PC for criada com êxito, aparece a seguinte mensagem:

```
INFORMAÇÕES
Lig. PC adic.
```

É atribuído à nova ligação de PC o nome predefinido de “Ligação PC N” e é colocada no fim da lista de ligações de PC. Agora o utilizador pode começar a editar os detalhes da ligação de PC para a nova ligação de PC.

9.4.1.n Seleccionar ligação

Selecione a ligação a configurar.

Nota: as opções específicas deste menu diferem relativamente aos caminhos de transmissão específicos. Para ver opções específicas, consulte:

- “Opções específicas de RTPC” na página nº 347
- “Opções específicas de IP” na página nº 348
- “Opções específicas de GSM” na página nº 348

Opções comuns

9.4.1.n.1 Nome

```
1 Nome
>Ligação PC 1 <
```

O nome da ligação pode ser constituído por até 16 caracteres.

9.4.1.n.2 Via de transmissao

```
2>Via transm
RTPC
```

A opção Via de transmissao define qual o caminho de comunicação utilizado para estabelecer a ligação de PC seleccionada.

Nota: as opções seguintes deste menu diferem para os caminhos de transmissão específicos. O texto entre parênteses rectos identifica o caminho de transmissão a que a opção se aplica.

9.4.1.n.4 No. telefone

```
4 No. telefone
> <
```

O menu N.º de telefone define o número de telefone 1 de Upload/Download. O número de telefone pode conter até 20 dígitos. Estão disponíveis os seguintes caracteres especiais:

- P: pausa (3 s).
- T: a aguardar o sinal de marcação.

Nota: para introduzir um caracter, prima duas vezes a tecla correspondente.

9.4.1.n.5 Lim.tentativas

```
5 Lim.tentativas  
> <
```

A opção Lim. tentativas define um número máximo de tentativas de ligação. O intervalo permitido situa-se entre 0 e 250. O contador de tentativas é reinicializado após cada ligação bem sucedida ou qualquer chamada recebida.

9.4.1.n.6 Apagar Lig. PC

Para remover uma ligação de PC, seleccione a ligação de PC com o cursor, ou introduza o número da ligação de PC e aceda ao menu Apagar Lig. PC.

O ecrã apresenta:

```
6 Apagar Lig. PC  
>Cancelar<
```

Selecione OK e prima Enter. Isto remove a ligação de PC.

Repita o comando para eliminar outras ligações de PC, ou prima Sair para sair e voltar ao nível superior de menu.

Nota: não pode apagar uma ligação de PC, a menos que o seu grupo de utilizadores o autorize a fazê-lo.

9.4.2 Chamada PC

```
1>Primário  
2 Backup
```

A opção Chamada PC define qual a ligação de PC utilizada como estação de retorno de chamadas.

Se a opção Chamada PC estiver definida como Desligado (nenhuma ligação atribuída), nesse caso está activo o atendimento automático.

Nota: as chamadas de retorno só são possíveis para ligações de modem.

9.4.2.1 Primário

9.4.2.2 Backup

Estes menus permitem configurar o destino de chamada principal e de backup, respectivamente.

Escolha uma ligação de PC para uma chamada, ou 0 para desactivá-la.

```
0>Desligado  
1 Ligação PC 1
```

Mediante um pedido de chamada, o Advisor Advanced procura estabelecer ligação ao destino de chamada principal. O número de tentativas é definido em “9.4.1.n.5 Lim.tentativas” acima. Quando o limite de tentativas é excedido, o painel estabelece ligação ao destino de chamada de backup.

9.4.3 Código de encriptação 1

9.4.4 Código de encriptação 2

```
3 Cód. Encrypt.1
>0000000000000000<
```

O painel de controlo do Advisor Advanced necessita de uma chave de encriptação para poder conceder acesso ao painel que utiliza o software de PC de upload/download. A chave de encriptação pode ser constituída por até 24 caracteres. Os dois menus Cód. Encrypt. representam respectivamente a primeira parte e a segunda parte da chave. A chave predefinida é 000000000000000000000000 (24 zeros).

Nota: uma ligação de PC através de caminho de transmissão IP é sempre encriptada. Em ligações RTPC e ISDN a encriptação é opcional. É definida através do menu “9.3.n.9 Encriptação” na página nº 331. As comunicações USB nunca são encriptadas.

Cuidado: recomenda-se vivamente alterar a chave de encriptação predefinida.

9.4.5 Porta de escuta

```
5 Porta escuta
> <
```

A opção Porta de escuta é uma porta IP utilizada para fazer o upload/download de pedidos do PC remoto. A porta predefinida é 32000.

Cuidado: os pedidos a entrar através de GPRS só são aceites se a ligação GPRS for permanente e se nunca fechar automaticamente. Consulte “9.3.n.7.8 Tempo desligar” na página nº 343 para obter mais informações.

9.4.6 ID painel

```
6 ID painel
> <
```

Utilize ID painel para distinguir entre alguns painéis ao utilizar os mesmos numa instalação com a ligação Downloader.

Opções específicas de RTPC

9.4.1.n.3 Protoc. modem

```
3 Protoc. modem
>V.21<
```

A opção Protoc. modem permite seleccionar um dos seguintes protocolos de modem: Bell-103, V.21, V.22 ou V.22bis.

Opções específicas de IP

9.4.1.n.4 IP/Destino

```
1>Nome destino
    Nada
```

O menu Destino define os detalhes de IP para a ligação ao PC seleccionada. Permite também efectuar “ping” ao host.

9.4.1.n.4.1 Nome de destino

```
1 Nome dest/IP
> <
```

A opção de nome de destino define qual o endereço IP utilizado para estabelecer a ligação de PC seleccionada.

Um nome de destino pode ser um endereço IP numérico ou um endereço de domínio alfabético. Consulte também “Como editar um endereço host” na página nº 138.

9.4.1.n.4.2 Porta de destino

```
2 Porta destino
> <
```

A opção Porta dest define qual a porta IP utilizada para estabelecer a ligação de PC seleccionada.

9.4.1.n.4.3 Ping host

```
Pinging...
    Tx/Rx: 2/2
```

O comando Ping host permite enviar um ping para o PC seleccionado. Este comando é utilizado para verificar se o PC está presente e acessível na rede a partir do painel.

O valor Tx/Rx indica o número de pacotes enviados e recebidos.

Opções específicas de GSM

9.4.1.n.3 Tipo ligação

```
3 Tipo ligação
    >CSD<
```

O menu Tipo ligação define qual a ligação GSM utilizada. Estão disponíveis as seguintes opções:

- CSD: utilizada a funcionalidade de modem.
- GPRS: utilizada a funcionalidade GPRS.

9.5 UltraSync

```
1>Conetividade
  Activado
```

O menu permite-lhe configurar a comunicação na “cloud” UltraSync. Consulte “UltraSync” na página nº 126 para obter mais informações.

9.5.1 Conetividade

```
1 Conetividade
  >Activado<
```

Ativar ou desativar a ligação à “cloud” UltraSync.

9.5.2 Número SID

```
2>Número SID
  084400412454
```

O ecrã de informação que mostra o número de série do painel.

9.5.3 Configurações

```
1>Password
  *****
```

O menu contém definições de ligação UltraSync.

9.5.3.1 Password cloud

```
1 Password
  > <
```

A palavra-passe UltraSync é necessária para ligar o painel remotamente utilizando o Downloader ou a aplicação móvel através da “cloud” segura UltraSync.

9.5.3.2 Upgrade FW

```
2 Upgrade FW
  >Activado<
```

Ativar ou desativar a atualização remota de firmware.

9.5.3.3 Configuração remota

```
3 Config. remota
  >Activado<
```

Ativar ou desativar a programação remota do painel.

9.5.3.4 Notificações

```
4 Notificações
  >Activado<
```

Ativar ou desativar as notificações push para smartphone.

As notificações push são configuradas em “9.5.4 Lista de notificações” abaixo.

9.5.3.5 Monitorização GPRS

```
5 Monitor GPRS
  >Ativado<
```

Ativar ou desativar a monitorização da ligação UltraSync através do painel de controlo.

O painel tenta ligar o UltraSync a cada 100 s para monitorizar a ligação. Desativar esta opção para limitar os dados enviados através de GPRS.

9.5.3.6 Servidores UHS

```
1 Servidor ETH 1
>192.168.1.1:44>
```

O menu permite predefinir 8 servidores predefinidos UltraSync e portas:

- 1 Servidor ETH 1: Predefinição servidor Ethernet primário
- 2 Servidor ETH 2: Predefinição de cópia de segurança de servidor Ethernet 1
- 3 Cópia de segurança de servidor Ethernet 2
- 4 Cópia de segurança de servidor Ethernet 3
- 5 ServidorWless1: Servidor sem fios primário predefinido
- 6 ServidorWless2: Predefinição de cópia de segurança de servidor sem fios 1
- 7 Cópia de segurança de servidor sem fios 2
- 8 Cópia de segurança de servidor sem fios 3

9.5.4 Lista de notificações

```
1>Notificação 1
2 Notificação 2
```

O menu permite-lhe configurar e remover as notificações push para smartphones.

Nota: o menu do painel não lhe permite adicionar notificações. Só pode adicionar notificações utilizando uma aplicação de smartphone.

9.5.4.n Selecionar notificação

```
1>Nome
  Notificação 1
```

Selecione uma notificação a configurar.

9.5.4.n.1 Nome da notificação

```
1 Nome
>Notificação 1<
```

Cada notificação push pode ser programada com um nome que a identifique.

Utilize o menu para introduzir ou alterar o nome da notificação push. O nome da notificação push pode conter até 16 caracteres.

9.5.4.n.2 Identificador

2>Identificador

O ecrã de informação que mostra o identificador de notificação do smartphone.

9.5.4.n.3 Utilizador

3>Utilizador
Utilizador 3

O ecrã de informação que mostra o utilizador que recebe a notificação push selecionada.

9.5.4.n.4 Estados

4>Estados
Ativo

O ecrã de informação que mostra o estado da notificação selecionada.

- Ativo: a notificação está ativa e pode ser recebida pelo utilizador.
- Inativo: A notificação encontra-se desabilitada pelo instalador ou supervisor, ou as permissões de grupo de utilizadores não permitem ao utilizador receber notificações, ou não existem eventos habilitados para notificações push em “9.5.4.n.5 Tipos de eventos” abaixo.

9.5.4.n.5 Tipos de eventos

1>Alarmes
Ativado

O menu permite selecionar tipos de eventos que serão enviados para o smartphone.

Se a opção estiver ativada, qualquer evento dessa categoria é enviado por notificação push ao utilizador atribuído.

Estão disponíveis as seguintes opções:

- 1 Alarmes: Alarmes pendentes, Pânico, Empastelamento, Tampers, Soak, Técnico
- 2 Arme/desarme: Arme, Desarme, Arme parcial, Inibição
- 3 Alimentação: Falha Bateria, Bateria baixa, Falha Alimentação Principal, Falha PSU
- 4 Sistema: Reset técnico, Manutenção, Programação local, Eventos RFU, CR Teste auto, Isolamento
- 5 Vídeo: Memória imagem cheia, Fotografia apagada, Fotografia obtida
- 6 Falha: Ligação Ethernet, Comunicação, Fusível, Alimentação e falhas internas, e restauros

- 7 Acesso: Acesso negado, acesso concedido

9.5.4.n.6 Apagar notificação

```
6 Apagar Notific  
>Cancelar<
```

Utilizar o menu para remover do sistema a notificação push selecionada. Para remover a notificação, selecione OK e prima Enter novamente. A notificação é eliminada.

Capítulo 6

Software

Resumo

Este capítulo descreve como ligar o painel de controlo Advisor Advanced ao PC para programação e upgrade do firmware.

Índice

Programar o Advisor Advanced através do software de configuração	354
Actualização de firmware Advisor Advanced	356
Instalar o AAFlash no PC	356
Ligar o Advisor Advanced ao PC	356
Arquivamento de firmware e definições actuais	357
Actualização de firmware Advisor Advanced	358
Atualização remota de firmware (RFU)	358
Atualizar o bootloader	358

Programar o Advisor Advanced através do software de configuração

Existem diferentes ferramentas de administração e configuração de PC concebidas para simplificar e acelerar a programação do sistema Advisor Advanced, sem necessidade de cadeias ou comandos complexos. Todas as informações são introduzidas directamente do ambiente de trabalho do Windows.

Para obter informações detalhadas sobre estas ferramentas e a ligação, consulte a respectiva ajuda online.

Cuidado: certifique-se de que a sua versão de software é compatível com a versão de firmware do seu painel de controlo, caso contrário poderá ser impossível fazer o upload ou o download das definições do painel. Contacte a assistência técnica da sua zona para obter informações sobre a compatibilidade das versões.

Primeira ligação do Advisor Advanced ao PC:

1. Instale o software de configuração.
2. Abra a caixa do painel e ligue um cabo USB à porta USB da PCI do painel. Ligue o cabo USB ao PC. Se esta for a primeira ligação, o sistema pede-lhe para encontrar controladores USB Advisor Advanced para instalar. Instale o controlador fornecido com o software de configuração. É instalada no sistema uma nova porta de comunicação, a porta de comunicação ATS CDC.
3. Abra o software de configuração.
4. Crie um novo sistema Advisor Advanced e seleccione-o.
Consulte a ajuda online aplicável.
5. O código de instalador utilizado é necessário para ter acesso ao painel. Os direitos de acesso baseiam-se nas opções de grupo de utilizadores definidas.
6. Se necessário, defina a mesma chave de encriptação, partes 1 e 2, conforme configurado no painel. Para mais informações sobre chaves de encriptação de painel, consulte “9.4.3 Código de encriptação 1” na página nº 347.

A comunicação entre o painel e o software de configuração poderá necessitar da assistência do utilizador para conceder acesso de serviço, se a opção “8.2.1 Aceit. necess” estiver definida como Ligado (consulte a página 288).

Neste caso, têm de ser efectuados os seguintes passos:

1. O utilizador autorizado acede ao menu Utilizador e activa a opção “Modo técnico”. Para mais detalhes, consulte o *Manual do Gestor do Advisor Advanced*. Em seguida, o utilizador tem de abandonar o menu.
2. O instalador poderá agora efectuar o upload ou o download.

3. Tenha em atenção que a sessão de comunicação é fechada após concluído o upload/download de dados. Isto significa que, depois de expirar o temporizador do Modo técnico (programado em “8.1.3.6 Manutenção em” descrito na página nº 286), é necessária uma nova autorização do utilizador.

Cuidado: Se a comunicação USB for interrompida durante uma operação de carregamento ou transferência, saia do software de configuração, estabeleça uma ligação fiável e aguarde 10 segundos para que a ligação seja reinicializada. Em seguida, volte a iniciar o software de configuração.

Actualização de firmware Advisor Advanced

O firmware do painel Advisor Advanced pode ser actualizado via interface USB DFU (device firmware upgrade). Utilize o software AAFlash para actualizar.

O nível de acesso 4 (fabricante) aplica-se quando se altera o software de programa operativo e necessita de ser executado no local de programação.

Não é permitida a mudança para a versão anterior.

Para receber o software AAFlash, bem como o último firmware, contacte o seu fornecedor.

Atenção

- Durante o processo de actualização do firmware, todas as funcionalidades do sistema de alarme estão desativadas. Algumas funções de controlo de acesso poderão também ser desativadas.

Assegure-se de que a alimentação da rede eléctrica e da bateria se mantém estável e sem interrupções durante todo o processo de actualização, salvo se o processo requerer que a fonte de alimentação se desligue e volte a ligar. O sistema poderá ficar danificado se a alimentação falhar durante a actualização.

Instalar o AAFlash no PC

Se o AAFlash não estiver instalado no PC, siga os passos seguintes para proceder à instalação.

Para instalar o AAFlash:

1. Certifique-se de que o Microsoft .Net 3.5 requerido pelo AAFlash se encontra instalado no PC. Caso contrário, utilize a actualização Microsoft para instalar ou faça o download a partir do site Microsoft para proceder à instalação manual.
2. Execute Setup.exe a partir do pacote de instalação AAFlash.
3. Escolha a directoria de instalação e prossiga com a instalação premindo Next (Seguinte), e de seguida Install (Instalar).
4. Finalize o processo de instalação premindo Finish (Terminar).

Ligar o Advisor Advanced ao PC

Para ligar o painel ao PC para actualização:

1. Abra a caixa do painel.
2. Ligue o teclado LCD ao painel.
3. Ligue a alimentação da rede eléctrica e da bateria ao painel.

4. Aguarde pelo menu de instalação.
5. Verifique se o menu 4. UltraSync está disponível
Se o menu não estiver disponível, contacte o suporte técnico; se estiver, prossiga.
6. Desligue a alimentação da rede elétrica e da bateria do painel.
7. Coloque o jumper T2.
8. Volte a ligar a alimentação da rede elétrica e da bateria. Os díodos RX e TX devem piscar.
Cuidado: Se os díodos não piscarem, e o painel começar a reiniciar, aguarde que o menu de Instalação seja exibido no teclado e retome a partir do passo 5.
9. Insira a ficha USB no conector localizado na placa principal da Advisor Advanced. Consulte “Informação de instalação geral” na página nº 8 para mais informações.

Os LED USB acendem, o LED TX apaga-se e o LED RX continua a piscar.

Se esta é a primeira ligação DFU, o sistema solicita a procura dos controladores Advisor Advanced USB DFU para instalar. Selecciono o controlador localizado no subdirectório “Driver” no directório de programa AAFlash (a predefinição é C:\Program Files\Advisor\AAFlash\driver).

É instalado um novo controlador USB (dispositivo STM em modo DFU) no sistema.

O painel está pronto para a actualização de firmware.

Arquivamento de firmware e definições actuais

Cuidado: Para prevenir qualquer potencial falha durante a programação, instalação ou inicialização de novo firmware ou nova funcionalidade, certifique-se que o firmware actual (incluindo as definições) está arquivado e pode ser reprogramado.

Para arquivar o firmware do painel:

1. Enquanto ligado ao painel Advisor Advanced, execute o AAFlash localizado em Iniciar > Programas.
2. Crie o nome de ficheiro para o backup apropriado de firmware *.dfu, clicando em “...” (Procurar). Introduza o nome do ficheiro e clique em Guardar.
3. Clique em Carregar.
O AAFlash carrega o firmware existente, incluindo as definições, num ficheiro dfu.

Actualização de firmware Advisor Advanced

Para actualizar o firmware do painel:

1. Enquanto ligado ao painel Advisor Advanced, execute o AAFlash localizado em Iniciar > Programas.
2. Seleccione o ficheiro de firmware aplicável *.dfu premindo “...” (Browse). Seleccione o ficheiro e clique em Open (Abrir).
3. Clique em Upgrade (Actualizar).

AAFlash apaga o firmware existente, escreve o novo e verifica-o.

Após a actualização do firmware, o LED TX pisca, indicando que o painel se encontra pronto para sair do modo de actualização.

Cuidado: Se o procedimento de actualização de firmware falhar, restabeleça o último firmware arquivado.

4. Desligue o cabo USB do painel e remova o jumper T2.
O LED TX deixa de piscar. O painel é automaticamente reinicializado.
5. Após reiniciar o painel, aguarde que seja exibido o menu Instalação.
Verifique se o menu 4. UltraSync está disponível
Se o menu não estiver disponível, contacte o suporte técnico..

Atualização remota de firmware (RFU)

O firmware do painel pode ser atualizado remotamente através do UltraSync ou do Downloader. Entre em contacto com o seu fornecedor de serviços UltraSync para obter detalhes. Consulte também a Ajuda online do Downloader para obter detalhes.

Atenção

- Durante o processo de atualização do firmware, todas as funcionalidades do sistema de alarme estão desativadas.
 - Após conclusão do processo de atualização do firmware remoto, o sistema poderá manter-se no estado Falha do Sistema durante até 3 minutos.
 - Todas as áreas ficam desarmadas após a atualização remota do firmware. Reponha as condições, se necessário.
 - O registo de eventos é apagado durante a atualização do firmware. Descarregue o registo antes da atualização.
-

Atualizar o bootloader

Painéis específicos com o firmware bootloader antigo não podem ser atualizados para um novo firmware. Neste caso é necessário actualizar o firmware de bootloader para uma nova versão. A actualização do firmware de bootloader é descrita de seguida.

Cuidado: o é uma parte crucial do painel Advisor Advanced panel. Certifique-se que o procedimento é efetuado na ordem correta (passos 5 a 7), e de que *a alimentação não é removida enquanto o passo 7 estiver a decorrer*, caso contrário o sistema pode ser danificado.

Para atualizar o firmware bootloader:

1. Instalar o software AAFlash version 2.3.0 ou seu superior.

Ver “Instalar o AAFlash no PC” na página nº 356.

2. Colocar o painel em modo DFU.
 - a. Desligue a alimentação principal e baterias do painel
 - b. Coloque o jumper T2 e ligue o cabo mini-B USB ao painel.
 - c. Volte a ligar a alimentação principal.

O painel encontra-se agora a funcionar em modo DFU, o LED RX encontra-se a piscar.

Se os LEDs RX e TX se encontrarem a piscar alternadamente, o PC ligado não tem o driver apropriado instalado. Neste caso, o sistema indica que deve procurar os drivers Advisor Advanced USB DFU para instalar. Selecione a localização do driver na diretoria AAFlash (“C:\Program Files(x86)\AAFlash\driver” por defeito).

3. Execute o AAFlash (versão 2.3.0 ou superior), clique “...” (Procurar), e abra o ficheiro *.dfu com bootloader fornecido.
4. Clique em Upgrade Bootloader.
5. *O programa indica que deve criar um backup do firmware e base de dados existentes. Clique em “Yes” e crie um novo ficheiro de backup, ou “No” para saltar este passo.*

Se efetuou clique em “Yes”, é lhe solicitado que introduza um nome para o ficheiro dfu de backup. Introduza o nome e aguarde instruções.

6. *Remova o jumper T2 e desligue o cabo USB.*
7. *Certifique-se de que a alimentação e baterias se encontram ligadas.*

A versão da imagem é comparada com a versão de bootloader atual. Se for a mesma ou mais antiga, a atualização não é efectuada.

Os setores da flash interna alocados para o bootloader são apagados e verificados.

O novo bootloader é implementado (flashed).

Após a operação se encontrar completa, o LED heartbeat começa a piscar.

8. Coloque o jumper T2 e ligue o cabo USB cable.

O painel reinicia. Encontra-se agora a funcionar em modo DFU com o novo firmware bootloader.

Se foi criado um backup no passo 5, o painel inicia o restauro do firmware da aplicação e da base de dados. Caso contrario, encontra-se pronto para actualização de firmware. Ver também “Actualização de firmware Advisor Advanced” na página nº 358.

Capítulo 7

Resolução de problemas

Resumo

O capítulo contém informações sobre a resolução de problemas de hardware e configuração conhecidos. Descreve também como recuperar o sistema quando se perde o acesso do instalador.

Índice

Procedimento de recuperação	362
Resolução de problemas do dispositivo	363
Painel de controlo do Advisor Advanced	363
Teclados LCD	364
Expansores remotos – Modelos ATS1201, ATS1210, ATS1211, ATS1220	364
Expansor remoto – Modelo ATS1236	365
Expansor remoto – Modelo ATS1238	366

Procedimento de recuperação

Se o PIN do instalador se perder, o acesso do instalador é impossível. Neste caso o instalador pode executar um procedimento de recuperação.

Para recuperar o acesso do instalador:

1. Retire do painel a alimentação de corrente eléctrica e de bateria.
2. Ajuste o jumper T1.
3. Aplique alimentação ao painel.

Durante os 3 minutos seguintes, será possível aceder ao menu do instalador utilizando o código predefinido. Não é necessário que um utilizador conceda acesso ao modo de programação de instalador.

Este procedimento é registado.

Nota: o procedimento de recuperação não é permitido se a opção “8.2.3 Bloqueio técnico” estiver definida como Sim.

