



Digistat® Care

Manual de Usuario

Versión 11.0

2023-09-22

Digistat® Care Versión 1.6

Digistat® Care es un producto de Ascom UMS s.r.l (<http://www.ascom.com>).



Digistat® Care tiene el marcado ⁰⁴⁷⁶ de acuerdo con el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios.

Ascom UMS está certificada conforme al estándar EN ISO 13485:2016 con el siguiente alcance: *"Product and specification development, manufacturing management, marketing, sales, production, installation and servicing of information, communication and workflow software solutions for healthcare including integration with medical devices and patient related information systems"*

Licencia de software

Digistat® Care debe utilizarse solo después de obtener una licencia válida de Ascom UMS o del Distribuidor.

Licencias y marcas registradas

Digistat® es una marca registrada de Ascom UMS s.r.l. Todas las demás marcas registradas son propiedad de sus respectivos propietarios.

En este documento, siempre que aparezcan Android™, Google™ and Google Play™ deberán considerarse marcas comerciales de Google, LLC.

Ninguna parte de esta publicación puede ser reproducida, transmitida, copiada, grabada o traducida, en cualquier forma, por cualquier procedimiento, en cualquier medio, sin previa autorización escrita de Ascom UMS.

Contenido

1. Uso del Manual	5
1.1 Objetivos.....	5
1.2 Caracteres y terminología utilizados.....	6
1.3 Convenciones.....	6
1.4 Símbolos	7
1.5 La suite Digistat - Visión general.....	8
1.6 La casilla «Acerca de» de Digistat	8
2. Digistat Care	9
2.1 Uso Previsto.....	10
2.2 Beneficios para el paciente / Reclamaciones	11
2.3 Uso “off-label” del Producto.....	11
2.4 Población de pacientes	11
2.5 Grupos de usuarios	11
2.6 Consejos de seguridad.....	12
2.7 Riesgos residuales	14
2.8 Responsabilidades de la organización sanitaria	15
2.9 Responsabilidad del fabricante.....	15
2.10 Trazabilidad del producto	16
2.11 Sistema de supervisión post-venta.....	16
2.12 Vida del producto	16
3. Especificaciones de Software y Hardware	17
3.1 Central & Bedside	18
3.1.1 Hardware	18
3.1.2 Sistema Operativo	18
3.1.3 Software del Sistema.....	18
3.2 Servidor de aplicaciones.....	19
3.2.1 Hardware.....	19
3.2.2 Sistema Operativo	19
3.2.3 Software del sistema.....	19
3.3 Servidor de base de datos.....	19
3.3.1 Hardware	19
3.3.2 Sistema Operativo.....	20
3.3.3 Software del sistema	20
3.4 Digistat “Mobile”	20
3.5 Digistat Gateway.....	20
3.6 Digistat “Web”	21
3.7 Ascom Telligence	22
3.8 Advertencias.....	22
3.9 Funcionalidades de transmisión de audio/vídeo.....	23
3.10 Firewall y Antivirus.....	24
3.10.1 Otras precauciones recomendadas para la protección cibernética	25
3.11 Características de la red local	26
4. Antes de empezar	27
4.1 Advertencias de instalación y mantenimiento.....	27

4.2 Gestión de la privacidad.....	28
4.2.1 Características y uso de las credenciales de usuario	31
4.2.2 Administradores de sistema.....	32
4.2.3 Registro de sistema	32
4.2.4 Registro forense	32
4.3 Dispositivos compatibles.....	33
4.3.1 Dispositivos DAS	33
4.3.2 Dispositivos DIS.....	37
4.3.3 Advertencias.....	37
4.4 Distribución segura de alarmas para fallos individuales	40
4.4.1 Torre de luces de alarma	41
4.5 Falta de fiabilidad del sistema	42
4.5.1 Escritorio	42
4.5.2 Móvil	43
4.5.3 Causas de la falta de fiabilidad	43
4.6 Producto no disponible.....	44
5. Contacto del Fabricante	45

1. Uso del Manual

Este manual de instrucciones se debe utilizar junto con los manuales específicos del módulo, enumerados a continuación. Consulte los manuales correspondientes, de acuerdo con los módulos de Digistat utilizados en la organización sanitaria:



USR ESP Controlbar
USR ESP Smart Central
USR ESP Fluid Balance
USR ESP Infusion
USR ESP Patient Explorer
USR ESP Scoring Calculator
USR ESP Therapy
USR ESP Smart Central Mobile
USR ESP BCMA (Mobile)
USR ESP Vitals Mobile
USR ESP Mobile Launcher
USR ESP CDSS Configurator Mobile

1.1 Objetivos

Este manual proporciona toda la información necesaria para garantizar un uso seguro y correcto de Digistat Care y para permitir la identificación del fabricante.

Además, proporciona una guía de referencia para el usuario que desea saber cómo realizar operaciones específicas y una guía para el uso correcto del software a fin de evitar usos indebidos potencialmente peligrosos.

1.2 Caracteres y terminología utilizados

El uso de los sistemas Digistat requiere un conocimiento básico de los términos y conceptos más comunes de TI. De la misma manera, la comprensión de este manual está sujeta a ese conocimiento.

Recuerde que el uso de los sistemas Digistat sólo debe autorizarse al personal profesionalmente calificado y con la formación adecuada.

Si se consulta la versión online en lugar de la versión impresa, las referencias cruzadas del trabajo documental actúan como enlaces hipertextuales. Esto significa que cada vez que se encuentre la referencia a una imagen (“Fig 10”, por ejemplo) o a un apartado (“apartado 2.2.1”, por ejemplo), se puede hacer clic en la referencia para acceder directamente a la figura o al apartado de que se trate.



Los datos clínicos que se muestran en las imágenes contenidas en los manuales de Ascom UMS son ejemplos creados en un entorno de prueba cuyo único propósito es explicar la estructura y los procedimientos del Producto. No son, ni se deben considerar, datos reales tomados de procedimientos clínicos de la vida real. Las piezas relacionadas con la configuración del Producto se presentan en inglés en los manuales de Ascom UMS. Estas configuraciones dependen de los procedimientos y nombres reales adoptados por la organización de atención médica que utiliza el Producto y, en consecuencia, estarán en el idioma solicitado por la organización de atención médica.

1.3 Convenciones

Las siguientes convenciones se utilizan en este documento:

- Los nombres de los botones, comandos de menú, opciones, iconos, campos y cualquier elemento de la interfaz de usuario con el que el usuario pueda interactuar (ya sea al tocar o hacer clic o seleccionar) están formateados en **negrita**.
- Los nombres/encabezados de las pantallas, ventanas y pestañas se citan con «Comillas dobles».
- El código de programación está formateado en Courier.
- El punto ➤ indica una acción que el usuario debe realizar para llevar a cabo una operación específica.
- Las referencias a documentos externos están formateadas en *cursiva*.

1.4 Símbolos

En el manual se usan los siguientes símbolos.

Información útil



Este símbolo aparece allí donde hay información adicional acerca de las características y del uso de Digistat Care. Pueden tratarse de ejemplos explicativos, procedimientos alternativos o cualquier información "extra" considerada útil para una mejor comprensión del producto.

¡Precaución!



Este símbolo se usa para destacar información que tiene por objeto prevenir acerca del uso indebido del software o llamar la atención sobre procedimientos críticos que pudieran causar riesgos. Por consiguiente, es necesario prestar la máxima atención cada vez que aparezca el símbolo.

Los siguientes símbolos se usan en el cuadro de información del Producto:



El nombre y la dirección del fabricante.



Atención, consulte los documentos adjuntos.



Este símbolo indica que el usuario debe consultar las instrucciones de uso para obtener información de seguridad relevante, como advertencias y precauciones que, por diversos motivos, no pueden mostrarse en el propio dispositivo médico.

1.5 La suite Digistat - Visión general

El paquete Digistat es un PDMS modular destinado a crear soluciones para atender las necesidades relacionadas con la gestión de datos de los pacientes. El paquete está formado por dos productos. Son los siguientes:

- Digistat Docs (no es un dispositivo médico);
- Digistat Care (producto sanitario de clase IIb en la UE según el Reglamento sobre los productos sanitarios).

Digistat Docs es un software que registra, transfiere, almacena, organiza y muestra la información del paciente y los datos relacionados con el mismo, con el fin de ayudar a los proveedores de atención médica a establecer un historial clínico electrónico del paciente. Digistat Docs no es un dispositivo médico.

Digistat Care es un software que gestiona la información del paciente y los datos relacionados con el paciente, incluidos los datos y eventos de dispositivos y sistemas médicos, y proporciona información para ayudar en el tratamiento, diagnóstico, prevención, supervisión, predicción, pronóstico y mitigación de enfermedades.

Digistat Care es un producto sanitario de clase IIb en la UE según el Reglamento sobre los productos sanitarios.

Ambos productos son modulares, por lo tanto, la organización de atención médica específica puede elegir si habilitar todos los módulos disponibles o solo un subconjunto, de acuerdo con sus necesidades y objetivos.

Los módulos se pueden añadir en diferentes momentos. El paquete de software resultante puede cambiar con el tiempo, de acuerdo con los posibles cambios en las necesidades de la organización. En estos casos, se proporciona formación adicional específica y la configuración se valida de nuevo con la participación de la organización responsable.

1.6 La casilla «Acerca de» de Digistat

El botón **Acerca de** en el menú principal muestra una ventana que contiene información sobre la versión y el producto instalado, así como las licencias relacionadas.

El etiquetado real es el cuadro Acerca de que se muestra en las estaciones de trabajo del cliente y en los dispositivos móviles donde está instalado el paquete Digistat.



De conformidad con el reglamento de ejecución (UE) 2021/2226 de la comisión de 14 de diciembre de 2021, las instrucciones de uso se proporcionan en formato electrónico. El cuadro Acerca de del producto contiene la dirección de un recurso web donde se puede descargar la última versión de las instrucciones de uso.

2. Digistat Care

Digistat Care es un sistema de gestión de datos de pacientes y un sistema de alarma que implementa un conjunto de funcionalidades diferentes.

Digistat Care permite mostrar paneles para la supervisión de los pacientes casi en tiempo real, añadir nuevos parámetros recopilados dentro del sistema, proporcionar una forma de calcular nuevos parámetros derivados (por ejemplo, puntuaciones o CDSS).

Digistat Care se integra con dispositivos médicos seleccionados (p. ej., bombas de infusión, monitor de paciente, respirador, máquina de diálisis, etc.) para mostrar, en PC de estaciones de trabajo y teléfonos inteligentes seleccionados, una notificación secundaria de eventos y alertas a los usuarios médicos.

Digistat Care puede mostrar datos tanto de los dispositivos destinados a utilizarse en un sistema de alarma distribuido fiable como de los dispositivos destinados a utilizarse en un sistema de información distribuido (no fiable).

