



Digistat® Care

Manual do Utilizador

Versão 2.0

7/7/2025

Digistat® Care versão 2.4

Digistat® Care é fabricado pela Ascom UMS (<http://www.ascom.com>).

O Digistat® Care está  marcado de acordo com o Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho de 5 de abril de 2017 relativo a dispositivos médicos (RDM).

Ascom UMS é certificada de acordo com a EN ISO 13485:2016 com o seguinte âmbito: “Desenvolvimento de produtos e especificações, marketing, vendas, produção, instalação e manutenção de soluções de informação, comunicação e fluxo de trabalho para cuidados de saúde, incluindo software e integração com dispositivos médicos e sistemas de informação relacionados com pacientes. Marketing, vendas e instalação de soluções de informação, comunicação e fluxo de trabalho para a saúde, incluindo hardware e software.

Licença de Software

O Digistat® Care deve ser utilizado apenas após a obtenção de uma licença válida da Ascom UMS ou do Distribuidor.

Marcas registadas e direitos de autor

A Digistat® é uma marca registada da Ascom UMS. Todas as outras marcas registadas são propriedade dos seus respetivos proprietários.

Neste documento, sempre que mencionado, Android™, Google™ e Google Play™ são marcas registadas da Google, LLC; iOS, Apple® e App Store® são marcas registadas da Apple.

Nenhuma parte desta publicação pode ser reproduzida, transmitida, copiada, gravada ou traduzida, de qualquer forma, por qualquer meio, em qualquer suporte, sem o consentimento prévio por escrito da Ascom UMS.

Índice

1. Usando o manual	5
1.1 Objetivos.....	5
1.2 Caracteres utilizados e terminologia	6
1.3 Convenções	6
1.4 Símbolos	7
1.5 A Digistat Suite - Visão Geral	8
1.6 A Caixa de Informação (About box)	8
2. Digistat Care	9
2.1 Propósito Pretendido	9
2.2 Benefícios para o doente / Alegações	11
2.3 Utilização “off-label” do Produto	11
2.4 População de Pacientes	11
2.5 Grupos de utilizadores.....	11
2.6 Avisos de Segurança	12
2.7 Riscos residuais	14
2.8 Responsabilidades do organismo de cuidados de saúde.....	15
2.9 Responsabilidade do fabricante	16
2.10 Rastreabilidade do produto	16
2.11 Vigilância pós-comercialização.....	16
2.12 Ciclo de vida do produto	17
3. Especificações de Software/Hardware	18
3.1 Central e Cabeceira	19
3.1.1 Hardware	19
3.1.2 Sistema Operativo	19
3.1.3 Software de Sistema	19
3.2 Servidor de Aplicações.....	20
3.2.1 Hardware	20
3.2.2 Sistema Operativo	20
3.2.3 Software de Sistema	20
3.3 Servidor de Base de Dados.....	20
3.3.1 Hardware	20
3.3.2 Sistema Operativo.....	21
3.3.3 Software de Sistema.....	21
3.4 Digistat Mobile.....	21
3.4.1 Android.....	21
3.4.2 iOS.....	21
3.5 Digistat Gateway.....	22
3.6 Digistat Web.....	22
3.7 Ascom Telligence	23
3.8 Avisos Gerais	23
3.9 Funcionalidade de transmissão de áudio/vídeo	25
3.10 Firewall e Antivírus	25
3.10.1 Recomendações adicionais para ciberproteção	26
3.11 Funcionalidades da rede local	27
4. Antes de começar	28
4.1 Aviso de instalação e manutenção.....	28
4.2 Política de Privacidade.....	29
4.2.1 Funcionalidades e utilização das credenciais do utilizador	31

4.2.2 Administradores de sistemas	32
4.2.3 Registos do sistema	33
4.2.4 Registos forenses.....	33
4.3 Dispositivos compatíveis	33
4.3.1 Dispositivos DAS	33
4.3.2 Dispositivos SID.....	38
4.3.3 Avisos	38
4.4 Distribuição de Alarmes com Segurança de Falha Única	41
4.4.1 Torre Luminosa com Alarme	41
4.5 Falta de fiabilidade do sistema.....	42
4.5.1 Ambiente de Trabalho.....	43
4.5.2 Mobile.....	43
4.5.3 Causas de falta de fiabilidade	43
4.6 Indisponibilidade da estação de trabalho	44
5. Contactos	45

1. Usando o manual



Este Manual do Utilizador deve ser utilizado em combinação com os manuais específicos dos módulos, listados abaixo. Consulte os manuais aplicáveis, de acordo com os módulos em uso no Organismo de cuidados de saúde.

USR POR Control Bar Web

USR POR Patient Explorer Web

USR POR multiAssist Module

1.1 Objetivos

Este manual fornece todas as informações necessárias para um uso seguro e correto do Digistat Care e permite a identificação do fabricante. Além disso, fornece um guia de referência ao utilizador que deseja saber como realizar operações específicas e um guia para o uso correto do software, de modo a prevenir utilizações potencialmente perigosas.

1.2 Caracteres utilizados e terminologia

O uso do Digistat Care requer um conhecimento básico dos termos e conceitos de TI mais comuns. Da mesma forma, a compreensão deste manual está sujeita a esse conhecimento. Além disso, o uso do Digistat Care deve ser concedido apenas a pessoal profissionalmente qualificado e autorizado, treinado, com exceção de utilizadores leigos para funções limitadas (tal exceção está especificada nas Instruções de Utilização relacionadas).

Ao consultar a versão online em vez da versão em papel, as referências cruzadas no documento funcionam como hiperligações. Isto significa que sempre que encontrar a referência a uma imagem (por exemplo, “Fig. 2”) ou a um parágrafo / secção (por exemplo, “Parágrafo 2.2.1”), pode clicar na referência para ir diretamente para essa figura específica ou para esse parágrafo / secção específica.

Os dados clínicos apresentados nas imagens contidas nos manuais Ascom UMS são exemplos criados num ambiente de teste cujo único propósito é explicar a estrutura e os procedimentos do Produto. Eles não são, e não devem ser considerados como, dados reais obtidos de procedimentos clínicos reais.



Imagens relacionadas com a configuração do produto são apresentadas em inglês nos manuais Ascom UMS. Estas configurações dependem dos procedimentos e nomes adotados pelo organismo de cuidados de saúde que utiliza o Produto e, consequentemente, estarão na língua solicitada por esta quando instalado na produção.

1.3 Convenções

As seguintes convenções são utilizadas neste documento:

- Os nomes de botões, comandos de menu, opções, ícones, campos e qualquer coisa na interface do utilizador com a qual o utilizador possa interagir (seja tocar, clicar ou seleccionar) estão formatados em **negrito**.
- Os nomes/títulos de ecrãs, janelas e separadores são citados com “aspas duplas”.
- O código de programação está formatado em Courier.
- O ➤ marcador indica uma ação que o utilizador deve realizar para executar uma operação específica.
- As referências a documentos externos são formatadas em *itálico*.

1.4 Símbolos

Os seguintes símbolos são utilizados neste manual.

Informação útil



Este símbolo aparece juntamente com informações adicionais sobre as características e uso do Digistat Care. Estes podem ser exemplos explicativos, procedimentos alternativos ou qualquer informação "extra" considerada útil para uma melhor compreensão do produto.

Aviso



Este símbolo é utilizado para destacar informações destinadas a prevenir o uso inadequado do software ou para chamar a atenção para procedimentos críticos que possam causar riscos. Consequentemente, é necessário prestar extrema atenção sempre que o símbolo aparecer.

Os símbolos seguintes são utilizados na caixa de informação (about box):



Indica o nome e endereço do fabricante

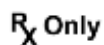


Atenção, consulte os documentos acompanhantes



Indica a necessidade de o utilizador consultar as instruções de utilização para obter informações de precaução importantes, tais como avisos e advertências que não podem, por diversas razões, ser apresentadas no próprio dispositivo médico.

Os seguintes símbolos são aplicáveis no mercado dos EUA:



Cuidado. A legislação federal dos EUA e do Canadá restringe a venda deste dispositivo a um médico licenciado ou por ordem deste

Identificação
Única do
Dispositivo
(IUD)

Identificação única do dispositivo. O sistema de identificação única do dispositivo (IUD) destina-se a atribuir um identificador único a dispositivos médicos nos Estados Unidos.

1.5 A Digistat Suite - Visão Geral

A Digistat Suite é um PDMS modular destinado a criar soluções para responder às necessidades relacionadas com a gestão de dados dos pacientes. As diferentes soluções são criadas ativando os módulos necessários que fazem parte dos dois produtos da Suite, que são:

- Digistat Docs (não é um dispositivo médico);
- Digistat Care (Dispositivo médico de classe IIb na UE, de acordo com o RDM).

O Digistat Docs é um software que regista, transfere, armazena, organiza e exibe informações e dados relacionados com o paciente, de modo a apoiar os cuidadores na criação de um registo eletrónico do paciente.

O Digistat Docs não é um dispositivo médico.

O Digistat Care é um software que gere informações e dados relacionados com o paciente, incluindo dados e eventos de dispositivos e sistemas médicos, fornecendo informações para apoiar o tratamento, diagnósticos, prevenção, monitorização, previsão, prognóstico e mitigação de doenças.

O Digistat Care é um dispositivo médico de Classe IIb na UE de acordo com o RDM.

Ambos os produtos são modulares, portanto, o organismo de cuidados de saúde específico pode escolher se deseja ativar todos os módulos disponíveis ou apenas um subconjunto, de acordo com as suas necessidades e objetivos.

Os módulos podem ser adicionados em momentos diferentes. A Suite de software resultante pode mudar ao longo do tempo de acordo com as possíveis alterações nas necessidades da organismo. Nesses casos, é ministrada formação adicional específica e a configuração é validada novamente envolvendo o organismo responsável.

1.6 A Caixa de Informação (About box)

O botão **About** no menu principal exibe uma janela que contém informações sobre a versão do Digistat Suite, os produtos instalados e as licenças relacionadas.

A rotulagem do produto é a Caixa de Informação (About Box) exibida nas estações de trabalho dos clientes e nos dispositivos móveis onde a Digistat Suite está instalada.



Em conformidade com o "Regulamento de Execução da Comissão (UE) 2021/2226" de 14 de dezembro de 2021, as instruções de utilização são apresentadas em formato eletrónico. A Caixa de informação (About box) do produto contém o endereço de um recurso web onde a última versão das instruções de uso pode ser descarregada.

2. Digistat Care

O Digistat Care é um sistema de gestão de dados de pacientes e sistema de alarme que implementa um conjunto de diferentes funcionalidades.

O Digistat Care possibilita a exibição de painéis de controlo para a monitorização quase em tempo real dos pacientes, adicionar novos parâmetros recolhidos dentro do sistema, fornecer uma forma de calcular novos parâmetros derivados (ex. pontuações ou SADC).

Digistat Care integra-se com dispositivos médicos selecionados (por exemplo, bombas de infusão, monitor de paciente, ventilador, máquina de diálise, etc.) para exibir, em PCs de estação de trabalho e smartphones selecionados, uma notificação secundária de eventos e alertas para utilizadores clínicos.

O Digistat Care é capaz de exibir dados tanto de dispositivos destinados a serem usados num sistema de alarme distribuído fiável como de dispositivos destinados a serem usados num sistema de informação distribuído (não fiável).