Cuidado

- Após o procedimento de recuperação são restabelecidas as limitações de acesso do teclado 1, o que permite visualizar e controlar todas as áreas a partir deste teclado. Consulte “2.2.1.n.3.4 Ver áreas” na página nº 177 e “2.2.1.n.3.6 Áreas de controlo” na página nº 177 para mais informações.
 - Se o keypad 1 comunica com o painel utilizando um canal seguro, o procedimento de recuperação redefine as respetivas chaves de encriptação. Consulte também “Segurança dos dados do cartão” na página nº 130.
-

Resolução de problemas do dispositivo

Painel de controlo do Advisor Advanced

Condição	Causa possível
O teclado LED tem todos os LEDs a piscar e apresenta a mensagem “Falha de Sistema”	<p>A linha do databus do sistema poderá não estar correctamente ligada.</p> <p>Os links de endereço do teclado poderão estar definidos incorrectamente.</p> <p>Foi efetuada uma atualização do firmware remoto. Deve aguardar até 3 minutos para a reposição do sistema. Ver também “Atualização remota de firmware (RFU)” na página nº 358.</p>
O painel não comunica com os teclados ou expansores	<p>A linha do databus do sistema poderá não estar correctamente ligada.</p> <p>Os números dos teclados ou expansores a ser sujeitos a polling poderão não estar programados, ou poderão não coincidir com os endereços definidos nas unidades.</p> <p>Existe um loop de terra na cablagem.</p>
Os teclados ou expansores parecem estar sempre a passar para offline e online (indicado pelos LEDs de falha de teclado ou expansor)	<p>A linha do databus do sistema poderá não estar correctamente ligada.</p> <p>A terminação poderá estar incorrecta. Os jumpers terminador (TERM links) poderão não ter sido removidos onde necessário. Consulte “Cablagem do Advisor Advanced” na página nº 24.</p>
A zona entra no modo de alarme embora a área esteja desarmada	<p>A zona está ligada incorrectamente, causando uma condição de tamper (circuito aberto ou curto-circuito) em vez de uma condição de activo. As resistências EOL poderão estar instaladas incorrectamente.</p> <p>Consulte “Cablagem do Advisor Advanced” na página nº 24.</p>
O painel não está a reportar à central receptora	<p>As ligações da linha telefónica poderão estar ligadas incorrectamente. Consulte “Cablagem do Advisor Advanced” na página nº 24.</p> <p>O receptor da central receptora não suporta o protocolo programado.</p> <p>O número de conta em “9.1.n.5 Contas” na página 318 poderá estar programado incorrectamente.</p> <p>O número de telefone da central receptora está incorrecto.</p> <p>Nenhuma central receptora está programada para reportar o evento. Consulte “9.1 Central Receptora” na página 316.</p> <p>A zona não está programada para ser reportada. Consulte “4.1.n.6.24 Reporte CRA” na página nº 219.</p> <p>Configuração de IP errada, por exemplo conflito no endereço de IP. Consulte também “Teclados LCD” na página nº 364.</p>

Teclados LCD

Condição	Causa possível
Todos os LEDs do teclado estão intermitentes	<p>Os DIP switches poderão estar ajustados incorrectamente (a definição do endereço do teclado poderá estar incorrecta e portanto o polling para o teclado poderá não estar a ser reconhecido).</p> <p>A linha do databus do sistema poderá não estar correctamente ligada.</p> <p>O teclado não está a ser sujeito a polling (poderá não ter sido incluído na lista de teclados sujeitos a polling, quando os teclados foram programados).</p>
Os LEDs não parecem estar a indicar a condição correcta	<p>O tipo de teclado poderá ter sido definido incorrectamente:</p> <p>O teclado LCD tem de estar definido como Sim.</p>
O teclado parece estar sempre a passar para offline e online (indicado pela mensagem “Falha de teclado” no ecrã LCD)	<p>A terminação poderá estar incorrecta. Consulte “Cablagem do Advisor Advanced” na página nº 24.</p>
É indicado um erro quando é introduzido um código no teclado (sete bips)	<p>Poderá ter sido utilizado um PIN inválido.</p> <p>O teclado poderá não ter sido programado com um grupo de alarmes.</p> <p>O grupo de alarmes do PIN poderá não permitir acesso a este teclado.</p>
É indicado no teclado um erro “conflito de IP”. A ligação de IP está indisponível.	<p>Configurado um endereço de IP errado.</p> <p>O conflito no endereço de IP tem de ser solucionado.</p> <p>O estado restaura em três minutos após o conflito ser solucionado.</p>
É indicado um erro de “Falha WAN” no teclado.	<p>A ligação com o UltraSync foi perdida.</p>

Expansores remotos – Modelos ATS1201, ATS1210, ATS1211, ATS1220

Condição	Causa possível
O LED “Tx” LED no expansor não está a piscar	<p>Os DIP switches poderão estar definidos incorrectamente (a definição do endereço do expansor poderá estar incorrecta e portanto o polling para o expansor poderá não ser reconhecido).</p> <p>O cabo do databus do sistema poderá não estar correctamente ligado.</p> <p>O expansor não está programado para polling.</p>
Os LEDs “Tx” e “Rx” não estão a funcionar	<p>Sem alimentação ou alimentação fraca.</p> <p>O cabo do databus do sistema poderá não estar correctamente ligado ou a fonte de alimentação está avariada (corrente ou bateria).</p>

Condição	Causa possível																				
O expansor parece estar sempre a passar para offline e online (indicado pela mensagem “Falha de expansor” num teclado LCD)	A terminação poderá estar incorrecta. Consulte “Cablagem do Advisor Advanced” na página nº 24.																				
Algumas ou todas as zonas de expansor estão permanentemente em tamper (ou permanentemente em alarme se “8.6.1 Modo entrada” na página 302 estiver definido como Simples NO/NC)	<p>Os números de zona do expansor foram calculados incorrectamente, e os números de tipo de zona foram, portanto, atribuídos a zonas incorrectas na base de dados de zonas. Consulte “Configuração” na página nº 32.</p> <p>As resistências de fim de linha (EOL) são incorrectas ou foi programado um valor incorrecto de resistência em “8.6.2 Resistência EOL” (consulte a página 302).</p> <p>Existe um problema com as ligações das zonas. Para verificar os valores de tensões e resistências, consulte “Ligação das zonas” na página nº 25.</p> <p>Os módulos de expansão ATS1202 (se instalados) têm os DIP switches definidos incorrectamente.</p> <table border="1"> <thead> <tr> <th>Módulo de expansão:</th> <th>1.º</th> <th>2.º</th> <th>3.º</th> </tr> </thead> <tbody> <tr> <td>DIP switch 1</td> <td>Lig</td> <td>Des</td> <td>Des</td> </tr> <tr> <td>DIP switch 2</td> <td>Des</td> <td>Lig</td> <td>Des</td> </tr> <tr> <td>DIP switch 3</td> <td>Des</td> <td>Des</td> <td>Lig</td> </tr> <tr> <td>DIP switch 4</td> <td colspan="3">não utilizado</td> </tr> </tbody> </table>	Módulo de expansão:	1.º	2.º	3.º	DIP switch 1	Lig	Des	Des	DIP switch 2	Des	Lig	Des	DIP switch 3	Des	Des	Lig	DIP switch 4	não utilizado		
Módulo de expansão:	1.º	2.º	3.º																		
DIP switch 1	Lig	Des	Des																		
DIP switch 2	Des	Lig	Des																		
DIP switch 3	Des	Des	Lig																		
DIP switch 4	não utilizado																				
Os módulos de relé de 4 vias (ATS1810) utilizados com o expansor não funcionam, mas alguns LEDs do módulo parecem estar permanentemente acesos	O DIP switch B do expansor está definido como Ligado (o DIP switch B só deveria estar definido como Ligado se forem utilizados módulos de relé de 8 vias (ATS1811) ou módulos colectores abertos de 16 vias (ATS1820)).																				
Os módulos de relé de 8 vias (ATS1811) ou módulos colectores abertos de 16 vias (ATS1820) ligados ao expansor não funcionam	O DIP switch B do expansor não foi definido como Ligado.																				

Expansor remoto – Modelo ATS1236

Condição	Causa possível e solução
O evento “Falha do DGP” surge no registo do painel de controlo.	<p>Configuração do expansor corrompida.</p> <p>Neste caso o DGP tem de ser configurado e os dispositivos sem fios novamente registados. Para limpar a falha, aceda às definições do Expansor, “2.2.2.n.4.11 Cfg. Fab. DGP” (descrita na página nº 191).</p>

Condição	Causa possível e solução
Não é possível registrar um dispositivo sem fios.	Foi registado um tipo de dispositivo não suportado. Se registar no ATS1236 um tipo de dispositivo não suportado (por exemplo, alarmes sonoros, comandos remotos, etc.), o ATS1236 deixará de aceitar sensores a partir dessa posição. Para desbloquear este estado, deve remover os dispositivos não suportados através do software de configuração ATS85xx ou repor as definições do ATS1236.

Expansor remoto – Modelo ATS1238

Condição	Possível causa e solução
O expansor fica offline após ter sido adicionado remotamente a partir do software Downloader.	O painel estabelece a comunicação com o expansor ATS1238 apenas durante a inicialização do sistema.
O expansor não é visível pelo painel depois de ter sido removido remotamente do software Downloader.	Reinicie o painel para iniciar a comunicação com o expansor ATS1238.

Capítulo 8

Normas

Resumo

Estas páginas apresentam definições e acções requeridas por normas e regulamentos específicos.

Índice

Opções afectadas pelas normas EN 50131	368
EN 50131 Grau 2	368
EN 50131 Grau 3	369
Política EN 50136	371
Requisitos de intervalo de polling de transmissor	371
Componentes certificados pela EN 50131 Grau 3	372
Precauções de conformidade da EN 50131	373
Opções afectadas por outros regulamentos	375
Política ACPO	375
Política INCERT	375
Política SES	376
Política SBSC	376

Opções afectadas pelas normas EN 50131

EN 50131 Grau 2

Definições necessárias

As seguintes opções e valores são obrigatórios para os regulamentos EN 50131-1 Grau 2.

- 1.2.6.n.3 Período, consulte “Requisitos de intervalo de polling de transmissor” na página nº 371.
- As definições 2.2.1.n.3.4 Ver áreas e 2.2.1.n.3.6 Áreas de controlo são idênticas
- 2.2.1.n.3.11 Besouro silenciado, Nunca
- 2.2.1.n.3.12 Arme rápido, desligado
- 2.2.1.n.3.13 Teclas Função, todas definidas como Nenhum
- 2.2.1.n.3.18 REC no RAS, definido como Nenhum para teclados não LCD
- 3.1.n.7.3 Controlo SMS, desactivado para todos os utilizadores
- 3.2.n.6 Opções de GU, opção 25. Sem reporte OP/CL definida como Não
- 4.1.n.6.1 Inibir, definido como Não para todas as zonas com o tipo 5. Pânico, 6. 24H
- 4.1.n.6.6 Swinger shunt, definido para Sim para todas as zonas
- 4.1.n.6.26 REC no RAS, definido como Nenhum para todas as zonas com o tipo 9. Comutador
- 4.2.n.3 Tempo de entrada, máximo 45 s
- 4.2.n.5.1 Alarmes de entrada, Imediato
- 7.2.n.2 Activo, definido para Não para todos os planos.
- 8.1.2.1 Activação, sirene externa 90 a 900 s
- 8.1.2.2 Retardo, sirene externa, máximo 600 s
- 8.1.3.1 Screensaver, definido para 00’00
- 8.1.3.4 Rtd.rep.230VAC, máximo 3600 s
- 8.2.1 Aceit. necess, activado
- 8.3.1 Modo Screensaver, sempre
- 8.3.3 Lista de alarmes, desactivado
- 8.4.1 Pront.Armaz, todas activadas, excepto alarme técnico de zona, que é opcional
- 8.4.2 Inibir inclusão, todos permitidos excepto reset técnico, que tem de estar desactivado
- 8.4.6 Alarmes em espera, Permitir EN50131
- 8.4.10 Relt.Falha ES, falha EE
- 8.6.4 Swinger shunt ≥ 3
- 8.6.5 Restauro de reporte, em RCO
- 8.7.8.1 Config. Remota, Não
- 8.8.14 Reporte sirene, Falha
- 9.3.n.2 Falha de linha, activado por caminho utilizado
- 9.3.n.3 Retardo FL, 0 s

É necessário aplicar as seguintes configurações de supervisão para os DGPs via rádio:

- Supervisão pequena: 20 minutos
- Supervisão longa: 2 horas
- Supervisão de fumo: 4 horas

Consulte as secções apropriadas e manuais.

Cuidado: quando qualquer opção, função adicional ou tipo de zona adicional nesta secção não cumprirem os requisitos da EN 50131, a etiqueta EN 50131 Grau 2 tem de ser retirada do sistema.

Funções adicionais

O funcionamento da Câmara PIR via rádio incorpora a funcionalidade de vídeo verificação, esta função adicional encontra-se totalmente disponível sem comprometer o cumprimento das normas que o sistema cumpre.

O sistema de câmara PIR via radio consiste no seguinte:

- Painel da série Advisor Advanced
- DGP Via radio avançado ATS1238
- Câmara PIR via radio TX-2344-03-1
- Módulo GSM/GPRS ATS73X0

Estas configurações da câmara PIR não têm influencia no cumprimento da EN 50131:

- 2.2.2.n.4.9.1.1.2 Taxa de frames para todos os tipos de evento
- 2.2.2.n.4.9.1.1.3 Resoluçao Foto para todos os tipos de evento
- 2.2.2.n.4.9.3 AutoapagarImag
- 4.5 Câmaras
- 9.1.n.4.5 Port dest vid
- 9.3.n.11 Foto max. 24h, 9.3.n.7.9 Max. Fotos 24h

EN 50131 Grau 3

Definições necessárias

As seguintes opções e valores são obrigatórios para os regulamentos EN 50131-1 Grau 3:

- Todas as definições necessárias de Grau 2 (consulte “EN 50131 Grau 2” na página nº 368)
- O PIN deve ter um mínimo de 6 dígitos. Consulte também “8.7.4 Comprim. PIN” na página nº 304.
- 3.2.n.6 Opções de GU, definir (6) Isolar, (22) Reporte SMS, (23) Controlo SMS como Não para todos os grupos de utilizadores excepto Instalador.
- 4.1.n.6.7 Anti-Mask, defina como Sim para todos os detectores de movimento I&HAS
- 4.2.n.2.1 Tempo de saída 1, ≤ 180 s

- 8.1.3.4 Rtd.rep.230VAC, ≤ 1 h
- 8.3.5 Ver tempo ES, definir como desligado
- 8.4.1 Pront.Armaz, defina Estado de Anti-Mask como Sim
- 8.4.2 Inibir inclusão, defina Estado de Anti-Mask como Nível Acesso 2
- O teste à bateria deve ser realizado diariamente. Consulte “1.2.9 Teste da bateria” na página nº 164 para obter mais informações.

Não são permitidas as seguintes funções (não avaliadas):

- Tipos de zona de interruptor de chave para armar e desarmar o sistema. Consulte “Tipos de zonas” na página nº 49.
- Indicação de predefinição e qualquer ignorar automático de prevenção definida.

Consulte a Tabela 29 abaixo para todas as opções suportadas para requisitos de notificação.

Tabela 29 Opções de EN 50131-1 2006

Equipamento de notificação (reporte de alarme)	Opções de grau 3			
	A	B	C	D
Dispositivo de aviso audível alimentado remotamente	2	Opcional	Opcional	Opcional
WD audível com alimentação automática	Opcional	1	Opcional	Opcional
ATS principal [1]	ATS 4	ATS 4	ATS 4	ATS 5
ATS adicional [1]	Opcional	Opcional	ATS 3	Opcional
ATS [2]	SP3	SP3	DP3 [3]	SP4

[1] Requisito em conformidade com EN 50136:2010

[2] Requisito em conformidade com EN 50136:2012

[3] Via primária — SP4, via de backup — SP2

Legenda:

- ATS: Sistema de transmissão de alarme
- SP: Sistema de transmissão de alarme de via única
- DP: Sistema de transmissão de alarme de via dupla

As variações de placas e teclas são as seguintes:

- Série cartões ATS147x (utilizado com ATS1135 e ATS119x): 67 milhões
- Série cartões ATS145x (utilizado com ATS1136 e ATS118x): 280 triliões

Os cartões utilizam o protocolo Hitag de 26 bit (a 48 bit)

O instalador (nível de utilizador 3) faz o comissionamento do sistema com as funções adicionais aplicáveis.

O utilizador final (nível de utilizador 2) pode utilizar todas essas funções.

O instalador só pode utilizar essas funções quando lhe é concedido acesso pelo utilizador final.

Definições RAS necessárias

O teclado/RAS tem de ser montado no interior das instalações seguras, no trajecto de entrada/saída.

Cada cenário de arme descrito abaixo cumpre os requisitos da norma EN 50131.

- 2.2.1.n.3.8.1 Modo cartão e PIN: Cartão e PIN sempre
Nota: Esta configuração deve ser aplicada manualmente pelo instalador após definidos os cartões apropriados no sistema.
- 2.2.1.n.3.8.3 1 x arme/desarme: Desligado
- 2.2.1.n.3.8.4 3xCartão arma: Arme
- 2.2.1.n.3.12 Arme rápido: Desligado
- 4.1.n.6.18 Desarme por chave: Desligado
- 8.4.4 Arme forçado: Desligado
- 8.4.7 AA tempo tent.: 15 minutos
- 8.4.8 AA tenta util: Desactivar

Para mais detalhes, consulte também o manual apropriado da RAS.

Política EN 50136

Definições necessárias:

- 9.1.n.7 Repetir contagem: 1
- 9.1.n.8.3.2 Tempo de Heartbeat: Em conformidade com a Tabela 30 abaixo.
- 9.1.n.8.3.5 Freq. tempo HB: Em conformidade com a Tabela 30 abaixo.
- 9.3.n.8.1 Firewall: Sim
- 9.3.n.8.2 Resposta PING: Não
- 9.3.n.7.6.1 Firewall: Sim
- 9.3.n.7.6.2 Resposta PING: Não
- 9.3.n.9 Encriptação: Sim
- 9.4.3 Código de encriptação 1 deve ser definido.

Consulte também “Requisitos de intervalo de polling de transmissor” abaixo.

Requisitos de intervalo de polling de transmissor

O intervalo de polling de transmissor deve ser definido em conformidade com requisitos específicos para diferentes sistemas de transmissão de alarme (ATS). Tabela 30 abaixo lista todas as definições necessárias para os padrões e comunicadores.

Tabela 30: Definições de polling de transmissor

Padrão e categoria	Intervalo de polling necessário	Via de comunicação e comunicador	Opção	Valor necessário
EN50136:2012				

Padrão e categoria	Intervalo de polling necessário	Via de comunicação e comunicador	Opção	Valor necessário
SP2	25 h	RTPC via ATS7700 e GPRS (backup) via ATS73X0	1.2.6.n.3 Período	24
SP3	30 min	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	00:29'00
SP4	3 min	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	00:02'30
SP5	90 s	IP incorporado	9.1.n.8.3.2 Tempo de Heartbeat	00:01'00
SP6	20 s	IP incorporado	9.1.n.8.3.2 Tempo de Heartbeat	00:00'10
EN50136:2010				
ATS2 (T2), ATS3 (T2)	25 h	RTPC via ATS7700 e GPRS (backup) via ATS73X0	1.2.6.n.3 Período	24
ATS4 (T3)	300 min	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	04:55'00
ATS5 (T4)	180 s	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	00:02'30
ATS6 (T6)	20 s	IP incorporado	9.1.n.8.3.2 Tempo de Heartbeat	00:00'10
LPS1277: Edição 3.0				
ATS4Plus	10 min	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	00:09'00

Componentes certificados pela EN 50131 Grau 3

O sistema Advisor Advanced EN 50131 Grau 3 é composto pelos seguintes componentes.

Painéis de controlo de intrusão

- ATS1500A(-IP). **Nota:** o painel ATS1500A(-IP)-MM pode ser atualizado para o grau de segurança 3 utilizando o kit de tamper ATS-MM-TK.
- ATS3500A(-IP).
- ATS4500A-IP.

Teclados / leitores (RAS, estação de arme remota)

O painel pode suportar até 8 ou 16 dispositivos RAS em simultâneo, dependendo do painel de intrusão, independentemente do tipo (independente de outros expansores).

- ATS1135: Teclado LCD

- ATS1190/1192: Leitor de cartão Smart Card
- ATS1151/ATS1156: Teclado
- ATS1136: Teclado LCD
- ATS118x: Série de leitores Smart Card

Expansor remoto (DGP, painel de recolha de dados)

O painel pode suportar até 7 ou 15 dispositivos DGP, dependendo do painel de intrusão, independentemente do tipo (independente de outros expansores).

- ATS1201E: Expansor DGP de 8 a 32 zonas com PSU de 3 A, caixa pequena, EN 50131 Grau 3
- ATS1204E: Expansor DGP de 8 a 32 zonas com PSU de 3 A, caixa grande, EN 50131 Grau 3

Expansores I/O

O painel pode suportar até 3 dispositivos I/O, consoante o tipo.

- ATS608: Expansor plug-in de 8 zonas
- ATS624: Placa de relé de 4 saídas
- ATS626: Placa de 16 saídas de colectador aberto

Dispositivos de reporte

O painel pode suportar 1 dispositivo GSM ligado a bus MI.

- ATS7310: Dispositivo de comunicação GSM
- ATS7320: Dispositivo de comunicação GSM
- ATS7440: Marcador de alarme IP/GPRS
- ATS7700: Placa de interface RTPC

quando qualquer opção, função adicional ou tipo de zona adicional nesta secção não cumprirem os requisitos da EN 50131, a etiqueta EN 50131 Grau 3 tem de ser retirada do sistema. Consulte também “Precauções de conformidade da EN 50131” abaixo.

Precauções de conformidade da EN 50131

Instalação

Para instalar um sistema em conformidade da EN 50131, certifique-se de que todos os componentes dos sistemas estão de acordo com a EN 50131. Para mais informações, consulte “Componentes certificados pela EN 50131 Grau 3” na página nº 372.

Programação

Certifique-se de que todas as definições do sistema estão de acordo com as directrizes reguladoras de conformidade. Para mais informações, consulte “EN 50131 Grau 3” na página nº 369.

Tamanho do histórico de registos/eventos

Para conformidade total da EN 50131 Grau 3, o sistema tem de guardar, pelo menos, 500 eventos.

Marcação

Só é permitido marcar o sistema com a etiqueta EN 50131 Grau 3, se forem cumpridos os seguintes requisitos:

- Todos os componentes do sistema estão conforme a EN 50131. Consulte “Componentes certificados pela EN 50131 Grau 3” na página nº 372.
- Todas as definições são feitas de acordo com “EN 50131 Grau 3” na página nº 369.

Se qualquer um destes dois itens não for válido, a etiqueta de EN 50131 Grau 3 tem de ser removida do sistema.

Opções afectadas por outros regulamentos

AVISO! Os produtos para alarme de incêndio e detecção de fumo usados com os sistemas Advisor Advanced destinam-se a ser utilizados exclusivamente por conveniência e não devem ser utilizados como produtos de proteção da vida. A combinação não cumpre com os requisitos legais para os produtos de proteção da vida ou para utilização como sistemas de detecção de incêndios. A Carrier não aceita qualquer responsabilidade por danos derivados da utilização incorreta dos produtos.

Política ACPO

As definições necessárias são todas definições em conformidade com EN 50131 Grau 2, com as seguintes modificações:

- 4.2.n.5.1 Alarmes de entrada, Retardado
- 8.2.4 Reset técnico, tamper activado
- 8.7.6 Confir. alarme:
 - Modo AB, activado para todas as áreas aplicáveis
 - Tempo AB, mínimo 30 min, máximo 60 min
 - Confirmação EE, activada
 - Confirmação TA, activada

Nota: A politica ACPO, permite que um gestor de nível superior se torne um utilizador de nível 3. Também, pode permitido o acesso a menu de utilizador de nível 3 sem autorização de utilizador de nível 2 se for facultado pelo cliente um acordo escrito apropriado.

Política INCERT

As definições necessárias para o INCERT Grau 2 são todas as definições necessárias EN 50131 Grau 2, e as definições para INCERT Grau 3 são todas as definições necessárias EN 50131 Grau 3, com as seguintes modificações:

- 1.2.9.1.m.n.2 Freq.TesteBat.: Todos os dias
- 8.2.1 Aceit. necess: Ativado
- 8.3.3 Lista de alarmes: Desativado
- 8.4.1 Pront.Armaz: Falha de FTC e Bateria definida para Ligada
- 8.4.2 Inibir inclusão: A falha da bateria tem de ser definida para Nível de acesso 2
- 8.4.6 Alarmes em espera: Ativar EN 50131
- 9.3.n.2 Falha de linha: Definir para Se utilizado ou Ligado
- 9.3.n.7.7 Falha de linha: Definido para Ligado

Veja também “EN 50131 Grau 2” na página nº 368 e “EN 50131 Grau 3” na página nº 369.

Política SES

Consoante a predefinição SES escolhida, as definições SES seguintes são necessárias para além de EN 50131 Grau 2 / Grau 3.

- Utilize um botão de pânico dedicado adequado (que não seja possível pressionar acidentalmente).
- O desarme automático não é permitido.
- Para SES Grau 3 não é permitido programar a comunicação GPRS como CRA primária, sendo permitido apenas para Grau 2.
- A tabela abaixo indica os intervalos de polling necessários para SES Grau 2 e Grau 3.

		CRA primária (IP)				
		AÜA-B25	AÜA-B5	AÜA-S180	AÜA-S20	
		25 h	5 h	180 seg.	20 seg.	
CRA de backup (GPRS)	AÜA-B25	25 h	2	2, 3	2, 3	2, 3
	AÜA-B5	5 h	2	2, 3	2, 3	2, 3

* 2, 3: Grau EN-CH do sistema

- Devem ser definidas as opções seguintes:

Padrão e categoria	Intervalo de polling necessário	Via de comunicação e comunicador	Opção	Valor necessário
SES CHD.07 (V3 / 01.01.2011)				
AÜA-B25	25 h	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	24
AÜA-B5	5 h	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	4
AÜA-S180	180 s	IP incorporado ou GPRS via ATS73X0	9.1.n.8.3.2 Tempo de Heartbeat	00:02'30
AÜA-S20	20 s	IP incorporado	9.1.n.8.3.2 Tempo de Heartbeat	00:00'10

Política SBSC

Larmklass 1

As definições necessárias são todas definições em conformidade com EN 50131 Grau 2, com as seguintes modificações:

- 4.2.n.5.1 Alarmes de entrada: Imediato

- 8.7.6.9 Retardo Rep.: Não

Consulte também “EN 50131 Grau 2” na página nº 368.

Larmklass 2

As definições necessárias são todas definições em conformidade com EN 50131 Grau 3, com as seguintes modificações:

- 4.2.n.5.1 Alarmes de entrada: Imediato
- 8.7.6.9 Retardo Rep.: Não

Consulte também “EN 50131 Grau 3” na página nº 369.

Anexo A

Eventos do Advisor Advanced

Para eventos do sistema Advisor Advanced, consulte Tabela 31 abaixo. Para eventos de controlo de acesso, utilizados para programar controladores de portas, consulte Tabela 32 na página nº 393.

Tabela 31: Eventos do Advisor Advanced

Grupo	Evento	#	Descrição do evento	Notas
Zona	Zona ACTIVA	01	Zona activa	Zona no estado activo
	TAMPER	02	Tamper de zona	Zona no estado de tamper (alarme de sabotagem)
	Zona em AM	03	Máscara de zona	Zona em estado de alarme anti-máscara
	FALHA BATERIA	04	Zona em falha de bateria	Zona no estado de falha de bateria
	FALHA ZONA	05	Falha de zona	Zona em estado de falha
	ZONA SUJA	06	Zona suja	Zona em estado sujo
	SUPERVISÃO C	07	Zona com falha de supervisão curta	Zona em estado de supervisão curta
	SUPERVISÃO L	08	Zona com falha de supervisão longa	Zona em estado de supervisão curta
	INIBIDO	09	Zona inibida	Estado da zona mudou para inibido
	ISOLADO	10	Zona isolada	Estado da zona mudou para isolado
	EM TESTE	11	Zona em soak test	O soak test está activo
	ARMADO	12	Zona armada	Zona em modo de arme parcial ou total.
	ALARME	13	Zona em alarme	Zona em alarme. Restaurada após confirmação do alarme.