Digistat Care está diseñado para proporcionar una visión general del estado de los dispositivos, destacando las alarmas o las advertencias que se producen en el dispositivo conectado seleccionado, de modo que el usuario esté informado de un vistazo sobre la situación en la sala.

Además, Digistat Care admite dispositivos ponibles. Digistat Care también proporciona información adicional a los médicos, como sistemas de puntuación (incluso en combinación con dispositivos ponibles) y apoyo para la toma de decisiones clínicas (p. ej., cálculo automático del equilibrio de fluidos, interacción de medicamentos o notificación de alergias del paciente).

2.1 Uso Previsto

Digistat Care (en adelante, «Producto») es un software que transfiere, almacena, elabora, agrega, organiza y muestra información del paciente y datos relacionados con el paciente, incluidos datos y eventos de dispositivos y sistemas médicos, así como la información introducida manualmente, con el fin de facilitar la gestión clínica al proporcionar información para:

- Ayudar en el tratamiento, diagnóstico, prevención, supervisión, predicción, pronóstico y mitigación de enfermedades.
- Triage o identificación de los primeros signos de la enfermedad o de las afecciones.

Digistat Care incluye:

- Recopilación de datos clínicos y eventos de dispositivos y sistemas médicos en tiempo casi real.
- Recolección de datos introducidos por el usuario;
- Procesamiento y filtros configurables para optimizar y reducir la frecuencia y el número de notificaciones de eventos a profesionales de la salud, con el fin de presentar información clínicamente procesable.
- Visualización de los datos del paciente y la información del estado del dispositivo en casi tiempo real y de forma retrospectiva a los profesionales de la salud en el/los dispositivo/s de visualización designado/s.
- Un integrador y comunicadores de un sistema de información distribuido (SID) destinados a proporcionar a los profesionales de la salud notificaciones de alarmas de carácter fisiológico y técnico, así como datos clínicos y no clínicos adicionales, con el fin de facilitar el seguimiento de los pacientes.
- Un integrador y comunicadores de un sistema de alarma distribuido (DAS/CDAS) pensado para transmitir de forma fiable alarmas de carácter fisiológico y técnico a los profesionales de la salud a partir de dispositivos y sistemas fuente seleccionados y de emitirlos en dispositivos con pantalla y sistemas especificados seleccionados.
- Elaboración de datos para proporcionar información adicional al médico, como sistemas de puntuación y apoyo a la decisión clínica.
- Transferencia de la información adquirida a sistemas externos, clínicos y no clínicos, casi en tiempo real a través de una interfaz de suscripción, o retrospectivamente a través de una consulta de datos.

Digistat Care es un software autónomo que se instala en un hardware específico y se basa en el uso y funcionamiento adecuado de los dispositivos médicos conectados, los sistemas, los dispositivos de visualización y la red informática médica.

Digistat Care trabaja junto con Digistat Docs, el otro producto del paquete Digistat.

Este producto se utiliza en instalaciones sanitarias, tales como unidades de cuidados intensivos y subintensivos, salas generales y otros departamentos, así como en el domicilio del paciente con funciones limitadas.

La población de pacientes y las afecciones de los pacientes se establecen por los dispositivos y sistemas médicos conectados y por la configuración particular de Digistat Care solicitada por la organización de atención médica.

Los usuarios son profesionales sanitarios formados o bien usuarios sin formación cuando se utilizan las funciones limitadas.

2.2 Beneficios para el paciente / Reclamaciones

El producto:

- Reduce la cantidad de mensajes de alerta recibidos por los cuidadores para intentar reducir la fatiga por alarmas.
- Los mensajes de alerta se envían casi en tiempo real para acortar el tiempo de respuesta del cuidador
- Los mensajes de alerta se envían casi en tiempo real para ayudar a los cuidadores a identificar las alarmas críticas
- Permite implementar un sistema DAS/CDAS que respalde la reducción del ruido de las alarmas para procurar un entorno más silencioso para el paciente
- Mejora la eficiencia del flujo de trabajo para el personal sanitario
- Ayuda a organizar la atención al paciente
- La monitorización de las bombas de infusión ayuda a mantener la continuidad de las mismas, un aspecto fundamental para la seguridad del paciente
- Los datos de los pacientes se recopilan automáticamente para reducir los errores de transcripción

2.3 Uso “off-label” del Producto

Todo uso del Producto fuera de lo indicado en la Finalidad de uso (lo que suele llamarse uso "off-label") se efectúa exclusivamente bajo el criterio y la responsabilidad del usuario y de la organización responsable.

El fabricante no garantiza en modo alguno que el Producto sea seguro y adecuado si se usa fuera de lo indicado en la Finalidad de uso.

2.4 Población de pacientes

El producto está destinado a ser utilizado en conexión con dispositivos y sistemas médicos y la población de pacientes está determinada por ellos.

El producto tiene los siguientes límites técnicos:

- Peso del paciente entre 0.1kg y 250kg
- Altura del paciente entre 15 cm y 250 cm

2.5 Grupos de usuarios

Los grupos de usuarios del producto se definen de la siguiente manera: usuarios que reaccionan a las alertas, enfermeros, médicos, usuarios técnicos y pacientes.

Los usuarios que reaccionan a las alertas corresponden a los usuarios principales, que incluyen: médico/a (Medical Doctor), enfermero/a titulado/a (Registered Nurse), auxiliar de enfermería (Nurse Assistant), enfermero/a responsable (Charge Nurse) y enfermero/a especialista (Nurse Practitioner). Esos usuarios pueden ver y gestionar las alertas del producto.

El grupo de enfermeros incluye a enfermeros titulados (Registered Nurse), auxiliares de enfermería (Nurse Assistant, enfermeros responsables (Charge Nurse) y enfermeros

especialistas (Nurse Practitioner), quienes, junto con los médicos (Medical Doctors), gestionan los datos del paciente en el producto para garantizar la mejor atención y cuidados al paciente, es decir, actualizar la historia clínica del paciente, controlar y registrar sus constantes vitales, establecer y documentar el plan de tratamiento, etc.

El grupo de usuarios técnicos está relacionado únicamente con la instalación y configuración del sistema. Los usuarios técnicos son usuarios secundarios que incluyen al ingeniero de servicio (Service Engineer), al ingeniero de campo (Field Engineer), al ingeniero de soporte (Support Engineer), al ingeniero biomédico (Biomedical Engineer) y al instructor técnico (Technical Instructor).

Los pacientes se consideran usuarios únicamente cuando se utilizan las funciones limitadas del producto. Ahora bien, dichas funciones no incluyen indicación alguna sobre un posible diagnóstico o tratamiento. En dichas funciones limitadas, el paciente puede introducir manualmente mediciones de las constantes vitales y visualizar las constantes vitales que se han extraído automáticamente de productos sanitarios conectados de terceros (p. ej., productos ponibles).

2.6 Consejos de seguridad

El Usuario deberá basar las decisiones y las intervenciones terapéuticas y diagnósticas solamente a partir de la verificación directa de la fuente primaria de información. Es responsabilidad exclusiva del Usuario el verificar que la información proporcionada por el Producto sea correcta, así como el uso apropiado de la misma.

Sólo las impresiones que lleven la firma digital o física de médicos profesionales autorizados deben ser consideradas documentación clínica válida. Al firmar dichas impresiones, el Usuario certifica que ha verificado que los datos presentes en el documento son completos y correctos.

Al introducir los datos relacionados con el paciente, el usuario tiene la responsabilidad de verificar que sean correctos la identidad del paciente, el departamento/la unidad de cuidados de la institución de atención sanitaria y la información de la cama que se muestra en el producto. Esta comprobación es de fundamental importancia en caso de operaciones críticas como, por ejemplo, la administración de medicamentos.

La institución de atención sanitaria es responsable de identificar e implementar los procedimientos apropiados para asegurar que los potenciales errores que se produzcan en el Producto y/o en el uso del Producto se detecten y corrijan rápidamente y que no constituyan un riesgo para el paciente o para el operador. Estos procedimientos dependen de la configuración del producto y del método de uso preferido por la institución de atención sanitaria.

El Producto, según la configuración, puede proporcionar acceso a información sobre los fármacos. La institución de atención sanitaria es responsable de verificar inicial y periódicamente que esta información esté al día.

Para utilizar el Producto en un entorno clínico, todos los componentes del sistema del que forma parte el Producto deberán cumplir con todos los requisitos reglamentarios aplicables. En caso de que el Producto forme parte de un «sistema eléctrico médico» a través de la conexión eléctrica y funcional con dispositivos médicos, la organización sanitaria se encargará de la verificación de la seguridad eléctrica requerida y de las pruebas de aceptación, incluso cuando Ascom UMS realice total o parcialmente las conexiones necesarias.

En caso de que algunos de los dispositivos en uso para el Producto se encuentren dentro del área de pacientes o estén conectados a instrumentos que se encuentren dentro del área de pacientes, La institución de atención sanitaria tiene la responsabilidad de asegurar que toda la combinación cumpla con la norma internacional IEC 60601-1 y con cualquier otro requisito adicional establecido por las regulaciones locales.

El producto es un software autónomo que funciona en ordenadores estándar y/o dispositivos móviles estándar conectados a la red local de la institución de atención sanitaria. La institución de atención sanitaria es responsable de proteger adecuadamente los ordenadores, los dispositivos y la red local contra los ataques cibernéticos.

El Producto debe instalarse solamente sobre ordenadores y dispositivos que cumplan con los requisitos mínimos de hardware y sólo en los sistemas operativos compatibles.

Es necesario garantizar el uso del producto mediante la configuración específica de las cuentas de usuario y una supervisión activa, únicamente a Usuarios; 1) adiestrados por personal autorizado por el fabricante o por sus distribuidores conforme a las indicaciones del Producto, y 2) profesionalmente cualificados para interpretar correctamente la información que el Producto proporciona y para implementar los debidos procedimientos de seguridad. La organización sanitaria es responsable definir un plan de recuperación en caso de catástrofes; ejemplos de buenas prácticas son, entre otros, las políticas de continuidad de las actividades y de copia de seguridad de los datos.



El Digistat Suite brinda una solución que puede ayudar a la organización sanitaria a aplicar la política de continuidad de las actividades. En los manuales de instalación y configuración encontrará información más detallada sobre el componente Export Scheduler.

2.7 Riesgos residuales

Se ha implementado un proceso de gestión de riesgos en el ciclo de vida del Producto adoptando los estándares técnicos pertinentes. Se han identificado e implementado medidas de control de riesgos para reducir los riesgos al nivel mínimo y hacer que sean aceptables en comparación con los beneficios que aporta el Producto. El riesgo residual global también es aceptable si se compara con los mismos beneficios.

Los riesgos residuales que se enumeran a continuación se han tenido en cuenta y se han reducido al mínimo posible. Dada la naturaleza inherente al concepto de «riesgo», no es posible eliminarlos completamente; estos riesgos residuales se comunicarán a los usuarios.