O Digistat Care é concebido para fornecer uma visão geral do estado dos dispositivos, destacando alarmes e/ou avisos que ocorrem no dispositivo conectado selecionado, para que o utilizador seja informado rapidamente sobre a situação na enfermaria.

Além disso, o Digistat Care introduz suporte para dispositivos vestíveis. O Digistat Care também fornece informações adicionais aos clínicos, como sistemas de pontuação (mesmo em combinação com dispositivos vestíveis) e suporte à decisão clínica (por exemplo, cálculo automático do equilíbrio de fluidos, interação de medicamentos ou notificação de alergia do paciente).

2.1 Propósito Pretendido

O Digistat Care (doravante “Produto”) é um software que transfere, armazena, elabora, agrega, organiza e exibe informações e dados relacionados com pacientes, incluindo dados e eventos de dispositivos e sistemas médicos, bem como informações inseridas manualmente, a fim de orientar a gestão clínica fornecendo informações para:

- Apoiar o tratamento, diagnóstico, prevenção, monitorização, previsão, prognóstico e mitigação de doenças.
- Triage ou identificação precoce de sinais de doenças ou patologias.

O Produto inclui:

- Recolha de dados clínicos e eventos de dispositivos e sistemas médicos em tempo quase real;
- Recolha de dados inseridos pelo utilizador;
- Processamento/filtros configuráveis para otimizar/reduzir a frequência e o número de notificações de eventos para profissionais de saúde, de modo a apresentar informações clinicamente acionáveis.
- Visualização de dados de pacientes e informações de estado de dispositivos em tempo quase real e retrospectivamente, para profissionais de saúde em dispositivo(s) de visualização designado(s);
- Integradores e Comunicadores de um sistema de informação distribuído (SID) destinado a fornecer notificações de alarmes fisiológicos e técnicos aos profissionais

de saúde, juntamente com dados clínicos e não clínicos suplementares para apoiar a monitorização de pacientes;

- Integradores e Comunicadores de um sistema de alarme distribuído (DAS/CDAS) destinado a encaminhar e entregar de forma fiável alarmes fisiológicos e técnicos de dispositivos e sistemas de origem selecionados para profissionais de saúde em dispositivos de visualização designados e para sistemas especificados;
- Elaboraões de dados para fornecer informações adicionais ao clínico, como sistemas de pontuação e apoio à decisão clínica;
- Transferir a informação adquirida para sistemas externos, clínicos e não clínicos, em tempo quase real através de uma interface de subscrição, ou retrospectivamente através de consulta de dados.

O Produto é um software autónomo que é instalado em hardware especificado e depende do uso e operação adequados de dispositivos médicos conectados, sistemas, dispositivos de visualização e da rede de TI médica.

O Produto funciona em conjunto com o Digistat Docs, o outro produto da Digistat Suite.

O produto é utilizado em instalações de cuidados de saúde em unidades de cuidados intensivos, unidades sub-intensivas, enfermarias gerais e outros departamentos e para funções limitadas no domicílio dos pacientes.

A população de pacientes e as condições dos pacientes são estabelecidas pelos dispositivos e sistemas médicos conectados e pela configuração particular do produto solicitado pelo organismo de cuidados de saúde.

Os utilizadores são profissionais de saúde treinados, com exceção dos utilizadores leigos para funções limitadas.

Informação sobre o propósito pretendido:



- O software suporta sistemas de pontuação e um motor de sistema de apoio à decisão clínica; no entanto, nenhum sistema de pontuação clínica nem algoritmos no sistema de apoio à decisão clínica são apresentados por defeito. O software pode realizar tais cálculos automáticos depois de serem validados e configurados de acordo com os utilizadores finais / clientes.
 - Os dados e os eventos clínicos geridos pelo software dependem sobretudo da sua configuração: o software pode transferir, armazenar, elaborar, agregar, organizar e apresentar dados e eventos clínicos provenientes de comandos do utilizador ou de qualquer outra fonte que tenha uma saída de dados compatível com o software e configurada durante a fase de instalação. De forma semelhante, a saída de dados do software, como os cálculos de pontuação mencionados anteriormente ou os dispositivos médicos disponíveis no local que estão conectados ao software, dependem da configuração do próprio software.
-

2.2 Benefícios para o doente / Alegações

O Produto:

- Reduz o número de mensagens de alerta recebidas pelos cuidadores, visando assim reduzir a fadiga de alarme;
- Mensagens de alerta são entregues em tempo quase real, com o objetivo de reduzir o tempo de resposta dos cuidadores.
- Mensagens de alerta são entregues em tempo quase real, com o objetivo de apoiar os cuidadores na identificação de alarmes críticos.
- Melhora a eficiência do fluxo de trabalho para o pessoal de saúde;
- Ajuda a organizar os cuidados prestados aos pacientes;
- Monitorizar as infusões ajuda a manter a continuidade da infusão, que é um aspeto importante para a segurança do paciente.
- Os dados dos pacientes são recolhidos automaticamente, com o objetivo de reduzir erros de transcrição.

2.3 Utilização “off-label” do Produto

Cada utilização do Produto fora do que está explicitamente declarado no "Uso pretendido" (geralmente referido como uso "off-label") é da total discricção e responsabilidade do utilizador e do organismo de cuidados de saúde.

O fabricante não garante de forma alguma a segurança e adequação do Produto para qualquer finalidade em que o Produto seja utilizado fora do "Uso pretendido" declarado.

2.4 População de Pacientes

O produto destina-se a ser utilizado em conexão com dispositivos e sistemas médicos e a população de pacientes é determinada por eles. O produto tem os seguintes limites técnicos:

- Peso do paciente entre 0,1 kg e 250 kg
- Altura do paciente entre 15cm e 250cm

2.5 Grupos de utilizadores

Os Grupos de Utilizadores do Produto são definidos da seguinte forma: "Utilizadores que Reagem a Alertas, Enfermeiros, Médicos, Utilizadores Técnicos e Pacientes".

Os utilizadores que reagem aos alertas são utilizadores primários que incluem Médico, Enfermeiro Registado, Assistente de Enfermagem, Enfermeiro Responsável e Enfermeiro Especialista. Esses utilizadores podem visualizar e agir sobre os alertas que são geridos pelo Produto.

O grupo de enfermeiros inclui Enfermeiro Registado, Assistente de Enfermagem, Enfermeiro Responsável e Enfermeiro Especialista e, juntamente com os Médicos, gere os dados dos pacientes no produto para apoiar os cuidados aos pacientes, ou seja, atualiza a ficha do paciente, monitoriza e regista os parâmetros vitais, define e documenta o plano de tratamento, etc.

O grupo de Utilizadores Técnicos está relacionado apenas com a instalação e configuração do sistema. Utilizadores Técnicos são utilizadores secundários que incluem Engenheiro de Serviço, Engenheiro de Campo, Engenheiro de Suporte, Engenheiro Biomédico e Instrutor Técnico.

Os pacientes atuam como utilizadores apenas para funções limitadas do produto: estas funções, no entanto, não incluem de forma alguma indicações sobre diagnóstico ou tratamento. Nessas funções limitadas, o paciente pode introduzir manualmente as medições dos parâmetros vitais e pode visualizar os parâmetros vitais adquiridos automaticamente a partir de dispositivos médicos de terceiros conectados (por exemplo, dispositivos vestíveis).

2.6 Avisos de Segurança

O Utilizador deve basear as decisões e intervenções terapêuticas ou de diagnóstico exclusivamente no exame direto da fonte original de informação. O utilizador tem a responsabilidade exclusiva de verificar se a informação exibida pelo Produto está correta e de fazer uso apropriado dela.

Apenas as impressões que forem assinadas com assinatura digital ou a tinta por profissionais médicos autorizados serão consideradas registos clínicos válidos. Ao assinar as referidas impressões, o Utilizador certifica que verificou a exatidão e a completude dos dados presentes no documento.

Ao introduzir os dados relativos ao paciente, o utilizador tem a responsabilidade de verificar se a identidade do paciente, o departamento da organização de cuidados de saúde/unidade de cuidados e as informações sobre as camas apresentadas no Produto estão corretas. Esta verificação é de extrema importância em casos de intervenções críticas, por exemplo, a administração de medicamentos.

O Organismo de cuidados de saúde é responsável por identificar e implementar procedimentos adequados para garantir que potenciais erros que ocorram no Produto e/ou na utilização do Produto sejam prontamente detetados e corrigidos e não constituam um risco para o paciente e o Utilizador. Esses procedimentos dependem da configuração do Produto e do método de utilização preferido pelo Organismo de cuidados de saúde.

O Produto pode fornecer, dependendo da configuração, acesso a informações sobre medicamentos. O Organismo de cuidados de saúde é responsável por verificar, inicial e periodicamente, que esta informação está atualizada.

Para utilizar o Produto num ambiente clínico, todos os componentes do sistema, do qual o Produto faz parte, devem cumprir todos os requisitos regulamentares aplicáveis.

Caso o Produto faça parte de um “sistema elétrico médico” através de ligação elétrica e funcional com dispositivos médicos, o organismo de cuidados de saúde é responsável pela verificação de segurança elétrica e testes de aceitação necessários, mesmo quando a Ascom UMS realizou, total ou parcialmente, as ligações necessárias.

Caso alguns dispositivos utilizados para o Produto estejam localizados na área do paciente ou estejam conectados a equipamentos presentes na área do paciente, o Organismo de cuidados de saúde tem a responsabilidade de garantir que toda a combinação esteja em conformidade com a norma internacional IEC 60601-1 e com qualquer requisito adicional estabelecido pelas regulamentações locais.

O Produto é um software autónomo que funciona em computadores padrão e/ou dispositivos móveis padrão conectados à rede local do Organismo de cuidados de saúde. O Organismo de cuidados de saúde é responsável por proteger adequadamente os computadores, dispositivos e a rede local contra ciberataques e outras falhas.

O Produto deve ser instalado apenas em computadores e dispositivos que cumpram os requisitos mínimos de hardware e em sistemas operativos e navegadores suportados.

O uso do Produto deve ser concedido, por meio de configuração específica de contas de utilizador e vigilância ativa, apenas ao Utilizador 1) treinado de acordo com as indicações do Produto por pessoal autorizado pelo fabricante ou distribuidores e 2) que possua as qualificações profissionais para interpretar corretamente as informações fornecidas e implementar os procedimentos de segurança adequados.

O Organismo de cuidados de saúde é responsável por definir um plano de recuperação de desastres; as melhores práticas incluem, mas não se limitam a, políticas de continuidade de negócios e de cópia de segurança de dados.



A Digistat Suite fornece uma solução que pode apoiar o Organismo de cuidados de saúde na implementação de uma política de continuidade de negócios. Consulte os detalhes sobre o componente Export Scheduler nos manuais de Instalação e Configuração.

2.7 Riscos residuais

Um processo de gestão de risco foi implementado no ciclo de vida do Produto, adotando as normas técnicas relevantes. Medidas de controlo de risco foram identificadas e implementadas para reduzir os riscos ao nível mínimo e torná-los aceitáveis em comparação com os benefícios trazidos pelo produto. O risco residual global é também aceitável se comparado aos mesmos benefícios.

Os riscos residuais listados abaixo foram considerados e reduzidos ao nível mínimo possível. Dada a natureza inerente do conceito de "risco", não é possível eliminá-los completamente; estes riscos residuais devem ser divulgados aos utilizadores.