Grupo	Evento	#	Descrição do evento	Notas
	RF APRENDIDO	14	Dispositivo sem fios programado	Activo durante 3 segundos após uma programação correcta
	Aceitar sinal RF	15	Encontrado dispositivo sem fios	Activo durante 3 segundos após a resposta do dispositivo
	Mantida aberta	16	Zona aberta demasiado tempo	Zone mantida aberta
	Dias inactivos	17	Walk test invertido de zona falhou	A zona está inactiva há mais tempo do que o limite de dias inactivos
	SHUNT	18	Zona em shunt	
	FALHA SHUNT	19	Zona em falha de shunt	Falha — zona está activa quando unshunt
	SHUNT PORTA	20	Shunt de porta	Shunt de zona por shunt de porta
	AV.SHUNTPORTA	21	Aviso de shunt de porta	Tempo de aviso de zona em shunt por shunt de porta

Grupo	Evento	#	Descrição do evento	Notas
Área	ARME TOTAL	01	Área totalmente armada	Área em estado de arme total
	ARME PARCIAL1	02	Área parcialmente armada 1	Área em estado de arme parcial 1
	DESARME	03	Área desarmada	Área em estado de desarme
	ALARME	04	Alarme de intrusão	O alarme de intrusão de área está activo
	ALARM.Á.ARMADA	05	Alarme durante arme total	Alarme de área enquanto em arme total
	ALARME G.PARC	06	Alarme durante arme parcial	Alarme de área enquanto em arme parcial
	ALARM.ÁREA DES	07	Alarme durante desarme	Alarme de área enquanto em desarme
	ALARME DE FTC	08	Alarme e FTC	Alarme de área enquanto FTC presente
	PORTA C.FOGO	09	Porta corta-fogo activa	O alarme de uma porta corta-fogo está activo
	ARMADO PCFOGO	10	Porta corta-fogo durante arme total	Uma porta corta-fogo activa enquanto arme total de área
	GP-PORTA CFOGO	11	Porta corta-fogo durante arme parcial	Uma porta corta-fogo activa enquanto arme parcial de área
	DES.PORT CFOGO	12	Porta corta-fogo durante desarme	Uma porta corta-fogo activa enquanto área desarmada

Grupo	Evento	#	Descrição do evento	Notas
	FTC E P.CFOGO	13	Porta corta-fogo e FTC	Uma porta corta-fogo activa enquanto FTC presente
	FOGO	14	Alarme de incêndio	Um alarme de incêndio activo
	AT - FOGO	15	Alarme de incêndio durante arme total	Um alarme de incêndio activo enquanto arme total de área
	ArP - FOGO	16	Alarme de incêndio durante arme parcial	Um alarme de incêndio activo enquanto arme parcial de área
	DS - FOGO	17	Alarme de incêndio durante desarme	Um alarme de incêndio activo enquanto área desarmada
	FTC E FOGO	18	Alarme de incêndio e FTC	Um alarme de incêndio activo enquanto FTC presente
	PÂNICO	19	Alarme de pânico	Um alarme de pânico activo
	AT - PÂNICO	20	Pânico durante arme total	Um alarme de pânico activo enquanto arme total de área
	ArP - PÂNICO	21	Pânico durante arme parcial	Um alarme de pânico activo enquanto arme parcial de área
	DS - PÂNICO	22	Pânico durante desarme	Um alarme de pânico activo enquanto área desarmada
	FTC E PÂNICO	23	Pânico e FTC	Um alarme de pânico activo enquanto FTC presente
	MÉDICO	24	Alarme médico	Um alarme médico activo
	AT - MÉDICO	25	Alarme médico durante arme total	Um alarme médico activo enquanto arme total de área
	ArP - MÉDICO	26	Alarme médico durante arme parcial	Um alarme médico activo enquanto arme parcial de área
	DS - MÉDICO	27	Alarme médico durante desarme	Um alarme médico activo enquanto área desarmada
	FTC E MÉDICO	28	Alarme médico e FTC	Um alarme médico activo enquanto FTC presente
	ALARME TÉCNIC	29	Alarme técnico	Um alarme técnico activo
	AT - AL.TÉCNIC	30	Alarme técnico durante arme total	Um alarme técnico activo enquanto arme total de área
	ArP - AL.TÉCNIC	31	Alarme técnico durante arme parcial	Um alarme técnico activo enquanto arme parcial de área
	DS - AL.TÉCNIC	32	Alarme técnico durante desarme	Um alarme técnico activo enquanto área desarmada
	FTC E TÉCNICO	33	Alarme técnico e FTC	Um alarme técnico activo enquanto FTC presente
	TAMPER	34	Alarme tamper	Um alarme de tamper activo
	AT - TAMPER	35	Alarme de tamper durante arme total	Um alarme de tamper activo enquanto área desarmada

Grupo	Evento	#	Descrição do evento	Notas
	ArP - TAMPER	36	Alarme de tamper durante arme parcial	Um alarme de tamper activo enquanto arme parcial de área
	DS - TAMPER	37	Tamper durante desarme	Um alarme de tamper activo enquanto área desarmada
	FTC E TAMPER	38	Tamper e FTC	Um alarme de tamper activo enquanto FTC presente
	CAMPAINHA ACT	39	Campainha	Activa durante 2 seg. quando zona com opção de campainha está activa
	ArPCAMPAINHA	40	Campainha durante arme parcial	Activa durante 2 seg. quando zona com opção de campainha está activa durante arme parcial
	DSCAMPAINHA	41	Campainha durante desarme	Activa durante 2 seg. quando zona com opção de campainha está activa durante desarme
	ZONA ACTIVA	42	Zona activa	Pelo menos uma zona da área está em estado activo
	ZONA INIBIDA	43	Zona inibida	Pelo menos uma zona da área está inibida
	ZONA ISOLADA	44	Zona isolada	Pelo menos uma zona da área está isolada
	FALHA ZONA	45	Falha de zona	Pelo menos uma zona da área está em estado de falha
	ZONA EM AM	46	Máscara de zona	Pelo menos uma zona da área está em estado de alarme anti-máscara
	TAMPER ZONA	47	Tamper de zona	Pelo menos uma zona da área está em estado de tamper
	TAMPER RAS	48	Tamper de teclado	Um teclado atribuído à área está em estado de tamper
	FALHA DE RAS	49	Falha de teclado	Um teclado atribuído à área está em estado de falha
	TAMPER DGP	50	Tamper de expansor	Um expansor atribuído à área está em estado de tamper
	FALHA DE DGP	51	Falha de expansor	Um expansor atribuído à área está em estado de falha
	COACÇÃO	52	Coacção	Código de coacção utilizado na área
	AT - COACÇÃO	53	Coacção durante arme total	Código de coacção utilizado enquanto arme total de área

Grupo	Evento	#	Descrição do evento	Notas
	ArP - COACÇÃO	54	Coacção durante arme parcial	Código de coacção utilizado enquanto arme parcial de área
	DS - COACÇÃO	55	Coacção durante desarme	Código de coacção utilizado enquanto área desarmada
	FTC E COACÇÃO	56	Coacção e FTC	Código de coacção utilizado enquanto FTC presente
	TAMPER CÓDIGO	57	Tamper de código	Activo quando um teclado atribuído à área é bloqueado por 2 minutos devido a 3 introduções de PIN incorrectas
	TEMP. ENTRADA	58	Entrada de área	Temporização de entrada de área activa
	TEMP. SAÍDA	59	Saída de área	Temporização de saída de área activa
	FALHA T.SAÍDA	60	Falha de saída	Alarme detectado durante o estado de saída antes de mudar para o estado de arme parcial ou total
	PRONTO ARMAR	61	Pronto a armar	Activo quando todas as condições configuradas de pronto a armar são válidas
	ARME OK	62	Arme de área OK	Activo durante 2 s quando a área é armada correctamente
	FALHA DE ARME	63	O arme da área falhou	Activo durante 30 s após tentativa mal sucedida de arme de área
	DESARME OK	64	Desarme de área OK	Activo durante 2 s quando a área é desarmada
	REC. ALARMES	65	Alarmes a confirmar	Alarmes à espera de confirmação
	RESET FOGO	66	Reinicialização de alarme de incêndio	Para a zona de incêndio, evento activo durante 10 s após confirmação de alarme de incêndio (também inibe a zona de incêndio durante 15 s). Também activo por 10 s durante o walk test da zona de incêndio
	WALK TEST	67	Walk test	O Walk Test de utilizador/instalador está activo
	WALK ZONA ACT	68	Zona de Walk Test activa	Zona em Walk Test está activada

Grupo	Evento	#	Descrição do evento	Notas
	ALARME - A	69	Alarme A	Alarme A activo (alarme não confirmado), reset depois de desarme ou expiração de temporizador AB e sem alarme B.
	ALARME B	70	Alarme B	Alarme B activo (alarme confirmado). Reset após desarme
	SIR. INT. ACT	71	Sirene interna	Sirene interna. Activada no alarme durante o tempo de sirene interna. A activação poderá ser retardada pelo tempo de retardo da sirene. Pode ser novamente accionada pelo alarme seguinte.
	SIR. EXT. ACT	72	Sirene externa	Sirene externa. Activada no alarme durante o tempo de sirene externa. A activação poderá ser retardada pelo tempo de retardo da sirene. Este flag não pode ser novamente accionado.
	STROBE	73	Saída de Strobe	Saída de Strobe. Activada pelo alarme durante o arme. Desactivada após o desarme.
	BESOURO	74	Saída do besouro	Flag de saída do besouro
	RESET AM	75	AM reset	Activado durante o procedimento de arme para efectuar reset aos detectores AM
	ARME PARCIAL 2	76	Arme parcial 2	Área em estado de arme parcial 2.
	AA_AVISO	77	Aviso auto arme	Área em estado de aviso antes de arme automático
	AUTO_ARME	78	Arme automático	Procedimento de arme automático em curso
	HA-ALARME	79	Alarme hold-up A	Reset após desarme
	HB-ALARME	80	Alarme hold-up B	Reset após desarme
	LIM INIB ZON	81	Limite de inibição	Limite de inibição de zona alcançado
	LIM ISOL ZON	82	Limite de isolamento	Limite de isolamento de zona alcançado
	LIM SHUNT ZON	83	Limite de shunt	Limite de shunt de zona alcançado
	FALHA ISOL ZON	84	Zona em falha isolada	

Grupo	Evento	#	Descrição do evento	Notas
	RTD.DESARME	85	Retardo de desarme de ATM	Retardo de desarme de ATM activo
	TEMPO DESARME	86	Tempo de desarme de ATM	Tempo de desarme de ATM activo
	T.AVISO DES.	87	Tempo de aviso de desarme de ATM	Tempo de aviso de ATM activo
	T.EST.DESARME	88	Tempo desarme estendido de ATM	Tempo de desarme estendido de ATM activo
	SHUNTPORTAARE A	89	Shunt de porta	Uma zona da área está em shunt
	AV.SHUNTPORTAAR	90	Aviso de shunt de porta	Uma zona da área está em tempo de aviso de shunt
	DESARMERETAR	91	Desarme retardado	desarme de área retardado
	PROIBID DESARM	92	Proibir desarm	Desarme de utilizador proibido
	SHUNTZON	93	Zona em shunt	Uma zona da área está em shunt
	FALHASHUNT	94	Zona em falha em shunt	Uma zona da área está em estado de falha de shunt
	RESET SENSOR	95	Reset sensor	
	ZH ATIVA	96	Zona horária ativa	
	TAMPER AUDIO	98	Tamper de dispositivo de áudio	Um dispositivo de áudio atribuído à área está em estado de tamper
	FALHA AUDIO	99	Falha de dispositivo de áudio	Um dispositivo de áudio atribuído à área está em estado de falha

Grupo	Evento	#	Descrição do evento	Notas
Teclado	OFFLINE	1	O teclado está offline	Activo se o teclado estiver offline
	RTE	2	RTE accionada	Entrada RTE do teclado accionada
	TAMPER CÓDIGO	3	Tamper de código	Activo quando o teclado é bloqueado por 2 minutos devido a 3 introduções de PIN incorrectas
	TAMPER	4	Tamper de teclado	Tamper de teclado
	COACÇÃO	5	Código coacção	Código de coacção introduzido neste teclado
	CARTÃO ATIVO	6	Cartão introduzido	Um cartão está introduzido neste teclado, activo durante 3 s
	PIN	7	PIN válido	PIN válido introduzido neste teclado, activo durante 3 s

Grupo	Evento	#	Descrição do evento	Notas
	ACESSO PORTA	8	Cartão ou PIN válido	PIN ou cartão válido introduzido neste teclado, activo durante 3 s
	RAS BLOQUEADO	9	Teclado bloqueado	Tamper de código. É restaurado depois de o limite de tempo ter expirado.
	ISOLADO	10	Teclado isolado	
	CAMPAINHA ACT	11	Campainha do teclado activo	
	CARTÃO VÁLIDO	12	Cartão válido	Cartão válido introduzido neste teclado, activo durante 3 s
	SAIDA INICIADA	13	Tempo de saída iniciado	Tempo de saída iniciado durante o arme a partir do teclado seleccionado
	ENTRADA PARADA	14	Tempo de entrada parado	Tempo de entrada parado durante o desarme a partir do teclado seleccionado
	C. INCÓGNITO	15	Cartão não reconhecido	
	ZH ATIVA	16	Zona horária ativa	

Grupo	Evento	#	Descrição do evento	Notas
Expansor	OFFLINE	1	Expansor offline	Activo se o dispositivo estiver offline
	FALHA 230VAC	2	Falha na alimentação de corrente	
	FLH.BATERIA	3	Falha de bateria	
	TAMPER	4	Tamper de expansor	Tamper de dispositivo
	FLH.FUSÍVEL	5	Falha de fusível	
	FLH.SIR.DGP	6	Falha de sirene	
	FALHA RECEPTOR	7	Falha de receptor	Falha de receptor do expansor sem fios
	ISOLADO	8	Expansor isolado	
	TESTBATBAIXA	9	Bateria baixa	A bateria do expansor está fraca
	TST.BAT.ACTIVO	10	Teste de bateria activo	O teste de bateria do expansor está activo
	FALHA TST.BAT	11	Falha do teste de bateria	O teste de bateria do expansor falhou
	FalhaAlimentação	12	Falha de PSU de expansor	

Grupo	Evento	#	Descrição do evento	Notas
Painel	FALHA 230VAC	1	Falha de corrente	Detectada falha na alimentação de corrente do painel
	FALHA BATERIA	2	Falha bateria	
	TAMPER PAINEL	3	Tamper de painel	
	FLH.FUS.PAINEL	4	Falha de fusível do painel	
	FLH.SIR.PAINEL	5	Falha de sirene do painel	
	FALHA DE LINHA	6	Falha de linha	Foi detectada uma falha de linha
	FALHA RTPC	7	Falha de linha RTPC	Foi detectada uma falha de linha RTPC
	FLH. L. ISDN	8	Falha de linha ISDN	Foi detectada uma falha de linha ISDN
	FLH. SINAL GSM	9	Falha de linha GSM	Foi detectada uma falha de linha GSM
	FTC	10	Falha ao Comunicar	Falhou a entrega de uma mensagem de alarme
	FALHA DISP. MI	11	Falha de linha RTPC	Falha de comunicação de bus MI
	FLH. ISDN - MI	12	Falha de linha ISDN	Falha do comunicador ISDN
	FLH. GSM - MI	13	Falha de linha GSM	Falha do comunicador GSM
	FLH. M.VOZ-MI	14	Falha ao Comunicar	Falha do módulo de voz
	FALHA NTP	15	Falha na conexão ao servidor NTP	Falha na conexão ao servidor NTP
	FALHA ETHERNET	16	Falha de linha Ethernet	Falha na ligação Ethernet
	FLIP	17	Falha IP	IP Ethernet não configurado
	FLGPRS	18	Falha de linha GPRS	Falha de ligação GPRS
	FLIPGPRS	19	Falha IP GPRS	IP GPRS não configurado
	FLTDA	20	Falha de linha TDA	Falha de linha de módulo TDA
	FLTDAGPRS	21	Falha de GPRS TDA	Falha de linha de módulo TDA (GPRS)
	FLTDAETH	22	Falha de ETH TDA	Falha de linha de módulo TDA (ETH)
	FMITDA	23	Falha de MI TDA	Falha de dispositivo de MI de painel (TDA)
	EMPASTGSM	24	Empastelamento do GSM	Detectado o empastelamento do GSM
	FalhaAlimentação	25	Falha de PSU de painel	

Grupo	Evento	#	Descrição do evento	Notas
	TST.BAT.PAINEL	26	Teste de bateria do painel activo	
	FLH.TST.BAT P	27	Falha de teste de bateria do painel	
	FALHABATCOM	28	Falha de bateria do comunicador	
	RESETMODCOM	29	Reset do módulo do comunicador	
	TAMPERDISPINB	30	Tamper de painel inibido	
	TAMPERSIRINIB	31	Tamper de sirene inibido	
	MIFAS	32	Falha do dispositivo MI (áudio de 2 vias)	
	WAN FL	33	Falha de linha (WAN em ETH)	

Grupo	Evento	#	Descrição do evento	Notas
Utilizador	CARTÃO/PIN OK	1	Cartão ou PIN apresentado	PIN ou cartão válido apresentado pelo utilizador seleccionado. Activo por 3 s após o evento. Pode ser utilizado para controlar o bloqueio da porta para utilizadores específicos.
	CONTROLOSMS	2	Controlo SMS activo	O controlo SMS está activo
	BLOQCONTROLSMS	3	Controlo SMS bloqueado	Controlo SMS desactivado devido a tentativas inválidas
	REPOTESMS	4	Reporte SMS activo	O reporte SMS está activo
	REPAPOSARME	5	Reporte SMS após arme	O reporte SMS será activado após arme

Grupo	Evento	#	Descrição do evento	Notas
Output	OUTPUT ACTIVA	1	Saída activa	A saída especificada está activa
	ON	2	Saída ligada	A saída física está activada
	FORÇADO	3	Saída de porta forçada	

Grupo	Evento	#	Descrição do evento	Notas
Filtro	FILT.COND.ACT	1	Condição verdadeira	A condição de filtro seleccionada é verdadeira/válida.

Grupo	Evento	#	Descrição do evento	Notas
Grupo de utilizadores	CARTÃO/PIN OK	1	Cartão ou PIN apresentado	Cartão ou PIN válido apresentado por um utilizador do grupo de utilizadores seleccionados. Activo por 3 s após o evento. Pode ser utilizado para controlar sirenes para grupos de utilizadores específicos.
	ZH ATIVA	2	Zona horária ativa	

Grupo	Evento	#	Descrição do evento	Notas
Sistema	TUDO ARMADO	1	Tudo armado	Todas as áreas do sistema estão armadas
	ATENDE AUTO	2	Atende Auto	O procedimento de atendimento automático iniciou-se (1 min.)
	PC REM. ACTIVO	3	Ligação remota	Ligação remota activa
	FLH. PC REMOTO	4	Falha de ligação remota	Falha de ligação remota (1 min.)
	EM PROG. LOCAL	5	Programação local	Programação local activa
	EM PROG. REMOT	6	Programação remota	Programação remota activa
	HORA ALTERADA	7	Hora alterada	Hora do sistema alterada
	SCRENSAVER ON	8	Visor armado	Visor armado activo
	SIR. INT. ACT	9	Sirene interna	Flag de evento de sirene interna (alarme do sistema)
	SIR. EXT. ACT	10	Sirene externa	Flag de evento de sirene externa (alarme do sistema)
	STROBE	11	Saída de Strobe	Flag de evento de Strobe (alarme do sistema)
	FALHA SISTEMA	12	Falha global	Flag de falha global de sistema
	TAMPER SISTEMA	13	Tamper global	Flag de tamper global de sistema
	MODO TÉCNICO	14	Modo técnico activo	O modo técnico está activo para o instalador
	MODO WT ON	15	Modo Walk Test ligado	
	Test Detector	16	Teste de detector activo	
	TstDet Falhou	17	Falha de teste de detector	
	AR HIEARQ 1	18	Hierarquia 1	Todas as áreas da hierarquia 1 estão armadas
	AR HIEARQ 2	19	Hierarquia 2	Todas as áreas da hierarquia 2 estão armadas

Grupo	Evento	#	Descrição do evento	Notas
	AR HIEARQ 3	20	Hierarquia 3	Todas as áreas da hierarquia 3 estão armadas
	FLHREPPowerUP	21	Falha de reporte de ligação do sistema	
	LIS-IN ATIVO	22	A escuta de áudio na sessão está ativa	
	Cloud disp.	23	O painel está pronto para a ligação à "cloud" UltraSync	O painel tem número de série
	Reg. Cloud	24	O painel está registado na "cloud" UltraSync	
	UltraSync SIM	25	O cartão SIM UltraSync está presente no módulo GSM	

Grupo	Evento	#	Descrição do evento	Notas
Porta	DESABILITADO	1	Porta desactivada	
	DESBLOQUEADA	2	Porta desbloqueada	Porta desbloqueada até bloqueio manual ou por um programa
	PERÍODO DESBL	3	Período porta desbloqueada	Porta desbloqueada automaticamente
	T DESBLOQUEADA	4	Desbloqueio temporizado de porta	Porta desbloqueada por um tempo específico
	ABERTA	5	Porta aberta	A porta fica desbloqueada durante o tempo configurado na respectiva configuração.
	ABERTA	6	Porta aberta	A zona da porta encontra-se no estado activo/tamper
	FORÇADA	7	Porta forçada	A zona da porta foi activada sem desbloquear
	DOTL	8	DOTL de porta	Zona da porta activa após tempo de shunt
	SHUNTING	9	Shunt de porta	A zona da porta foi inibida
	FALHA LEITOR	10	Falha do leitor de porta	Problema de comunicação do leitor de porta
	TAMPER LEITOR	11	Tamper do leitor de porta	O tamper do leitor de porta está activo
	LTR NÃO SEGURO	12	Porta não segura	A zona da porta encontra-se no estado activo/tamper, ou a porta está desbloqueada, ou a segunda zona da porta encontra-se no estado activo/tamper

Grupo	Evento	#	Descrição do evento	Notas
	INPUT PORTA	13	Entrada de porta	A zona da porta encontra-se no estado activo/tamper

Grupo	Evento	#	Descrição do evento	Notas
CRA	FTC	1	Falha ao comunicar	Falhou a entrega de uma mensagem de alarme
	HB	2	Falha de heartbeat OH	Falha de protocolo OH heartbeat
	OCUPADO	3	CRA ocupada	CRA ocupada (em utilização)
	LIS-IN ATIVO	4	Listen-in ativo	Ativo quando a sessão de listen-in com a central recetora seleccionada estiver ativa
	LIS-IN FLAG1	5	Flag de listen-in 1	Uma flag programável, que pode ser ativada durante 3 s por um código DTMF
	LIS-IN FLAG2	6	Flag de listen-in 2	Uma flag programável, que pode ser ativada durante 3 s por um código DTMF
	LIS-IN FLAG3	7	Flag de listen-in 3	Uma flag programável, que pode ser ativada durante 3 s por um código DTMF
	LIS-IN FLAG4	8	Flag de listen-in 4	Uma flag programável, que pode ser ativada durante 3 s por um código DTMF

Grupo	Evento	#	Descrição do evento	Notas
Trigger	S1 1230/34	1	Botão de comando 1	Alternar o estado quando o botão de comando 1 é premido
	S2 1230/34	2	Botão de comando 2	Alternar o estado quando o botão de comando 2 é premido
	S1S2 1230/34	3	Botões de comando 1 e 2	Estado armado quando botão de comando 1 é premido, estado de rearme quando botão de comando 2 é premido
	REMOTEOUT	4	Controlo à distância	
	TECLA FUNÇÃO	5	Controlo por tecla de função	
	PROGRAMA	6	Controlo por programa	
	Comando (1235)	7	O trigger é activado por um comando	

Grupo	Evento	#	Descrição do evento	Notas
Calendário	Comutar de H/H	1	A cada hora	O flag de evento é comutado cada hora aos 00 min
	Comutar Diária	2	Todos os dias	O flag é comutado todos os dias às 00:00
	Segunda-feira	3	Segunda	Activo às segundas
	Terça-feira	4	Terça	Activo às terças
	Quarta-feira	5	Quarta	Activo às quartas
	Quinta-feira	6	Quinta	Activo às quintas
	Sexta-feira	7	Sexta	Activo às sextas
	SÁBADO	8	Sábado	Activo aos sábados
	DOMINGO	9	Domingo	Activo aos domingos

Grupo	Evento	#	Descrição do evento	Notas
Comando	COMANDO APRENDIDO	1	Comando programado	Activo durante 3 segundos após uma programação correcta
	BOTÃO 1	2	Botão 1 premido	
	BOTÃO 2	3	Botão 2 premido	
	BOTÃO 3	4	Botão 3 premido	
	BOTÃO 4	5	Botão 4 premido	
	BOTÃO 1+2	6	Botões 1 + 2 premidos	
	BOTÃO 1+3	7	Botões 1 + 3 premidos	
	BOTÃO 1+4	8	Botões 1 + 4 premidos	
	BOTÃO 2+3	9	Botões 2 + 3 premidos	
	BOTÃO 2+4	10	Botões 2 + 4 premidos	
	BOTÃO 3+4	11	Botões 3 + 4 premidos	
	BATBAIXACMD	12	Bateria fraca do comando	

Grupo	Evento	#	Descrição do evento	Notas
Câmara	Imag Capturada	1	Foi obtida uma imagem	Activo durante 3 segundos
	Exc limit imag	2	O limite da imagem foi excedido	

Grupo	Evento	#	Descrição do evento	Notas
Grupo de áreas	Arme	1	Todas as áreas armadas	Todas as áreas do grupo de áreas estão armadas
	ArmeP1	2	Arme parcial 1 todas	Todas as áreas do grupo de áreas têm arme parcial 1
	ArmeP2	3	Arme parcial 2 todas	Todas as áreas do grupo de áreas têm arme parcial 2

Grupo	Evento	#	Descrição do evento	Notas
	PAR	4	Todas pronto a armar	Todas as áreas do grupo de áreas estão no estado pronto a armar
	DESARME	5	Todas desarmadas	Todas as áreas do grupo de áreas estão desarmadas
	ARMETOTAL	6	Todas as áreas com arme total	Todas as áreas do grupo de áreas estão no estado de arme total
	ALARME	7	Um estado de alarme	Pelo menos uma área está em alarme
	SAIR	8	Um estado de saída	Pelo menos uma área está em estado de saída
	NPA	9	Não pode armar	Pelo menos uma área do grupo de áreas não está no estado pronto a armar
	ARMEÁREA	10	Uma área foi armada	Activo durante 3 seg
	DESARMEÁREA	11	Uma área foi desarmada	Activo durante 3 seg

Grupo	Evento	#	Descrição do evento	Notas
Programa	ZH ATIVA	1	Programa activo	

Grupo	Evento	#	Descrição do evento	Notas
Dia especial	DIA ESP ATIVO	1	Dia especial está activo	

Grupo	Evento	#	Descrição do evento	Notas
Leitor	OFFLINE	1	O leitor está offline	
	TAMPER	2	Tamper do leitor	

Tabela 32: Eventos de controladores de portas

Grupo	Evento	N.º	Descrição do evento	Notas
Porta	Porta aberta	1		O comando de abertura de porta está activo (para desbloquear/iniciar shunt)
	Porta desbloq.	2		A saída de desbloqueio é activada para desbloquear a porta
	Porta bloq.	3		A saída de desbloqueio é desactivada para bloquear a porta
	Ignorar porta	4		O programa de baixa segurança atribuído à porta é válido