- Incapacidad de utilizar el Producto o algunas de sus funcionalidades previstas, lo que podría causar retrasos y/o errores en las acciones terapéuticas/diagnósticas.
 - Un ejemplo de este riesgo es una fallo del usuario para detectar una alarma (p. ej., debido a una distracción temporal). Se utiliza una notificación acústica para llamar la atención del usuario y así reducir el riesgo.
- Ralentización del rendimiento del Producto, lo que podría causar retrasos o errores en las acciones terapéuticas o diagnósticas.
- Acciones no autorizadas realizadas por los usuarios, lo que podría causar errores en las acciones terapéuticas o diagnósticas y en la asignación de responsabilidades de estas acciones.
- Configuración incorrecta o incompleta del producto, que podría causar retrasos o errores en las acciones terapéuticas o diagnósticas.
- Atribución de información al paciente equivocado (intercambio accidental de pacientes), lo que podría causar retrasos y/o errores en las acciones terapéuticas/diagnósticas.
- Una manipulación incorrecta de los datos del paciente, incluyendo errores en la visualización, adición, modificación y eliminación de datos que podrían causar retrasos y/o errores en las acciones terapéuticas/diagnósticas.
- Uso no autorizado (off-label) del Producto (por ejemplo, Producto utilizado como sistema primario de notificación de alarmas cuando los dispositivos médicos conectados no lo admiten, decisiones terapéuticas o diagnósticas e intervenciones basadas únicamente en la información proporcionada por el Producto).
- Divulgación no autorizada de los datos personales de los usuarios y/o del paciente.

RIESGOS EN RELACIÓN CON LA PLATAFORMA DE HARDWARE UTILIZADA

- Sacudida eléctrica para el paciente y/o el usuario, que puede causar accidentes y/o la muerte al paciente/usuario.
- Sobrecalentamiento de los componentes de hardware, que puede causar heridas al paciente/usuario.
- El paciente/usuario puede contraer infecciones.

2.8 Responsabilidades de la organización sanitaria

Ascom UMS se exime de toda responsabilidad en relación con los efectos sobre la seguridad y la eficiencia del dispositivo determinados por intervenciones técnicas de reparación o mantenimiento no llevadas a cabo por el Servicio Técnico de Ascom UMS, los Técnicos autorizados por Ascom UMS o los distribuidores autorizados.

La atención del usuario y del representante legal de la organización de salud donde se utiliza el dispositivo se centra en sus responsabilidades, considerando la legislación local vigente en materia de seguridad y salud en el trabajo y cualquier otro procedimiento local adicional de seguridad en el lugar de trabajo.

El Servicio de Ascom UMS y de los distribuidores autorizados puede proporcionar a los clientes la asistencia necesaria para mantener a largo plazo la eficiencia y la seguridad de los dispositivos suministrados, asegurando la competencia, el equipamiento instrumental y los repuestos adecuados para garantizar que los dispositivos cumplan totalmente con las especificaciones originales del fabricante.



El producto está diseñado teniendo en cuenta los requisitos y las mejores prácticas presentes en la norma IEC 80001 y sus informes técnicos colaterales. En particular, la IEC/TR 80001-2-5 tiene una gran relevancia para el producto. Como se aclara en la serie IEC 80001, parte de las actividades necesarias y de las medidas de control de riesgos están bajo el control y la responsabilidad de la organización sanitaria. Consulte la norma y sus garantías para identificar las actividades necesarias y las medidas de control de riesgos; en particular, consulte la versión actual válida de los siguientes 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

2.9 Responsabilidad del fabricante

Ascom UMS se considera responsable de la seguridad, la fiabilidad y las prestaciones del producto únicamente si:

- La instalación y configuración fueron realizadas por personal capacitado y autorizado por Ascom UMS;
- El uso y el mantenimiento cumplen con las instrucciones proporcionadas en la documentación del Producto (incluyendo este Manual de instrucciones);
- Solo el personal formado y autorizado por Ascom UMS lleva a cabo las configuraciones, los cambios y el mantenimiento;
- El entorno en el que se utiliza el Producto (incluidos ordenadores, equipos, conexiones eléctricas, etc.) cumple con la normativa local aplicable y con las instrucciones de seguridad aplicables.

2.10 Trazabilidad del producto

Para garantizar la trazabilidad del dispositivo y las acciones correctivas en el sitio, de conformidad con la norma EN 13485 y el Reglamento (UE) 2017/745 sobre los productos sanitarios, se le solicita al propietario que informe a Ascom UMS o al Distribuidor sobre cualquier traspaso de propiedad mediante notificación por escrito en la que se indique el producto y los datos de identificación del anterior y el nuevo propietario.

Los datos del dispositivo se pueden encontrar en la etiqueta del producto ("Casilla Acerca de" que se muestra dentro del producto, véase párrafo 1.6).

En caso de dudas o preguntas sobre la identificación del Producto, póngase en contacto con el servicio de asistencia técnica de Ascom UMS o del Distribuidor (para acceder a los contactos, consulte la sección 5).

2.11 Sistema de supervisión post-venta

El dispositivo con la marca  de conformidad con el Reglamento sobre los productos sanitarios, queda sujeto a una vigilancia posterior a la comercialización, que Ascom UMS y el Distribuidor proporcionan para cada copia comercializada, en relación con los riesgos reales y potenciales, ya sea para el paciente o para el usuario, durante el ciclo de vida del producto. El usuario deberá contactar inmediatamente con ASCOM UMS o con el distribuidor en caso de mal funcionamiento o deterioro de las características o del rendimiento del producto, incluido el error de uso debido a características ergonómicas, así como cualquier insuficiencia en la información suministrada que haya sido o pudiera ser un peligro para la salud del paciente o del usuario o la seguridad ambiental.

Al recibir las opiniones de los usuarios, o si tiene conocimiento interno, Ascom UMS o el Distribuidor iniciará inmediatamente el proceso de revisión y verificación y tomará las medidas correctivas necesarias.

2.12 Vida del producto

La vida útil del producto no depende del desgaste u otros factores que puedan comprometer la seguridad. Está condicionada por la obsolescencia del entorno de software (por ejemplo, OS, .NET Framework) y, por lo tanto, se establece en 3 años a partir de la fecha de lanzamiento de la versión del producto (disponible en la casilla «Acerca de»).

3. Especificaciones de Software y Hardware



La instalación de Digistat debe ser realizada únicamente por personal capacitado y autorizado. Esto incluye al personal de Ascom UMS/Distribuidores y cualquier otra persona específicamente formada y explícitamente autorizada por Ascom UMS/Distribuidor. Sin una autorización explícita y directa de Ascom UMS/Distribuidor, el personal de la organización sanitaria no está autorizado para realizar procedimientos de instalación y/o modificar la configuración de Digistat.



Digistat solo debe ser utilizado por personal capacitado. No se puede utilizar Digistat sin haber recibido una formación adecuada por el personal de Ascom UMS/Distribuidores.

Este capítulo recoge las características software y hardware necesarias para que el Producto pueda funcionar correctamente. Las informaciones que se dan en esta sección cubren las obligaciones informativas a cargo del fabricante identificadas en la norma IEC 80001-1:2010 (Application of risk management for IT-networks incorporating medical devices).

Es responsabilidad de la organización de atención médica mantener el entorno de ejecución del producto, incluido el hardware y el software, tal como se describe en este capítulo. El mantenimiento incluye mejoras, actualizaciones y parches de seguridad de sistemas operativos, navegadores web, Microsoft .NET Framework, Adobe Reader, etc., así como la adopción de otras prácticas recomendadas para el mantenimiento de componentes de software y hardware.

Conforme al estándar IEC 60601-1, en caso de colocar dispositivos eléctricos cerca de la cama, es necesario el uso de dispositivos de grado médico. En estas situaciones suelen usarse PANEL PC de grado médico. Si se solicita, Ascom UMS puede sugerir algunos posibles aparatos de este tipo.



Se debe instalar un lector de PDF compatible en la estación de trabajo para visualizar la ayuda en línea.

3.1 Central & Bedside

3.1.1 Hardware

Requisitos hardware mínimos:

- Procesador x64 (por ejemplo: Intel® i3)
- Memoria RAM 4GB
- Disco duro con un mínimo de 60 GB de espacio libre
- Monitor: pantalla de 22", resolución mínima de 1920x1080, con altavoz integrado. Pantalla táctil recomendada.
- Ratón o aparato compatible
- Interfaz de red Ethernet 100 Mb/s (o superior)

En caso de que una estación de trabajo central o de cabecera esté configurada para mostrar flujos de vídeo (función solo compatible con Smart Central con la integración de cámara habilitada), los requisitos mínimos son los siguientes. :

- Procesador x64 (por ejemplo: Intel® i3)
- Memoria: 4 GB de RAM + 50 MB por cada retransmisión de cámara que se muestre simultáneamente (por ejemplo, 4 GB + 1 GB en el caso de 20 cámaras retransmitiendo)
- Disco duro con un mínimo de 60 GB de espacio libre
- Monitor: pantalla de 22", resolución mínima de 1920x1080, con altavoz integrado. Pantalla táctil recomendada.
- Ratón o aparato compatible
- Interfaz de red Ethernet 100 Mb/s (o superior)

Algunos ejemplos: con Intel i7-6600 de 2,60 Ghz y streaming de 10 cámaras con una tasa de bits de 3138 kbps, el uso de CPU es de aproximadamente el 45 %. Con i3-7100T de 3,4 Ghz y streaming de 16 cámaras con una tasa de bits de 958 kbps, el uso de CPU es de aproximadamente el 30 %.

3.1.2 Sistema Operativo

- Microsoft Corporation Windows 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10
- Microsoft Corporation Windows 11

3.1.3 Software del Sistema

- Microsoft Framework .NET 4.7.2
- Adobe Acrobat Reader 10



El Manual de usuario del Producto es un archivo PDF elaborado de acuerdo con la versión estándar PDF 1.5 y, por lo tanto, legible por Adobe Acrobat 6.0 o superior. Además, el manual de usuario del producto se ha probado con Adobe Acrobat Reader 10. La organización del hospital puede utilizar una versión diferente de Acrobat Reader: la verificación del producto instalado incluirá la comprobación de la correcta lectura del Manual del usuario.

3.2 Servidor de aplicaciones

3.2.1 Hardware

Requisitos mínimos de hardware (instalación pequeña, 20 camas, 4 dispositivos cada una):

- Procesador x64 (por ejemplo: Intel® i5) con 4 núcleos;
- Memoria RAM 8 GB (se aconsejan 8 GB)
- Disco duro con un mínimo de 120 GB de espacio libre
- Interfaz de red Ethernet 100 Mb/s (o superior). Se aconseja 1 Gb/s.