- Incapacidade de utilizar o Produto ou algumas das suas funcionalidades conforme esperado, o que pode causar atrasos e/ou erros nas ações terapêuticas/diagnóstico.
 - Um exemplo deste risco é a falha do utilizador em detetar um alarme (por exemplo, devido a uma distração temporária). Uma notificação acústica é utilizada para chamar a atenção do utilizador e assim reduzir o risco.
- Desaceleração do desempenho do produto, o que pode causar atrasos e/ou erros nas ações terapêuticas/diagnóstico.
- Ações não autorizadas realizadas por utilizadores, que podem causar erros nas ações terapêuticas/diagnóstico e na atribuição de responsabilidades dessas ações.
- Configuração incorreta ou incompleta do Produto que pode causar atrasos e/ou erros nas ações terapêuticas/diagnóstico.
- Atribuição de informações ao paciente errado (troca accidental de pacientes), o que pode causar atrasos e/ou erros nas ações terapêuticas/diagnóstico.
- Manuseamento incorreto de dados de pacientes, incluindo erros na visualização, adição, modificação e eliminação de dados que podem causar atrasos e/ou erros nas ações terapêuticas/diagnóstico.
- Uso "off-label" do produto (por exemplo, produto utilizado como sistema de notificação de alarme primário quando os dispositivos médicos conectados não o suportam; decisões terapêuticas ou de diagnóstico e intervenções baseadas unicamente nas informações apresentadas pelo produto).
- Divulgação não autorizada de dados pessoais de utilizadores e/ou pacientes.

RISCOS RELACIONADOS COM A PLATAFORMA DE HARDWARE EM USO (NÃO FAZ PARTE DO PRODUTO)

- Choque elétrico para o paciente e/ou o utilizador, o que pode causar lesões e/ou morte para o paciente/utilizador.
- Componentes de hardware a sobreaquecer, o que pode causar lesões ao paciente/utilizador.
- Risco de infeção para o paciente/utilizador.

2.8 Responsabilidades do organismo de cuidados de saúde

A Ascom UMS declina toda a responsabilidade pelas consequências na segurança e eficiência do produto determinadas por reparações técnicas ou manutenção não realizadas pelo seu próprio pessoal de Serviço Técnico ou por técnicos autorizados pela Ascom UMS. Chama-se a atenção do utilizador e do representante legal do Organismo de cuidados de saúde onde o dispositivo é utilizado para as suas responsabilidades, tendo em conta a legislação local em vigor em matéria de segurança e saúde no trabalho e qualquer segurança local adicional.

O Serviço UMS da Ascom é capaz de oferecer aos clientes o suporte necessário para manter a segurança e eficiência a longo prazo dos dispositivos fornecidos, garantindo a competência, equipamento instrumental e peças suplentes necessárias para assegurar a total conformidade dos dispositivos com as especificações de construção originais ao longo do tempo.



O produto é concebido tendo em conta os requisitos e as melhores práticas presentes na norma IEC 80001 e nos seus relatórios técnicos colaterais. Em particular, o IEC/TR 80001-2-5 tem grande relevância para o produto. Conforme esclarecido na série IEC 80001, parte das atividades necessárias e das medidas de controlo de risco estão sob o controlo e responsabilidade do organismo de cuidados de saúde. Por favor, consulte a norma e os seus colaterais para identificar as atividades necessárias e as medidas de controlo de risco; em particular, consulte os seguintes documentos:

- IEC 80001-1
- IEC/TR 80001-2-1
- IEC/TR 80001-2-2
- IEC/TR 80001-2-3
- IEC/TR 80001-2-4
- IEC/TR 80001-2-5



O produto não foi concebido nem fornece funções para consultar ou armazenar a documentação gerada.

Os documentos gerados são produzidos dinamicamente com base nos dados e configurações disponíveis no momento da sua criação.

Consequentemente, não se pode garantir que as impressões subsequentes mantenham o mesmo conteúdo ou formato das versões anteriores.

Recomenda-se guardar uma cópia digital oficial para quaisquer fins de verificação.

2.9 Responsabilidade do fabricante

A Ascom UMS é responsável pela segurança, fiabilidade e desempenho do produto apenas se:

- A instalação e configuração foram realizadas por pessoal treinado e autorizado pela Ascom UMS;
- A utilização e a manutenção respeitam as instruções apresentadas na documentação do Produto (incluindo este Manual do Utilizador);
- As configurações, alterações e manutenção são efetuadas apenas por pessoal formado e autorizado pela Ascom UMS ;
- O ambiente em que o Produto é utilizado (incluindo computadores, equipamentos, ligações elétricas, etc.) está em conformidade com as regulamentações locais aplicáveis e instruções de segurança.

2.10 Rastreabilidade do produto

Para garantir a rastreabilidade do dispositivo e ações corretivas no local, em conformidade com a EN 13485 e o RDM 2017/745, solicita-se ao proprietário que informe a ASCOM UMS/Distribuidor sobre qualquer transferência de propriedade, fornecendo um aviso por escrito que indique o Produto, dados de identificação do antigo proprietário e do novo proprietário.

Os dados do dispositivo podem ser encontrados na etiqueta do Produto ("Caixa de informação" (About box) exibida dentro do Produto – ver secção 1.6).

Em caso de dúvidas/perguntas sobre a identificação do Produto, por favor contacte a Assistência Técnica da ASCOM UMS/Distribuidor (para contactos ver secção 5).

2.11 Vigilância pós-comercialização

O  dispositivo marcado em conformidade com o RDM está sujeito a uma vigilância pós-comercialização - que a ASCOM UMS e o Distribuidor fornecem para cada cópia comercializada - relativamente a riscos reais e potenciais, quer para o paciente quer para o Utilizador, durante o ciclo de vida do Produto.

Em caso de avaria ou deterioração nas características ou desempenho de um dispositivo, incluindo erro de utilização devido a características ergonómicas, bem como qualquer inadequação na informação fornecida que tenha sido ou possa ser um perigo para a saúde do paciente ou do Utilizador ou para a segurança ambiental, o Utilizador deve notificar imediatamente a ASCOM UMS ou o Distribuidor.

Após a receção de um feedback do utilizador ou se for informado internamente, a ASCOM UMS/Distribuidor iniciará imediatamente o processo de revisão e verificação e realizará as ações corretivas necessárias.

2.12 Ciclo de vida do produto

A vida útil do Produto não depende do desgaste ou de outros fatores que possam comprometer a segurança. É influenciado pela obsolescência do ambiente de software (por exemplo, SO, .NET Framework) e, portanto, está definido para 3 anos a partir da data de lançamento da versão do Produto (disponível na Caixa de informação (About box)).

3. Especificações de Software/Hardware



O Produto deve ser instalado apenas por pessoal autorizado e treinado. Isto inclui o pessoal da Ascom UMS/Distribuidores e qualquer outra pessoa especificamente treinada e explicitamente autorizada pela Ascom UMS/Distribuidor. Sem uma autorização explícita e direta da Ascom UMS/Distribuidor, o pessoal do organismo de cuidados de saúde não está autorizado a realizar procedimentos de instalação e/ou a modificar a configuração do Produto.



O produto deve ser utilizado apenas por pessoal treinado. O Produto não pode ser utilizado sem um treino adequado, realizado pelo pessoal da Ascom UMS/Distribuidores.

A informação apresentada neste capítulo abrange as obrigações do fabricante identificadas pela norma IEC 80001-1 (Aplicação da gestão de risco para redes de TI que incorporam dispositivos médicos).

É responsabilidade do organismo de cuidados de saúde manter o ambiente de execução do produto, incluindo hardware e software, conforme descrito neste capítulo. A manutenção inclui atualizações, melhorias e patches de segurança de sistemas operativos, navegadores de internet, Microsoft .NET Framework, Adobe Reader, etc., bem como a adoção de outras melhores práticas para a manutenção de componentes de software e hardware.

De acordo com a norma IEC 60601-1, no caso de um equipamento elétrico ser colocado perto da cama, é necessário o uso de dispositivos de “grau médico”. Nestas situações, geralmente são utilizados PCs de PAINEL de grau médico. Se solicitado explicitamente, a Ascom UMS é capaz de fornecer informações sobre dispositivos adequados.



Um leitor de PDF suportado deve estar instalado na estação de trabalho para mostrar a ajuda online. Consulte a secção 3.1.3.

3.1 Central e Cabeceira

3.1.1 Hardware

Requisitos mínimos de hardware:

- Processador x64 (por exemplo: Intel® i3);
- Memória: 4 GB RAM
- Disco Rígido: pelo menos 60 GB de espaço disponível
- Monitor: ecrã de 22", resolução mínima de 1920x1080, com altifalante integrado. Ecrã tátil recomendado.
- Rato ou outro dispositivo compatível.
- Interface Ethernet 100 Mb/s (ou superior)

No caso de uma estação de trabalho Central/de Cabeceira estar configurada para exibir transmissões de vídeo (funcionalidade suportada apenas na Smart Central com a integração de câmaras ativada), os requisitos mínimos são os seguintes:

- Processador x64 (por exemplo: Intel® i3);
- Memória: 4 GB RAM + 50 MB por cada transmissão de câmara exibido simultaneamente (ex. com 20 câmaras exibidas 4 GB + 1 GB)
- Disco Rígido: pelo menos 60 GB de espaço disponível
- Monitor: ecrã de 22", resolução mínima de 1920x1080, com altifalante integrado. Ecrã tátil recomendado.
- Rato ou outro dispositivo compatível
- Interface Ethernet 100 Mb/s (ou superior)

Alguns exemplos: com o Intel i7 6600 2,60 Ghz, com a transmissão de 10 câmaras a uma taxa de 3138 kbps, a utilização do CPU é de cerca de 45%. Com o I3 7100t 3.4 Ghz, com uma transmissão de 16 câmaras a uma taxa de 958 kbps, a utilização do CPU é de cerca de 30%.

3.1.2 Sistema Operativo

- Microsoft Corporation Windows 10
- Microsoft Corporation Windows 11

3.1.3 Software de Sistema

- Microsoft Framework .NET 4.8
- Adobe Acrobat Reader versão 24



Os Manuais do Utilizador são ficheiros PDF, versão 1.5, compatíveis com o Acrobat 6.x ou superior. O produto foi testado com o Adobe Acrobat Reader 124.

A organização hospitalar pode usar uma versão diferente do Acrobat Reader, é parte da Verificação do produto instalado para assegurar que o sistema de ajuda está a funcionar corretamente.

3.2 Servidor de Aplicações

3.2.1 Hardware

Requisitos mínimos de hardware (instalação pequena, 20 camas, 4 dispositivos cada):

- Processador x64 (por exemplo: Intel® i5) com 4 núcleos;
- Memória: 8 GB RAM.
- Disco Rígido: 120 GB de espaço disponível.
- Interface Ethernet 100 Mb/s.

Requisitos de hardware recomendados (instalação de tamanho médio, 100 camas, 4 dispositivos cada, Connect e Mobile):

- Processador x64 (por exemplo: Intel® i7) com 8 núcleos;
- Memória: 32 GB RAM.
- Disco Rígido: 120 GB de espaço disponível.
- Interface Ethernet: 1 Gb/s.