Grupo	Evento	N.º	Descrição do evento	Notas
	IgnPortalnib	5	Inibir ignorar porta	O programa de baixa segurança é inibido
	Porta desabil.	6		A porta é totalmente desactivada (a partir do teclado ou do computador)
	Porta habilit.	7		
	Leitor desabil	8		O leitor de porta é desactivado
	Leitor habilit	9		O leitor de porta é activado
	2cart interior	10		É necessário o acesso com dois cartões no leitor de entrada
	2cart exterior	11		É necessário o acesso com dois cartões no leitor de saída
	Baixa seg.int.	12	Baixa segurança de porta no interior	Cartão ou PIN necessários para aceder no leitor de entrada
	Baixa seg.ext.	13	Baixa segurança de porta no exterior	Cartão ou PIN necessários para aceder no leitor de saída
	Anti-Passback	14		Anti-Passback está activo
	Shunt da porta	15		O temporizador de shunt está a contar
	Aviso shunt	16		O temporizador de aviso está a contar
	P.Área armada	17		A área atribuída à porta está armada. Como saída de macro, este evento desactiva a porta quando "Negar acesso quando armada" estiver definido como Sim.
	Coacção teclado	18		O PIN de coacção é introduzido através do teclado da porta
	DOTL	19		O contacto de porta está activo após expirar o temporizador de shunt
	Forçado	20		O contacto de porta está activo sem um comando de porta válido
	LED 1	21		A saída de LED 1 está activa
	LED 2	22		A saída de LED 2 está activa
	Besouro	23		A saída de besouro está activa

Grupo	Evento	N.º	Descrição do evento	Notas
Acesso a portas	Interbloqueio	1		As zonas de interbloqueio estão activas
	Interbloq.igno	2		O interbloqueio foi ignorado
	Negado	3		O acesso à porta não foi autorizado
	Concedido	4		O acesso à porta foi autorizado
	Acesso seguido	5		O acesso à porta foi concedido a um utilizador com seguimento ligado
	Conc.1passagem	6		O acesso à porta foi concedido após uma passagem
	Conc.2passagem	7		O acesso à porta foi concedido após duas passagens
	Conc.3passagem	8		O acesso à porta foi concedido após três passagens
	Conc.botãoENT	9		O acesso à porta foi concedido e o botão de ENTRADA foi premido
	Conc.botãoSAI	10		O acesso à porta foi concedido e o botão de SAÍDA foi premido
	Fogo ignorar	11		A anulação secundária está activa
	Normal	12		A porta está bloqueada e fechada.
	Anti-psbck des	13	Desactivar anti-passback	Desactivar anti-passback para a porta seleccionada

Grupo	Evento	N.º	Descrição do evento	Notas
Região	Limite	1	Limite de região	Activo quando o número de pessoas em qualquer região atinge o presente limite (255 eventos, 1 por região)
	Util para Ext	2	Mover os utilizadores da região para a região 1 exterior	Mover utilizadores da região seleccionada (1 a 255) para a região 1 exterior (255 eventos)
	Todos Exterior	3	Mover todos os utilizadores para a região 1 exterior	Mover todos os utilizadores para a região 1 exterior
	Util sem Reg.	4	Repor os utilizadores da região para a região 256 (nenhuma região)	O valor da região dos utilizadores da região seleccionada (1 a 255) é repostado para 256 (255 eventos, 1 por região)

Grupo	Evento	N.º	Descrição do evento	Notas
	Todos sem Reg	5	Repor todas as regiões de utilizadores para 256 (nenhuma região)	O valor das regiões de todos os utilizadores é reposto para 256
	ZHorária ativa	6	Programa activo	Activado se um programa seleccionado estiver activo (24 eventos, 1 por programa)

Grupo	Evento	N.º	Descrição do evento	Notas
Falhas	FihLeitorPorta	1		
	FalhaBloqPorta	2		
	RAS offline	3		O RAS no databus local do controlador de portas está offline (16 eventos, 1 por endereço RAS)
	DGP offline	4		O DGP no databus local do ATS1260 está offline
	Fih 230VAC DGP	5	Falha de rede do controlador de portas	Condição de falha de rede existente no controlador de portas
	Bat. baixa DGP	6	Bateria fraca do controlador de portas	Condição de bateria fraca existente no controlador de portas
	FihFusivel DGP	7	Falha de fusível do controlador de portas	Condição de falha de fusível existente no controlador de portas
	Fih SIR DGP	8	Falha de sirene do controlador de portas	Condição de falha de sirene (tamper de sirene) existente neste controlador de portas
	Tamper DGP	9	Tamper de controlador de portas	Condição de tamper de armário existente neste controlador de portas
	DGP offline	10	DGP do controlador de portas offline	O controlador de portas não comunica com o Advisor Master

Grupo	Evento	N.º	Descrição do evento	Notas
Outros	Área desarmada	1	Área desarmada	Área desarmada (16 eventos, 1 por área)
	Alarme de área	2	Alarme de área	Zonas em alarme na área (16 eventos, 1 por área)
	Out.DGP ativo	3	Saídas DGP	A saída de sistema atribuída a este DGP está activa (16 eventos, 1 por saída). Primeiros 16 no DGP podem também ser activados pela função de saída física

Grupo	Evento	N.º	Descrição do evento	Notas
	Zona DGP ativa	4	Zonas	Zona neste DGP activa (16 eventos, 1 por zona)
	OutFisicaAtiva	5	Saídas físicas	A saída ligada a este DGP está activa (255 eventos, 1 por saída). As saídas acima de 16 só são activadas pela macro de porta.
	Tst Bat At DGP	6	Teste de bateria do controlador de portas activo	Teste de bateria em execução neste controlador de portas
	FihTestBat DGP	7	Falha do teste de bateria do controlador de portas	O teste de bateria falhou neste controlador de portas
	SIR DGP ativa	8	Sirene do controlador de porta activa	A saída de sirene (16º relé) está activa

Anexo B

Códigos de reporte utilizados no Advisor Advanced

Tabela 33 abaixo apresenta os códigos de reporte SIA, CID e VdS utilizados no Advisor Advanced.

Tabela 34 na página nº 407 - indica os valores permitidos para os códigos de reporte aplicáveis.

Tabela 33: Descrição dos códigos de reporte SIA, CID e VdS

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
1.	AN	0xB0	14	R393	Restauração de detector sujo		Baixa
2.	AR	0xB2	7	R301	Restauração AC		Baixa
3.	AS	0x30	14	E393	Detector sujo		Baixa
4.	AT	0x32	7	E301	Problema AC		Média
5.	BA	0x22	3	E130	Alarme anti-roubo	Alarme / entrada em máscara / anomalia quando armado	Média
6.	BB	0x51	11	E570	Bypass de intrusão	Inibição do alarme	Baixa
7.	BC	0xA2	3	E406	Alarme anti-roubo cancelado	Cancelar alarme por utilizador / tecla / remotamente	Baixa
8.	BJ	0xB0	14	R381	Restauração de supervisão do detector		Baixa
9.	BR	0xA2	3	R130	Restauração intrusão		Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
10.	BT	0x30	14	E380	Anomalia intrusão	Entrada em máscara/anomalia quando desarmado	Baixa
11.	BU	0xD1	11	R570	Unbypass de intrusão	Desinibição de alarme	Baixa
12.	BV	0x00	5	E139	Confirmação do alarme	ACPO	Média
13.	BW	0x80	5	R139	Restauração de alarme confirmado	ACPO	Baixa
14.	BZ	0x30	14	E381	Supervisão do detector		Baixa
15.	CF	0x61	8	E408	Arme forçado	Arme por utilizador/por tecla	Baixa
16.	CG	0x62	8	E456	Arme parcial	Arme parcial por utilizador / tecla / remotamente	Baixa
17.	CL	0x61	8	R401	Arme normal	Arme por utilizador	Baixa
				R407	Arme normal	Arme remotamente	Baixa
				R409	Arme normal	Arme por tecla	Baixa
18.	EE	0x30	14	E374	Erro de saída	Falha de saída	Média
19.	ER	0xB0	14	R143	Restauração Expansão	Restauração de anomalia do expansor / teclado / áudio	Baixa
				R300	Restauração expansão	Restauração de fusível do expansor	Baixa
				R330	Restauração expansão	Restauração de comunicação do expansor / teclado / áudio / memória de imagens libertada manualmente	Baixa
				R333	Restauração expansão	Restauração de módulo externo	Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
20.	ET	0x30	14	E143	Anomalia Expansão	Anomalia do expansor / teclado / áudio / memória de imagens cheia	Baixa
				E300	Anomalia Expansão	Falha de fusível do expansor	Baixa
				E330	Anomalia Expansão	Falha de comunicação do expansor / teclado / áudio	Baixa
				E333	Anomalia Expansão	Falha do módulo externo	Baixa
21.	FA	0x10	1	E110	Alarme de incêndio		Alta
22.	FB	0x51	11	E570	Bypass de incêndio	Inibição de incêndio	Baixa
23.	FJ	0xB0	14	R373	Restauração de anomalia de incêndio		Baixa
24.	FR	0x90	1	R110	Restauração de incêndio		Baixa
25.	FT	0x30	14	E373	Anomalia de incêndio		Baixa
26.	FU	0xD1	11	R570	Unbypass de incêndio	Desinibição de incêndio	Baixa
27.	FW	0x30	14	–	Fogo supervisionado longo		Baixa
28.	HA	0x24	9	E121	Suspender alarme	Coacção	Alta
29.	HR	0xA4	9	R121	Restauração de suspensão	Restauração de coacção	Baixa
30.	JP	0x63	14	E466	Entrada de serviço		Baixa
31.	JR	0xE3	14	R466	Saída de serviço		Baixa
32.	JT	0x53	14	E625	Hora alterada		Baixa
33.	LB	0x01	14	E627	Início de programação local		Baixa
34.	LR	0xBA	12	R351	Restauração de linha		Baixa
35.	LS	0x81	14	R628	Fim de programação local		Baixa
36.	LT	0x3A	12	E351	Falha de linha		Baixa
37.	MA	0x48	10	E100	Alarme médico		Alta
38.	MB	0x51	11	E570	Bypass médico		Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
39.	MJ	0xB0	14	–	Restaura supervisão longa médica		Baixa
40.	MR	0xC8	10	R100	Restauo médico		Baixa
41.	MS	0x30	14	–	Médico supervisionado longo		Baixa
42.	MU	0xD1	11	R570	Unbypass médico		Baixa
43.	OP	0xE1	8	E401	Desarme normal	Desarme pelo utilizador	Baixa
				E407	Desarme normal	Desarme remotamente	Baixa
				E409	Desarme normal	Desarme por tecla	Baixa
44.	OU	0xE1	8	E406	Desarme de alarme	Desarme por utilizador / tecla / remotamente	Baixa
45.	PA	0x21	2	E120	Alarme de pânico		Alta
46.	PB	0x51	11	E570	Bypass de pânico		Baixa
47.	PJ	0xA1	2	R375	Restauo de anomalia de pânico		Baixa
48.	PR	0xA1	2	R120	Restauo de pânico		Baixa
49.	PT	0x21	2	E375	Anomalia de pânico		Baixa
50.	PU	0xD1	11	R570	Unbypass de pânico		Baixa
51.	RB	0x74	14	E416	Início de programação remota		Baixa
52.	RP	0x40	0	E602	Teste automático/teste tocar		Baixa
53.	RR	0x53	15	E305	Arranque	Ligação do sistema	Baixa
54.	RS	0xF4	14	R416	Sucesso de programação remota		Baixa
55.	RU	0x55	14	R416	Falha de programação remota		Baixa
56.	RX	0x40	0	E601	Teste CRA manual		Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
57.	TA	0x23	4	E144	Alarme tamper	Tamper de zona	Média
				E145	Alarme tamper		Média
				E320	Alarme tamper	Tamper de sirene do expansor	Média
58.	TB	0x51	11	E570	Bypass de tamper		Baixa
59.	TR	0xA3	4	R144	Restauração de tamper	Restauração de tamper de zona	Baixa
				R145	Restauração de tamper		Baixa
				R320	Restauração de tamper	Restauração de sirene do expansor	Baixa
				R370	Restauração de tamper	Restauração de tamper de KeyBox	Baixa
60.	TT	0x23	4	E370	Zona 'Key Box' activa		Alta
61.	TU	0xD1	11	R570	Unbypass de tamper		Baixa
62.	UB	0x51	14	E570	Expansor / teclado / áudio / zona ignorada	Expansor / teclado / áudio / zona isolado	Baixa
63.	UU	0xD1	14	R570	Expansor / teclado / áudio / zona não ignorado	Expansor / teclado / áudio / zona em serviço	Baixa
64.	WF	0xF6	13	E612	Falha de Walk Test		Baixa
65.	WP	0x76	13	E611	Êxito de Walk Test		Baixa
66.	XH	0xB0	14	R344	Rest. Empast. RF		Baixa
67.	XQ	0x30	14	E344	Empastelamento		Baixa
68.	XR	0xB0	14	R384	Restauração de bateria fraca de detector ou comando		Baixa
69.	XT	0x30	14	E384	Bateria fraca de detector ou comando		Baixa
70.	YC	0x37	12	E350	Falha de comunicação	Falha de dispositivo ISDN / GSM / voz / áudio	Baixa
71.	YK	0xB9	12	R354	Restauração de comunicações	Restauração de dispositivo ISDN / GSM / voz / áudio	Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
72.	YR	0xB3	6	R302	Restauo de fusível/bateria do sistema	Restauo de fusível/bateria do expansor / marcador	Baixa
73.	YS	0x39	12	E354	Anomalia de comunicação	Falha em comunicar (FTC)	Baixa
74.	YT	0x33	6	E302	Anomalia de fusível / bateria do sistema	Falha de fusível / bateria fraca de expansor / marcador	Baixa
75.	ZA	0x40	13	E152	Alarme técnico — temperatura baixa	Alarme de detector de temperatura baixa	Média
76.	ZB	0x51	11	E570	Restauo técnico — temperatura baixa	Restauo de detector de temperatura baixa	Baixa
77.	ZJ	0xB0	14	R381	Bypass técnico — temperatura baixa	Inibição de detector de temperatura baixa	Baixa
78.	ZR	0xC0	13	R152	Unbypass técnico — temperatura baixa	Desinibição de detector de temperatura baixa	Baixa
79.	ZS	0x30	14	E381	Supervisão longa técnica — temperatura baixa	Alarme de supervisão longa de detector de temperatura baixa	Baixa
80.	ZU	0xD1	11	R570	Restauo de supervisão longa técnica — temperatura baixa	Restauo de supervisão longa de detector de temperatura baixa	Baixa
81.	YA	0x23	4	E321	Falha de sirene		Baixa
82.	YH	0xA3	4	R321	Restauo de sirene		Baixa
83.	NC	0x34	12	E356	Falha de poll de CS	Heartbeat inactivo	Baixa
84.	NR	0xB4	12	R356	Restauo de poll de CS	Heartbeat activo	Baixa
85.	CP	0x61	8	R403	Arme automático	Armar por programa	Baixa
86.	OA	0xE1	8	E403	Desarme automático	Desarmar por programa	Baixa
87.	OT	0x61	8	E608	Fecho tardio	Arme automático adiado	Baixa
88.	OK	0xE1	8	R608	Abertura precoce	Desarmar manualmente antes do desarme automático	Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
89.	IA	0x63	14	E313	Pedido de reset técnico		Baixa
90.	IR	0xE3	14	R313	Restauo de reset técnico		Baixa
91.	GA	0x73	13	E151	Alarme técnico — gás	Alarme de detector de gás	Alta
92.	GR	0xF3	13	R151	Restauo técnico — gás	Restauo de detector de gás	Alta
93.	GB	0x51	11	E570	Bypass técnico — gás	Inibição de detector de gás	Baixa
94.	GU	0xD1	11	R570	Unbypass técnico — gás	Desinibição de detector de gás	Baixa
95.	GS	0x30	14	E381	Supervisão longa técnica — gás	Alarme de supervisão longa de detector de gás	Baixa
96.	GJ	0xB0	14	R381	Restauo de supervisão longa técnica — gás	Restauo de supervisão longa de detector de gás	Baixa
97.	KA	0x78	5	E158	Alarme técnico — temperatura alta	Alarme de detector de temperatura alta	Média
98.	KR	0xF8	5	R158	Bypass técnico — temperatura alta	Inibição de detector de temperatura alta	Média
99.	KB	0x51	11	E570	Restauo de supervisão longa técnica — temperatura alta	Restauo de supervisão longa de detector de temperatura alta	Baixa
100.	KU	0xD1	11	R570	Restauo técnico — temperatura alta	Restauo de detector de temperatura alta	Baixa
101.	KS	0x30	14	E381	Supervisão longa técnica — temperatura alta	Alarme de supervisão longa de detector de temperatura alta	Baixa
102.	KJ	0xB0	14	R381	Unbypass técnico — temperatura alta	Inibição de detector de temperatura alta	Baixa
103.	WA	0x72	13	E154	Alarme técnico — água	Alarme de detector de água	Média
104.	WR	0xF2	13	R154	Restauo técnico — água	Restauo de detector de água	Média
105.	WB	0x51	11	E570	Bypass técnico — água	Inibição de detector de água	Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
106.	WU	0xD1	11	R570	Unbypass técnico — água	Desinibição de detector de água	Baixa
107.	WS	0x30	14	E381	Supervisão longa técnica — água	Alarme de supervisão longa de detector de água	Baixa
108.	WJ	0xB0	14	R381	Restauro de supervisão longa técnica — água	Restauro de supervisão longa de detector de água	Baixa
109.	ES	0x23	4	E145	Alarme tamper	Alarme de tamper de expansor / teclado / áudio	Média
				E341	Alarme de tamper	Tamper de módulo externo	Média
110.	EJ	0xA3	4	R145	Restauro de tamper	Restauro de tamper de expansor / teclado / áudio	Média
				R341	Restauro de tamper	Restauro de tamper do módulo externo	Média
111.	HV	0x00	2	E129	Alarme hold-up confirm		Média
112.	HW	0xA1	2	R129	Restauro alarme hold-up confirmado		Baixa
113.	UA	0x00	5	E150	Zona técnica — alarme geral		Média
114.	UR	0x80	5	R150	Zona técnica — restauro de alarme geral		Média
115.	IT	0x71	13	E607	Início de walk test de zona única / início teste bateria	Início de walk test de zona única, também para zonas múltiplas seleccionadas / início teste bateria	Alta
116.	FT	0xF1	13	R607	Fim de walk test de zona única / fim teste bateria	Fim de walk test de zona única, também para zonas múltiplas seleccionadas / fim teste bateria	Baixa
117.	LU	0x55	14	R628	Falha de programação local		Baixa

#	Código SIA	Código VdS	Canal VdS	Código CID	Função	Nota	Prioridade de relatório
118.	YP	0x32	7	E301	Problemas de alimentação eléctrica		Baixa
119.	YQ	0xB2	7	R301	Alimentação eléctrica restabelecida		Baixa
120.	CI	0xF9	8	E455	Falha de arme automático		Baixa
121.	DD	0xFA	—	E421	Acesso negado	Cartão desconhecido	Baixa
122.	JA	0x23	—	R461	Introdução de código incorreta	Tamper código	Baixa
123.	EX	0x54	14	E308	Falha de dispositivo	Falha do sistema ou dispositivo e reinicializar	Baixa
124.	JV	—		E928	PIN alterado		Baixa
125.	JX	—		E928	Utilizador eliminado		Baixa
126.	JY	—		E928	Utilizador adicionado		Baixa

Tabela 34: Valores dos códigos de reporte SIA e CID

#	Código SIA	Intervalo e tipo de subevento	Código CID	Intervalo de grupos	Intervalo de pontos
1.	AN	Zona (1–512)	R393	Área (1–64)	Zona (1–512)
2.	AR	Expansor (299–307)	R301	Sistema (0)	Expansor (65–72)
3.	AS	Zona (1–512)	E393	Área (1–64)	Zona (1–512)
4.	AT	Expansor (299–307)	E301	Sistema (0)	Expansor (65–72)
5.	BA	Zona (1–512)	E130	Área (1–64)	Zona (1–512)
6.	BB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
7.	BC	Sistema (0), Utilizador (1–50)	E406	Área (1–64)	Utilizador (0), Utilizador (1–50)
8.	BJ	Zona (1–512)	R381	Área (1–64)	Zona (1–512)
9.	BR	Zona (1–512)	R130	Área (1–64)	Zona (1–512)
10.	BT	Zona (1–512)	E380	Área (1–64)	Zona (1–512)
11.	BU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
12.	BV	Zona (1–512)	E139	Área (1–64)	Zona (1–512)
13.	BW	Zona (1–512)	R139	Área (1–64)	Zona (1–512)
14.	BZ	Zona (1–512)	E381	Área (1–64)	Zona (1–512)
15.	CF	Utilizador (1–50) Zona (1–512)	E408	Sistema (0) Área (1–64)	Utilizador (1–50) Zona (1–512)

#	Código SIA	Intervalo e tipo de subevento	Código CID	Intervalo de grupos	Intervalo de pontos
16.	CG	Utilizador (1–50) Zona (1–512)	E456	Sistema (0) Área (1–64)	Utilizador (1–50) Zona (1–512)
17.	CL	Teclado (401–408)	–	–	–
		Utilizador (1–50)	R401	Área (1–64)	Utilizador (1–50)
		Sistema (0)	R407	Sistema (0)	
		Zona (1–512)	R409	Área (1–64)	Zona (1–512)
18.	EE	Utilizador (1–50)	E374	Área (1–64)	Zona (1–512)
19.	ER	Expansor (299–307), teclado (401–408)	R143	Sistema (0)	Expansor (65–72), teclado (1–8)
		N.º fusível expansor (316–324)	R300	Sistema (0)	Expansor (65–72)
		N.º polling expansor (332–340), N.º polling teclado (465–472)	R330	Sistema (0)	Expansor (65–72), teclado (1–8)
		Zona (1–512), expansor (299–307), teclado (401–408)	R333	Área (1–64)	Zona (1–512)
20.	ET	Expansor (299–307), teclado (401–408)	E143	Sistema (0)	Teclado (1–8), Expansor (65–72)
		N.º fusível expansor (316–324)	E300	Sistema (0)	Expansor (65–72)
		N.º polling expansor (332–340), N.º polling teclado (465–472)	E330	Sistema (0)	Expansor (65–72), teclado (1–8)
		Zona (1–512), expansor (299–307), teclado (401–408)	E333	Área (1–64)	Zona (1–512)
21.	FA	Sistema (0) Zona (1–512)	E110	Sistema (0) Área (1–64)	Teclado (1–8) Zona (1–512)
22.	FB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
23.	FJ	Zona (1–512)	R373	Área (1–64)	Zona (1–512)
24.	FR	Zona (1–512)	R110	Área (1–64)	Zona (1–512)
25.	FT	Zona (1–512)	E373	Área (1–64)	Zona (1–512)
26.	FU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
27.	FW	Zona (1–512)	–	Área (1–64)	Zona (1–512)
28.	HA	Utilizador (1–50) Zona (1–512)	E121	Área (1–64) Área (1–64)	Utilizador (1–50) Zona (1–512)
29.	HR	Teclado (401–408)	R121	Sistema (0)	Teclado (1–8)
30.	JP	Sistema (0)	E466	Sistema (0)	–
31.	JR	Sistema (0)	R466	Sistema (0)	–
32.	JT	Utilizador (1–50)	E625	–	–
33.	LB	Sistema (0)	E627	–	–
34.	LR	Caminho de comunicação (0–6) [1]	R351	Sistema (0)	–
35.	LS	Sistema (0)	R628	–	–
36.	LT	Caminho de comunicação (0–6) [1]	E351	Sistema (0)	–

#	Código SIA	Intervalo e tipo de subevento	Código CID	Intervalo de grupos	Intervalo de pontos
37.	MA	Sistema (0) Zona (1–512)	E100	Sistema (0) Área (1–64)	Teclado (1–8) Zona (1–512)
38.	MB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
39.	MJ	Zona (1–512)	–	Área (1–64)	Zona (1–512)
40.	MR	Zona (1–512)	R100	Área (1–64)	Zona (1–512)
41.	MS	Zona (1–512)	–	Área (1–64)	Zona (1–512)
42.	MU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
43.	OP	Utilizador (1–50) Sistema (0) Zona (1–512)	E401 E407 E409	Área (1–64) Sistema (0) Área (1–64)	Utilizador (1–50) Zona (1–512)
44.	OR	Utilizador (1–50) Zona (1–512)	E406	Sistema (0) Área (1–64)	Utilizador (1–50) Zona (1–512)
45.	PA	Sistema (0) Utilizador (1–50) Zona (1–512)	E120	Sistema (0) Área (1–64) Área (1–64)	Teclado (1–8) Utilizador (1–50) Zona (1–512)
46.	PB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
47.	PJ	Zona (1–512)	R375	Área (1–64)	Zona (1–512)
48.	PR	Zona (1–512)	R120	Área (1–64)	Zona (1–512)
49.	PT	Zona (1–512)	E375	Área (1–64)	Zona (1–512)
50.	PU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
51.	RB	Não utilizado (0)	E416	Sistema (0)	–
52.	RP	Não utilizado (0)	E602	–	–
53.	RR	Expansor (299–307), teclado (401–408)	E305	Sistema (0)	Expansor (65–72), teclado (1–8)
54.	RS	Sistema (0)	R416	Sistema (0)	–
55.	RU	Sistema (0)	–	–	–
56.	RX	Sistema (0)	E601	Sistema (0)	–
57.	TA	Zona (1–512) Expansor (299–307), teclado (401–408) Expansor (316–324)	E144 E145 E320	Área (1–64) Sistema (0) Sistema (0)	Zona (1–512) Expansor (65–72), teclado (1–8) Expansor (65–72)
58.	TB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
59.	TR	Zona (1–512) Expansor (299–307), teclado (401–408) Expansor (316–324)	R144 R145 R320	Área (1–64) Sistema (0) Sistema (0)	Zona (1–512) Expansor (65–72), teclado (1–8) Expansor (65–72)
60.	TT	Zona (1–512)	E370	Área (1–64)	Zona (1–512)