Requisitos de hardware recomendados (instalación de tamaño mediano, 100 camas, 4 dispositivos cada una, Connect y Mobile):

- Procesador x64 (por ejemplo: Intel® i7) con 8 núcleos;
- Memoria RAM 32 GB
- Disco duro con un mínimo de 120 GB de espacio libre
- Interfaz de red Ethernet 1 Gb/s.

3.2.2 Sistema Operativo

Debe estar instalado uno de los siguientes sistemas operativos:

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019
- Microsoft Corporation Windows Server 2022

3.2.3 Software del sistema

- Microsoft Framework.NET 4.7.2

Net Core Runtime & Hosting Bundle (Para más información, véase el manual *INST ENG Digistat Web*)

3.3 Servidor de base de datos

3.3.1 Hardware

Requisitos mínimos de hardware (instalación pequeña, 20 camas, 4 dispositivos cada una):

- Procesador x64 (por ejemplo: Intel® i5) con 4 núcleos;
- Memoria RAM 8 GB (se aconsejan 8 GB)
- Disco duro con un mínimo de 120 GB de espacio libre
- Interfaz de red Ethernet 100 Mb/s (o superior). Se aconseja 1 Gb/s.

Requisitos de hardware recomendados (instalación de tamaño mediano, 100 camas, 4 dispositivos cada una, Connect y Mobile):

- Procesador x64 (por ejemplo: Intel® i7) con 8 núcleos;
- Memoria RAM 32 GB.
- Disco duro con un mínimo de 120 GB de espacio libre
- Interfaz de red Ethernet 1 Gb/s.

3.3.2 Sistema Operativo

Debe estar instalado uno de los siguientes sistemas operativos:

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019
- Microsoft Corporation Windows Server 2022

3.3.3 Software del sistema

Debe estar instalada una de las siguientes versiones de Microsoft SQL Server:

- Microsoft SQL Server 2014;
- 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”

Digistat Mobile es compatible con dispositivos Android desde la versión 5.1 hasta la 13.0. Se ha verificado en Ascom Myco SH2 – Wi-fi, móvil y Dect en Android 10 (Myco3), en Samsung Galaxy 10 con Android 11, en Google Pixel 3a con Android 12 y en Zebra TC51 - Android 7.1. La aplicación está diseñada para ser compatible con otros dispositivos Android con un tamaño mínimo de pantalla de 3.5“; la compatibilidad con un dispositivo específico debe verificarse antes del uso clínico.



Los módulos Vitals Mobile, BCMA y CDSS Configurator Mobile de Digistat Mobile son compatibles con dispositivos Android 6.0+.



Después de la instalación de Digistat Mobile, antes del uso clínico, es necesario hacer una verificación y validación de la compatibilidad, de acuerdo con los pasos detallados y definidos en el documento Digistat Mobile compatibility checklist ACDM-585-12771 de la lista de comprobación de compatibilidad de Digistat Mobile.

3.5 Digistat Gateway

Digistat Gateway es compatible con dispositivos Android versión 9.0 a 12.0. Se ha comprobado en el Ascom Myco SH2 Wi-Fi/Cellular (wifi/móvil) (Android 10), en Samsung A10 (Android 11), y en Google Pixel 3a (Android 12). La aplicación está diseñada para que sea compatible con otros dispositivos Android con un tamaño de pantalla mínimo de 5”. La compatibilidad con un dispositivo específico se debe verificar antes de cualquier uso clínico. Para poder acceder a todas las funciones de Digistat Gateway se requiere una tarjeta SIM con un plan de llamadas. En el caso de una instalación sin conexión wifi que permita el acceso al controlador de la pasarela, también se precisa un plan de datos (se recomienda encarecidamente conectividad LTE).

Para conocer la lista completa de dispositivos compatibles con Digistat Gateway, contacte con Ascom UMS o con el distribuidor.



Después de la instalación de Digistat Mobile, antes del uso clínico, es necesario hacer una verificación y validación de la compatibilidad, de acuerdo con los pasos detallados y definidos en el Digistat Gateway compatibility checklist ACDM-585-13656, de la lista de comprobación de compatibilidad de Digistat Mobile.

3.6 Digistat “Web”

Los siguientes navegadores son compatibles para su uso con aplicaciones web Digistat:

- Chrome 109
- Firefox 109
- Edge 109



La escala de visualización del navegador siempre debe establecerse en 100%.



No utilice más de un navegador simultáneamente.



No utilice el modo de incógnito.



En caso de que se utilice Digistat Web para mostrar notificaciones generadas por el sistema de soporte a la toma de decisiones clínicas, la organización sanitaria debería considerar aplicar las siguientes medidas de mitigación: el navegador web de una estación de trabajo de Digistat Web debe estar siempre en primer plano. El navegador web debe destinarse únicamente a Digistat Web y a ningún otro uso. Por lo tanto, la página de inicio predeterminada del navegador debe ser Digistat Web.



Digistat Web utiliza cookies para almacenar información sobre la sesión de trabajo actual.

Las cookies están vinculadas al dominio web de las aplicaciones.

Por lo tanto, si los módulos y componentes de Digistat Web están instalados en diferentes servidores, es necesario adoptar un balanceador de carga para utilizar URLs con un dominio web común permitiendo así la consistencia de las cookies.

Además, el balanceador de carga deberá configurarse de modo que las llamadas https se redirijan al servidor correcto.

Por ejemplo: queremos instalar Vitals Web en un servidor y Vitals Web API en otro servidor.

El balanceador de carga debe configurarse para que las llamadas https como <https://MYDOMAIN/VitalsWeb> se dirijan al servidor donde está instalado Vitals Web, y las llamadas https como <https://MYDOMAIN/VitalsWebAPI> se dirijan al otro servidor.

3.7 Ascom Telligence

Digistat Care es compatible con Ascom Telligence.

Versiones compatibles: 6.10, 7.0, 7.1



Todos los componentes de Telligence (servidor, estación de personal, etc.) deben configurarse de acuerdo con la versión compatible

3.8 Advertencias



En caso de que el Producto se utilice para la notificación primaria de alarmas, se instalarán al menos dos estaciones de trabajo cliente en el mismo departamento o, como alternativa, al menos una estación de trabajo Digistat Care y una Torre de luces de alarma. Consulte la sección 4.4 para obtener más información.



El separador decimal y, en general, la configuración regional (por ejemplo, formatos de fecha) utilizados por el producto dependen de la configuración del sistema operativo de la estación de trabajo o dispositivo móvil donde está instalado el Producto.

Para los módulos web, el separador decimal y, de forma más general, la configuración regional (por ejemplo, formatos de fecha) utilizados por el Producto dependen de la configuración de este.



Para utilizar correctamente el Producto es necesario que el valor del ajuste de escala de pantalla de Microsoft Windows sea del 100%. Otras configuraciones pueden impedir la ejecución del producto o crear problemas de funcionamiento a nivel de representación gráfica. Para establecer el valor de escala de pantalla, consultar la documentación de Microsoft Windows.



Es obligatorio seguir las indicaciones del fabricante para el almacenaje, transporte, instalación, mantenimiento y eliminación del hardware de terceras partes. Dichas operaciones deberán ser efectuadas únicamente por personal competente y con la formación adecuada



Los requisitos de hardware y software de dispositivos de terceros (incluido el Smart Adapter Module de Project Engineering, Port Servers de Lantronix, etc.) se describen en sus instrucciones de uso, proporcionadas por los proveedores. Los contactos de los proveedores de dispositivos de terceros pueden ser proporcionados por Ascom o por distribuidores autorizados.



La organización clínica debe implementar un mecanismo de sincronización de la fecha y hora de las estaciones de trabajo en las que el Producto funciona con una fuente temporal de referencia.

El Producto ha sido verificado y validado durante la fase de instalación o actualización, y su prueba de aceptación se ha realizado en el hardware (PC, servidor, dispositivos móviles) y software (por ejemplo, sistema operativo) junto con otros componentes de software (por ejemplo, navegador, antivirus, etc.) ya presentes. Cualquier otro hardware o software instalado puede comprometer la seguridad, la eficacia y los controles de diseño del Producto.



Es obligatorio consultar a un distribuidor/UMS autorizado de Ascom antes de usar junto con el Producto cualquier otro software que no sea el validado en la fase de instalación o actualización.

Si es necesario instalar cualquier otro software (utilidades o programas de aplicaciones) en el hardware en el que se ejecuta el Producto, la organización de atención médica informará a distribuidor/UMS de Ascom para realizar una validación adicional. Se sugiere aplicar una política de permisos que evite que los usuarios realicen procedimientos como la instalación de un nuevo software.

3.9 Funcionalidades de transmisión de audio/vídeo

En ciertas configuraciones, el Producto implementa funcionalidades de transmisión de audio/vídeo.

En los casos en que partes del Producto actúan como visores de flujos de vídeo; el Producto no es la fuente del flujo de vídeo y no graba esta información de ninguna manera. La organización sanitaria debe encargarse de gestionar el sistema desde una perspectiva de protección de datos, incluida la instalación y la configuración de las cámaras de origen

En los casos en que partes del Producto manejan el audio y las imágenes relacionados con los usuarios y/o pacientes, incluida su captación, elaboración y grabación. La organización sanitaria debe implementar los procedimientos necesarios para cumplir con la normativa local de protección de datos, incluyendo, entre otras cosas, la definición de los límites de uso y la formación de usuarios.

La funcionalidad de transmisión de vídeo en estaciones de trabajo de escritorio se ha probado con códecs de vídeo H264 y H265.

Cualquier otro códec de vídeo propio o instalado por aplicaciones de terceros (por ejemplo, VLC Media Player) se debe probar antes de utilizarlo.

Cada fuente de vídeo admite un número máximo de clientes conectados simultáneamente. La organización sanitaria debe determinar este número máximo e informar a los usuarios.

La funcionalidad de transmisión de vídeo en dispositivos móviles solo es compatible con flujos de vídeo RTSP con lo siguientes tipos de autenticación:

- Sin autenticación;
- Autenticación básica;
- Autenticación Digest.

La funcionalidad de transmisión de vídeo en dispositivos móviles solo es compatible con códecs de vídeo H263, H264 y H265.

3.10 Firewall y Antivirus



El contenido de este apartado está reservado exclusivamente al personal técnico (p. ej.: administradores de sistemas).

Para proteger el Producto contra posibles ataques informáticos, es necesario que:

- el Firewall de Windows esté activo, tanto en las estaciones de trabajo como en el servidor;
- en las estaciones de trabajo y en los servidores haya un software antivirus/antimalware activo y regularmente actualizado.

Corre a cargo de la organización de salud asegurarse de la implementación de esas dos protecciones. Ascom UMS probó el Digistat Suite con el antivirus WithSecure (anteriormente F-SECURE) utilizando las debidas exclusiones para la carpeta “./Server”, donde está instalado el servidor del Digistat Suite. Ahora bien, la elección definitiva del antivirus es responsabilidad de la organización sanitaria en función de sus estrategias y políticas que ya sean de aplicación.