3.2.2 Sistema Operativo

Um dos seguintes sistemas operativos deve estar instalado:

- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019
- Microsoft Corporation Windows Server 2022
- Microsoft Corporation Windows Server 2025

3.2.3 Software de Sistema

- Microsoft Framework.NET 4.8
- Runtime & Hosting Bundle do Net Core (ver manual INST ENG Digistat Web para detalhes)

3.3 Servidor de Base de Dados

3.3.1 Hardware

Requisitos mínimos de hardware (instalação pequena, 20 camas, 4 dispositivos cada):

- Processador x64 (por exemplo: Intel® i5) com 4 núcleos;
- Memória: 8 GB RAM;
- Disco Rígido: 100 GB de espaço disponível;
- Disco Rígido de Backup: 1TB de espaço disponível;
- Interface Ethernet 100 Mb/s.

Requisitos de hardware recomendados (instalação de tamanho médio, 100 camas, 4 dispositivos cada, Connect e Mobile):

- Processador x64 (por exemplo: Intel® i7) com 8 núcleos;

- Memória: 16 GB RAM;
- Disco Rígido: 100 GB de espaço disponível, Unidade de Estado Sólido;
- Disco Rígido de Backup: 1TB de espaço disponível;
- Interface Ethernet: 1 Gb/s.

3.3.2 Sistema Operativo

Um dos seguintes sistemas operativos deve estar instalado:

- Microsoft Corporation Windows Server 2016;
- Microsoft Corporation Windows Server 2019;
- Microsoft Corporation Windows Server 2022;
- Microsoft Corporation Windows Server 2025.

3.3.3 Software de Sistema

Uma das seguintes versões do Microsoft SQL Server deve estar instalada:

- Microsoft SQL Server 2016;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2019.
- Microsoft SQL Server 2022;
- Microsoft SQL Server 2022 Express.

3.4 Digistat Mobile

3.4.1 Android

Digistat mobile é compatível com dispositivos Android a partir da versão 5.1 até 15.0. A compatibilidade foi verificada nos dispositivos Myco 3, Myco 4 (até Android 14.0), Google Pixel 9a (Android 15.0) e iPhone 14.

A aplicação foi concebida para ser compatível com outros dispositivos Android com um tamanho de ecrã mínimo de 3,5", e a compatibilidade com um dispositivo específico deve ser verificada antes do uso clínico.



Os módulos Vitals Mobile, BCMA e SADC Configurator Mobile do Digistat Mobile são compatíveis com dispositivos Android 6.0+.



Após a instalação do Digistat Mobile, antes da utilização clínica, caso os dispositivos selecionados não sejam os mencionados acima, deve ser realizada a verificação e validação de compatibilidade, de acordo com os passos detalhados definidos no documento [de lista de verificação de compatibilidade do Digistat Mobile ACDM-585-12771](#).

3.4.2 iOS

Digistat Mobile é compatível com dispositivos iOS. A compatibilidade foi verificada no dispositivo iPhone 14.

A compatibilidade com um dispositivo iOS diferente deve ser verificada antes do uso clínico.



Após a instalação do Digistat Mobile (antes da utilização clínica), caso os dispositivos selecionados não sejam iPhone 14, deve ser realizada a verificação e validação de compatibilidade, de acordo com o [documento de lista de verificação de compatibilidade do Digistat Mobile ACDM-585-12771](#).

3.5 Digistat Gateway

O Digistat Gateway é compatível com dispositivos Android da versão 9.0 até 15.0. A compatibilidade foi verificada nos dispositivos Myco 3 e Myco 4 (até Android 14.0) e Google Pixel 9a (Android 15.0).

A aplicação foi concebida para ser compatível com outros dispositivos Android com um tamanho de ecrã mínimo de 5", e a compatibilidade com um dispositivo específico deve ser verificada antes do uso clínico.

Para poder aceder à funcionalidade completa do Digistat Gateway, é necessário um cartão SIM com um plano de voz. No caso de uma instalação sem ligação Wi-Fi que permita o acesso ao driver do Gateway, também é necessário um plano de dados (é fortemente sugerida a conectividade LTE).

Por favor, contacte a Ascom UMS/Distribuidor para obter a lista completa de dispositivos que suportam o Digistat Gateway.



Após a instalação do Digistat Gateway, antes da utilização clínica, caso os dispositivos selecionados não sejam os mencionados acima, deve ser realizada a verificação e validação de compatibilidade, de acordo com os passos detalhados definidos na [lista de verificação de compatibilidade do Digistat Gateway ACDM-585-13656](#).

3.6 Digistat Web

Os seguintes navegadores são suportados para uso com aplicações Web do Digistat:

- Chrome 133 ou posterior
- Firefox 135 ou posterior
- Edge 133 ou posterior



A escala de exibição do navegador deve estar sempre definida para 100%.



Não utilize mais do que um navegador simultaneamente.



Não utilize o modo incógnito.



No caso de o Digistat Web ser utilizado para exibir notificações produzidas pelo Sistema de Suporte à Decisão Clínica, o organismo de cuidados de saúde deve avaliar a aplicação das seguintes mitigações: o navegador web de uma estação de trabalho do Digistat Web deve estar sempre em primeiro plano. O navegador web deve ser dedicado apenas ao Digistat Web, não deve ser permitido qualquer outro uso. Portanto, a página inicial padrão do navegador web deve ser o Digistat Web.



O Digistat Web utiliza Cookies para armazenar informações sobre a sessão de trabalho atual.

Os cookies estão ligados ao domínio web das aplicações.

Portanto, se os módulos e componentes do Digistat Web estiverem instalados em servidores diferentes, é necessário adotar um Balanceamento de Carga para usar URLs com um domínio web comum, permitindo assim a consistência dos cookies.

Além disso, o Balanceamento de Carga deverá ser configurado para que as chamadas https sejam redirecionadas para o servidor correto.

Por exemplo: queremos instalar o Vitals Web num servidor e a API do Vitals Web noutro servidor.

O Balanceamento de Carga deve ser configurado para que chamadas https como <https://MYDOMAIN/VitalsWeb> sejam encaminhadas para o servidor onde o Vitals Web está instalado, e as chamadas https como <https://MYDOMAIN/VitalsWebAPI> sejam encaminhadas para o outro servidor.”

3.7 Ascom Telligence

Digistat Care é compatível com o Ascom Telligence.

Versões suportadas do Ascom Telligence: 6.10, 7.0, 7.1, 7.3, 7.4, 7.5.



Todos os componentes Telligence (servidor, estação de pessoal, etc.) devem estar alinhados com a versão suportada

3.8 Avisos Gerais



No caso de o Produto ser utilizado para notificação primária de alarmes, devem ser instaladas pelo menos duas estações de trabalho de cliente dentro do mesmo departamento ou, alternativamente, pelo menos uma estação de trabalho Digistat Care e um sistema de sinalização de terceiros (por exemplo, uma Torre Luminosa com Alarme).



Para módulos móveis e de desktop, o separador decimal e, de forma mais geral, as definições regionais (por exemplo, formatos de data) utilizadas pelo Produto dependem das definições do sistema operativo da estação de trabalho ou dispositivo móvel onde o Produto está instalado. Para os módulos web, o separador decimal e, de forma mais geral, as definições regionais (por exemplo, formatos de data) utilizadas pelo Produto dependem da configuração do Produto.



Para utilizar corretamente o Produto, a Escala de Exibição do Microsoft Windows deve estar definida para 100%. Configurações diferentes podem impedir o produto de iniciar ou causar mau funcionamento na forma como o produto é visualmente exibido. Por favor, consulte a documentação do Microsoft Windows para obter instruções sobre as definições de Escala de Ecrã.



É obrigatório seguir as instruções do fabricante para armazenamento, transporte, instalação, manutenção e descarte de hardware de terceiros. Esses procedimentos devem ser realizados apenas por pessoal qualificado e autorizado.



O Organismo de cuidados de saúde deverá fornecer um "Servidor de Tempo" (ou seja, um Servidor que fornece uma referência única e partilhada para data e hora); todos os servidores e estações de trabalho onde a Digistat Suite está instalada devem usar a data/hora do Servidor de Tempo.



O Produto foi verificado e validado durante a fase de instalação ou atualização e os testes de aceitação foram realizados no hardware (PC, servidor, dispositivos móveis) e software (por exemplo, sistema operativo) juntamente com outros componentes de software (por exemplo, navegador, antivírus, etc.) já presentes. Qualquer outro hardware ou software instalado pode comprometer a segurança, eficácia e controlos de design do Produto.

É obrigatório consultar um Distribuidor/UMS autorizado da Ascom antes de utilizar com o Produto qualquer outro software que não tenha sido validado na fase de instalação ou atualização.

Se for necessário instalar outro software (utilitários ou programas de aplicação) no hardware em que o Produto funciona, o organismo de cuidados de saúde deve informar a Ascom UMS/Distribuidor para validação adicional. É sugerido aplicar uma política de permissões que impeça os utilizadores de realizar procedimentos como a instalação de novo software.



Os requisitos de hardware e software de dispositivos de terceiros (incluindo o Módulo Adaptador Inteligente da Project Engineering, Servidores de Porta da Lantronix, etc.) são divulgados nas suas instruções de uso, apresentadas pelos fornecedores. Os contactos dos fornecedores de dispositivos de terceiros podem ser apresentados pela Ascom ou por distribuidores autorizados.

3.9 Funcionalidade de transmissão de áudio/vídeo

Em certas configurações, o Produto implementa funcionalidades de transmissão de áudio/vídeo.

Nos casos em que partes do Produto atuam como visualizador de transmissões de vídeo, o Produto não é a fonte da transmissão de vídeo e não grava esta informação de forma alguma. É responsabilidade do organismo de cuidados de saúde gerir o sistema do ponto de vista da proteção de dados, incluindo a instalação e configuração das câmaras de origem.

Nos casos em que partes do Produto lidam com áudio e imagens relacionadas com os utilizadores e/ou pacientes, incluindo aquisição, elaboração e gravação, é da responsabilidade do organismo de cuidados de saúde implementar os procedimentos necessários para cumprir com a regulamentação local de proteção de dados. Incluindo, mas não se limitando à definição de limites de uso e formação de utilizadores.

A funcionalidade de transmissão de vídeo em estações de trabalho de secretária foi testada com os codecs de vídeo H264 e H265. Qualquer outro codec de vídeo presente nativamente ou instalado por aplicações de terceiros (por exemplo, VLC Media Player) deve ser testado antes de ser utilizado.

Cada fonte de vídeo suporta um número máximo de clientes conectados simultaneamente. É responsabilidade do organismo de cuidados de saúde determinar este número máximo e informar os utilizadores.

A funcionalidade de transmissão de vídeo em dispositivos móveis apenas suporta transmissões de vídeo RTSP com os seguintes tipos de autenticação:

- Sem autenticação.
- Autenticação básica.
- Autenticação digest.

A funcionalidade de transmissão de vídeo em dispositivos móveis apenas suporta os codecs de vídeo H263, H264 e H265.

3.10 Firewall e Antivírus



O conteúdo deste parágrafo destina-se a ser utilizado apenas por técnicos (por exemplo, administradores de sistemas).

Para proteger o Produto de possíveis ciberataques, é necessário que:

- A Firewall do Windows® esteja ativa tanto nos PCs dos clientes como no servidor;
- O software antivírus/antimalware esteja instalado e seja regularmente atualizado tanto nos PCs dos clientes como no servidor.

O Organismo de cuidados de saúde deve garantir que estas duas proteções estão ativadas. A Ascom UMS testou o Digistat Suite com o Antivírus WithSecure (anteriormente F-SECURE), utilizando as exclusões adequadas para a pasta “./Server” onde o Digistat Suite Server está instalado. No entanto, considerando as estratégias e políticas já existentes no Organismo de cuidados de saúde, a escolha efetiva do antivírus é da responsabilidade deste.