#	Código SIA	Intervalo e tipo de subevento	Código CID	Intervalo de grupos	Intervalo de pontos
61.	TU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
62.	UB	Expansor (299–307), teclado (401–408)	E570	Sistema (0)	Expansor (65–72), teclado (1–8)
		Zona (1–512)	–	–	–
63.	UU	Expansor (299–307), teclado (401–408)	R570	Sistema (0)	Expansor (65–72), teclado (1–8)
		Zona (1–512)	–	–	–
64.	WF	Área (1–64)	E612	Área (1–64)	Área (1–64)
65.	WP	Área (1–64)	E611	Área (1–64)	Área (1–64)
66.	XH	Expansor (299–307) Caminho de comunicação (0–6) [1]	R344	Sistema (0)	Expansor (65–72)
67.	XQ	Expansor (299–307) Caminho de comunicação (0–6) [1]	E344	Sistema (0)	Expansor (65–72)
68.	XR	Zona (1–512) Comando (1–112)	R384	Área (1–64)	Zona (1–512)
69.	XT	Zona (1–512) Comando (1–112)	E384	Área (1–64)	Zona (1–512)
70.	YC	Sistema (0)	E350	Sistema (0)	–
71.	YK	Sistema (0)	R354	Sistema (0)	–
72.	YR	Expansor (299–307)	R302	Sistema (0)	Expansor (65–72)
73.	YS	Sistema (0)	E354	Sistema (0)	–
74.	YT	Expansor (299–307) Zona (1–512)	E302	Sistema (0)	Expansor (65–72)
75.	ZA	Zona (1–512)	E152	Área (1–64)	Zona (1–512)
76.	ZB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
77.	ZJ	Zona (1–512)	R381	Área (1–64)	Zona (1–512)
78.	ZR	Zona (1–512)	R152	Área (1–64)	Zona (1–512)
79.	ZS	Zona (1–512)	E381	Área (1–64)	Zona (1–512)
80.	ZU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
81.	YA	Expansor (316–324)	E321	Sistema (0)	Expansor (65–72)
82.	YH	Expansor (316–324)	R321	Sistema (0)	Expansor (65–72)
83.	NC	CS (1–16)	E356	Sistema (0)	CS (1–16)
84.	NR	CS (1–16)	R356	Sistema (0)	CS (1–16)
85.	CP	Sistema (0)	R403		
86.	OA	Sistema (0)	E403		
87.	OT	Utilizador (1–50)	E608		
88.	OK	Utilizador (1–50)	R608		

#	Código SIA	Intervalo e tipo de subevento	Código CID	Intervalo de grupos	Intervalo de pontos
89.	IA	Sistema (0)	E313		
90.	IR	Utilizador (1–50)	R313		
91.	GA	Zona (1–512)	E151	Área (1–64)	Zona (1–512)
92.	GR	Zona (1–512)	R151	Área (1–64)	Zona (1–512)
93.	GB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
94.	GU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
95.	GS	Zona (1–512)	E381	Área (1–64)	Zona (1–512)
96.	GJ	Zona (1–512)	R381	Área (1–64)	Zona (1–512)
97.	WA	Zona (1–512)	E154	Área (1–64)	Zona (1–512)
98.	WR	Zona (1–512)	R154	Área (1–64)	Zona (1–512)
99.	WB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
100.	WU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
101.	WS	Zona (1–512)	E381	Área (1–64)	Zona (1–512)
102.	WJ	Zona (1–512)	R381	Área (1–64)	Zona (1–512)
103.	KA	Zona (1–512)	E158	Área (1–64)	Zona (1–512)
104.	KR	Zona (1–512)	R158	Área (1–64)	Zona (1–512)
105.	KB	Zona (1–512)	E570	Área (1–64)	Zona (1–512)
106.	KU	Zona (1–512)	R570	Área (1–64)	Zona (1–512)
107.	KS	Zona (1–512)	E381	Área (1–64)	Zona (1–512)
108.	KJ	Zona (1–512)	R381	Área (1–64)	Zona (1–512)
109.	ES	Expansor (299–307), teclado (401–408)	R145	Sistema (0)	Expansor (65–72), teclado (1–8)
		Zona (1–512), expansor (299–307), teclado (401–408)	R341	Área (1–64)	Zona (1–512)
110.	EJ	Expansor (299–307), teclado (401–408)	E145	Sistema (0)	Expansor (65–72), teclado (1–8)
		Zona (1–512), expansor (299–307), teclado (401–408)	E341	Área (1–64)	Zona (1–512)
111.	HV	Zona (1–512)	E129	Área (1–64)	Zona (1–512)
112.	HW	Zona (1–512)	R129	Área (1–64)	Zona (1–512)
113.	UA	Zona (1–512)	E140	Área (1–64)	Zona (1–512)
114.	UR	Zona (1–512)	R140	Área (1–64)	Zona (1–512)
115.	TS	Área (1–64) Expansor (299–307)	E607	Área (1–64)	Área (1–64)
116.	TE	Área (1–64) Expansor (299–307)	R607	Área (1–64)	Área (1–64)
117.	LU	Sistema (0)	R628	Área (1–64)	Área (1–64)
118.	YP	Expansor (299–307)	E301	Sistema (0)	Expansor (65–72)

#	Código SIA	Intervalo e tipo de subevento	Código CID	Intervalo de grupos	Intervalo de pontos
119.	YQ	Expansor (299–307)	R301	Sistema (0)	Expansor (65–72)
120	CI	Utilizador (1–50)	E455	Área (1-8)	Utilizador (1–50)
121	DD	Teclado (401–408)	E421	Sistema (0)	Teclado (1-8)
		Cartão			
122.	JA	Teclado (401–408)	R461	Sistema (0)	Teclado (1-8)
123.	EX	Sistema (0)	E308	Sistema (0)	—
124.	JV	Utilizador (1–50)	E928	Sistema (0)	Utilizador (1–50)
125.	JX	Utilizador (1–50)	E928	Sistema (0)	Utilizador (1–50)
126.	JY	Utilizador (1–50)	E928	Sistema (0)	Utilizador (1–50)

[1] O caminho de comunicação é um dos seguintes:

- 1: RTPC
- 2: ISDN
- 3: GSM
- 4: IP
- 5: TDA9xx
- 6: TDA74xx
- 7: TDA75xx
- 61: Porta virtual TDA74xx GPRS
- 62: Porta virtual TDA74xx ETH
- 71: Porta virtual TDA75xx GPRS
- 72: Porta virtual TDA75xx ETH

Nota: O intervalo de relatório SIA assume a numeração de expansores de 0 a 8, em que o expansor 0 é o próprio painel de controlo.

Glossário

Acção	Uma acção é uma função programada pelo utilizador, que pode ser executada automaticamente de acordo com o programa configurado.
Activo	Consulte Normal / Activa / Sabotagem / Inibida / Isolada / Mascarada / Falha.
Alarme	O estado de um sistema de segurança quando um dispositivo ligado a uma zona é activado e a condição da área é de tal ordem que a activação deve ser assinalada. Por exemplo, o fecho da porta está partido, fazendo soar a sirene.
Alarme de incêndio	Um alarme accionado por detectores de fogo ou de fumo, que indica um incêndio.
Alarme de intrusão	Um alarme accionado por um dispositivo de segurança, como um PIR ou contacto da porta, indicando que alguém entrou sem acesso autorizado. Também pode ser denominado alarme de intrusão.
Anti-passback	A função anti-passback permite que os utilizadores sejam transferidos de uma região para outra. Entrar numa região duas vezes seguidas ou não é possível, ou resultará no registo e reporte de um evento ao operador.
Área	Uma secção da instalação que tem requisitos de segurança específicos. O sistema Advisor Advanced permite a divisão de todas as instalações em áreas diferentes com diferentes requisitos de segurança. Cada área tem as suas próprias zonas. Cada área é identificada por um número ou um nome. Por exemplo, área 1, Oficina, etc.
Armado	Consulte Arme.
Arme	A condição de uma área em que uma alteração do estado de qualquer zona (de normal para activa) provoca um alarme. Umas instalações ou uma área só é armada quando está desocupada. Algumas zonas (como cofres) podem estar continuamente armadas.
Arme automático	Arme automático das instalações, iniciado por um programa. Ver programa.
Arme parcial	A condição da parte integrante de uma área onde a alteração do estado de determinadas zonas (de normal para activa) provoca um alarme. Uma área ou instalação está armada parcialmente, quando está parcialmente desocupada, por exemplo, o exterior de uma casa está armada parcialmente, mas o interior ainda está desarmado.
Áudio de duas vias	O áudio de duas vias permite ao operador da central recetora ouvir áudio ao vivo a partir das instalações protegidas em alarme e responder de volta.
Botão de pânico	Consulte Suspeito.

Câmara PIR sem fios	Um detector PIR sem fios com câmara digital incorporada, que obtém imagens e envia as mesmas para o painel de controlo quando zonas específicas ficam activas.
Cartão	Um suporte de dados que aloja credenciais através das quais um utilizador pode ser identificado num sistema de segurança. Na configuração do utilizador, o cartão está associado a um utilizador e define os respectivos direitos de acesso. Também denominado badge (crachá). Os cartões são utilizados em leitores ou teclados com leitores integrados.
Central receptora	Uma empresa que monitoriza se ocorreu um alarme num sistema de segurança. A central receptora está localizada fora das instalações/área que monitoriza.
Coacção	Uma situação em que um utilizador é forçado a violar o sistema de segurança (por exemplo, forçado a abrir a porta com arma apontada). A função de coacção do Advisor Advanced permite que um sinal seja activado pelo utilizador (por exemplo, uma notificação para uma central receptora). Isto é efectuado introduzindo um dígito de coacção em conjunto com um PIN.
Comando	Um dispositivo sem fios pessoal, utilizado para realizar funções programadas, por exemplo, armar ou desarmar instalações, abrir portas.
Comunicador	Um dispositivo electrónico que permite ao sistema Advisor Advanced transmitir alarmes e outros eventos para uma central receptora. Também pode ser utilizado para efectuar upload/download.
Comutador de chave	Um dispositivo que utiliza um comutador para armar ou desarmar áreas. O comutador necessita de uma chave para comutar.
Consola de arme (RAS)	Consulte Teclado.
Contacto de porta	Um contacto magnético utilizado para detectar se uma porta ou janela é aberta.
Controlador de portas	Um expansor de quatro portas é um painel de controlo de acesso que alarga o sistema ATS com funções avançadas de controlo de acesso.
Controlo de acesso	O controlo de entrada ou saída de uma área de segurança através de portas.
Controlo de alarme	O controlo das funções de alarme.
Controlo de porta	O controlo de portas. Faz parte das funções de controlo de acesso.
Cursor	Um carácter de sublinhado a piscar no ecrã de cristais líquidos (LCD) que indica onde irá aparecer o próximo carácter introduzido no teclado.
Desarme	Uma condição de uma área, quando está ocupada e a actividade normal não acciona um alarme.
DGP	Expansor de dados. Consulte Expansor.
Dia especial	Uma data na qual as janelas de tempo alternativas num programa activo são válidas.
Dispositivo de áudio	Os dispositivos de áudio são utilizados para a verificação áudio duas vias de um alarme.
DTMF	Sinalização de multifrequência de tom duplo. O DTMF permite ao operador da central receptora enviar comandos específicos ao painel de controlo utilizando uma sessão de áudio ativa.

Duplo	Detector duplo. Um dispositivo de segurança utilizado para detectar intrusos numa determinada parte de uma área ou instalações. A técnica utilizada baseia-se em duas técnicas, como PIR e RADAR ou PIR e ultrasónica.
Expansor	Um dispositivo que recolhe dados de outros dispositivos de segurança dentro de uma área e transfere-os para o painel de controlo Advisor Advanced.
Expansor de câmara PIR sem fios	Um expansor sem fios que recolhe dados de câmaras PIR sem fios e transfere os mesmos para o painel de controlo.
Expansor de saídas	Um módulo de PCI que se liga ao painel de controlo Advisor Advanced ou a um expansor para fornecer relé ou saídas de colectador aberto.
Expansor remoto	Consulte Expansor.
Expansor sem fios	Um expansor que recolhe dados de comandos e sensores sem fios e transfere os mesmos para o painel de controlo.
Falso alarme	Um alarme que é accionado por um dispositivo de segurança, sem qualquer intrusão. Pode ser provocado por uma janela aberta, animais de estimação ou projecção incorrecta do equipamento de segurança.
Filtro de condição	Um conjunto de regras que é criado por entradas e equações lógicas. Utilizado para controlar saídas (outputs) e grupos de utilizadores.
Grupo de portas	Os grupos de portas especificam quando é concedido acesso a uma porta específica. Os grupos de portas são atribuídos a utilizadores. Cada grupo de portas pode ter um período de tempo diferente (programa) quando pode ser concedido acesso à porta.
Grupo de utilizadores	Os grupos de utilizadores definem as opções e permissões disponíveis a utilizadores.
Histórico	Uma lista dos alarmes antigos e de eventos de controlo de acesso armazenada na memória que pode ser visualizada num teclado LCD ou através de ligações ao PC.
Inibir	Consulte Normal / Activa / Sabotagem / Inibida / Isolada / Mascarada / Falha.
Instalador	Uma empresa que instala e faz a manutenção do equipamento de segurança.
LCD	Ecrã de cristais líquidos. A parte do teclado em que as mensagens são apresentadas.
LED	Díodo Emissor de Luz. Um indicador luminoso num teclado que comunica uma condição. Por exemplo, área em alarme, falha de comunicação, etc.
Leitor	Um dispositivo utilizado para o controlo de acesso que lê cartões para autorizar o acesso. Consoante as necessidades e o tipo de cartões, o leitor pode, por exemplo, ser um leitor de cartão magnético ou leitor de proximidade. Poderá estar integrado num teclado.
Lista de acções	As listas de acções são utilizadas para agrupar acções configuradas. Podem ser executadas automaticamente consoante o programa configurado.
Listen-in	Consulte Áudio de duas vias.

Normal / Activa / Sabotagem / Inibida / Isolada / Mascarada / Falha	<p>Descreve a condição de uma zona.</p> <ul style="list-style-type: none"> • Normal: a zona NÃO está activada. Por exemplo, porta de saída de emergência fechada. • Activo: a zona está activada. Por exemplo, porta de saída de emergência aberta. • Tamper (Sabotagem): a zona está aberta ou sofreu um curto-circuito. Alguém pode ter tentado sabotar o dispositivo de segurança. • Inibida: a zona foi inibida de indicar estado normal ou activo. Está excluída de funcionar como parte integrante do sistema durante um determinado tempo. Contudo, os tampers são ainda monitorizados. • Isolada: a zona foi inibida de indicar estado normal ou activo. Está excluída de funcionar como parte integrante do sistema de forma permanente. • Mascarada: o detector está coberto (mascarado). • Falha: o detector reporta uma falha interna.
Online/offline	Operacional/não operacional. Um dispositivo pode estar offline devido a uma falha no próprio dispositivo ou pode estar desligado do controlo.
Painel de controlo	Um dispositivo electrónico que é utilizado para recolher todos os dados das zonas das instalações. Consoante a programação e o estado das áreas, gera sinais de alarme. Se necessário, os alarmes e outros eventos podem ser reportados à central receptora.
Pedido para sair da zona	Uma zona que está programada para abrir uma porta utilizando um botão ou um PIR. Utilizado para permitir aos utilizadores sair sem utilizar o leitor da porta. Pedido para sair é geralmente abreviado para RTE. Também denominado “egress”.
PIN	Um número de 4 a 10 dígitos atribuído a, ou seleccionado por um utilizador. É necessário introduzir um PIN num teclado Advisor como um pré-requisito para efectuar a maioria das opções do Advisor Advanced. Na configuração do Advisor Advanced, o PIN está associado a um número de utilizador que identifica o detentor do PIN ao sistema.
PIR	Detector de infra-vermelhos passivo. Um dispositivo de segurança utilizado para detectar intrusos numa determinada parte de uma área ou instalação. A técnica utilizada baseia-se na detecção por infravermelhos.
Poll	Uma mensagem de consulta enviada continuamente pelo painel de controlo do Advisor Advanced para expansores e teclados. O polling permite à unidade remota transferir dados para o painel de controlo.
Porta inteligente	<p>Existem dois tipos de portas no sistema ATS.</p> <ul style="list-style-type: none"> - Porta inteligente: Uma porta controlada por um controlador de portas. Esta porta pode ser utilizada para o controlo de acesso avançado. - Porta padrão: Uma porta controlada pelo painel de controlo. Permite apenas funções de controlo de acesso básico.
Programa	Um conjunto de acções programadas.
Protecção de ecrã	Consulte Visor armado

RAS	Consola de arme remota. Consulte Teclado.
Região	Uma região é uma área de controlo de acesso definida que possui portas que actuam como fronteiras. As regiões são utilizadas pelas funções de anti-passback para monitorizar em que regiões estão presentes utilizadores. As transferências de uma região para outra podem ser proibidas pelas definições de anti-passback.
Região de alta segurança (HSR - High Security Region)	<p>As regiões de alta segurança (HSR) exigem que um determinado número de utilizadores de alta segurança (HSU) estejam presentes nas mesmas para permitir a entrada de utilizadores normais. Se um utilizador de alta segurança deixar a região, fazendo com que demasiado poucos HSU estejam presentes na mesma, é emitido um alarme precedido por um tempo de pré-aviso.</p> <p>O sistema não permite que o utilizador normal permaneça na HSR sem HSU presentes, pelo que o último utilizador de alta segurança não poderá abandonar a área de alta segurança se utilizadores normais estiverem presentes na mesma.</p>
Reportes de alarme	Um procedimento para transmitir eventos de alarme ou outros eventos para a central receptora através de um comunicador e um conjunto de regras denominado protocolo.
Screensaver	Consulte Visor armado
Shunt	Um procedimento que inibe automaticamente uma zona de gerar um alarme quando é activada. Por exemplo, o shunt proíbe que uma porta gere um alarme quando permanece aberta durante um período de tempo curto.
Suspensão	Um alarme (silencioso) que é accionado por um botão de suspensão. Geralmente, não acciona nenhuma sirene, apenas envia uma mensagem para uma central receptora. Por vezes também denominado botão de pânico.
Tamper	<p>Uma situação em que uma zona, teclado, painel de controlo, expansor ou ligações associadas são sabotados ou danificados acidentalmente. A função de sabotagem do Advisor Advanced activa um sinal quando ocorre uma sabotagem.</p> <p>Os alarmes de tamper das zonas são denominados tampers de zona.</p>
Teclado	Um dispositivo que é o painel de controlo do utilizador para opções de segurança de áreas ou de pontos de acesso (portas). O teclado pode ser uma consola (teclado LCD utilizado para programar o painel de controlo, efectuar opções do utilizador, ver alarmes, etc.) ou qualquer outro dispositivo que possa ser utilizado para efectuar a função de segurança, como armar/desarmar, abrir portas, etc.
Teclado remoto	Consulte Teclado.
Técnico	Pessoal de uma empresa instaladora que está qualificado para instalar e fazer a manutenção do painel de controlo.
Test detector	Função de sistema de alarme para detectores com uma entrada de teste dedicada. Após a activação da entrada de teste de detector, o painel verifica se é emitido um sinal de alarme adequado pelo detector para o sistema. Esta funcionalidade permite testar os detectores de difícil acesso.

Trigger	Os triggers (accionadores) são variáveis de sistema que podem ser utilizadas em filtros de condições para controlar saídas remotamente. Cada trigger possui 7 flags (alarmes) independentes que podem ser definidos ou redefinidos. Os flags podem ser controlados de diversas formas, por exemplo: programa, comando SMS, botão de comando, software de PC.
Up/Download	Um protocolo que proporciona formas de visualizar o estado de um sistema Advisor Advanced ou de alterar os parâmetros no sistema, seja no local ou remotamente.
Utilizador	Qualquer pessoa que utilize o sistema Advisor Advanced. Os utilizadores são identificados no sistema Advisor Advanced por um número exclusivo, que está associado ao PIN ou cartão do utilizador.
Utilizador de alta segurança (HSU - High Security User)	Consulte Região de alta segurança.
Visor armado	O visor armado é activado num teclado após um tempo de inactividade específico. Neste modo, a informação apresentada no LCD e LED é muito limitada por motivos de segurança. É necessária uma intervenção do utilizador para voltar ao modo de apresentação normal.
Walk test	Um teste executado por um utilizador ou instalador. Para passar o teste, o utilizador ou instalador tem de passar pelos detectores para os activar. A intenção é verificar a funcionalidade do sistema de segurança.
Walk test invertido	Um teste baseado em contar os dias de inactividade para cada zona.
Zona	Um sinal eléctrico de um dispositivo de segurança ou de um grupo de dispositivos (detector PIR, contacto de porta) para o sistema Advisor Advanced. Cada dispositivo é identificado por um número ou um nome de zona. Por exemplo, zona 14, Porta de saída de emergência.
Zona virtual	Uma zona cujo estado depende do estado de uma saída programada em vez de depender de um sinal eléctrico numa entrada. As zonas virtuais são utilizadas na programação de funcionalidades avançadas.

Índice remissivo

A

- abertura do painel, 173
- abertura temporizada, 170
- abrir porta, 170
- acção, **92**, **277**, 281
 - criar, 281
 - eliminar, 282
 - nome, 281
- acções
 - ver, 277
- acesso a zona, 51
- acesso negado, 248, 257
- activar porta, 170
- actualizar, 358
- adicionar
 - acção, 281
 - central receptora, 318
 - comando, 114, 236
 - dia especial, 282
 - dispositivo de áudio, 201
 - evento, 270
 - expansor, 187
 - filtro, 269
 - grupo de pisos, 267
 - grupo de portas, 263
 - grupo de utilizadores, 210
 - janela de tempo, 280
 - leitor, 199
 - ligação de PC, 347
 - macro, 196
 - piso, 266
 - porta, 243
 - programa, 279
 - RAS, 177
 - região, 265
 - saída, 271
 - trigger, 275
 - utilizador, 203
 - zona, 213
- adicionar filtro ao sistema, 269
- adicionar um dia especial, 282
- adicionar um grupo de pisos, 267
- adicionar um grupo de portas, 263
- adicionar um grupo de utilizadores, 210
- adicionar um piso ao sistema, 266
- adicionar um programa, 279
- adicionar um trigger, 275
- adicionar um utilizador ao sistema, 203
- adicionar uma acção, 281
- adicionar uma central receptora, 318
- adicionar uma janela de tempo, 280
- adicionar uma ligação de PC, 347
- adicionar uma macro ao sistema, 196
- adicionar uma porta ao sistema, 243
- adicionar uma região, 265
- Advisor Advanced Pro, **131**
- alarme, 156
 - confirmação, 234
 - restaurar, 305
- alarme de pânico, 185, 311
- alarme manter aberto, 223
 - tempo, 289
- alarme técnico, 219
- alarmes de entrada, 233
- alta segurança, 234
- alterar grupo de utilizadores, 211
- alterar PIN, 204
- alterar um piso, 266
- alterar um utilizador, 204
- alterar uma porta, 244
- anti-máscara, 217
- anti-passback, **84**, 262
- apagar automaticamente imagens, 195
- apagar um trigger, 276
- apagar uma central receptora, 323
- apagar uma ligação de PC, 348
- aplicação móvel, **131**
- APN, 344
- aprender cartão, 205
- área, **57**, 215, **229**
 - hierarquia, 57, 234
 - hora de saída remota, 231
 - modo de selecção, 207
 - retardo desarme, 233
 - tempo de aviso, 232
 - tempo de entrada/saída, 230, 231
 - tempo de pré-alarme, 232
- arm, 59
- arme, **59**
- arme automático, 111, 232
- arme final, 288
- arme forçado, 299

arme parcial, 59, 223
 nome, 299
 opções, 298
arme rápido, 183
árvore de menus, 432
ATM, **124**, 316
 retardo, 316
 tempo de aviso de desarme, 317
 tempo desarme, 317
 tempo desarme estendido, 317
atualização do firmware
 remoto, 351
atualização do firmware remoto, 351
áudio de duas vias, **125**, 171, 186, 200, 225,
 238, 327
 teste, 171
auto teste, 224
aviso de shunt de porta, 250

B

baixa segurança, 247
bateria
 estado, 166
besouro, 313
blindagem, 23
bloquear dados do utilizador, 72
bloquear e desbloquear com impulso, 86
 procedimento de abertura de porta, 87
 procedimento de bloqueio de porta, 87
bloquear porta, 170, 248
bloquear quando fechada, 256
bloqueio, 64, 136
bloqueio de dados do utilizador, 72
bloqueio do teclado, 64, 136
bloqueio técnico, 290
bus do sistema, 24

C

calendário, **92**, 277
câmara, 119, **239**
 filtro, 240
 isolar, 241
 lista de zona, 239
 obter imagem, 241
caminho de transmissão, 319, 330
campanha, 217, 312
canal seguro, 186
capacidade de zonas, 151
cartão
 atribuir, 205
 remover, 206
 verificar, 169
cartão de utilizador, 205
cartão e PIN, 253

central receptora, 318
 apagar, 323
 backup, 104
 criar, 318
 mapeamento, 102
 primária, 103
chamada, 348
chamada de teste, 160, 162
 chamada de teste frequente, 162
 expandir chamada de teste, 161
 FTC, 162
chamada de teste frequente, 162
chave de encriptação, 186
coacção
 desactivar, 255
código desafio, 294
código do instalador, 146
código do sistema, 292
códigos CID, 403
códigos SIA, 403
comando, 206, **236**
 adicionar, 114, 236
 botões, 237
 nome, 237
 remover, 239
 utilizador atribuído, 237
comunicação, **318**
 atender automático, 348
 caminho de transmissão, 319, 330
 central receptora, 318
 chamada, 348
 código de conta, 320
 Downloader, 356
 encriptação, 326
 eventos, 329
 GSM, 337
 heartbeat frequente, 326
 ligação de PC, 346
 nome de destino, 324, 350
 número de linha, 326
 número de receptor, 326
 número de telefone, 324
 nuvem, 351
 porta de destino, 324, 350
 porta de vídeo, 326
 protocolo, 319, 321
 rede GSM, 338, 339
 subeventos, 322
 teste, 100
 Titan, 356
 UltraSync, 351
comutador de chave, 52, 219
configuração automática, **4**, 146
configuração remota, 310, 351
 assistência técnica, 310
 supervisor, 310
configurações de imagem, 193

- configurar
 - área, 230
 - arme parcial, 298
 - comando, 236
 - dispositivo de áudio, 201
 - entrada, 304
 - evento, 197, 270
 - expansor, 187
 - filtro de condição, 269
 - grupo de áreas, 236
 - leitor, 199
 - macro, 196
 - macro output, 198
 - piso, 266
 - porta, 244
 - saída, 271
 - teclado, 177
 - utilizador, 204
 - zona, 214, 304
- confirmação de alarme, 234, 307
- confirmação de zona, 221
- confirmação do utilizador, 290
- conflito de IP, 367, 368
- conta, 340
- contagem de impulsos, 227
- controlador de porta
 - sincronização, 198
- controlador de portas, **82**
 - opções, 303
 - saídas, 261
- controlo de acesso, **82**
 - reporte, 258
- controlo de alarme, 246
- controlo de porta, 170
- controlo DTMF, **126**, 328
- crédito, 340
- criar filtro, 269
- criar um dia especial, 282
- criar um grupo de pisos, 267
- criar um grupo de portas, 263
- criar um grupo de utilizadores, 210
- criar um piso, 266
- criar um programa, 279
- criar um trigger, 275
- criar um utilizador, 203
- criar uma acção, 281
- criar uma central receptora, 318
- criar uma janela de tempo, 280
- criar uma ligação de PC, 347
- criar uma macro, 196
- criar uma porta, 243
- criar uma região, 265