Se aconseja encarecidamente mantener abiertos únicamente los puertos TCP y UDP efectivamente necesarios. Estos pueden variar en función de la configuración del Producto. En relación con esto, es importante consultar los detalles específicos del caso con el servicio de asistencia técnica.



Ascom UMS no puede garantizar que el Digistat Suite sea compatible con cualquier antivirus o antimalware diferente de WithSecure (anteriormente F-SECURE).

Se han notificado incompatibilidades graves entre Digistat y otros programas antivirus o antimalware (p. ej., pérdidas de memoria, retrasos de más de 20 segundos en el intercambio de mensajes, etc.). Asegúrese de configurar una exclusión para toda la carpeta “./Server”, donde está instalado el servidor del Digistat Suite.

A continuación se ofrece una lista de antivirus que han provocado incompatibilidades con Digistat:

- Microsoft Windows Defender
 - Kaspersky
 - Trend Micro Apex One
-



Algunos antivirus delegan la protección en tiempo real en Microsoft Windows Defender. Compruebe siempre que dicho antivirus no esté presente en los servidores consultando la sección «Protección contra virus y amenazas» en la configuración de Windows. Si está presente, añada la exclusión mencionada de la carpeta del servidor de Digistat.

3.10.1 Otras precauciones recomendadas para la protección cibernética

Para proteger aún más el Producto de posibles ataques cibernéticos, se recomienda encarecidamente:

- planificar e implementar el «endurecimiento» de la infraestructura informática, incluida la plataforma informática que representa el entorno de tiempo de ejecución para el Producto;
- implementar un Sistema de Detección y Prevención de Intrusos (IDPS);
- realizar una Prueba de penetración y, si se detecta alguna debilidad, realizar todas las acciones necesarias para mitigar el riesgo de intrusión cibernética;
- desechar los dispositivos cuando ya no sean actualizables;
- planificar y realizar una verificación periódica de la integridad de los archivos y las configuraciones;
- implementar una solución DMZ (zona desmilitarizada) para servidores web que deben ser expuestos en internet.

3.11 Características de la red local

En este apartado se indican las características que debe tener la red local en la que se instale el Producto para que el Producto funcione correctamente.

- El Producto utiliza tráfico de tipo TCP/IP estándar.
- La red LAN debe estar libre de congestiones y saturaciones.
- El Producto requiere una LAN de al menos 100 Megabites disponible para la estación de trabajo cliente. Una red troncal Ethernet de 1 Gigabit sería muy válida.
- Entre las estaciones de trabajo, los servidores y los dispositivos secundarios no debe haber filtros al tráfico TCP/IP.
- Si los dispositivos (servidores, estaciones de trabajo y dispositivos secundarios) están conectados a subredes distintas, dichas subredes deben estar enrutadas.
- Se sugiere adoptar técnicas de redundancia a fin de asegurar el servicio de red incluso en caso de problemas de funcionamiento.
- Se aconseja programar, junto con Ascom UMS/Distribuidores, un calendario de mantenimiento de modo que Ascom UMS o el Distribuidor autorizado apoyen eficientemente al instituto sanitario a la hora de gestionar los posibles problemas de servicio causados por las actividades de mantenimiento.



Si la red local se basa al menos de forma parcial en conexiones wifi, la posible intermitencia de la conexión wifi puede dar lugar a desconexiones de red, lo que provoca la activación del «Modo de recuperación o desconexión», el cual, en caso de que se utilice el producto para la notificación primaria de alarmas, puede provocar la falta de fiabilidad del sistema. La Organización de atención médica asegurará una cobertura y estabilidad óptimas de la red, y formará a los usuarios sobre cómo gestionar estas desconexiones temporales.



En los *manuals de instalación y configuración del Digistat Suite* se pueden encontrar más detalles sobre las características necesarias de la red local (incluida la red inalámbrica) donde está instalado el Digistat Suite.

4. Antes de empezar

4.1 Advertencias de instalación y mantenimiento

Las siguientes advertencias acerca de la correcta instalación y del mantenimiento del producto deben respetarse escrupulosamente.



La instalación, el mantenimiento y la reparación deben ser realizados de acuerdo con los procedimientos y las pautas de Ascom UMS solo por técnicos de Ascom UMS/Distribuidor o personal capacitado y autorizado por Ascom UMS/Distribuidor.



Se recomienda que la organización sanitaria que utilice el Producto estipule un contrato de mantenimiento con Ascom UMS o con un distribuidor autorizado.



El Producto debe ser instalado y configurado por personal específicamente adiestrado y autorizado. Esto incluye al personal de Ascom UMS (o Distribuidor autorizado) y a cualquier otra persona específicamente formada y autorizada por Ascom UMS/Distribuidor.

Del mismo modo, las intervenciones de mantenimiento y reparaciones del Producto deben realizarse de conformidad con las directrices Ascom UMS y únicamente por personal de Ascom UMS/Distribuidor u otra persona específicamente formada y autorizada por Ascom UMS/Distribuidor.

- Utilice los dispositivos de terceras partes recomendados por Ascom UMS/Distribuidores. Solamente el personal adiestrado y autorizado puede instalar dispositivos de terceras partes.
- La Organización de atención médica se asegurará de que la instalación y el mantenimiento del producto y de cualquier dispositivo de terceros se implemente según lo solicitado para garantizar la seguridad y la eficiencia, así como para reducir el riesgo de mal funcionamiento y la aparición de posibles riesgos para el paciente o el usuario.
- La llave USB del Producto, si se utiliza, debe almacenarse y usarse en condiciones ambientales aptas (temperatura, humedad, campos electromagnéticos, etc.), según lo especificado por el fabricante de la llave. Estas condiciones son equivalentes a las requeridas por los dispositivos electrónicos de oficina habituales.
- La organización sanitaria es responsable de seleccionar los equipos adecuados para el entorno en el que se instalan y utilizan. La organización sanitaria debe tener en cuenta, entre otras cosas, la seguridad eléctrica, las emisiones de CEM, las interferencias de las señales de radio, la desinfección y la limpieza. Se debe prestar especial atención a los dispositivos instalados en la zona de pacientes.
- La organización de atención médica deberá definir procedimientos de trabajo alternativos en caso de que el sistema no sea fiable o deje de funcionar.

4.2 Gestión de la privacidad

Se tomarán las precauciones adecuadas para proteger la intimidad de los usuarios y pacientes y para garantizar que los datos personales se traten respetando los derechos, las libertades fundamentales y la dignidad de las personas a las que se refieren los datos, en particular por lo que respecta a la confidencialidad, la identidad personal y el derecho a la protección de los datos personales.



Se entenderá por «datos personales» toda información relativa a una persona física identificada o identificable (el «titular de los datos»); se entenderá por «persona física identificable» toda persona física que pueda ser identificada, directa o indirectamente, en particular mediante un identificador, como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios factores específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona física.

Se prestará especial atención a los datos definidos en el «Reglamento general de protección de datos de la UE 2016/679 (RGPD)» como «Categorías especiales de datos personales».

Categorías especiales de datos personales:

(...) Datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la pertenencia a un sindicato, y (...) datos genéticos, datos biométricos con el fin de identificar de manera exclusiva a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

La organización sanitaria debe asegurarse de que el uso del Producto se ajusta a los requisitos de la normativa aplicable en materia de privacidad y protección de datos personales, respetando específicamente la gestión de dicha información.

El Producto gestiona y muestra datos personales.

El Producto se puede configurar para ocultar automáticamente en las pantallas de la aplicación, cuando ningún usuario ha iniciado sesión, el subconjunto de datos personales que se pueden utilizar para identificar a una persona física. Los campos ocultos son:

- Nombre y apellidos
- Fecha de nacimiento
- Sexo
- Código del paciente
- Fecha de ingreso
- Fecha de alta
- Peso del paciente
- Altura del paciente

El conjunto de campos que están ocultos se puede ajustar durante la configuración del Producto.

Para ello, en la aplicación de configuración del Producto ajuste la opción del sistema denominada «Modo de privacidad» a «verdadero» (consulte el manual de configuración e instalación del Producto para conocer el procedimiento detallado). Su valor predeterminado es «verdadero».

Si la opción «Modo de privacidad» está ajustada a verdadero, es posible que se den los siguientes casos:

- sin ningún usuario conectado, no se muestra la información del paciente.
- con un usuario conectado, pero sin un permiso específico, no se muestra la información del paciente.
- con un usuario conectado y con un permiso específico, se muestra la información del paciente.

La opción se puede aplicar a una sola estación de trabajo (es decir, diferentes estaciones de trabajo se pueden configurar de forma diferente).

Leer atentamente las precauciones presentadas en este apartado y respetarlas escrupulosamente.

- Los ordenadores en uso no deben quedar accesibles y sin vigilancia durante las sesiones de trabajo con el Producto. Es importante realizar el cierre de sesión para salir del Producto al alejarse de la estación de trabajo.
- Los datos personales introducidos en el Producto, como contraseñas o datos personales de los usuarios o de los pacientes deben ser protegidos contra todo intento de acceso no autorizado a través de software adecuados (antivirus y firewall). El instituto sanitario es responsable de implementar este software y mantenerlo actualizado.
- Un uso frecuente de la función “bloquear” no es en absoluto aconsejable. La función de cierre automático de sesión se ha implementado porque hace menos probables los accesos al sistema por parte de personas no autorizadas.
- Los datos personales pueden estar presentes dentro de algunos informes producidos por el Producto. La organización sanitaria debe gestionar estos documentos de acuerdo con las normas actuales sobre privacidad y protección de datos personales.
- Las estaciones de trabajo (tanto de escritorio como de móvil) no almacenan datos del paciente en el disco. Los datos del paciente sólo se almacenan dentro de la base de datos y el almacenamiento de bases de datos depende de los procedimientos y opciones de la estructura sanitaria (ejemplos: máquina física, San, software de virtualización). Los datos de los pacientes serán tratados de acuerdo con todas las normas vigentes sobre privacidad y protección de datos personales.
- La organización sanitaria se encarga de impartir formación básica en materia de privacidad, es decir, principios básicos, normas, reglamentos, responsabilidades y sanciones en el entorno laboral específico. Ascom UMS/Distribuidor proporcionará formación especializada sobre el mejor uso del Producto en relación con cuestiones de privacidad (por ejemplo, anonimato de la base de datos, modo de privacidad, permisos de usuario, etc.).

- La organización sanitaria debe producir y mantener la siguiente documentación:
 - a. la lista actualizada de los administradores del sistema y del personal de mantenimiento;
 - b. los formularios de asignación firmados y las certificaciones de asistencia a los cursos de formación;
 - c. un registro de credenciales, permisos y privilegios otorgados a los usuarios;
 - d. una lista actualizada de los usuarios del Producto.
- La organización sanitaria deberá implementar, probar y certificar un procedimiento de desactivación automática de los usuarios inactivos después de un cierto período de tiempo.
- La organización sanitaria deberá codificar, implementar y documentar un procedimiento para la verificación periódica de la pertenencia a la función de administrador de sistemas y personal técnico de mantenimiento.
- La organización sanitaria debe llevar a cabo auditorías y controles sobre el correcto comportamiento de los operadores.