Sugere-se que se mantenham abertas apenas as portas TCP e UDP efetivamente necessárias. Estas podem mudar de acordo com a configuração do sistema. Para mais informações, por favor, consulte a assistência técnica da Ascom UMS.



A Ascom UMS não pode garantir que o Digistat Suite seja compatível com qualquer antivírus ou anti-malware que não seja o WithSecure (anteriormente F-SECURE). Foram relatadas incompatibilidades graves (por exemplo, fugas de memória, atraso superior a 20 segundos na troca de mensagens, etc.) entre o Digistat e outros softwares antivírus/anti-malware. Certifique-se de definir uma exclusão para toda a pasta “./Server” onde o Digistat Suite Server está instalado.

Aqui está uma lista de antivírus que causaram incompatibilidades comprovadas com o Digistat:

- Windows Defender
 - Kaspersky
 - Trend Micro Apex One
-



Alguns antivírus delegam a proteção em tempo real ao antivírus Microsoft Windows Defender. Verifique sempre se o antivírus do Windows Defender não está presente nos servidores, verificando a secção “Proteção contra vírus e ameaças” nas definições do Windows. Se presente, certifique-se de adicionar a exclusão mencionada da pasta do servidor Digistat.

3.10.1 Recomendações adicionais para ciberproteção

Para proteger ainda mais o Produto de possíveis ciberataques, é altamente recomendável:

- planear e implementar o “Endurecimento” da infraestrutura de TI, incluindo a plataforma de TI que representa o ambiente de execução para o Produto,
- implementar um Sistema de Detecção e Prevenção de Intrusões (SDPI),
- realizar um Teste de Penetração e, se for detetada alguma vulnerabilidade, executar todas as ações necessárias para mitigar o risco de ciberintrusão,
- descartar os dispositivos quando já não forem atualizáveis,
- planear e realizar uma verificação periódica da integridade dos ficheiros e configurações,
- implementar uma solução de DMZ (zona desmilitarizada) para servidores web que precisam ser expostos na internet.

3.11 Funcionalidades da rede local

Esta secção lista as características da rede local na qual o Produto está instalado, de modo a garantir a plena funcionalidade do Produto.

- O Produto utiliza um protocolo de tráfego TCP/IP.
- A LAN não deve estar congestionada e/ou sobrecarregada.
- O Produto requer pelo menos uma LAN de 100 Megabit disponível para a estação de trabalho do cliente. Seria vantajoso utilizar backbones Ethernet de 1 Gigabit.
- Não deve haver filtros no tráfego TCP/IP entre as estações de trabalho, o servidor e os dispositivos secundários.
- Se os dispositivos (servidor, estações de trabalho e dispositivos secundários) estiverem conectados a sub-redes diferentes, deve haver encaminhamento nessas sub-redes.
- Recomenda-se adotar estratégias de redundância para garantir a disponibilidade do serviço de rede em caso de avaria.
- É recomendável agendar, juntamente com a Ascom/Distribuidores, o calendário de manutenção para permitir que a Ascom ou o Distribuidor autorizado apoiem eficientemente o organismo de cuidados de saúde na gestão dos possíveis inconvenientes causados pelas atividades de manutenção.



Se a rede local for pelo menos parcialmente baseada em ligações WiFi, dada a possível intermitência da ligação WiFi, são possíveis desconexões de rede, que causam a ativação do “Modo de Recuperação ou Desconectado”, o que, no caso de o produto ser utilizado para notificação primária de alarmes, pode causar falta de fiabilidade do sistema. O Organismo de cuidados de saúde deve garantir uma cobertura de rede e estabilidade ótimas, e formar os utilizadores na gestão destas desconexões temporárias.



Detalhes adicionais sobre as características necessárias da rede local (incluindo a rede sem fios) onde a Digistat Suite está instalada estão disponíveis nos Manuais de Instalação e Configuração da Digistat Suite.

4. Antes de começar

4.1 Aviso de instalação e manutenção

As seguintes advertências fornecem informações importantes sobre os procedimentos corretos de instalação e manutenção do Produto. Elas devem ser estritamente respeitadas.



A instalação, manutenção e reparações devem ser realizadas em conformidade com os procedimentos e diretrizes da Ascom, apenas por técnicos da Ascom/Distribuidor ou pessoal treinado e autorizado pela Ascom/Distribuidor.



Recomenda-se que o organismo de cuidados de saúde que utiliza o Produto estipule um contrato de manutenção com a Ascom UMS ou um Distribuidor autorizado.



O produto deve ser instalado e configurado por pessoal especificamente treinado e autorizado. Isto inclui o pessoal da Ascom UMS (ou Distribuidor autorizado) e qualquer outra pessoa especificamente treinada e autorizada pela Ascom UMS/Distribuidor. Da mesma forma, as intervenções de manutenção e reparações no Produto devem ser realizadas de acordo com as diretrizes da Ascom UMS, apenas por pessoal da Ascom UMS/Distribuidor ou outra pessoa especificamente treinada e autorizada pela Ascom UMS/Distribuidor.

- Use dispositivos de terceiros recomendados pela Ascom UMS/Distribuidores.
- Apenas pessoal treinado e autorizado pode instalar dispositivos de terceiros.
- O Organismo de cuidados de saúde deve assegurar que a instalação e manutenção do produto e de qualquer dispositivo de terceiros seja implementada conforme solicitado para garantir a segurança e eficiência e reduzir o risco de mau funcionamento e a ocorrência de possíveis perigos para o paciente e/ou utilizador.
- O dongle USB do produto, se utilizado, deve ser armazenado e utilizado em condições ambientais adequadas (temperatura, humidade, campos eletromagnéticos, etc.), conforme especificado pelo fabricante do dongle. Estas condições são equivalentes às exigidas pelos dispositivos eletrónicos comuns de escritório.
- O organismo de cuidados de saúde é responsável por selecionar equipamentos que sejam adequados para o ambiente em que são instalados e utilizados. O organismo de cuidados de saúde, entre outras, deve considerar a segurança elétrica, as emissões de CEM, as interferências de sinais de rádio, a desinfecção e a limpeza. Atenção deve ser dada aos dispositivos instalados na área do paciente.
- O organismo de cuidados de saúde deve definir procedimentos de trabalho alternativos caso o sistema se torne pouco fiável ou deixe de funcionar.

4.2 Política de Privacidade

Devem ser tomadas precauções adequadas para proteger a privacidade dos utilizadores e pacientes, e para garantir que os dados pessoais são processados respeitando os direitos dos titulares dos dados, as liberdades fundamentais e a dignidade, particularmente no que diz respeito à confidencialidade, identidade pessoal e ao direito à proteção de dados pessoais.



‘Dados pessoais’ significa qualquer informação relativa a uma pessoa singular identificada ou identificável (‘titular dos dados’); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Atenção especial deve ser dedicada aos dados definidos no "Regulamento Geral sobre a Proteção de Dados da UE 2016/679 (RGPD)" como "Categorias especiais de dados pessoais".

Categorias especiais de dados pessoais:

(...) dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, e (...) dados genéticos, dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular.

O organismo de cuidados de saúde precisa assegurar que a utilização do Produto está em conformidade com os requisitos da regulamentação aplicável sobre privacidade e proteção de dados pessoais, respeitando especificamente a gestão das informações mencionadas.

O Produto gere e exibe dados pessoais.

O Produto pode ser configurado para ocultar automaticamente nos ecrãs da aplicação, quando nenhum utilizador tem sessão iniciada, o subconjunto de dados pessoais que pode ser utilizado para identificar uma pessoa singular.

Os campos ocultos são:

- Nome próprio e apelido
- Data de nascimento
- Sexo
- Código do paciente
- Data de admissão
- Data de alta
- Peso do paciente
- Altura do paciente

O conjunto de campos que estão ocultos pode ser ajustado durante a configuração do Produto. Para o efeito, na “Digistat Configuration Application”, defina a opção do sistema “Privacy Mode” como “true” (consulte o manual de configuração e instalação do Digistat para obter o procedimento pormenorizado). O seu valor padrão é “true”.

Se a opção "Privacy Mode" estiver definida como verdadeira, os seguintes casos são possíveis:

- Sem nenhum utilizador com sessão iniciada, não são exibidas quaisquer informações sobre o paciente.
- Com um utilizador com sessão iniciada, e o utilizador não tem uma permissão específica, nenhuma informação do paciente é exibida.
- Com um utilizador autenticado, e o utilizador tem uma permissão específica, a informação do paciente é exibida.

A opção pode ser aplicada a uma única estação de trabalho (ou seja, diferentes estações de trabalho podem ser configuradas de forma diferente).

Por favor, leia atentamente as seguintes precauções e cumpra-as rigorosamente.

- As estações de trabalho não devem ser deixadas sem supervisão e acessíveis durante as sessões de trabalho. É recomendável terminar a sessão ao deixar uma estação de trabalho.
- Os dados pessoais guardados no sistema, como palavras-passe ou dados pessoais de utilizadores e pacientes, devem ser protegidos de possíveis tentativas de acesso não autorizado através de software de proteção adequado (antivírus e firewall). O organismo de cuidados de saúde é responsável por implementar este software e mantê-lo atualizado.
- O utilizador é aconselhado a não usar frequentemente a função de bloqueio. O encerramento automático protege o sistema de acessos não autorizados.
- Os dados pessoais podem estar presentes em alguns relatórios produzidos pelo Produto. O organismo de cuidados de saúde precisa de gerir estes documentos de acordo com as normas atuais sobre privacidade e proteção de dados pessoais.
- Os postos de trabalho dos clientes (tanto de secretária como móveis) não armazenam dados de pacientes no disco. Os dados dos pacientes são armazenados apenas dentro da base de dados e o armazenamento da base de dados depende dos procedimentos e escolhas do organismo de cuidados de saúde (exemplos: máquina física, SAN, ambiente de virtualização). Os dados dos pacientes devem ser tratados de acordo com todas as normas atuais sobre privacidade e proteção de dados pessoais.
- O organismo de cuidados de saúde é responsável por fornecer formação básica sobre questões de privacidade: ou seja, princípios básicos, regras, regulamentos, responsabilidades e sanções no ambiente de trabalho específico. A Ascom UMS/Distribuidor pode fornecer formação especializada sobre a melhor utilização do Produto em relação a questões de privacidade (ou seja, anonimização de bases de dados, modo de privacidade, permissões de utilizador, etc.).
- O organismo de cuidados de saúde deve produzir e manter a seguinte documentação:
 - a. a lista atualizada dos administradores de sistema e do pessoal de manutenção;
 - b. os formulários de afetação assinados e os certificados de participação nos cursos de formação;
 - c. um registo de credenciais, permissões e privilégios concedidos aos utilizadores;
 - d. uma lista atualizada dos utilizadores do Produto.

- O organismo de cuidados de saúde deve implementar, testar e certificar um procedimento de desativação automática de utilizadores que já não estão ativos após um determinado período.
- O organismo de cuidados de saúde deve codificar, implementar e documentar um procedimento para a verificação periódica da pertença ao papel de administrador de sistema e pessoal de manutenção técnica.
- O organismo de cuidados de saúde deverá realizar auditorias e verificações sobre o comportamento correto dos operadores.



Bases de dados contendo dados de pacientes/informação sensível não podem sair do organismo de cuidados de saúde sem estarem encriptadas/ofuscadas.



Os dados dos pacientes não são armazenados em ficheiros proprietários. O único local onde os dados dos pacientes são armazenados é na base de dados.