D

- data, 285
- demo, 170
- desactivar coacção, 255
- desactivar porta, 170

- desarme, **59**
 - desarme retardado, 60
- desarme duplo, 234
- desarme retardado, 60
- desarme temporizado, 316
 - retardo, 316
 - tempo, 317
 - tempo de aviso, 317
 - tempo estendido, 317
- desativar porta, 251
- desbloquear porta, 170, 247
 - saída, 245
- desinibir, 216
- DGP
 - remover, 190
- DHCP, 334
- dia especial, 277, 282
 - criar, 282
 - eliminar, 283
 - hora de fim, 283
 - hora de início, 283
 - nome, 283
- diagnóstico do painel, 169
- diagnóstico IP, 162
- dias da semana, 280
- dias inactivos, 153, 290
- disarm, 59
- disposição do teclado, 141
- dispositivo de áudio, **125**, **200**
 - configurações, 201
 - isolar, 202
 - nome, 201
- dispositivo RF
 - configuração, 227, 238
 - remover, 229, 238
 - supervisão, 229
- dispositivo sem fios, 112, 227, 238
 - supervisão, 229
- dispositivos bus, **69**, **176**
- DNS, 335
- dois cartões, 253
- DOTL
 - saída, 261
- Downloader, **356**
- DST, 285
- duplo impulso, 216
 - temporizadores, 288
- duração do teste, 154

E

eliminar

- DGP, 190
- dispositivo de áudio, 202
- expansor, 190
- leitor, 200
- macro, 198
- notificação, 354
- porta, 252
- saída, 275
- teclado, 187
- zona, 226

eliminar um dia especial, 283

eliminar um grupo de pisos, 268

eliminar um grupo de portas, 264

eliminar um grupo de utilizadores, 212

eliminar um piso, 266

eliminar um programa, 284

eliminar um utilizador, 207

eliminar uma acção, 282

eliminar uma janela de tempo, 281

eliminar uma região, 265

emparelhamento de zona, 217

encriptação, 326, 333

encriptação

- código, 349

endereçamento, 33, 310

endereço IP, 334

entrada, 213

- opções, 304

prolongar tempo, 218

resistência, 153

retardo, 289

teste, 151

entrada/saída, 51, 53, 223

acesso, 299

arme total, 299

bloqueio PIN, 182

entradas do menu, 295

acesso, 136

acesso não autorizado, 136

com o PIN, 136

como editar texto, 139

como editar um endereço host, 140

como editar uma lista, 140

como programar opções Sim/Não, 139

como programar valores, 139

confirmação de alterações, 140

explicação do ecrã LCDy, 138

percorrer a lista de menus, 138

programação, 138

sair, 141

EOL, 27, 189, 304

EOL de sirene, 305

erro de saída, 301

esquema, 33, 310

esquema de endereçamento clássico, 310

esquema de endereçamento flexível, 310

estado de área, 184

estado de entrada, 151, 156

estado de RF, 152

estado painel, 156

estados de dispositivos, 176

estatísticas IP, 163

evento, 95

eventos, **329**

- mapeamento, 329

expandir chamada de teste, 161

expansão de zona, 32

expansor, 69, **70**, 176, **187**

- definições, 188

- EOL, 189

- isolar, 189

- loop dupla, 189

- modo de input, 189

- nome, 188

- remover, 190

- resolução de problemas, 368, 369, 370

- valores da resistência, 189

- versão de firmware, 198

- violação, 189

- zona única, 189

F

falha, 156

falha de linha

- WAN, 337

falha de linha WAN, 337

falha de saída, 301

- reportar, 301

falha do sistema, 173

falha EE

- reportar, 301

filtro, **269**

- criar, 269

- remover, 271

filtro de condições, 89, 283

filtro de início, 272

filtro parar, 272

filtros de condições, **269**, 272

firewall, 336

firmware, 358

flash, 358

formato do cartão, 254

formato Tecom de 27 bits, 303

fórmula, 197, 269

frequência SIA, 322

FTC, 104

funções programáveis, 107

funções programáveis pelo utilizador, 107

G

gateway, 335
 gestão de utilizadores, 203
 glossário, 417
 GPRS, 344
 falha de linha, 344
 nome de utilizador, 344
 password, 344
 tempo de desligar, 345
 grupo de áreas, **57, 235**
 atribuir áreas, 236
 nome, 236
 grupo de pisos, **83, 267**
 criar, 267
 eliminar, 268
 nome, 267
 grupo de portas, **83, 263**
 criar, 263
 eliminar, 264
 nome, 264
 grupo de utilizadores, **74, 210, 256**
 alterar, 211
 criar, 210
 eliminar, 212
 funções, 74
 limitação de privilégios, 76
 nome, 211
 opções, 212
 tipo, 211
 GSM, 337
 estado da bateria, 166
 relatório, 327

H

hardware, 173
 HDR, 152
 heartbeat, 325
 frequente, 326
 heartbeat frequente, 326
 hierarquia, 234
 histórico de alarmes, 150
 hora de fim, 280, 283
 hora de início, 280, 283
 hora de saída remota, 231
 hora e data, 285
 horário de verão, 285
 HSR, **85, 263**
 HSU, **85, 263**

I

ID do painel, 349
 indicação de falha, 296
 indicador de área, 183
 informação do painel, 172
 inibir, **62, 216**
 inspeção, 294
 data, 294

instalação, **144**
 instalação de bateria, 18
 instalação rápida, **2**
 instalador, **71**
 acesso, 288
 confirmação do utilizador, 290
 interbloqueio, 259
 interface IP, 162
 inverter saída, 272
 isolar, **62, 215, 216**
 câmara, 241
 teclado, 182

J

janela de tempo, 277
 criar, 280
 dias da semana, 280
 eliminar, 281
 fim, 280
 início, 280

K

key box
 tempo, 289

L

LCD
 tempo ES, 297
 LDR, 152
 LED, 254
 leitor, **199, 244**
 canal seguro, 186
 cartão e PIN, 253
 dois cartões, 253
 formato do cartão, 254
 iluminação de fundo, 185
 LED, 254
 programa, 254
 redefinir chave de comunicação, 186
 RTE, 185
 leitor de cartões, **15**
 leitor de entrada, 244
 leitor de saída, 244
 leitor LCD, 200
 ligação à terra, 22
 ligação das zonas, 25
 ligação de PC, 346, 356
 apagar, 348
 criar, 347
 host, 350
 porta, 350
 limitação de privilégios, 76
 limitar relatórios, 225, 305
 limite contagem região, 196
 limite de tempo de cartão e PIN, 287
 limite inibição, 235
 limite isolamento, 235

limite shunt, 235
lista de acções, 92
lista de eventos, 383
listar zonas abertas, 151
listen in, 171, 186, 200, 225, 238, 327
 teste, 171
logic, 89
login remoto, 205
loop dupla, 189

M

MAC, 337
macro, 196
 criar, 196
 eliminar, 198
mapa de programação, 432
mapear LEDs do painel, 303
mapear relés de controladores de portas, 303
marcador
 bateria, 166
mensagem de utilizador no LCD, 296
mensagem no LCD, 296
mensagem personalizada no LCD, 296
MMS, 345
 limite, 346
modificação de área, 320, 323
modo cartão e PIN, 180
modo de input, 189
modo de selecção de área, 207
modo instalador, 174, 293
modo técnico, 137, 174, 293
modo Walk Test, 99, 159
Monitorização GPRS, 352
mover uma porta, 251

N

necess. armar, 159
necessita de aceitação, 137
negar acesso, 257
nível de impacto, 227
nome de utilizador, **204**
normas, 372
notificação, 351
 eliminar, 354
 estado, 353
 evento, 353
 identificador, 353
 nome, 352
 utilizador, 353
NTP, 164, 336
número da chave de encriptação, 329
número de linha, 326
número de receptor, 326
número de série, 351
número de telefone, 324
número de toques, 332
nuvem, 351
nuvem segura, 128

O

O menu permite-lhe ver as informações sobre
 a última falha crítica do sistema, 173
OH2000, 325
omitir a primeira chamada, 332
opções de acesso, 301, 302
opções de arme, 297
opções de imagem, 193
opções de LCD, 295
opções de leitor, 253
opções de sistema, **285**
opções de VdS, 329
opções de zona, 216
opções remotas, 309

P

painel de predefinições, 32
parar reporte por voz, 224
PCB, 12
pedido de saída, 185
PIN, **79, 204**, 338
PIN diário, 294
PIN remoto, **204**, 205
ping, 163, 324, 337, 350
pisos, **83, 266**
 a eliminar, 266
 alterar, 266
 criar, 266
 grupo, 267
 grupo de pisos, 83
 nome, 266
ponto a ponto, 334
porta, **82, 243**
 alterar, 244
 anti-passback, 262
 áreas, 246
 baixa segurança, 247, 260
 bloquear, 248
 bloquear e desbloquear com impulso, 86,
 256
 bloquear quando fechada, 256
 controlo, 170
 controlo de alarme, 257
 controlo RTE, 258
 criar, 243
 desactivar RTE, 258
 desativar, 251
 desbloquear, 247, 249
 eliminar, 252
 estender tempo de desbloqueio até abrir,
 256
 grupo, 83, 263
 grupo de utilizadores, 256
 grupos de áreas, 247
 indicação, 252, 261
 interbloqueio, 259
 leitores, 244
 localização, 244

mover, 251
 negar acesso, 248, 257
 nome, 244
 opções de leitor, 253
 porta forçada, 259, 261
 porta inteligente, 82
 porta padrão, 82
 programa, 248
 programa RTE, 260
 região, 261
 reporte, 258
 reporte de abertura e fecho, 259
 reporte de DOTL, 259
 reporte de RTE, 259
 RTE, 248
 saída, 245, 263
 saída de aviso, 261
 saída DOTL, 261
 segunda zona, 255
 shunt, 84, 249
 tempo, 245
 tempo alargado, 245
 utilizador exterior, 262
 zona, 246
 zona DOTL, 255
 zona RTE, 257
 porta aberta, 252
 porta corta-fogo, 54
 porta de vídeo, 326
 porta final, 219
 porta inteligente, 82
 porta padrão, 82
 predefinições, 144, 306
 predefinido, 175
 prefácio, iii
 pré-pago, 340
 privilégio de utilizador, 211
 programa, **92**, 254
 criar, 279
 data, 279
 desbloquear porta, 249
 dia especial, 282
 eliminar, 284
 filtro de condições, 283
 janela de tempo, 280
 lista de acções, 281
 nome, 279
 programa activo, 279
 RTE, 260
 tempo, 279
 programação, 89, 432
 programação de utilizadores, 203
 programação rápida, **4**
 programar câmaras, 119
 programar dispositivos sem fios, 112
 prolongar temporização de entrada, 218
 pronto a armar, 297
 protocolo, 319, 321
 PUK, 164, 338

Q

qualidade de imagem, 194

R

RAS, **177**
 RDIS
 ponto a ponto, 334
 rede GPRS
 estado, 165
 registo, 165
 rede GSM, 338
 código, 165
 diagnóstico, 164
 disponibilidade, 339
 estado PIN, 164
 força do sinal, 165
 procura, 339
 registo, 164
 região, **84**, 261
 criar, 265
 eliminar, 265
 limite contagem, 196
 nome, 265
 região de alta segurança, **85**, 263
 registo, 150
 reinstalar, 175
 remover
 comando, 239
 DGP, 190
 dispositivo RF, 229, 238
 expansor, 190
 filtro, 271
 reportar falha de saída, 301
 reporte, 102
 código de conta, 320
 números de telefone, 324
 reporte combinado, 103
 reportes
 limitar relatórios, 225, 305
 reportes de alarme, 102
 reset técnico, **123**, 291
 desactivar com modo técnico, 292
 reset automático, 292
 resistência, 153
 resolução, 194
 resolução de problemas, **367**
 painéis de recolha de dados, 368, 369, 370
 teclados LCD, 368
 restaurar alarme, 305
 retardo de rebloqueio, 303
 retardo de zona, 221
 retardo desarme, 233
 retardo do reporte de falha de rede, 287
 retirar isolamento, 215, 216
 retroiluminação do LDC, 184
 revisão de software, 172
 RSSI, 152, 162

RTE, 185, 248
 controle, 258
 desactivado quando áreas armadas, 258
 programa, 260
RTS, 297

S

saída, 32, **81**, 263, **269**
 adicionar, 271
 alarme, 263
 aviso, 261
 DOTL, 261
 editar, 271
 eliminar, 275
 modo, 272
 nome, 271
 porta forçada, 261
 retardo, 274
 sirene, 313
 tempo activo, 274
 teste, 155
saída de alta corrente, 313
saída de monitor 3, 313
saída de sirene, 313
saída terminal, 219
sair de sessão, 174, 293
sensor de choque, 155, 218, 227
sensor de choque sensibilidade, 227
sensor de zona técnica, 221
sensor sem fios, 112
serviço, **150**
 confirmação doutilizador, 290
 tempo, 288
sessão de áudio, 328
 teste, 100
shunt, 54, **62**, 155, 224
 porta, 84, 249
 tempo, 249
 tipo, 250
 zona, 62
shunt de área, 250
shunt de porta, **84**, 252
 aviso, 250
 entrada/saída, 252
 tempo, 249
 tempo alargado, 250
 zonas, 261
shunt de porta de entrada/saída, 252
shunt de zona, 250
shunt porta, 249
SIM, 338
sincronização, 198
sirene, 30
sistema de testes, **97**

SMS, 342
 cabeçalho, 343
 caracteres, 343
 centro, 342
 contador, 166
 controle, 77, 208
 limite de mensagens, 343
 PIN, 343
 reenvio, 342
 reporte, 77, 208
soak test, 218
 tempo, 289
software de configuração, 356
solução na nuvem, 128
status, 156
subeventos, **322**
substituição da bateria, 18, 168
substituir a bateria, 18
supervisão, 229
suprimir FTC, 322
swinger shunt, 217, 305

T

tamper
 teclado, 179
tamper área, 178
tamper de código, 64, 136
taxa de frames, 194
taxa de frames de imagem, 194
tecla, **64**, 219
tecla de função, 183
tecla de funções, 67
teclado, **13**, 69, **70**, 176
 besouro, 313
 resolução de problemas, 368
 tamper, 179
telefone de utilizador, 208
tempo alargado, 245
tempo alargado de shunt de porta, 250
tempo cartão p/ PIN, 302
tempo de aviso, 232, 317
tempo de dois cartões, 302
tempo de entrada, 218, 231, 301
tempo de entrada/saída, 230, 231
tempo de pré-alarme, 232
tempo de saída, 230, 301
tempo de shunt de porta, 249
tempo desarme estendido, 317
tempo e participação, 255
tempo multi cartões, 302
tempo teste, 154
temporizador de entrada, 297
temporizador de saída, 297
temporizadores, **285**
temporizadores de sirene, 286
terminador de saída, 52, 288

test detector, 154
 auto teste, 224
 duração, 154
 tempo, 154
 teste manual, 154
 teste, 151
 áudio de duas vias, 171
 bateria, 166, 168
 comunicação, 100
 listen in, 171
 sessão de áudio, 100
 teste automático da bateria, **167**
 teste da bateria, **166, 168**
 duração, 168
 substituição da bateria, 168
 teste de alarme confirmado, 99, 160
 teste de alcance, 153
 teste de alcance de câmara, 153
 teste de bateria
 duração, 167
 frequência, 167
 tempo de início, 167
 teste automático, 167
 teste de LED, 156
 teste de notificação, 172
 teste manual, 154, **162**
 tipo de grupo de utilizadores, 74
 tipo de sensor, 221
 tipo de zona, **51**, 215
 Titan, 356
 trigger, **91, 269**
 apagar, 276
 criar, 275
 estado, 156
 nome, 276

U

UltraSync, **128**, 351, 352
 canal, 328
 utilizador, **71, 203**
 alterar, 204
 cartão, 205
 criação, 203
 eliminar, 207
 grupo de utilizadores, 74, 210
 idioma, 206
 modo de selecção de área, 207
 PIN, 204
 programação, 203
 utilizador de alta segurança, **85**, 263
 tempo de pré-aviso, 263
 utilizador exterior, 262
 utilizadores predefinidos, 71
 utilizar câmaras, 119

V

valor da chave de encriptação, 329
 valores da resistência, 189, 304, 305

valores predefinidos, 32
 VdS
 número da chave de encriptação, 329
 valor da chave de encriptação, 329
 versão, 329
 verificar cartão, 169
 versão, 329, 358
 versão de firmware, 198
 versão do painel, 172
 visor armado, 295
 limite de tempo, 287

W

walk test, **97**, 99, 157, 160, 218
 alarme confirmado, 99, 160
 frequência, 158
 limite de tempo, 287
 walk test activo, 99, 160
 walk test reduzido, 159
 walk test standard, 157
 zona única, 159
 walk test activo, 99, 160
 walk test de técnico, 97, 157, 218
 walk test de utilizador, 157, 158, 218
 walk test de zona única, 159
 walk test invertido, 153
 temporizador, 290
 walk test reduzido, 159
 walk test standard, 157

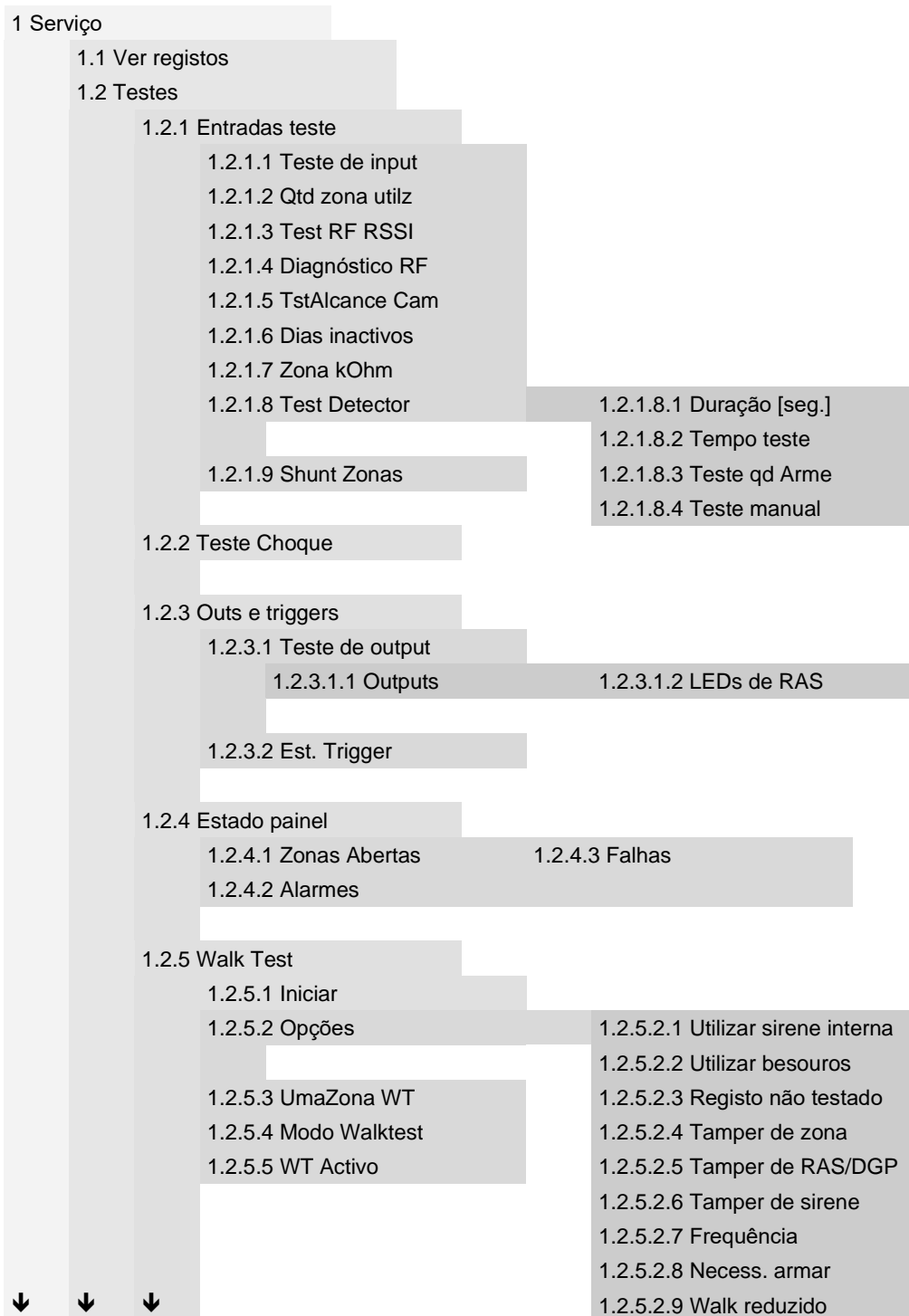
Z

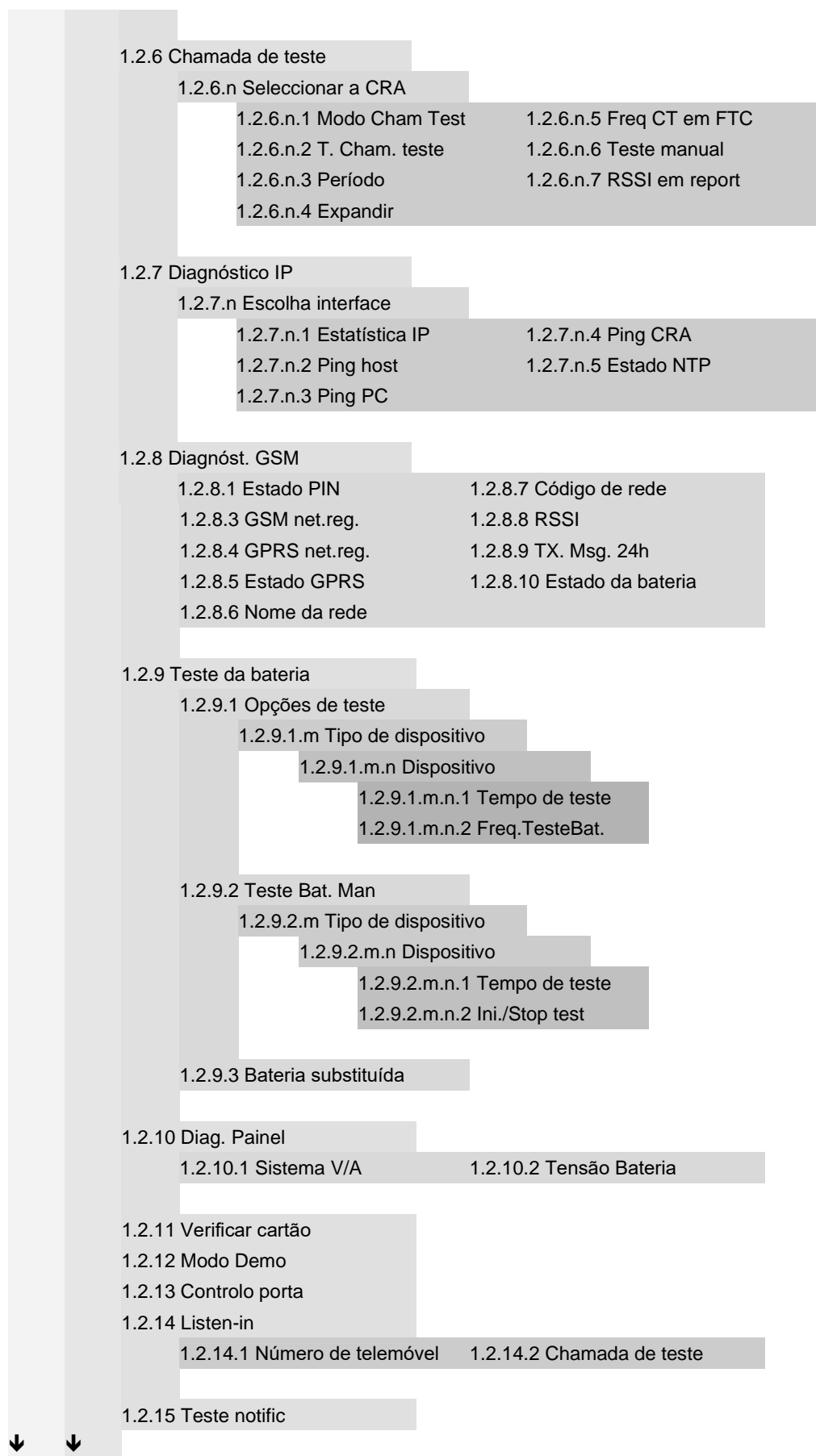
zona, **51**, **213**

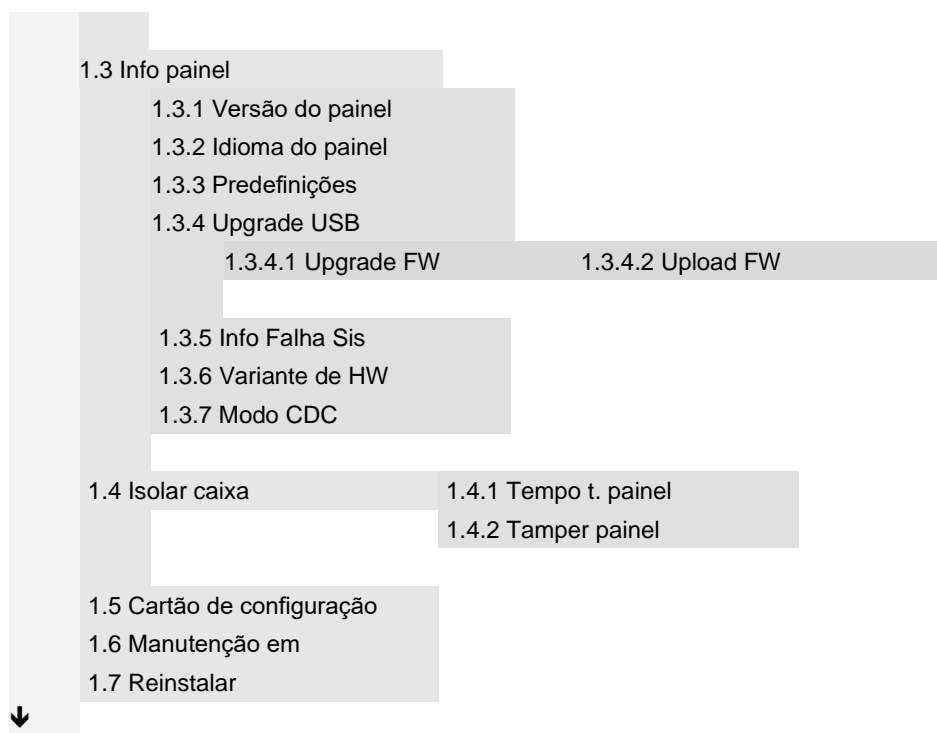
- aberto demasiado tempo, 289
- acesso, 223
- alarme manter aberto, 223
- área, 215
- arme parcial, 59
- auto teste, 224
- copiar, 225
- desinibir, 216
- eliminar, 226
- entrada/saída, 223
- inibir, 216, 298
- isolar, 215, 216, 224
- limitar relatórios, 225
- mover, 226
- nome, 214
- opções, 216, 304
- parar reporte por voz, 224
- reportar como coacção, 224
- reportar como pânico, 224
- reporte, 221
- resistência, 153
- retirar isolamento, 215, 216
- RTE, 257
- shunt, 54, 62, 155, 224
- tempo de aviso, 232
- tempo de entrada/saída, 230, 231
- tempo de pré-alarme, 232
- tipo, **51**, 215