Los datos del paciente no se almacenan en formato propietario. El único lugar en el que se almacenan los datos del paciente es la base de datos.



En algunas circunstancias se transmiten datos personales en formato no encriptado y utilizando una conexión no intrínsecamente segura. Un ejemplo de esa situación son las comunicaciones HL7. La organización responsable debe encargarse de disponer, dentro de la red hospitalaria, mecanismos de seguridad adecuados para garantizar la conformidad con las leyes y los reglamentos en relación con la privacidad.



Se sugiere configurar el servidor de base de datos para que la base de datos del Producto esté cifrada en el disco. Para habilitar esta opción se requiere SQL Server Enterprise Edition y durante su instalación es necesario habilitar la opción TDE (Cifrado de datos transparente).



Las bases de datos que contienen datos de pacientes/información sensible no pueden salir del centro de salud sin encriptarse/cifrarse.

4.2.1 Características y uso de las credenciales de usuario

Esta sección explica las características de las credenciales de usuario del Producto (nombre de usuario y contraseña), su uso y la reglamentación recomendada.

- Cada usuario debe tomar todas las precauciones posibles para mantener en secreto su nombre de usuario y su contraseña.
- El nombre de usuario y la contraseña son privados y personales. El nombre de usuario y la contraseña no se deben comunicar a nadie.
- Cada encargado puede tener una o varias credenciales de identificación (nombre de usuario y contraseña). Distintos encargados no deben compartir los mismos nombres de usuario y contraseña.
- Los perfiles de autorización deben ser controlados y renovados al menos una vez al año.
- Los perfiles de autorización pueden agruparse según la homogeneidad de las tareas de los usuarios.
- Cada cuenta de usuario se vinculará con una persona concreta. Se debe evitar el uso de usuarios genéricos (por ejemplo, "ADMIN", o "ENFERMERA"). En otras palabras, por cuestiones de trazabilidad, es necesario que cada cuenta de usuario sea utilizada por un solo usuario.
- Cada usuario tiene asignado un perfil de autorización que le permite acceder únicamente a las funciones que son relevantes para las tareas de su trabajo.
- La contraseña debe estar formada por un mínimo de ocho caracteres.
- La contraseña no debe tener referencias que remitan fácilmente al encargado (por ejemplo, nombre, apellidos, fecha de nacimiento, etc.).
- La contraseña es asignada por el administrador del sistema y el usuario deberá cambiarla la primera vez que utilice el Producto.
- A partir de entonces, la contraseña debe cambiarse al menos cada tres meses.
- El nombre de usuario y la contraseña que dejen de usarse durante más de 6 meses, deben deshabilitarse. Las credenciales específicas de usuario, utilizadas con fines de mantenimiento técnico. Ver en el manual de configuración del Producto los procedimientos de configuración de esta característica.
- Las credenciales de acceso se desactivan también en caso de pérdida por parte del usuario de la calificación correspondiente a dichas credenciales (en caso, por ejemplo, de que un usuario se transfiera a otro hospital). El administrador del sistema puede habilitar/inhabilitar manualmente a un usuario. El procedimiento se describe en el manual de configuración del Producto.

Las siguientes informaciones van dirigidas a los técnicos administradores del sistema:

La contraseña debe respetar una expresión regular definida en la configuración del Producto (En predefinido es ^.....*, es decir 8 caracteres).

La contraseña es asignada por el administrador del sistema en el momento en que se crea una nueva cuenta para un usuario. El administrador de sistema puede imponer al usuario el cambio de contraseña la primera vez que acceda al Producto. La contraseña caduca una vez superado un determinado período de tiempo, que puede configurarse, el usuario debe cambiar la contraseña al cumplirse ese plazo. También puede hacerse que la contraseña de un usuario no caduque.

Ver en el manual de configuración del Producto para información más detallada sobre la definición de las cuentas de usuario y sobre la configuración de las contraseñas.

4.2.2 Administradores de sistema

En el desempeño de las normales actividades de instalación, actualización y asistencia técnica del Producto, el personal de Ascom UMS o de los Distribuidores autorizados podrá tener acceso y tratar datos personales y sensibles memorizados en la base de datos del Producto.

Ascom UMS/Distribuidores, en relación con la gestión y el tratamiento de los datos personales y sensibles, adopta procedimientos e instrucciones de trabajo que son conformes a las prescripciones de la normativa vigente en materia de privacidad ("General Data Protection Regulation - EU 2016/679").

A fin de cumplir con los requisitos establecidos por los "Administradores de sistema", la organización responsable debe:

- defina los accesos en modo nominativo;
- active el registro de los accesos a nivel de sistema operativo tanto en el servidor como sobre los clientes;
- active el registro de los accesos a la base de datos del servidor Microsoft SQL Server (Audit Level);
- configure y gestione ambos registros para así mantener la trazabilidad de los accesos durante un período mínimo de un año.

4.2.3 Registro de sistema

El Producto memoriza los registros de sistema en la base de datos. Dichos registros se mantienen durante un período de tiempo que puede configurarse. Los registros se mantienen durante períodos de tiempo distintos según su naturaleza. De manera predefinida, los tiempos son los siguientes:

- los registros informativos se mantienen durante 10 días;
- los registros correspondientes a advertencias se mantienen durante 20 días;
- los registros correspondientes a errores se mantienen durante 30 días.

Estos plazos se pueden configurar. Ver el manual de configuración para el procedimiento de definición de los plazos de mantenimiento de los registros.

4.2.4 Registro forense

Puede enviarse un subconjunto de los registros de sistema antes mencionados, definidos de acuerdo con la política de cada estructura sanitaria específica que utiliza el Producto como «clínicamente relevante» o «clínicamente útil», a un sistema externo (ya sea una base de datos SQL o Syslog) para almacenarlo de acuerdo con las necesidades y normas de la estructura sanitaria.

4.3 Dispositivos compatibles

4.3.1 Dispositivos DAS

Dispositivos que permiten la implementación de un sistema de alarma distribuido fiable.

Los datos adquiridos por este tipo de dispositivos se muestran en el Producto.

Los datos adquiridos por este tipo de dispositivos también se pueden transmitir como HL7.

La comunicación de salida HL7 no es fiable.

Dispositivos compatibles:

- *Respirador Hamilton S1 y C6 y otros modelos que admitan el mismo protocolo.*
- *Bombas de infusión Arcomed Syramed μ SP6000 Chroma series y Volumed μ VP7000 Chroma series conectadas a Arcomed UniQueConcept (y otros dispositivos compatibles con el mismo protocolo).*
- *Controlador TAS.*

Para utilizar los dispositivos compatibles en un sistema de alarma distribuido hay que configurar bien los ajustes de comunicación de los dispositivos siguiendo las instrucciones de la documentación técnica del fabricante.

Dispositivos Hamilton

El ventilador Hamilton admite la opción "UCI silenciosa". Esto significa que se puede utilizar, con el producto para funcionar en modo silencioso.

Para utilizar el respirador Hamilton en un sistema de alarma distribuido como respirador silencioso (por ejemplo, en una UCI silenciosa), es posible hacerlo funcionar en un estado de AUDIO OFF global.

Primero, el ventilador debe estar bien configurado. Consulte la documentación técnica del dispositivo para ver las instrucciones técnicas y de usuario sobre cómo utilizarlo en modo silencioso (estado AUDIO OFF).



Consulte la documentación del respirador Hamilton para obtener instrucciones más detalladas.



El retraso máximo medido en un entorno de prueba entre la pantalla de notificación en el ventilador Hamilton y la pantalla de notificación en el Producto es de 600 ms.
El retraso máximo medido en un entorno de prueba entre la pantalla de notificación en el ventilador Hamilton y la pantalla de notificación en el Producto (versión móvil) es de 1000 ms.



El retraso máximo medido en un entorno de prueba entre la conexión del dispositivo de respiración Hamilton y la visualización de datos en el Producto es de 22900 ms.
El retraso máximo medido en un entorno de prueba entre la conexión del dispositivo de respiración Hamilton y la visualización de datos en el Producto (versión móvil) es de 20233 ms.

Pueden transcurrir hasta dos segundos entre la generación de la alarma y el envío de la alarma en el respirador Hamilton.

Después, el respirador espera una confirmación por parte del Producto. Si dicha confirmación no se recibe en dos segundos, se produce un error de tiempo de espera.

Por lo tanto, el retraso máximo después del cual se entrega una notificación de alarma es de cuatro segundos.



Si hay un error de tiempo de espera:

- Se dispara una alarma de conexión. El usuario puede cancelar la alarma. También se cancela si se establece una nueva conexión con Entrega confirmada.
- Se cancela cualquier estado activo de AUDIO OFF.
- El envío de datos del ventilador y la entrega confirmada se detienen hasta que se establezca una nueva conexión. Si Digistat Care no aparece con estado Fiable, inmediatamente intenta restablecer la conexión sin entrega confirmada.



En caso de que los ventiladores Hamilton estén configuradas como parte de un sistema de alarma distribuida, el estado global AUDIO OFF se deshabilita automáticamente si:

- Los resultados del controlador Hamilton no están disponibles
- Los resultados del sistema DAS no son fiables

Dispositivos Arcomed

La bomba Arcomed admite la opción "UCI silenciosa". Esto significa que se puede utilizar, con Digistat Care para funcionar en modo silencioso.

Para utilizar la bomba Arcomed en un sistema de alarma distribuida en modo silencioso (p. ej.: en una UCI silenciosa) se puede utilizar con estado AUDIO OFF.

Primero, la bomba debe estar bien configurada. Consulte la documentación técnica del dispositivo para ver las instrucciones técnicas y de usuario sobre cómo utilizarlo en modo silencioso (estado AUDIO OFF).



Para instrucciones detalladas, consulte la documentación de la bomba Arcomed.



La demora máxima medida en un entorno de prueba entre la pantalla de notificación en la bomba Arcomed y la pantalla de notificación en Digistat Care es de 3927 ms.

La demora máxima medida en un entorno de prueba entre la pantalla de notificación en el ventilador y la pantalla de notificación en Digistat Care (versión móvil) es de 4350 ms.



La demora máxima medida en un entorno de prueba entre la pantalla de notificación en la bomba Arcomed y la pantalla de datos en Digistat Care es de 63 s.

La demora máxima medida en un entorno de prueba entre la pantalla de notificación en la bomba Arcomed y la pantalla de datos en Digistat Care (versión móvil) es de 63 s.



Pueden transcurrir hasta 10 segundos entre la generación de la alarma y el envío de la alarma a las bombas Arcomed. Luego, la bomba espera una confirmación de Digistat Care. Si no se recibe confirmación al cabo de 20 segundos, se produce un tiempo de espera.