Em algumas circunstâncias, os dados pessoais são transmitidos em formato não encriptado e utilizando uma ligação que não é fisicamente segura. Um exemplo deste tipo de transmissão são as comunicações HL7. O organismo de cuidados de saúde é responsável por fornecer medidas de segurança adequadas para cumprir as leis e regulamentos locais de privacidade.

4.2.1 Funcionalidades e utilização das credenciais do utilizador

Esta secção explica as funcionalidades das credenciais do utilizador (nome de utilizador e palavra-passe), a sua utilização e a política recomendada.

- Todas as precauções devem ser tomadas para manter o nome de utilizador e a palavra-passe pessoais em segredo.
- O nome de utilizador e a palavra-passe devem ser mantidos privados. Não deixe ninguém saber o seu nome de utilizador e palavra-passe.
- Cada utilizador pode possuir uma ou mais credenciais para aceder ao sistema (nome de utilizador e palavra-passe). O mesmo nome de utilizador e palavra-passe não devem ser usados por mais de um utilizador.
- Os perfis de autorização devem ser verificados e renovados pelo menos uma vez por ano.
- É possível agrupar diferentes perfis de autorização considerando a semelhança das tarefas dos utilizadores.
- Cada conta de utilizador deverá estar associada a uma pessoa específica. A utilização de termos genéricos (por exemplo, “ADMIN” ou “ENFERMEIRO/A”) deve ser evitada. Por outras palavras, por razões de rastreabilidade, é necessário que cada conta de utilizador seja utilizada por apenas um utilizador.
- Cada utilizador tem um perfil de autorização atribuído que lhes permite aceder apenas às funcionalidades que são relevantes para as suas tarefas de trabalho. O administrador do sistema deve atribuir um perfil de utilizador apropriado ao criar a conta de utilizador. O perfil deve ser revisto pelo menos uma vez por ano. Esta revisão também pode ser realizada para classes de utilizadores. Os procedimentos de

definição do perfil do utilizador estão descritos no manual de configuração do Produto.

- A palavra-passe deve ter pelo menos 8 caracteres.
- A palavra-passe não deve referir-se diretamente ao utilizador (contendo, por exemplo, o primeiro nome do utilizador, apelido, data de nascimento, etc.).
- A palavra-passe é fornecida pelo administrador do sistema no momento da criação da conta de utilizador. Deve ser alterada pelo utilizador no primeiro acesso caso este procedimento seja definido pela configuração.
- Depois disso, a palavra-passe deve ser alterada pelo menos a cada três meses.
- Se o nome de utilizador e a palavra-passe não forem utilizados por mais de 6 meses, devem ser desativados. Credenciais de utilizador específicas, utilizadas para fins de manutenção técnica, são uma exceção. Consulte o manual técnico para a configuração desta funcionalidade.
- As credenciais do utilizador devem também ser desativadas se o utilizador já não estiver qualificado para essas credenciais (é o caso, por exemplo, de um utilizador que é transferido para outro departamento ou estrutura). Um administrador de sistema pode ativar/desativar manualmente um utilizador. O procedimento está descrito no manual de instalação e configuração do produto.

A seguinte informação está reservada aos administradores do sistema:

A palavra-passe deve corresponder a uma expressão regular definida na configuração do Produto (o padrão é `^.....*` ou seja, 8 caracteres). A palavra-passe é atribuída pelo administrador do sistema quando uma nova conta para um utilizador é criada. O administrador do sistema pode obrigar o utilizador a alterar a palavra-passe no primeiro acesso ao sistema. A palavra-passe expira após um determinado período (configurável), após esse período, o utilizador deve alterar a palavra-passe. Também é possível (por configuração) evitar a expiração da palavra-passe.

Consulte o manual de configuração do produto para obter informações detalhadas sobre os procedimentos de criação de contas de utilizador e configuração de palavras-passe.

4.2.2 Administradores de sistemas

A equipa técnica da Ascom UMS/Distribuidor, ao realizar a instalação, atualizações e/ou Assistência técnica, pode ter acesso e lidar com dados pessoais/sensíveis armazenados na base de dados e atuar como "Administrador do Sistema" para o Produto.

A Ascom UMS/Distribuidor adota procedimentos e instruções de trabalho em conformidade com a regulamentação de privacidade em vigor ("Regulamento Geral sobre a Proteção de Dados - UE 2016/679").

O Organismo de cuidados de saúde deve avaliar, entre outras, as seguintes medidas técnicas:

- definir acessos nominais;
- ativar os registos de acesso do sistema operativo tanto ao nível do cliente como do servidor;
- ativar os registos de acesso no servidor de base de dados Microsoft SQL Server (Nível de Auditoria);
- configurar e gerir todos estes registos para acompanhar os acessos durante pelo menos um ano.

4.2.3 Registos do sistema

O Produto regista os logs do sistema na base de dados. Esses registos são mantidos por um período de tempo configurável. Além disso, os registos são mantidos por diferentes períodos de tempo, dependendo da sua natureza. Os tempos padrão são:

- os registos de informação são mantidos por 10 dias;
- os registos de mensagens de aviso são mantidos por 20 dias;
- registos de mensagens de alarme são mantidos por 30 dias.

Esses períodos são configuráveis. Consulte o manual de configuração do Produto para os procedimentos de configuração.

4.2.4 Registos forenses

Um subconjunto dos registos do sistema mencionados anteriormente, definido de acordo com a política de cada organismo de cuidados de saúde específica que utiliza o Produto como “cl clinicamente relevante” ou “cl clinicamente útil”, pode ser enviado para um sistema externo (seja uma base de dados SQL ou Syslog) para ser armazenado de acordo com as necessidades e regras do organismo de cuidados de saúde.

4.3 Dispositivos compatíveis

4.3.1 Dispositivos DAS

Estes são dispositivos que permitem a implementação de um sistema de alarme distribuído fiável.

Os dados adquiridos por este tipo de dispositivos são exibidos no Produto.

Os dados adquiridos por este tipo de dispositivos podem também ser exportados como HL7.

A comunicação de saída HL7 não é fiável.

Dispositivos suportados:

- *Ventilador Hamilton S1 e C6 e outros modelos que suportam o mesmo protocolo.*
- *Bombas de infusão Arcomed Syramed SP6000 e Volumed VP7000 conectadas à estação Arcomed UniQueConcept (e outros dispositivos que suportam o mesmo protocolo).*
- *Dispositivos médicos conectados ao Dräger Targeted Alarm Service.*

Para utilizar os dispositivos suportados num Sistema de Alarme Distribuído, é necessário configurar corretamente as definições de comunicação dos dispositivos de acordo com a documentação técnica do fabricante.

Dispositivos Hamilton

O ventilador Hamilton suporta a "silent ICU option". Isto significa que pode ser utilizado, com o Digistat Care, para operar em modo silencioso.

Para utilizar o ventilador Hamilton num Sistema de Alarme Distribuído como ventilador silencioso (por exemplo, numa UCI silenciosa), é possível utilizá-lo num estado global de ÁUDIO DESLIGADO.

Primeiro, o ventilador será corretamente configurado. Consulte a documentação técnica do dispositivo para obter as instruções técnicas e de utilização sobre como operá-lo no modo silencioso (estado ÁUDIO DESLIGADO).



Consulte a documentação do Ventilador Hamilton para obter instruções detalhadas.



O atraso máximo medido num ambiente de teste entre a ligação do dispositivo ventilador Hamilton e a exibição de dados no Produto é de 22900 ms.

O atraso máximo medido num ambiente de teste entre a ligação do dispositivo ventilador Hamilton e a exibição de dados no Produto (versão móvel) é de 20233 ms.



O atraso máximo medido num ambiente de teste entre a exibição de notificação no ventilador Hamilton e a exibição de notificação no Produto é de 600 ms.

O atraso máximo medido num ambiente de teste entre a exibição da notificação no ventilador e a exibição da notificação no Produto (versão Móvel) é de 1000 ms.

Pode demorar até dois segundos entre a geração do alarme e o envio do alarme no ventilador Hamilton.

O ventilador aguarda então um reconhecimento do Produto. Se tal reconhecimento não for recebido dentro de dois segundos, ocorre um tempo limite.

Portanto, o atraso máximo após o qual é apresentada uma notificação de alarme é de 4 segundos.



Se houver um tempo limite:

- Um alarme de ligação é acionado. O alarme pode ser cancelado pelo utilizador. É também cancelado se uma nova ligação com Entrega Confirmada for estabelecida.
 - Qualquer estado ativo global de ÁUDIO DESLIGADO é cancelado.
 - A transmissão de dados do ventilador e a Confirmação de Entrega estão paradas até que uma nova ligação seja estabelecida. Se o Digistat Care não estiver em estado Fiável, tenta imediatamente restabelecer a ligação sem Entrega Confirmada.
-



Caso os ventiladores Hamilton estejam configurados como parte de um Sistema de Alarme Distribuído, o estado global de ÁUDIO DESLIGADO é automaticamente desativado se ocorrer uma das seguintes condições:

- Os resultados do driver Hamilton não estão disponíveis;
 - O sistema DAS não apresenta resultados fiáveis.
-

Dispositivos Arcomed

A bomba / estação da Arcomed suporta a "silent ICU option". Isso significa que pode ser usado, com Digistat Care, para operar em modo silencioso.

Para utilizar a bomba/estação Arcomed num sistema de alarme distribuído como bomba/estação silenciosa (por exemplo, numa UCI silenciosa), é possível utilizá-la num estado global de ÁUDIO DESLIGADO.

Primeiro, a bomba / estação deve ser configurada corretamente. Consulte a documentação técnica do dispositivo para obter as instruções técnicas e de utilização sobre como operá-lo no modo silencioso (estado ÁUDIO DESLIGADO).



Consulte a documentação da bomba / estação Arcomed para obter instruções detalhadas.



O atraso máximo medido num ambiente de teste entre a exibição de notificação na bomba / estação Arcomed e a exibição de notificação no Digistat Care é de 3927 ms.

O atraso máximo medido num ambiente de teste entre a exibição da notificação no ventilador e a exibição da notificação no Digistat Care (versão móvel) é de 4350 ms.



O atraso máximo medido num ambiente de teste entre a ligação do dispositivo da bomba / estação Arcomed e a exibição de dados no Digistat Care é de 63 s.

O atraso máximo medido num ambiente de teste entre a ligação do dispositivo da bomba / estação Arcomed e a exibição de dados no Digistat Care (versão Mobile) é de 63 s.

Pode demorar até 10 segundos entre a geração do alarme e o envio do alarme nas bombas / estações Arcomed. A bomba / estação aguarda então um reconhecimento do Digistat Care. Se tal reconhecimento não for recebido dentro de 20 segundos, ocorre um tempo limite.

Portanto, o atraso máximo após o qual é apresentada uma notificação de alarme é de 20 segundos.

Se houver um tempo limite de comunicação:



- Um alarme de conexão é acionado nas bombas. O alarme pode ser cancelado pelo utilizador. É também cancelado se uma nova ligação com Entrega Confirmada for estabelecida.
 - Qualquer estado ativo global de ÁUDIO DESLIGADO é cancelado.
 - Se uma nova ligação com Entrega Confirmada for estabelecida e se o Digistat Care estiver em estado Fiável, o estado de ÁUDIO DESLIGADO é automaticamente restaurado pelas bombas de infusão.
 - O Digistat Care tenta restaurar a comunicação.
-



As bombas de infusão Arcomed requerem uma rede separada para funcionar como parte de um Sistema de Alarme Distribuído. “Rede separada” significa: rede física diferente, VLAN ou sub-redes IP separadas. Isto é necessário para evitar possíveis conflitos com uma política específica de segurança de rede, conforme indicado pelo fabricante da bomba / estação.