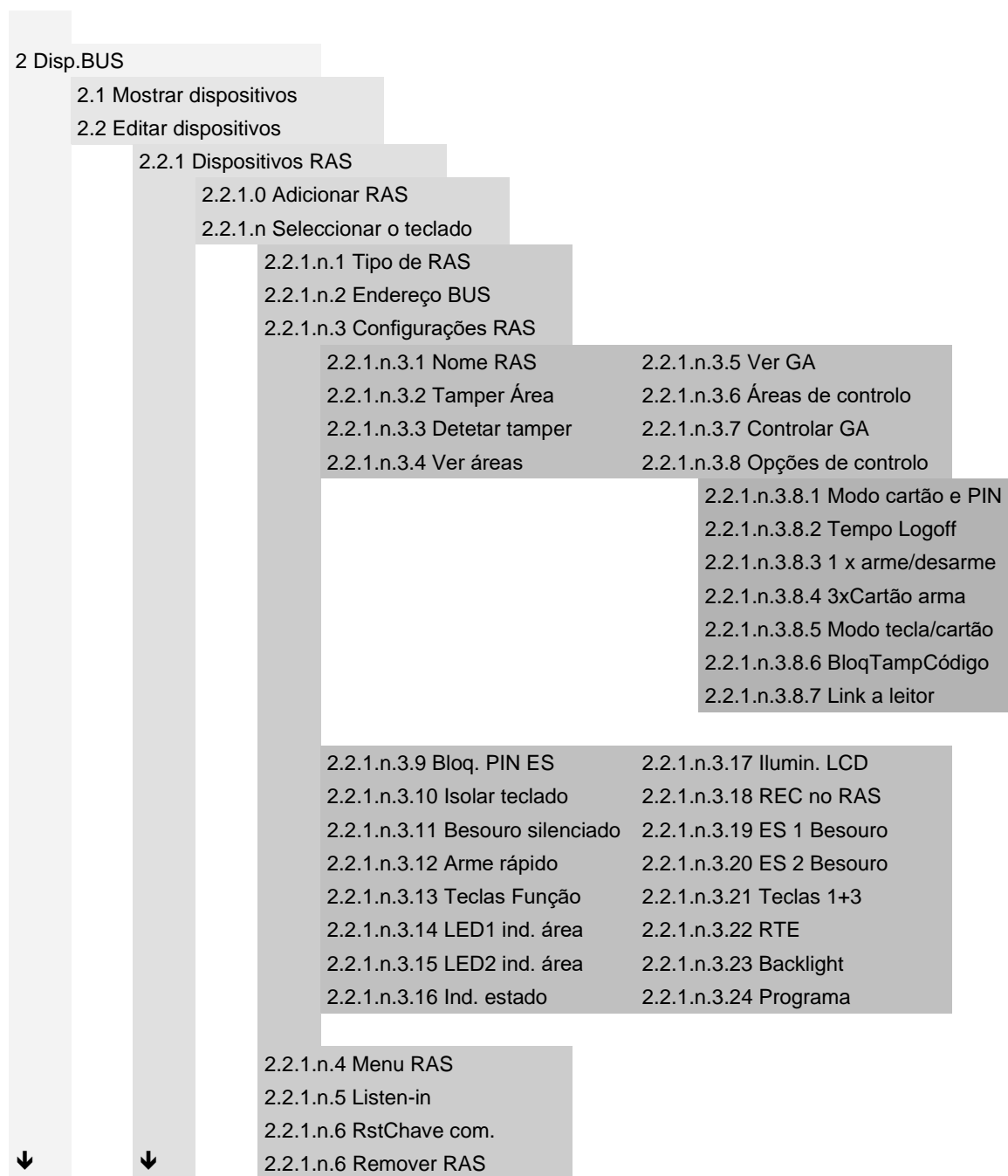
- zona DOTL, 255
- zona entrada/saída, 185
- zona horária, 285
- zona RTE, 257
- zona única, 189
- zona virtual, 222
- zonas abertas, 151
- zonas de shunt, 261
- zonas usadas, 151

Mapa de programação



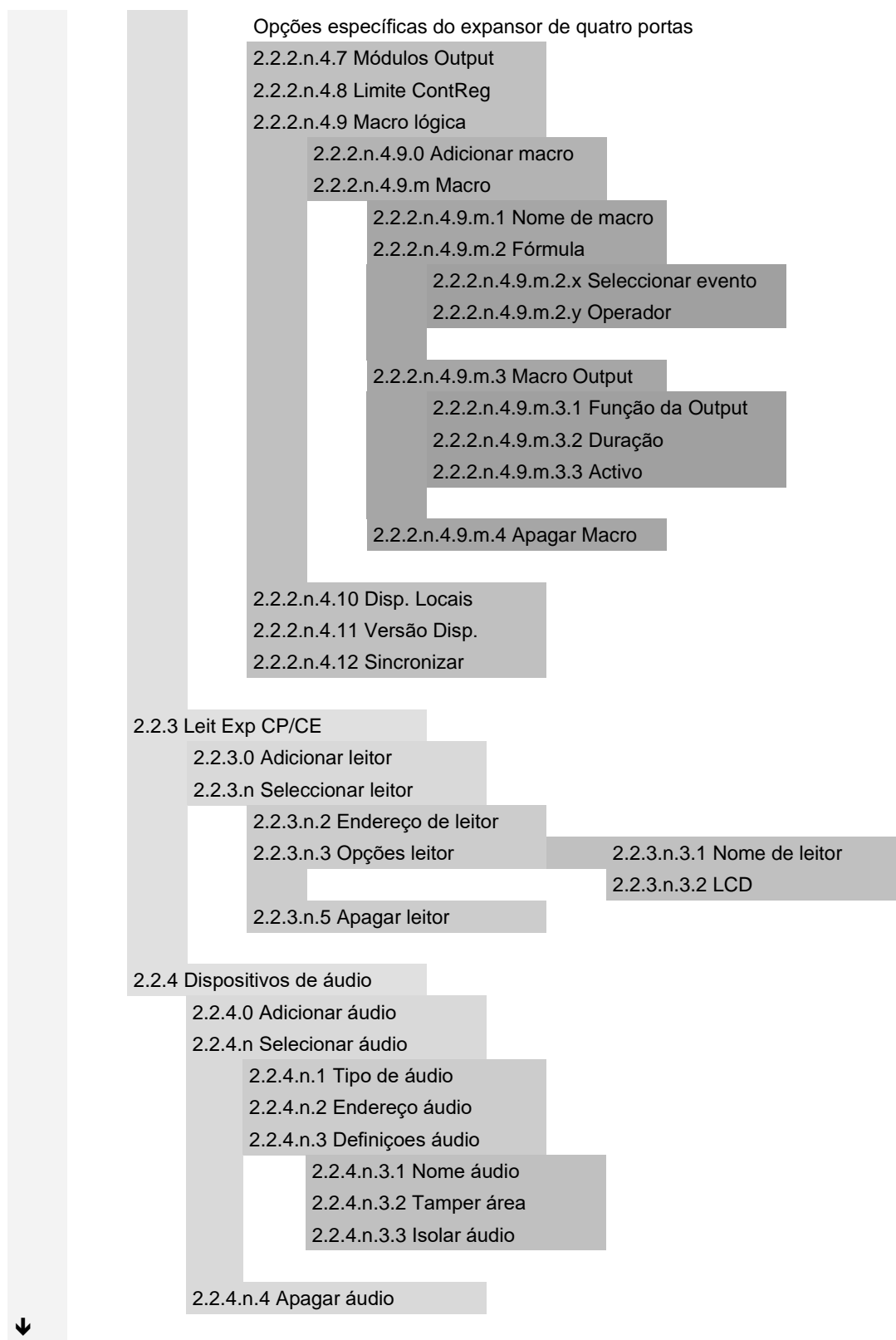


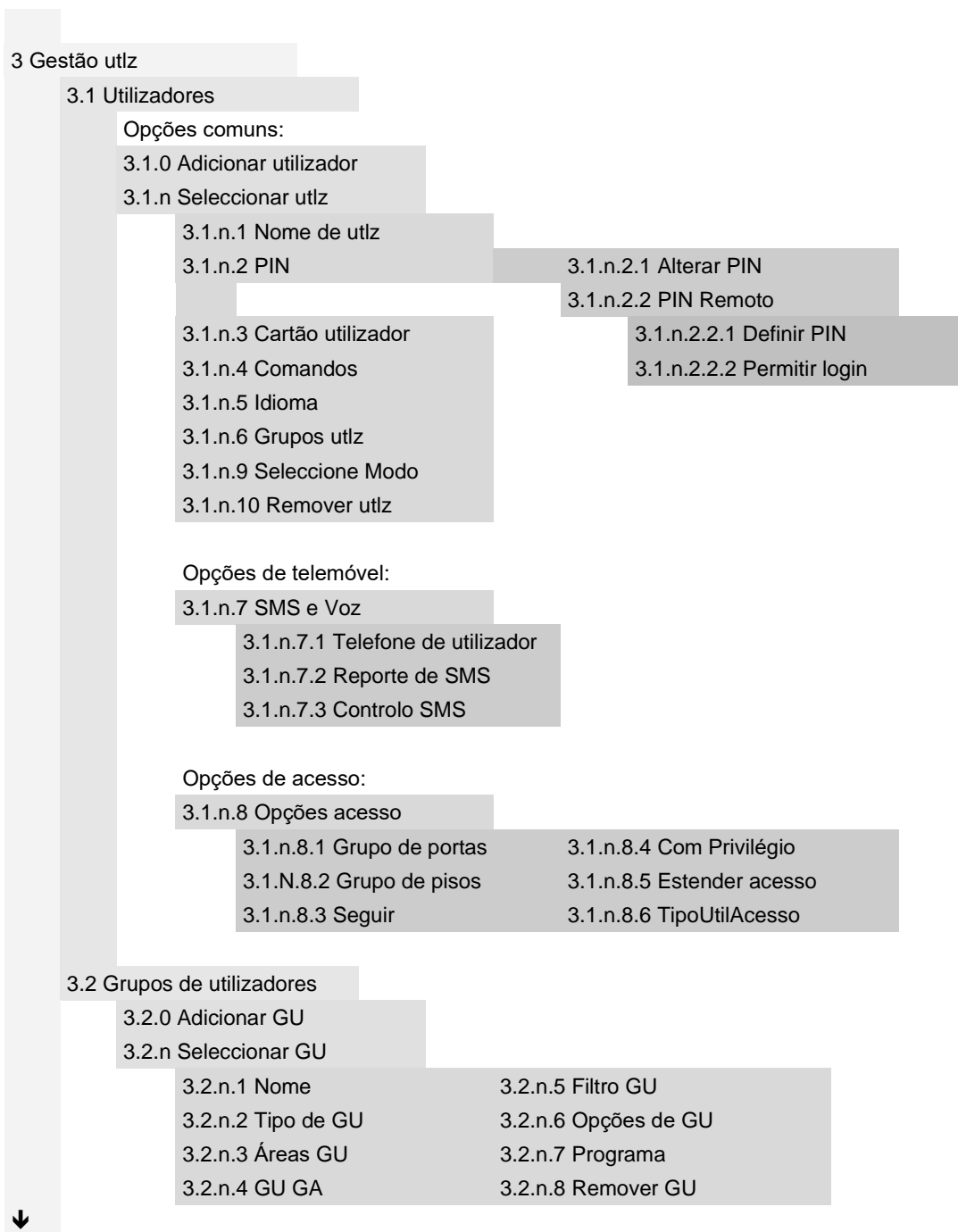




- 2.2.2 Dispositivos DGP
 - 2.2.2.0 Adicionar DGP
 - 2.2.2.n Seleccionar expansor
 - 2.2.2.n.1 Tipo de DGP
 - 2.2.2.n.2 Endereço BUS
 - 2.2.2.n.3 Entradas DGP
 - 2.2.2.n.4 Configurações DGP
 - 2.2.2.n.4.1 Nome DGP
 - 2.2.2.n.4.2 Tamper Área
 - 2.2.2.n.4.3 Detetar tamper
 - 2.2.2.n.4.4 Isolar DGP
 - 2.2.2.n.4.5 Modo de input
 - 2.2.2.n.4.6 EOL
 - 2.2.2.n.5 Menu DGP
 - 2.2.2.n.6 Remover DGP
- Opções específicas sem fios:
 - 2.2.2.n.4.4 Supervisão
 - 2.2.2.n.4.4.1 Super. pequena
 - 2.2.2.n.4.4.2 Super. longa
 - 2.2.2.n.4.4.3 Super. fumo
 - 2.2.2.n.4.5 Sens. Recpt.
 - 2.2.2.n.4.6 DGP modo
 - 2.2.2.n.4.7 DGP versão
 - 2.2.2.n.4.8 Menu empaste
 - 2.2.2.n.4.8.1 Empastelamento
 - 2.2.2.n.4.8.2 Empast. segundos
 - 2.2.2.n.4.8.3 Thresh Empast.
- 2.2.2.n.4.11 Cfg. Fab. DGP

- Opções específicas da câmara:
- 2.2.2.n.4.9 Opções Imagem
 - 2.2.2.n.4.9.1 Config. Imagem
 - 2.2.2.n.4.9.1.1 Conf. Alarme
 - 2.2.2.n.4.9.1.1.1 Qtd imagens
 - 2.2.2.n.4.9.1.1.2 Taxa de frames
 - 2.2.2.n.4.9.1.1.3 Resoluçao Foto
 - 2.2.2.n.4.9.1.2 Conf. incêndio
 - 2.2.2.n.4.9.1.3 Conf. pânico
 - 2.2.2.n.4.9.1.4 Conf. médico
 - 2.2.2.n.4.9.1.5 Conf. tamper
 - 2.2.2.n.4.9.1.6 Conf. falhas
 - 2.2.2.n.4.9.1.7 Configur. tipo 1
 - 2.2.2.n.4.9.1.8 Configur. tipo 2
 - 2.2.2.n.4.9.2 Ver mem imagem
 - 2.2.2.n.4.9.3 AutoapagarImag
 - 2.2.2.n.4.9.4 Cont Total Foto
- 2.2.2.n.4.11 Apagar imagem



4 Zonas e áreas

4.1 Zonas

4.1.0 Adicionar zona

4.1.n Seleccionar zona

Opções comuns

4.1.n.1 Nome da zona

4.1.n.2 Tipo de zona

4.1.n.3 Isolado

4.1.n.4 Localiz. zona

4.1.n.5 Zona áreas

4.1.n.6 Opções de zona

- | | |
|-------------------------------|---------------------------------|
| 4.1.n.6.1 Inibir | 4.1.n.6.21 Arme parcial técnico |
| 4.1.n.6.2 Isolar | 4.1.n.6.22 RAS LCD |
| 4.1.n.6.3 Excl. em ArP1 | 4.1.n.6.23 Registo |
| 4.1.n.6.4 Excl. em ArP2 | 4.1.n.6.24 Reporte CRA |
| 4.1.n.6.5 Duplo impulso | 4.1.n.6.25 Temp. Retardo |
| 4.1.n.6.6 Swinger shunt | 4.1.n.6.26 REC no RAS |
| 4.1.n.6.7 Anti-Mask | 4.1.n.6.27 REC p/ Utiliz |
| 4.1.n.6.8 Empar. zona | 4.1.n.6.28 Sensor tipo |
| 4.1.n.6.9 Campainha | 4.1.n.6.29 Zona virtual |
| 4.1.n.6.10 Soak test | 4.1.n.6.30 Mantida aberta |
| 4.1.n.6.11 Walk Test técnico | 4.1.n.6.31 ES verif arme |
| 4.1.n.6.12 Walk Test utl | 4.1.n.6.32 Alarme em AP1 |
| 4.1.n.6.13 Sensor choque | 4.1.n.6.33 Alarme em AP2 |
| 4.1.n.6.14 Prolongar EE | 4.1.n.6.34 Reportar como |
| 4.1.n.6.15 Porta final | 4.1.n.6.35 Auto Teste |
| 4.1.n.6.16 Chave latch | 4.1.n.6.36 Shunt |
| 4.1.n.6.17 Arme por chave | 4.1.n.6.37 Ver isolados |
| 4.1.n.6.18 Desarme por chave | 4.1.n.6.38 Stop Reporte |
| 4.1.n.6.19 Arme total técnico | 4.1.n.6.39 Limitar relatórios |
| 4.1.n.6.20 Desarme técnico | |

4.1.n.8 Listen-in

- 4.1.n.8.1 Modo de escuta
- 4.1.n.8.2 Link áudio

4.1.n.8 Copiar e Adic

- 4.1.n.8.1 Cópia par. de
- 4.1.n.8.2 Atribuir bloco

4.1.n.9 Mover zona

4.1.n.10 Remover zona

Opções de sensor de choque

4.1.n.7 Sensor Choque

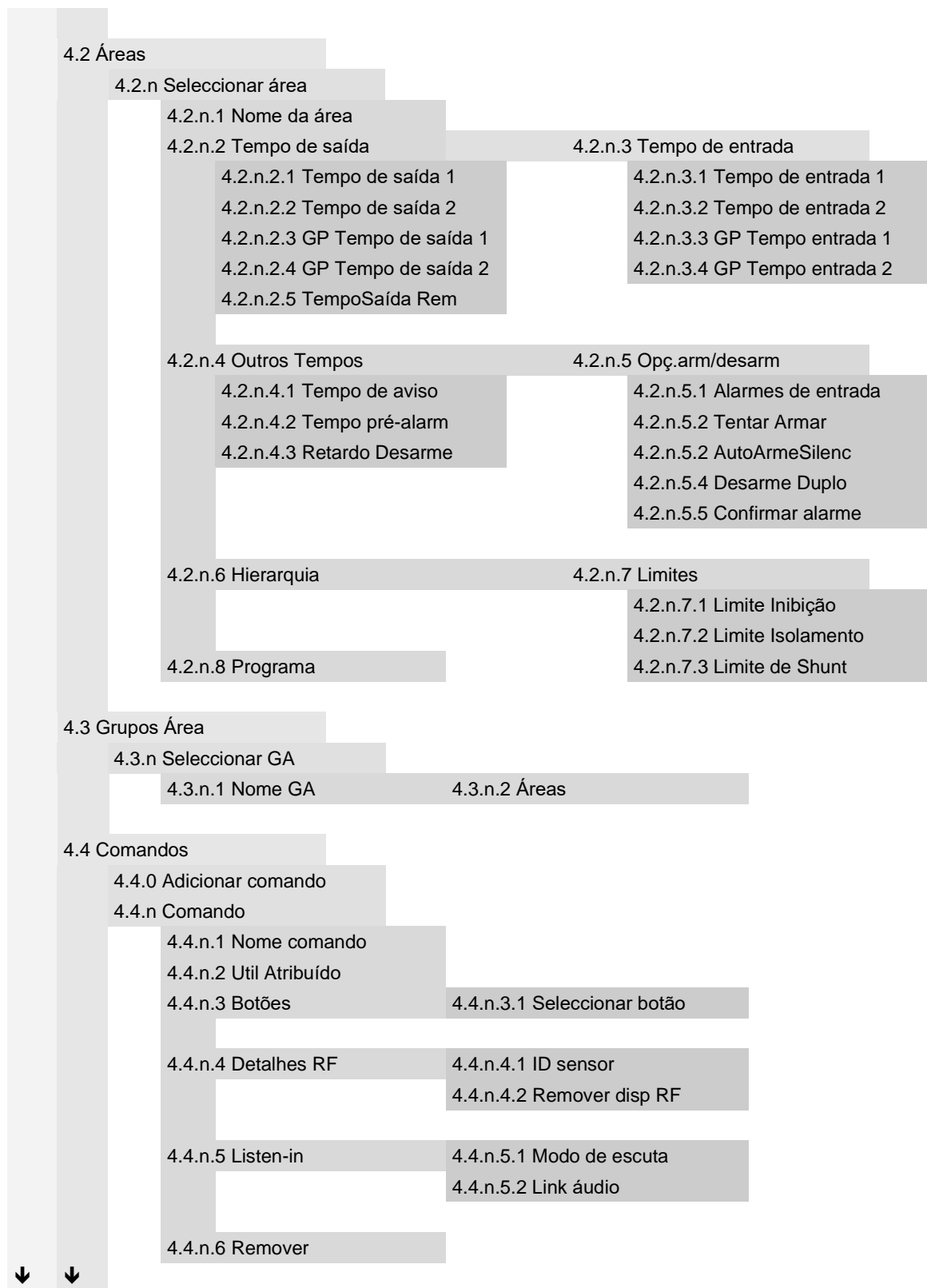
- 4.1.n.7.1 Número de impulsos
- 4.1.n.7.2 Nível de impacto

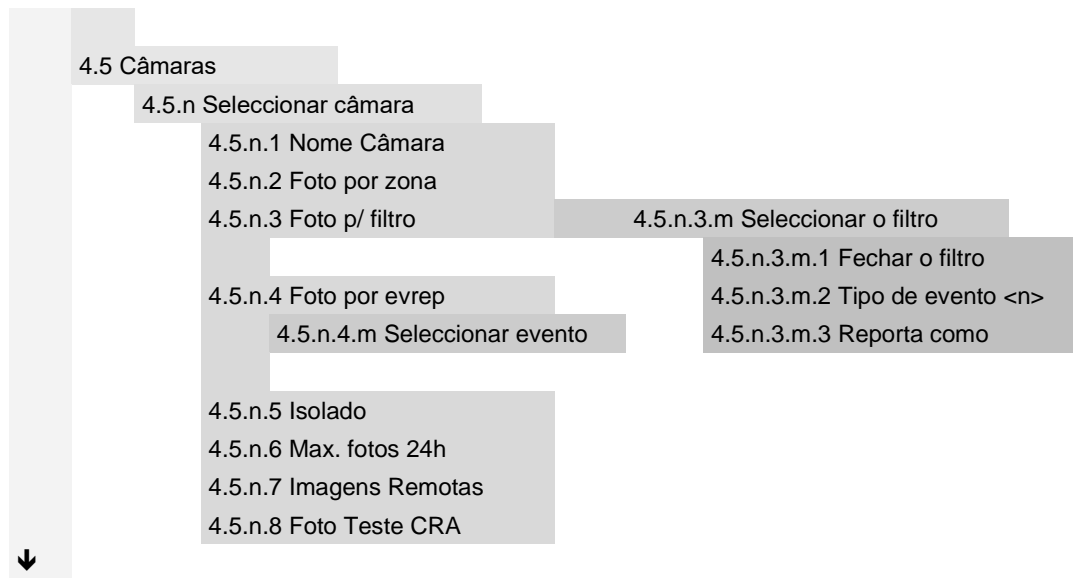
Opções de sensores sem fios:

4.1.n.7 Detalhes RF

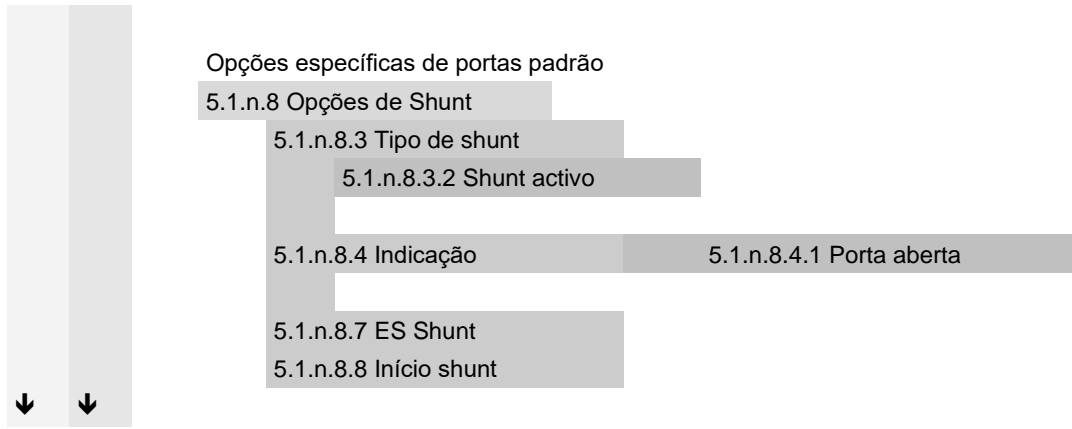
- 4.1.n.7.1 ID sensor
- 4.1.n.7.2 Tipo de sensor
- 4.1.n.7.3 Modo sensor
- 4.1.n.7.4 Supervisão
- 4.1.n.7.5 Opções sensor
- 4.1.n.7.6 Remover disp RF







5	Menu Porta	
5.1	Portas	
	Opções comuns de portas	
5.1.0	Adic. Porta	
5.1.n	Seleccionar porta	
5.1.n.1	Nome da Porta	
5.1.n.2	Localização de Porta	
5.1.n.3	Leitores de porta	
5.1.n.4	Output Porta	
5.1.n.5	Tempos de portas	5.1.n.5.1 Tempo de desbloqueio
		5.1.n.5.2 Tempo alargado
5.1.n.6	Opções de porta	
5.1.n.6.1	Zona de porta	5.1.n.6.1.1 Zona de porta
5.1.n.6.3	Controlo de Alarme	
5.1.n.6.3.1	Áreas de porta	
5.1.n.6.3.2	Grp Área Porta	
5.1.n.6.3.3	Quando desarmado	5.1.n.6.3.3.1 Baixa Segurança
		5.1.n.6.3.3.2 Desbloquear Porta
5.1.n.6.3.4	Quando armado	5.1.n.6.3.4.1 Negar acesso
		5.1.n.6.3.4.2 Bloquear porta
		5.1.n.6.3.4.3 Bloq.PIN ES
5.1.n.6.4	Opções RTE	
5.1.n.6.4.1	Usar RTE	
5.1.n.7	Opções de zona horária	
5.1.n.7.1	Porta desbloqueada	5.1.n.7.1.1 Programa
5.1.n.8	Opções de Shunt	
5.1.n.8.2	Tempo shunt	5.1.n.8.2.1 Tempo Shunt
		5.1.n.8.2.2 Temp alargado
		5.1.n.8.2.3 Aviso Shunt
5.1.n.8.3	Tipo de shunt	
5.1.n.8.3.1	Shunting	
5.1.n.8.5	Até porta fech	
5.1.n.8.6	CancelApósFech	
5.1.n.10	Mover Porta	
5.1.n.11	Desabilitar porta	
5.1.n.11	Apagar porta	