Por tanto, la demora máxima después de la cual se envía una notificación de alarma es de 20 segundos.

Si hay un tiempo de espera de comunicación:

- Se dispara una alarma de conexión en las bombas. El usuario puede cancelar la alarma. También se cancela si se establece una nueva conexión con Entrega confirmada.
- Se cancela cualquier estado activo de AUDIO OFF.
- Si se establece una nueva conexión con Entrega confirmada y si Digistat Care está en estado Fiable, las bombas de infusión restauran automáticamente el estado AUDIO OFF.
- Digistat Care intenta restablecer la comunicación.



Las bombas de infusión Arcomed requieren una red separada para funcionar como parte de un sistema de alarma distribuida. “Red separada” significa: red física diferente, VLAN o subredes IP separadas. Esto es necesario para evitar posibles conflictos con una política de seguridad de red en particular, según lo indicado por el fabricante de la bomba.



En caso de que las bombas Arcomed estén configuradas como parte de un sistema de alarma distribuida, el estado global AUDIO OFF se deshabilita automáticamente si:

- Los resultados del controlador Arcomed no están disponibles
- Los resultados del sistema DAS no son fiables

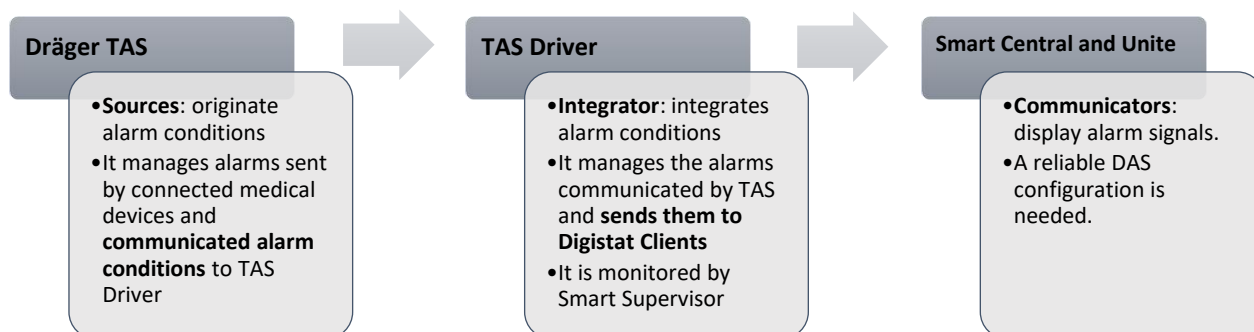


El controlador Arcomed es un controlador multicama, por lo que solo una bomba podría tener un estado poco fiable mientras que las demás funcionan bien.

Controlador TAS

El **controlador del servicio de alarma dirigido** (TAS - Targeted Alarm Service) actúa como puerta de enlace de alarma e **integrador** (según el estándar IEC 60601-1-8:2020) de **condiciones de alarma** originadas por **dispositivos médicos** conectados a la red privada de Dräger, comunicados según el protocolo de comunicación estándar SDC. (IEEE 11073) y

gestionado por el **Servicio de alerta dirigido (TAS)** de Dräger, a **comunicadores Digistat**, como Smart Central y Unite, donde finalmente se muestran las señales de alarma.



El TAS comunica al controlador del TAS a través de las API del TAS versión 1.1 las condiciones de alerta de los dispositivos conectados a la red del TAS (hasta 100 dispositivos por TAS). El controlador TAS admite una conexión cifrada y autenticación conforme a los requisitos de seguridad TLS 1.2, y la corrección de los mensajes está garantizada por el protocolo TCP/IP.

El controlador TAS es un controlador de tipo DAS y admite el estado **Global AUDIO OFF** activo en los dispositivos médicos. Junto con el Servicio de Alerta Dirigida (TAS) de Dräger, se puede configurar para implementar **un Sistema de Alarma Distribuido (DAS)**, que requiere una configuración fiable con **Smart Supervisor** activo (*SmartCentralMode* de «Opción del sistema» configurado en **Fiabilidad o Supervisión y Fiabilidad**) y **Smart Central dual**.

El TAS puede enviar alertas en más de un idioma al mismo tiempo y los idiomas admitidos pueden establecerse en la configuración de parámetros personalizados del controlador TAS. En caso de que el idioma de alerta recibido de los dispositivos médicos sea diferente del idioma configurado en los ajustes del TAS, se informará del idioma de alerta junto con el texto de alarma recibido del dispositivo TAS y una advertencia sobre la imposibilidad de proporcionar una traducción diferente.



Durante la configuración, debe establecerse el parámetro personalizado *BedNameFormat* en la página *Edit Device Driver > Custom Parameters > Custom tab* (*Configurator Web > Connect > Drivers > Device driver management* y, a continuación, seleccionar la instancia de controlador TAS) de la instancia de controlador TAS para gestionar la asignación de camas.



Dependiendo de la configuración de los dispositivos conectados al TAS, es posible utilizar varios idiomas para los textos de alarma.



El técnico encargado de configurar el controlador de Digistat TAS debe comprobar que el certificado recibido por Dräger se corresponde con el utilizado por el servidor TAS utilizando al menos dos medios diferentes (por ejemplo, por correo y por voz).

4.3.2 Dispositivos DIS

Dispositivos que no permiten la implementación de un sistema de alarma distribuido fiable. Esta comunicación no es fiable, por lo que no puede usarse para implementar un sistema de alarma distribuido seguro. En su lugar, se puede utilizar para implantar un sistema de información distribuido.

Póngase en contacto con Ascom UMS o el distribuidor para obtener la lista actualizada de dispositivos disponibles.



Por razones que están fuera del control del software, por ejemplo, la forma en que se instalan o cablean los dispositivos físicos reales, es posible que haya demoras entre la generación de notificaciones y la visualización real de las notificaciones.



La actualización de los datos que se muestran en la pantalla causados por la conexión, el apagado, la desconexión y el cambio de estado del dispositivo depende del tiempo requerido por el propio dispositivo para comunicar los cambios. Este tiempo depende de varios factores. Entre ellos se encuentra el tipo de dispositivo y el tipo de conexión. En algunos dispositivos, existen condiciones en las cuales la demora en comunicar los cambios puede ser importante. Como pueden cambiar según la configuración de los dispositivos y las condiciones de funcionamiento, no es posible proporcionar una indicación de los retrasos para todos los dispositivos posibles.



Los controladores utilizados para leer los datos de los dispositivos médicos conectados tienen un ciclo de lectura de menos de tres segundos (es decir, todos los datos de los dispositivos se leen cada tres segundos como máximo). Sin embargo, hay dispositivos que comunican la información con menos frecuencia (intervalo de 5-10 segundos). Consulte la documentación específica del controlador para obtener información sobre el ciclo de lectura.

En un entorno de prueba instalado y configurado como se indica en el manual de instalación y configuración, tan pronto como un controlador detecta una notificación se tarda un máximo de un segundo en mostrarla en la interfaz de usuario.

4.3.3 Advertencias



El Producto recibe datos de varias fuentes: dispositivos médicos, sistemas de información hospitalaria, así como los introducidos manualmente por el usuario.

Además, el Producto calcula la información derivada (p. ej., la puntuación).

El alcance, la precisión y la exactitud de estos datos dependen de las fuentes externas, de los datos introducidos por el usuario y de la arquitectura subyacente de hardware y software.



Dependiendo de las características de los dispositivos médicos conectados, el Producto puede usarse para notificaciones de alarmas primarias (DAS/CDAS) o secundarias (DIS). La presencia de un único dispositivo DIS requiere que la aplicación muestre una advertencia que indique que algunos de los dispositivos conectados no son compatibles con la notificación primaria de alarmas.



El Producto no ha sido diseñado para comprobar que los dispositivos funcionen correctamente.



Desconectar un dispositivo en funcionamiento causa la interrupción de la adquisición de datos en el Producto. El Producto no recupera los datos de dispositivo que se pierden durante el período de desconexión una vez conectado de nuevo el dispositivo.



Nunca desactive los sistemas de alarma de los dispositivos médicos fuera de los casos permitidos en los procedimientos habituales de la estructura sanitaria.



La organización de atención médica es responsable de garantizar (p. ej., mediante listas de comprobación apropiadas) que la recepción correcta de la alarma se gestiona en el Producto tanto cuando los sonidos de notificación están desactivados como cuando están activados para un paciente específico en el dispositivo móvil.



En caso de que se conecte una bomba de infusión al Producto, se advierte al usuario que nunca debe cambiar el número de serie de la bomba de infusión.



Nunca desactive el sonido en las estaciones de trabajo en que esté funcionando el Producto.



Periódicamente (por ejemplo, al comienzo de cada turno) compruebe en la estación central que se visualicen correctamente los datos de cada cama procedentes de los dispositivos médicos conectados.



Si se está usando la unidad genérica Alaris®, será necesario esperar al menos diez segundos después de desconectar una bomba de infusión y antes de conectar otra.



Según la decisión de la Organización de atención médica, el producto podría configurarse para filtrar o reasignar alarmas generadas por los dispositivos médicos conectados.

Los usuarios deben tener en cuenta que, dependiendo de la configuración, las alarmas podrían presentarse con una prioridad o mensaje diferentes, o podrían no anunciarse.

La Organización de atención médica se encarga de proporcionar información y formación a los usuarios con respecto a la configuración del filtrado de alarmas. Se informará a los usuarios sobre cualquier cambio posterior en la configuración del filtrado de alarmas.

El operador se situará a una distancia máxima de 1m (3,28 ft) para poder leer las alarmas en Smart Central. El Operador puede ver si hay una alarma a una distancia máxima de 4m (13,12 ft).

Esto solo se cumple si:



- el Operador tiene una agudeza visual de 0 en la escala logMAR o de 6-6 (20/20) Snellen (corregida si es necesario),
- con punto de vista desde la posición del Operador o desde cualquier otro punto dentro de la base de un cono subtendido en un ángulo de 30° al eje horizontal o a la normal al centro del plano de visualización de la pantalla de monitorización o de la indicación visual,
- la iluminación ambiente está entre 100 lx y 1500 lx.

La organización sanitaria, en consonancia con su política de gestión de riesgos y en función del entorno en el que se ejecute Digistat Care (p. ej., tamaño y ajustes de color del monitor, ubicación de la estación de trabajo en la sala, etc.), puede definir la distancia máxima real para que el operador vea que hay una alarma presente.



Utilice el procedimiento de comprobación de sonido para verificar si el audio en la estación de trabajo o dispositivo portátil funciona correctamente (consulte los documentos *USR ESP Smart Central* y *USR ESP Mobile Launcher* para ver el procedimiento en estaciones de trabajo de escritorio y dispositivos móviles). Si los módulos Smart Central / Smart Central Mobile no están instalados, entonces el procedimiento no es relevante.