Caso as bombas Arcomed estejam configuradas como parte de um Sistema de Alarme Distribuído, o estado global de ÁUDIO DESLIGADO é automaticamente desativado se ocorrer uma das seguintes condições:

- Os resultados do driver Arcomed estão indisponíveis;
- O sistema DAS não apresenta resultados fiáveis.



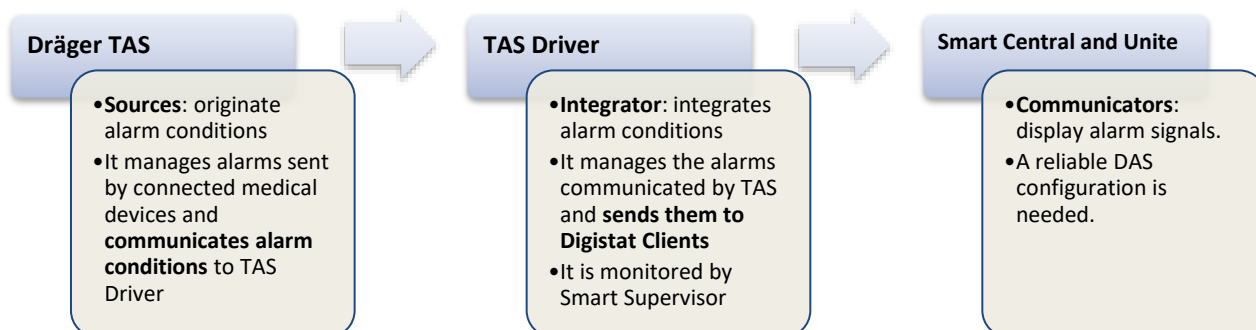
O controlador Arcomed é um controlador multicamadas, pelo que uma única estação pode estar num estado não fiável enquanto as outras estão a funcionar de forma fiável.

Dispositivos médicos conectados ao Dräger Targeted Alarm Service



Num Sistema de Alarme Distribuído com o TAS Draeger, deve haver pelo menos dois Dispositivos Médicos (AlertProvider) com o menor tempo de Autoverificação. Consulte as instruções de utilização do servidor TAS Draeger para mais informações.

O **driver do Targeted Alarm Service (TAS)** atua como um gateway de alarme e **integrador** (de acordo com a norma IEC 60601-1-8:2020) das **condições de alarme** originadas de **dispositivos médicos** conectados à rede privada Dräger. Dispositivos médicos na rede privada Dräger estão a comunicar com o **Dräger Targeted Alarm Service Gateway (TAS Gateway)**, de acordo com o protocolo de comunicação padrão SDC (IEEE 11073). O Dräger TAS encaminha condições de alarme para o TAS driver que as entrega aos **comunicadores Digistat**, como o Smart Central e o Unite, onde os sinais de alarme são finalmente exibidos.



O TAS comunica ao driver TAS através do protocolo TAS versão 1.1 as condições de alerta dos dispositivos conectados à rede TAS (até 100 dispositivos por TAS). O driver TAS suporta uma ligação encriptada e autenticação de acordo com os requisitos de segurança TLS 1.2 e a correção das mensagens é garantida pelo protocolo TCP/IP.

O driver TAS é um driver do tipo DAS, e suporta o estado **global de ÁUDIO DESLIGADO** ativo em dispositivos médicos. Juntamente com o Gateway TAS Dräger, pode ser configurado para implementar um Sistema de Alarme **Distribuído** (DAS), que requer uma configuração fiável com **Supervisor** Inteligente ativo (“Opções do Sistema” SmartCentralMode definido para **Fiabilidade** ou **Monitorização e Fiabilidade**) e **Central Inteligente dupla**.

O Gateway TAS pode enviar alertas em mais de um idioma ao mesmo tempo. Por predefinição, o driver utiliza o idioma definido para o Nó de Aquisição de Dados (opção do sistema *Idioma* com a aplicação *DASNODE*). É possível substituir o idioma e definir um ou mais idiomas diferentes no driver TAS. Se o idioma do alerta recebido dos dispositivos médicos for diferente do idioma configurado, o idioma do alerta será comunicado juntamente com o texto do alarme recebido do gateway TAS, juntamente com um aviso sobre a impossibilidade de encontrar uma tradução adequada.



Durante a configuração, o parâmetro personalizado BedNameFormat deve ser definido na página Edit Device Driver > Custom Parameters > Custom tab (Configurator Web > Connect > Drivers > Device driver management, em seguida, selecione a instância do driver TAS) da instância do driver TAS para gerir o mapeamento de camas.



Dependendo da configuração dos dispositivos conectados ao TAS, é possível o uso de idiomas mistos para os textos de alarme.



Se o produto for utilizado para a notificação primária de alarmes, qualquer dispositivo físico ligado ao mesmo através do dispositivo TAS (fabricado pela Dräger) que suporte a ativação de ÁUDIO GLOBAL DESLIGADO (conforme definido pela IEC 60601-1-8), deve desativar o ÁUDIO GLOBAL DESLIGADO em caso de:

- uma falha do Sistema de Alarme Distribuído ou
 - uma desconexão do dispositivo físico (por exemplo, da rede do Hospital, do dispositivo TAS, do Sistema de Alarme Distribuído, etc.).
-



O técnico responsável por configurar o driver Digistat TAS deve verificar duas vezes se o certificado recebido pela Dräger corresponde ao utilizado pelo servidor TAS, utilizando pelo menos dois meios diferentes (por exemplo, por correio e por voz).



Medições de atraso foram executadas num ventilador Dräger Babylog VN800, conectado à rede privada Dräger.

O atraso máximo medido num ambiente de teste entre a exibição de notificação no ventilador Dräger Babylog VN800 e a exibição de notificação no Digistat Care é de 500 ms. O atraso máximo medido num ambiente de teste entre a exibição da notificação no ventilador e a exibição da notificação no Digistat Care (versão móvel) é de 900 ms.

4.3.2 Dispositivos SID

Esses dispositivos não permitem a implementação de um sistema de alarme distribuído fiável. Esta comunicação não é fiável, portanto não pode ser utilizada para implementar um Sistema de Alarme Distribuído (DAS/CDAS) fiável. Portanto, só podem ser utilizados para implementar um Sistema de Informação Distribuído (SID). Por favor, contacte a Ascom UMS/Distribuidor para obter a lista atualizada de dispositivos disponíveis.



Por razões que estão fora do controlo do software, por exemplo, a forma como os dispositivos físicos reais estão instalados/cabados, é possível que haja atrasos entre a geração da notificação e a apresentação efetiva da notificação.



A atualização dos dados exibidos no ecrã causada pela ligação do dispositivo, desligamento, desconexão e alteração de estado depende do tempo necessário pelo próprio dispositivo para comunicar as alterações. Este tempo depende de vários fatores. Entre eles está o tipo de dispositivo e o tipo de ligação. Para alguns dispositivos, existem condições em que o atraso na comunicação de alterações pode ser importante. Como podem variar dependendo da configuração dos dispositivos e das condições operacionais, não é possível fornecer uma indicação dos atrasos para todos os dispositivos possíveis.



Os drivers utilizados para ler os dados dos dispositivos médicos conectados têm um ciclo de leitura inferior a 3 segundos (ou seja, todos os dados dos dispositivos são lidos a cada 3 segundos no máximo). No entanto, existem dispositivos que comunicam a informação com menos frequência (intervalo de 5-10 segundos). Consulte a documentação específica do driver para obter detalhes sobre o ciclo de leitura.

Num ambiente de teste instalado e configurado conforme indicado no manual de instalação e configuração, assim que um driver deteta uma notificação, demora no máximo 1 segundo a exibi-la na interface do utilizador.

4.3.3 Avisos



O Produto recebe dados de várias fontes: dispositivos médicos, sistemas de informação hospitalar e introduzidos manualmente pelo utilizador.

Além disso, o Produto calcula informações derivadas (por exemplo, pontuação). O alcance, a precisão e a exatidão destes dados dependem das fontes externas, dos dados introduzidos pelo utilizador e da arquitetura subjacente de hardware e software.



Dependendo das características dos dispositivos médicos conectados, o Produto pode ser utilizado para notificação primária (DAS/CDAS) ou secundária (SID) de alarmes. A presença de um único dispositivo SID requer que a aplicação mostre um aviso indicando que alguns dos dispositivos conectados não suportam a notificação primária de alarmes.



O Produto não foi concebido para verificar se os dispositivos conectados estão a funcionar corretamente.



Desligar um dispositivo enquanto está em funcionamento causa a interrupção da aquisição de dados no Produto. Os dados do dispositivo que são perdidos durante o período de desconexão não são recuperados pelo Produto após a reconexão.



Nunca desative a notificação de alarme nos dispositivos médicos, a menos que seja explicitamente permitido pela documentação do fabricante do dispositivo médico e pelo procedimento do organismo de cuidados de saúde.



O organismo de cuidados de saúde é responsável por garantir (por exemplo, através de listas de verificação apropriadas) ue a receção correta do alarme é tratada no Produto, tanto quando os sons de notificação estão desativados como quando estão ativados para um doente específico no dispositivo móvel.



No caso de uma bomba de infusão estar ligada ao Produto, não modifique o Número de Série da bomba de infusão.



Nunca desative o áudio nas estações de trabalho onde o Produto está a funcionar.



De acordo com a decisão do Organismo de cuidados de saúde, o produto pode ser configurado para filtrar e/ou remapear alarmes gerados pelos dispositivos médicos conectados.

Os utilizadores devem estar cientes de que, dependendo da configuração, os alarmes podem ser apresentados com uma prioridade e/ou mensagem diferente ou podem não ser anunciados.

O Organismo de cuidados de saúde é responsável por fornecer informações e formação aos utilizadores sobre a configuração do filtro de alarmes.

Os utilizadores serão informados de qualquer alteração subsequente à configuração de filtragem de alarmes.



Utilize o procedimento de verificação de som para verificar se o áudio na estação de trabalho/dispositivo portátil está a funcionar corretamente (consulte os documentos USR PT Smart Central e USR PT Mobile Launcher para o procedimento em estações de trabalho de secretária e dispositivos móveis). Se os módulos Smart Central / Smart Central Mobile não estiverem instalados, então o procedimento não é relevante.

Até uma distância de 1m (3,28 pés), o Operador é capaz de ler as notificações no Produto.

Dentro de uma distância máxima de 4m (13,12 pés), é possível que o Operador veja que há um alarme.

Estas duas afirmações são verdadeiras se:



- o Operador tem uma acuidade visual de 0 na escala logMAR ou visão de 6-6 (20/20) (corrigida, se necessário),
- o ponto de vista está na posição do Operador ou em qualquer ponto dentro da base de um cone subtendido por um ângulo de 30° em relação ao eixo horizontal ou normal ao centro do plano de exibição do monitor de visualização ou indicação visual,
- a iluminância ambiente está na faixa de 100 lx a 1 500 lx,
- o ecrã onde a Interface do Utilizador do Produto é exibida é, no mínimo, um monitor de 22 polegadas com resolução Full HD (1.920 x 1.080).