Opções específicas de portas inteligentes

5.1.n.3 Leitores de porta

5.1.n.3.5 Opções de leitores

- | | |
|-------------------------------|--------------------------------|
| 5.1.n.3.5.1 Cartão e PIN | 5.1.n.3.5.5 Opções de LEDs |
| 5.1.n.3.5.2 Dois cartões | 5.1.n.3.5.6 Time&Attendance |
| 5.1.n.3.5.3 Sem ZH Req | 5.1.n.3.5.7 Desabilitar coação |
| 5.1.n.3.5.4 Formato do cartão | |

5.1.n.6 Opções de porta

5.1.n.6.1 Zona de porta

- | |
|--------------------------|
| 5.1.n.6.1.2 Segunda zona |
| 5.1.n.6.1.3 Zona DOTL |

5.1.n.6.2 Porta desbloqueada

- | |
|----------------------------|
| 5.1.n.6.2.3 Bloq/Dbloq Imp |
| 5.1.n.6.2.1 Até fechar |
| 5.1.n.6.2.2 Até abrir |

5.1.n.6.3 Controlo de Alarme

- | |
|-----------------------------------|
| 5.1.n.6.3.5 Grupo de utilizadores |
| 5.1.n.6.3.6 Tipo Controlo |
| 5.1.n.6.3.7 Se PIN arma |
| 5.1.n.6.3.7.1 Negar acesso |

5.1.n.6.4 Opções RTE

- | | |
|----------------------------|--------------------------|
| 5.1.n.6.4.2 Zona RTE | 5.1.n.6.4.4 Controlo RTE |
| 5.1.n.6.4.3 Desb.qd Armado | |

5.1.n.6.5 A reportar

- | | |
|----------------------------|---------------------------|
| 5.1.n.6.5.1 Fech. & Bloq. | 5.1.n.6.5.4 Porta forçada |
| 5.1.n.6.5.2 AbDbl como Dbl | 5.1.n.6.5.5 DOTL |
| 5.1.n.6.5.3 Abertura/fecho | 5.1.n.6.5.6 RTE |

5.1.n.6.6 Interbloqueio

5.1.n.7 Opções de zona horária

5.1.n.7.1 Porta desbloqueada

- | |
|--------------------------|
| 5.1.n.7.1.2 Após entrada |
|--------------------------|

5.1.n.7.2 Baixa Segurança

5.1.n.7.3 Zona Horária RTE

5.1.n.8 Opções de Shunt

5.1.n.8.1 Zonas

5.1.n.8.4 Indicação

- | |
|-----------------------------|
| 5.1.n.8.4.2 Output DOTL |
| 5.1.n.8.4.3 Output de aviso |
| 5.1.n.8.4.4 Porta forçada |

5.1.n.9 Regiões & AP

5.1.n.9.1 Regiões

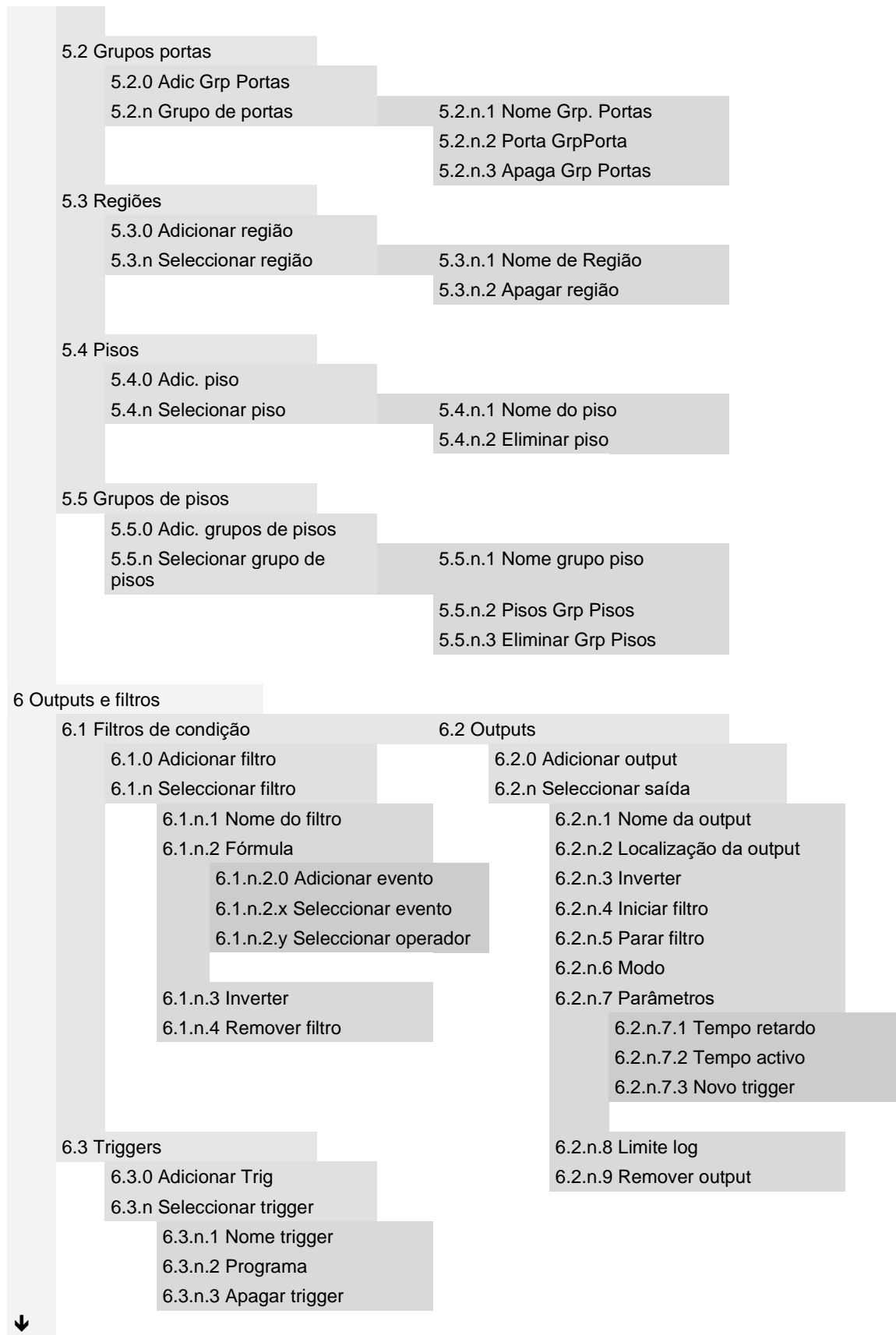
5.1.n.9.2 Anti-passback

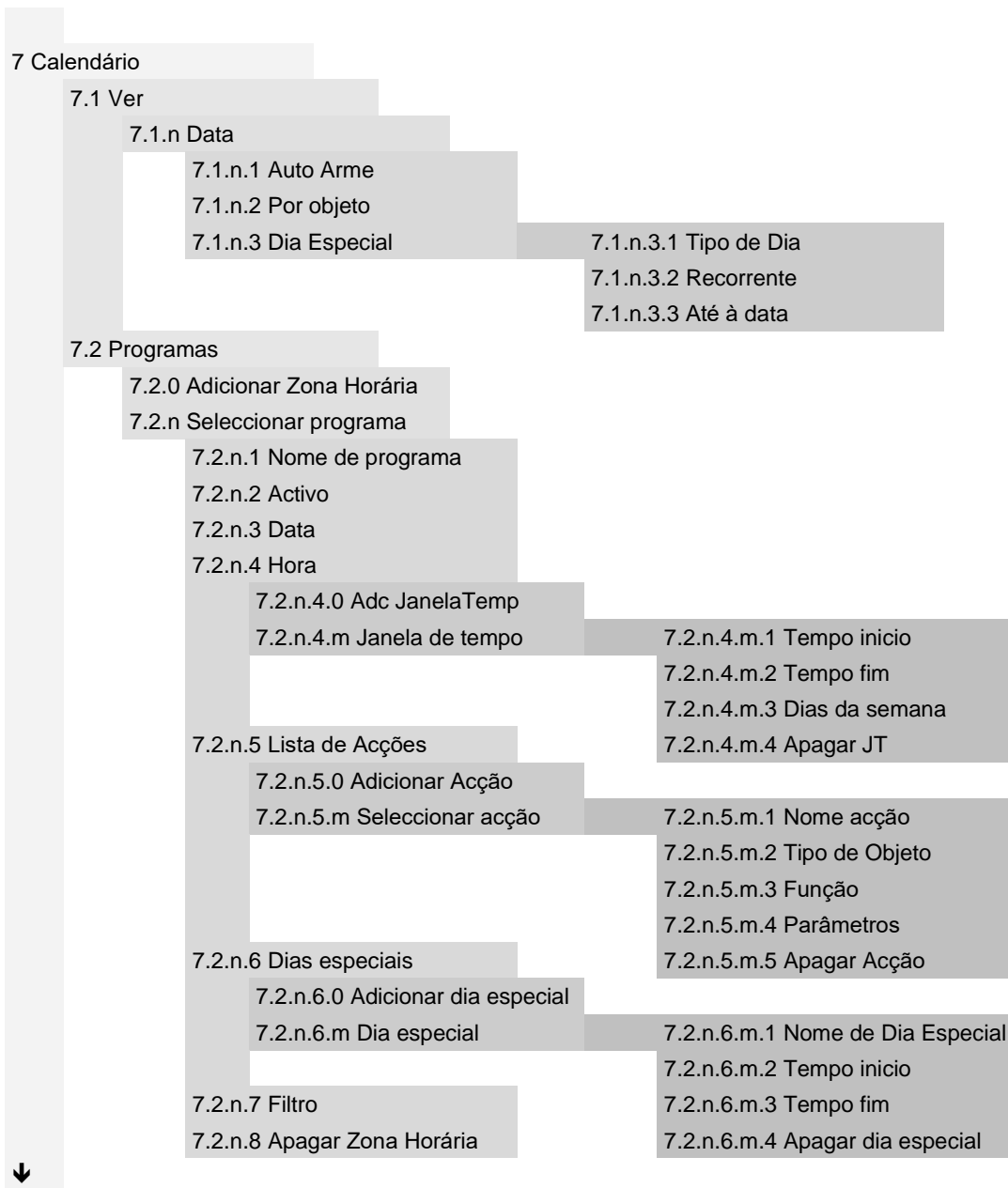
5.1.n.9.3 Inib Reg 1 Utl

5.1.n.9.4 Opções HSU

- | |
|----------------------------|
| 5.1.n.9.4.1 Req nr HSU |
| 5.1.n.9.4.2 Temp pré-aviso |
| 5.1.n.9.4.3 AS Out Alarme |







8 Sistema

8.1 Temporizadores

8.1.1 Hora e data

8.1.2 Sirenes

8.1.2.1 Activação

8.1.2.2 Retardo

8.1.2.1.1 Sirene interior

8.1.2.2.1 Sirene interna

8.1.2.1.2 Sirene exterior

8.1.2.2.2 Sirene externa

8.1.2.1.3 Interior F/P/M

8.1.2.1.4 Exterior F/P/M

8.1.3 Sistema

8.1.3.1 Screensaver

8.1.3.4 Rtd.rep.230VAC

8.1.3.2 Cartão e PIN

8.1.3.5 Rtd.arme final

8.1.3.3 Walk Test

8.1.3.6 Manutenção em

8.1.4 Zonas

8.1.4.1 Intervalo duplo impulso

8.1.4.5 Tempo key box

8.1.4.2 Abertura duplo impulso

8.1.4.6 Tempo Manter Aberto

8.1.4.3 Soak Test

8.1.4.7 Dias Inactivos

8.1.4.4 Retardo de input

8.2 Opções de técnico

8.2.1 Aceit. necess

8.2.2 Tamper necessário

8.2.3 Bloqueio técnico

8.2.4 Reset técnico

8.2.4.1 Alarme

8.2.4.8 Falha de sirene

8.2.4.2 Tamper

8.2.4.9 Falha interlig

8.2.4.3 Pânico

8.2.4.10 Reset auto

8.2.4.4 Confir. alarme

8.2.4.11 Disp p/ srv

8.2.4.5 Falha de bateria

8.2.4.12 Código sistema

8.2.4.6 Fusível aux

8.2.4.13 Efectuar reset

8.2.4.7 Falha 230VAC

8.2.4.14 Configurar texto

8.2.5 Manutenção em

8.2.6 Código desafio

8.2.7 Inspeção

8.2.7.1 Data

8.2.7.2 Msg. personal

8.2.8 Grp instalador

8.2.8.1 Muitos instaladores

8.2.8.2 SW de gestão

8.3 Menu e LCD

8.3.1 Modo Screensaver

8.3.4 Indicar falhas

8.3.2 Msg personalizada

8.3.5 Ver tempo ES

8.3.3 Lista de alarmes

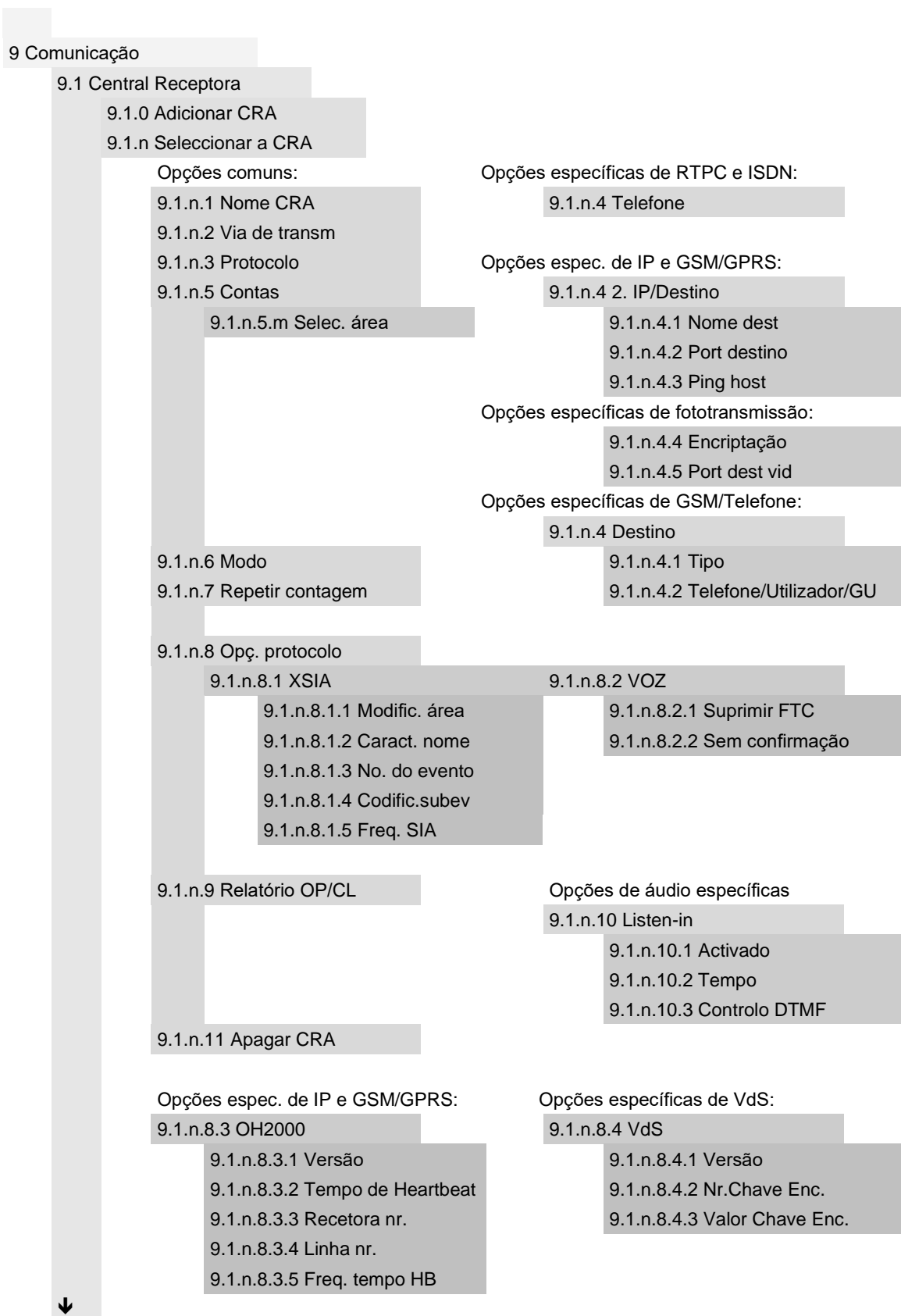


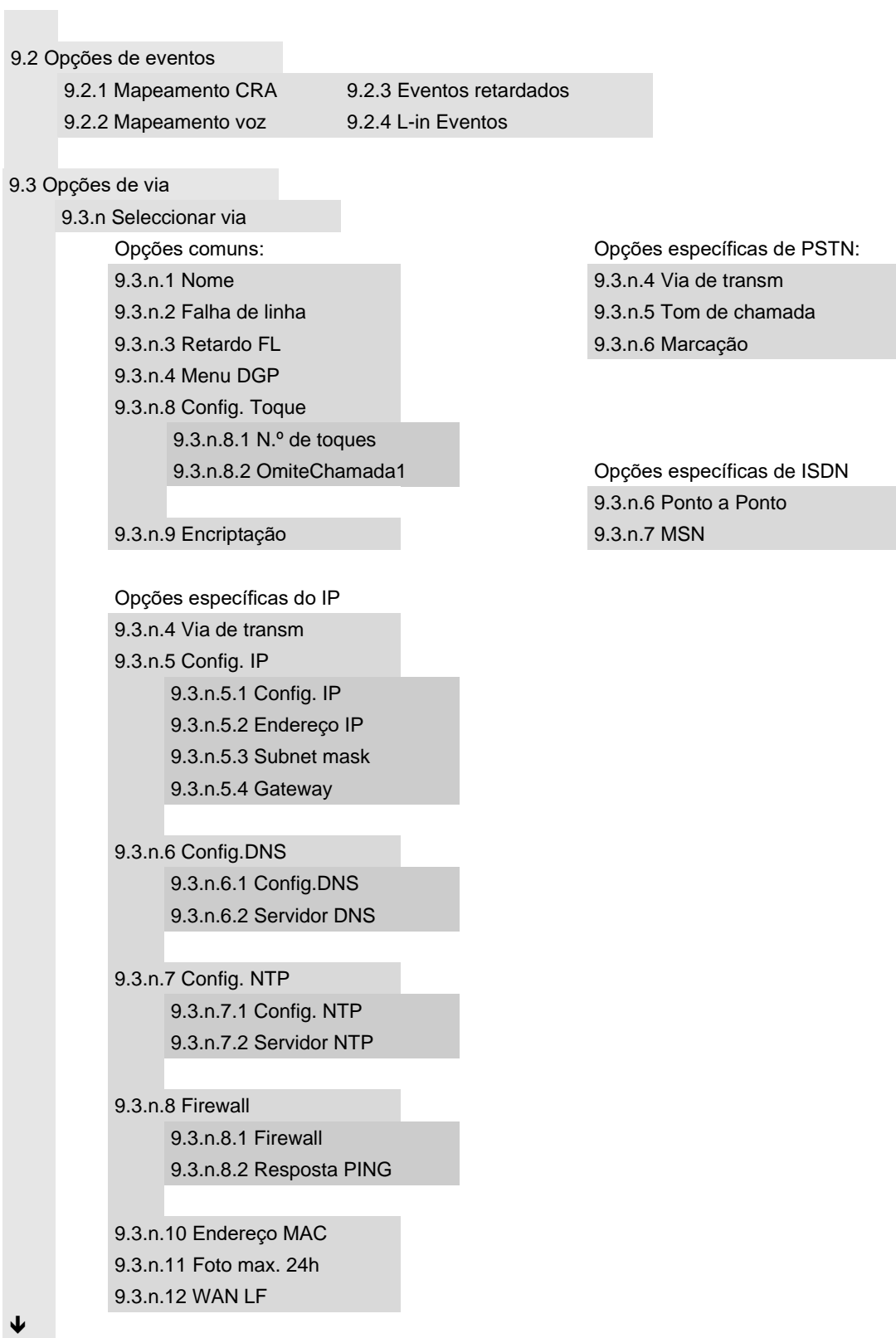
8.4 Opções de arme	
8.4.1 Pront.Armaz	
8.4.2 Inibir inclusão	
8.4.3 Arme parcial	
8.4.3.1 Reporte BA	8.4.3.4 Nome AP1
8.4.3.2 Acesso para ES	8.4.3.5 Nome AP2
8.4.3.3 EE arme total	
8.4.4 Arme forçado	
8.4.5 Op. arme forçado	
8.4.6 Alarmes em espera	
8.4.7 AA tempo tent.	
8.4.8 AA tenta util	
8.4.9 Falha de saída	
8.4.10 Relt.Falha ES	
8.5 Opções de acesso	
8.5.1 Temporizadores acesso	
8.5.1.1 Cartão p/ PIN	8.5.1.3 Multip Cartões
8.5.1.2 Dois cartões	8.5.1.4 Rtd rebloqueio
8.5.2 Opções de DGP	
8.5.2.1 Mapear relés	8.5.2.2 Mapear LED's Painel
8.5.3 Usa 27bitTecom	
8.6 Opções de zona	
8.6.1 Modo entrada	8.6.4 Swinger shunt
8.6.2 Resistência EOL	8.6.5 Restauo de reporte
8.6.3 Tamper Sir EOL	8.6.6 Limitar relatórios



8.7 Painel	
8.7.1 Nome do painel	8.7.4 Comprim. PIN
8.7.2 Idioma do painel	8.7.5 Modo alt. PIN
8.7.3 Método coacção	
8.7.6 Confir. alarme	
8.7.6.1 Modo AB	
8.7.6.2 Tempo AB	8.7.6.2.1 Tempo Alarm AB
	8.7.6.2.2 Tempo Holdup AB
8.7.6.3 Confirma.Sist	8.7.6.7 Sirenes
8.7.6.4 Confirmação EE	8.7.6.8 Ligar msg CRA
8.7.6.5 EE inibido	8.7.6.9 Retardo Rep.
8.7.6.6 Confirmação TA	
8.7.7 Desarme Fácil	
8.7.8 Opções remoto	
8.7.8.1 Config. Remota	8.7.8.3 Acesso remoto
8.7.8.2 Config. superv.	
8.7.9 Esquema Objeto	
8.8 Outro	
8.8.1 Modo de pânico	
8.8.2 Campanha	8.8.2.1 Campanha ArP
	8.8.2.2 Campanha auto
8.8.3 TampSist áreas	
8.8.4 Reactiv sirene	
8.8.5 Aprende cartão	
8.8.5.1 Tec. aprender	8.8.5.2 Porta aprender
8.8.6 Testar zonas	
8.8.7 Modo besouro	
8.8.8 Saída de mon. 3HC	
8.8.9 Nr. de cartão	
8.8.10 Reg. Anónimo	
8.8.11 Segur. LEITOR	
8.8.11.1 Modo seguro	8.8.11.5 App.IDFicheiro
8.8.11.2 Chave Config.	8.8.11.6 ChaveResetTamp
8.8.11.3 Chave App.	8.8.11.7 Limit Bit Cart
8.8.11.4 Nome App.	8.8.11.8 Predefinição
8.8.12 RAS LEDLaranja	
8.8.13 Configuração no arme	
8.9 DesarmTemp/ATM	
8.9.1 Retardo	8.9.3 Temp DesarmEst
8.9.2 Tempo Desarme	8.9.4 T.AvisoDesarme







Opções espec. de GSM/SMS/GPRS:

9.3.n.4 Via transm

9.3.n.5 Config. GSM

9.3.n.5.1 PIN cartão SIM

9.3.n.5.2 Redes

9.3.n.5.2.1 Selecção rede

9.3.n.5.2.2 Selec. só rede

9.3.n.5.2.3 Procurar rede

9.3.n.5.2.3.0 Nova proc.rede

9.3.n.5.2.3.m Selec.uma rede

9.3.n.5.2.3.m.1 Nome da rede

9.3.n.5.2.3.m.2 Código de rede

9.3.n.5.2.3.m.3 Disponibilidade

9.3.n.5.2.3.m.4 RSSI

9.3.n.5.2.3.m.5 Usar esta rede

9.3.n.5.3 Crédito

9.3.n.5.3.1 Verificar já

9.3.n.5.3.4 Pedir código

9.3.n.5.3.2 Verificar modo

9.3.n.5.3.5 Verif. período

9.3.n.5.3.3 Verificar no.

9.3.n.5.3.6 Verif. tempo

9.3.n.5.4 Det.Empast.

9.3.n.5.4.1 Det.Empast.

9.3.n.5.4.2 Thresh.Empast.

9.3.n.6 Config. SMS

9.3.n.6.1 N. Centro SMS

9.3.n.6.4 Cabeçalho SMS

9.3.n.6.2 Reenvio de SMS

9.3.n.6.5 PIN Util. Req

9.3.n.6.3 Máx. Msg 24h

9.3.n.6.6 Ext.Caracteres

9.3.n.7 Config. GPRS

9.3.n.7.1 Nome APN

9.3.n.7.6 Firewall

9.3.n.7.2 Nome de utilizador

9.3.n.7.7 Falha de linha

9.3.n.7.3 Password

9.3.n.7.8 Tempo desligar

9.3.n.7.4 Config. IP

9.3.n.7.9 Max. Fotos 24h

9.3.n.7.5 Config. DNS

9.3.n.10 Configuração de MMS

9.3.n.10.1 MMS Center

9.3.n.10.5 Proxy

9.3.n.10.2 APN

9.3.n.10.6 Porta proxy

9.3.n.10.3 Nome de utlz

9.3.n.10.7 Máx MMS 24h

9.3.n.10.3 Password

9.3.n.11 Info módulos