El Producto adquiere la información generada por los dispositivos médicos primarios (es decir, respiradores pulmonares, bombas de infusión, etc.) y los muestra. Por lo tanto, el Producto siempre informa lo que los dispositivos médicos primarios comunican. La asignación de prioridades de alarma se decide en función del dispositivo médico primario. Es posible decidir en el Producto el orden de los dispositivos médicos para cada cama de acuerdo con la preferencia del cliente: por tipo de dispositivo, modelo o fabricante. Este tipo de pedido se configura en el Producto durante la implementación del Producto de acuerdo con las solicitudes o preferencias del usuario. El color de cada tarjeta de cama (es decir, el área de la cama) es siempre el color de la alarma de mayor prioridad entre todas las alarmas que saltan en esa cama.



Los niveles de presión sonora inferiores al ruido ambiente pueden impedir que el usuario perciba las alarmas.

4.4 Distribución segura de alarmas para fallos individuales

Dependiendo de las características de los dispositivos médicos conectados, el producto puede estar a salvo contra fallos individuales en lo que respecta a la distribución de las alarmas si se instala y configura de forma adecuada. Esto significa que todas las partes del sistema que intervienen en la distribución de alarmas se supervisan constantemente, incluido el propio «controlador» (es decir, el agente de supervisión) y, si se produce algún fallo en cualquiera de esas partes, se notifica a los usuarios. En caso de fallo, el Producto deja de funcionar hasta que se detecta y elimina la causa del fallo.

En el caso de las estaciones de trabajo móviles (dispositivos Myco), se entrega una notificación en las mismas condiciones descritas anteriormente a todos los dispositivos conectados. Esta notificación tiene el mismo nivel de gravedad de una alarma médica y no se puede eliminar hasta que se elimine la causa.

Para garantizar la seguridad contra fallos individuales, se instalarán al menos dos estaciones de trabajo Digistat Care dentro del mismo departamento o, como alternativa, al menos una estación de trabajo Digistat Care y una Torre de luces de alarma.

Cada estación de trabajo o torre de luces puede supervisar de esta manera el funcionamiento correcto de los otros componentes. Las estaciones de trabajo de escritorio y la torre de luces también supervisan el «Controlador». Consulte el manual de configuración del Producto para obtener una descripción detallada de la arquitectura del sistema.



La organización de atención médica implementará procedimientos internos para asegurar siempre la presencia de al menos un miembro del personal médico cerca de cada estación de trabajo Smart Central Desktop y, si está presente, de la torre de luces de alarma para estar al tanto de cualquier alarma.

La organización sanitaria implementará procedimientos adecuados para que el Producto vuelva a funcionar en el menor tiempo posible. Además, la organización de atención médica deberá definir procedimientos de trabajo alternativos en caso de que el sistema no sea fiable o deje de funcionar.

4.4.1 Torre de luces de alarma

Digistat Care está diseñado para comunicarse con una torre de luces de alarma opcional que utilice un protocolo estándar. Cuando Digistat Care se instala y configura para la distribución fiable de alarmas, la Torre de luces produce notificaciones informativas visuales y sonoras, informando de manera redundante a los usuarios sobre si el sistema funciona correctamente o no.

La torre de luces se puede utilizar como una alternativa a la segunda estación de trabajo Digistat Care, la cual por otra parte es obligatoria para la distribución fiable de las alarmas.

La presencia de la torre de luces depende de una opción del sistema. Si la torre de luces está presente, entonces el sistema se puede validar como fiable con solo una estación de trabajo Digistat Care. Consulte el manual de configuración del Producto para obtener más información.

En la torre de luces:

- la luz verde está encendida y no se emite ningún sonido si el sistema funciona correctamente;
- la luz roja se enciende y se emite un sonido de alarma cuando se produce una alarma técnica (un fallo del sistema; consulte las secciones 4.5 y 4.5.3);
- la luz roja se enciende y se emite un sonido de alarma cuando se interrumpe la comunicación entre la torre de luces y el Smart Supervisor (el «controlador» mencionado anteriormente); al mismo tiempo, el Smart Supervisor emite una alarma técnica cuando se interrumpe la comunicación con la torre de luces.

La verificación de Digistat Care se ha realizado con la Network Monitor Signal Tower de Patlite, pero otros modelos podrían ser compatibles con Digistat Care. Para obtener más información, póngase en contacto con la asistencia técnica de Ascom UMS o del distribuidor.

La Network Monitor Signal Tower de Patlite es una torre de señalización de tres niveles con un zumbador. Tiene la capacidad de informar inmediatamente cuando se produce un evento de la red a través de una conexión de red.



Fig. 1

4.5 Falta de fiabilidad del sistema

En caso de que el sistema no sea fiable, se entrega una notificación específica de «Error del sistema» en las estaciones de trabajo de escritorio (Fig. 2), en los dispositivos portátiles y en la torre de luces de alarma opcional (luz roja encendida, sonido de alarma).

Cuando se produce un «Error del sistema» en todas las camas, no se muestran datos del paciente hasta que el sistema vuelve a ser fiable.

Las posibles causas de la falta de fiabilidad se enumeran en el párrafo 4.5.3.

4.5.1 Escritorio

En las estaciones de trabajo de escritorio, las notificaciones permanecen en la barra lateral (Fig. 2 **B**) hasta que se eliminen las causas de la falta de fiabilidad y el sistema vuelva a ser fiable. En todas las camas afectadas por la falta de fiabilidad, no se muestran datos del paciente hasta que el sistema vuelva a ser fiable.

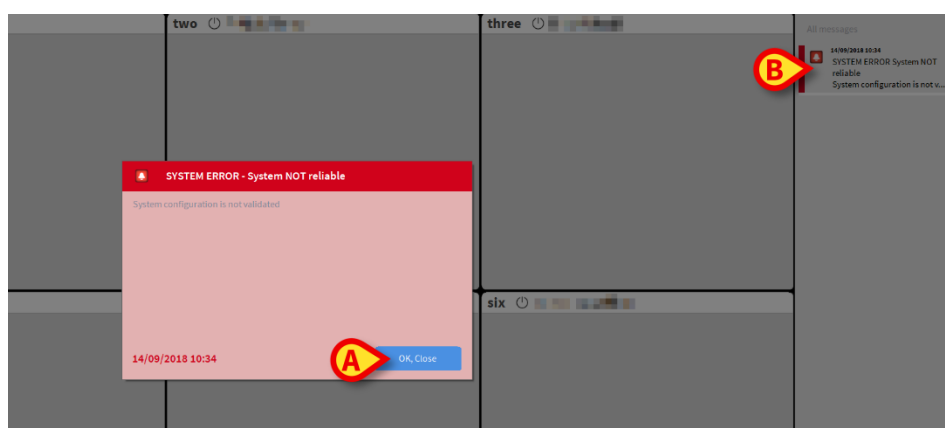


Fig. 2: Sistema no fiable (escritorio)

- Haga clic en **Aceptar, Cerrar** en la notificación para confirmarla (Fig. 2 **A**).

4.5.2 Móvil

En los dispositivos móviles, se entrega una notificación. También se emite una alarma de sonido o vibración.

- Deslice la notificación hacia abajo para confirmarla en el móvil. Después de esta acción, el sonido o vibración se detiene.

Una advertencia permanece en la parte superior de cada pantalla del móvil hasta que se eliminen las causas de la falta de fiabilidad y el sistema sea fiable de nuevo. En ninguna de las camas afectadas por la falta de fiabilidad se muestran los datos de los pacientes hasta que el sistema vuelva a ser fiable.

4.5.3 Causas de la falta de fiabilidad

En caso de falta de fiabilidad del sistema, se entrega una alarma técnica. La alarma es una notificación de «Error del sistema», que también proporciona una breve descripción de las causas de la falta de fiabilidad.

Las posibles causas de la falta de fiabilidad son las siguientes:

- «La configuración del sistema no está validada»
- “Smart Central no funciona correctamente. Errores no gestionados. Póngase en contacto con los administradores del sistema.”
- "Error de conexión de Light Tower ({0})"
- «Error de tiempo de espera de respuesta en sistema CDAS externo»
- «Sistema CDAS externo desconectado»
- «Error al acceder a la base de datos»
- «Anomalía en el componente {0} ({1})»
- «El componente {0} ({1}) no responde»
- "El controlador {0} en {1} no responde"
- Texto gratis enviado desde el controlador del dispositivo

NOTA: Los caracteres «{0} y {1}» representan el nombre del componente real.

Cuando se produce un «Error del sistema» en todas las camas afectadas, no se muestran datos del paciente hasta que el sistema vuelve a ser fiable.

4.6 Producto no disponible

En caso de que la estación de trabajo (incluidos los dispositivos móviles) donde está instalado el producto encuentre problemas al conectarse al servidor, se muestra un mensaje de información específico.



Si la red no coincide con las características solicitadas, el rendimiento del Producto se deteriora gradualmente hasta que se producen errores de tiempo de espera. El sistema puede cambiar finalmente al modo de «Recuperación».

El producto intenta recuperarse automáticamente. Si la recuperación automática falla, es necesario ponerse en contacto con la asistencia técnica (consulte la sección 5 para ver la lista de contactos).



La estructura que usa el Producto debe definir un procedimiento de emergencia a aplicar en caso de Producto no disponible. Debe hacerse así para

- 1) Permitir a los departamentos seguir desempeñando sus actividades
 - 2) Restablecer lo antes posible la disponibilidad del Producto (la política de copias de seguridad es parte de esta gestión).
-

Ascom UMS o el Distribuidor de referencia están disponibles para proporcionar pleno apoyo en la definición de ese procedimiento.

Ver en la sección 5 la lista de contactos.

Las características y funcionalidades descritas en las secciones 4.4 y 4.5 también se pueden aplicar cuando el producto no está instalado y configurado para la distribución principal de alarmas (por ejemplo: cuando el protocolo de comunicación del dispositivo médico no está pensado para este fin).

En estos casos, las características y funcionalidades mencionadas funcionan como un mecanismo de seguridad adicional y redundante que supervisa los componentes del producto. Pueden o no supervisar la conexión con los productos sanitarios dependiendo de la configuración del producto y de las características técnicas del producto sanitario.



En este supuesto, no se puede considerar que el sistema en su conjunto sea seguro frente a condiciones de primer defecto, y no se puede utilizar para comunicar las alarmas de forma fiable y predeterminada.

5. Contacto del Fabricante

Para cualquier problema, consultar primero al Distribuidor que instaló el Producto.
Referencias de contacto del fabricante:

Ascom UMS s.r.l

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

Tfno. (+39) 055 0512161

Fax (+39) 055 8290392

Asistencia técnica

support.it@ascom.com

800999715 (sin cargo, solo para Italia)

Ventas e información de productos

it.sales@ascom.com

Información General

it.info@ascom.com