O Organismo de cuidados de saúde, de acordo com a sua política de gestão de risco e dependendo do ambiente onde o Digistat Care é executado (por exemplo, tamanho do monitor, definições de cor do monitor, colocação da estação de trabalho na enfermaria, etc.), pode definir a distância máxima real para que o Operador veja que um alarme está presente.



Periodicamente (por exemplo, no início de cada turno) verifique na estação central se para cada cama os dados provenientes dos dispositivos médicos conectados são exibidos corretamente.



Se o driver genérico Alaris® estiver em uso, é necessário esperar pelo menos dez segundos após desconectar uma bomba de infusão antes de conectar outra.



Níveis de pressão sonora abaixo do ruído ambiente podem dificultar a perceção dos utilizadores em relação aos alarmes.



O Produto adquire as informações geradas pelos dispositivos médicos primários (ou seja, ventiladores pulmonares, bombas de infusão, etc.) e exibe-as. Portanto, o Produto reporta sempre o que os dispositivos médicos primários comunicam. A atribuição de prioridades de alarme é decidida de acordo com o dispositivo médico primário. No Produto é possível decidir a ordem dos dispositivos médicos, para cada cama, de acordo com a preferência do cliente: por tipo de dispositivo, modelo / fabricante. Este tipo de ordenação é configurada no Produto durante a sua implementação de acordo com os pedidos/preferências do utilizador. A cor de cada cartão de cama (ou seja, área da cama) é sempre a cor do alarme de maior prioridade entre todos os alarmes que ocorrem nessa cama.

4.4 Distribuição de Alarmes com Segurança de Falha Única

Dependendo das características dos dispositivos médicos conectados, o produto pode ser seguro em caso de falha única no que diz respeito à distribuição de alarmes, se instalado e configurado adequadamente. Isso significa que cada parte do sistema envolvido na distribuição de alarmes é constantemente monitorizado, incluindo o próprio "controlador" (ou seja, o agente de monitorização) e, se ocorrer alguma falha em qualquer uma dessas partes, é apresentada uma notificação aos utilizadores. Em caso de avaria, o Produto deixa de funcionar até que a causa da avaria seja detetada e removida.

Para as estações de trabalho móveis (dispositivos Myco), nas mesmas condições descritas acima, é apresentada uma notificação a todos os dispositivos conectados. Esta notificação tem o mesmo nível de gravidade de um alarme clínico e não pode ser removida até que a causa seja eliminada.

Para garantir a segurança em caso de falha única, devem ser instaladas pelo menos duas estações de trabalho Digistat Care dentro do mesmo departamento ou, alternativamente, pelo menos uma estação de trabalho Digistat Care e um sistema de sinalização de terceiros (por exemplo, uma Torre Luminosa com Alarme).

Cada estação de trabalho ou torre luminosa pode, desta forma, monitorizar o funcionamento correto dos outros componentes. As estações de trabalho de secretária e a torre luminosa também monitorizam o "Controlador". Consulte o manual de configuração do produto para uma descrição detalhada da arquitetura do sistema.



O organismo de cuidados de saúde deve implementar procedimentos internos para assegurar sempre a presença de pelo menos um membro do pessoal clínico perto de cada estação de trabalho Digistat Care Desktop e, se presente, a torre luminosa com alarme, para estar prontamente ciente de qualquer alarme.

O organismo de cuidados de saúde deve implementar procedimentos adequados para restaurar a funcionalidade do Produto no menor tempo possível. Além disso, o organismo de cuidados de saúde deve definir procedimentos de trabalho alternativos caso o sistema se torne pouco fiável ou deixe de funcionar.

4.4.1 Torre Luminosa com Alarme

O Digistat Care é concebido para comunicar com uma torre luminosa com alarme opcional disponível no mercado, utilizando um protocolo padrão. Quando o Digistat Care está instalado e configurado para a distribuição fiável de alarmes, a Torre Luminosa produz notificações informativas visuais e audíveis, informando redundantemente os utilizadores se o sistema está a funcionar corretamente ou não.

A torre luminosa pode ser usada como uma alternativa à segunda estação de trabalho Digistat Care, que de outra forma é obrigatória para a distribuição fiável de alarmes.

A presença da torre luminosa depende de uma opção do sistema. Se a torre luminosa estiver presente, então o sistema pode ser validado como fiável com apenas uma estação de trabalho Digistat Care. Consulte o manual de configuração do produto para mais informações.

Na torre luminosa:

- a luz verde está acesa e nenhum som é emitido se o sistema estiver a funcionar corretamente;
- a luz vermelha acende e um som de alarme é emitido quando ocorre um alarme técnico (uma falha do sistema - ver secções 4.5 e 4.5.3);
- a luz vermelha acende e um som de alarme é emitido quando a comunicação entre a torre luminosa e o Smart Supervisor (o “controlador” mencionado acima) é interrompida; ao mesmo tempo, o Smart Supervisor fornece um alarme técnico quando a comunicação com a torre luminosa é interrompida.

A verificação do Digistat Care foi realizada com a Torre de Sinalização de Monitorização de Rede da Patlite, mas outros modelos podem ser compatíveis com o Digistat Care. Para mais informações, contacte a assistência técnica da Ascom UMS/Distribuidor.

A Torre de Sinalização de Monitorização de Rede da Patlite é uma torre de sinalização de três níveis com um alarme sonoro. Tem a capacidade de reportar imediatamente quando ocorre um evento de rede através da ligação de rede.



Fig 1

4.5 Falta de fiabilidade do sistema

Caso o sistema se torne pouco fiável, é apresentada uma notificação específica de "Erro do sistema" nas estações de trabalho Fig 2 de secretária (), nos dispositivos portáteis e numa eventual torre luminosa com alarme (luz vermelha acesa, som de alarme).

Quando ocorre um "Erro do sistema" que pode comprometer a validade dos dados, em todas as camas envolvidas não são exibidos dados de pacientes até que o sistema se torne novamente fiável.

Possíveis causas de falta de fiabilidade estão listadas no parágrafo 4.5.3 .

4.5.1 Ambiente de Trabalho

Nas estações de trabalho de secretária, as notificações permanecem na barra lateral (Fig 2 **B**) até que as causas de falta de fiabilidade sejam removidas e o sistema volte a ser fiável. Em todas as camas envolvidas com a falta de fiabilidade, nenhum dado do paciente é exibido até que o sistema seja novamente fiável.

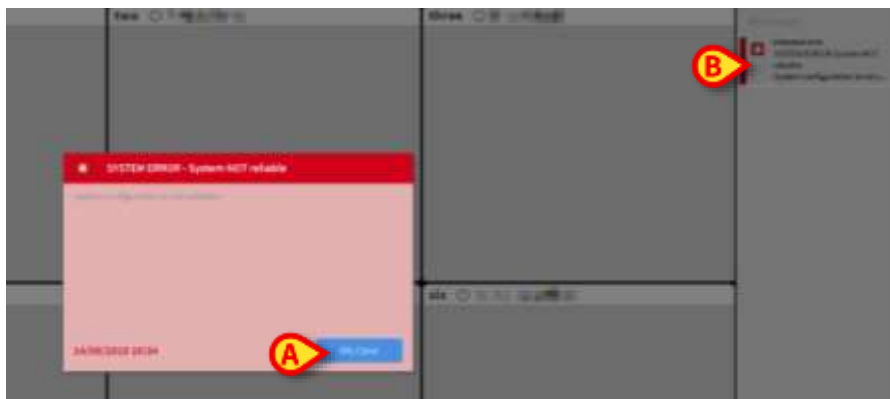


Fig 2 - Sistema não fiável (computador de secretária)

- Clique em **Ok, Close** na notificação para a reconhecer (Fig 2 **A**).

4.5.2 Mobile

Nos dispositivos móveis, é apresentada uma notificação de "Erro do sistema". Um alarme de som/vibração também é emitido.

- Deslize a notificação para baixo para a reconhecer no telemóvel. Após esta ação, o som/vibração para.

Um aviso permanece no topo de cada ecrã do telemóvel até que as causas da falta de fiabilidade sejam removidas e o sistema seja novamente fiável. Em todas as camas envolvidas com a falta de fiabilidade, nenhum dado do paciente é exibido até que o sistema seja novamente fiável.

4.5.3 Causas de falta de fiabilidade

Em caso de falta de fiabilidade do sistema, é apresentado um alarme técnico. O alarme é uma notificação de "Erro do sistema", que também fornece uma breve descrição das causas da falta de fiabilidade.

As possíveis causas de falta de fiabilidade são as seguintes:

- "A configuração do sistema não foi validada"
- "O Smart Central não está a funcionar corretamente. Erros não geridos. Contacte os Administradores do Sistema."
- "Erro de ligação da Torre Luminosa ({0})"
- "Reply timeout on external CDAS system"
- "External CDAS system disconnected"
- "Erro ao aceder à base de dados"
- "Anomalia no componente {0} ({1})"
- "Componente {0} ({1}) não responde"

- “Driver {0} em {1} não responde”
- Texto livre enviado do driver do dispositivo

NOTA: os caracteres “{0} e {1}” representam o nome do componente real.

Quando ocorre um "Erro do sistema" que pode comprometer a validade dos dados, em todas as camas envolvidas não são exibidos dados de pacientes até que o sistema se torne novamente fiável.

4.6 Indisponibilidade da estação de trabalho

Caso a estação de trabalho (incluindo dispositivos móveis) onde o produto está instalado encontre problemas ao conectar-se ao servidor, é exibida uma mensagem de informação específica.



Se a rede não corresponder às funcionalidades solicitadas, o desempenho do Produto deteriora-se gradualmente até ocorrerem erros de tempo limite. O sistema pode finalmente mudar para o modo "Recovery".

O produto tenta recuperar-se automaticamente. Se a recuperação automática falhar, é necessário contactar a Assistência Técnica (ver secção 5 para obter a lista de contactos).



É responsabilidade do organismo de cuidados de saúde que utiliza o Produto definir um procedimento de emergência a ser implementado em caso de indisponibilidade do sistema. Isto é necessário para

1. Permitir que os departamentos continuem a trabalhar.
 2. Restaure o sistema para plena disponibilidade o mais rapidamente possível (a política de backup faz parte desta gestão).
-

A Ascom UMS/Distribuidor oferece total apoio na definição de tal procedimento. Consulte a secção 5 para obter a lista de contactos.

As características e funcionalidades descritas nas secções 0 e 4.5 também são aplicáveis quando o produto não está instalado e configurado para a distribuição primária de alarmes (por exemplo: quando o protocolo de comunicação do dispositivo médico não se destina a este fim).

Nesses casos, as características e funcionalidades acima mencionadas funcionam como um mecanismo de segurança adicional e redundante, supervisionando os componentes do produto. Eles podem ou não supervisionar a ligação com os dispositivos médicos, dependendo da configuração do produto e das características técnicas do dispositivo médico.



Nestas condições, o sistema inteiro não pode ser considerado seguro contra falhas únicas e não pode ser utilizado para comunicação primária e fiável de alarmes.

5. Contactos

Para qualquer problema, por favor, consulte primeiro o Distribuidor que instalou o Produto.

Contactos do fabricante:

Ascom UMS s.r.l unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Itália

Tel. (+39) 055 0512161

Fax (+39) 055 8290392

Assistência técnica

support.it@ascom.com

800999715 (chamada gratuita, apenas Itália)

Informação sobre vendas e produtos

it.sales@ascom.com

Informação geral

it.info@ascom.com