SOTI

UNA PLATAFORMA
TODO CONECTADO

EL DILEMA DIGITAL EN SALUD:

LA PRESIÓN PARA INNOVAR Y LOS RIESGOS SILENCIOSOS

NOTA DE BIENVENIDA

La atención sanitaria está en la cúspide de los avances tecnológicos. Las innovaciones en el terreno de la IA, la telemedicina, la tecnología móvil y la automatización están abriendo nuevas posibilidades para ofrecer una atención más inteligente y conectada. A pesar de estos avances, los sistemas legacy y las ineficiencias operativas siguen frenando a muchas organizaciones de atención sanitaria.

Para los líderes de TI, el desafío es obvio. Las organizaciones deben acelerar la adopción de tecnología moderna para mejorar los resultados, empoderar al personal y ofrecer las experiencias de atención fluidas que los pacientes esperan.

Los sistemas legacy retrasan el acceso a información fundamental, que, a fin de cuentas, reduce la calidad de la atención. Mientras tanto, la IA puede mejorar diagnósticos, optimizar los flujos de trabajo y predecir las necesidades de los pacientes, pero solo cuando se cuenta con infraestructura moderna.

El alcance de la integración de la nueva tecnología y la capacidad de maximizar los beneficios de todos los dispositivos y las aplicaciones son aspectos fundamentales en la influencia de los resultados de los pacientes y la calidad de la atención sanitaria. Las organizaciones deben priorizar la integración del sistema, el acceso a los datos en tiempo real y la distancia de la tecnología obsoleta para desbloquear los beneficios de la transformación digital.

Stephanie Lopinski, vicepresidenta, Marketing global

En nuestra investigación más reciente, se examina el estado actual de las organizaciones de atención sanitaria, los desafíos a los que se enfrentan y las estrategias para progresar.

El informe de 2025 de SOTI destaca tres temas principales:

Inteligencia artificial

La adopción de la IA en el ámbito de la atención sanitaria está creciendo rápidamente; el **81 %** de las organizaciones a nivel mundial la utilizan para atender a los pacientes, cifra que aumentó del **61 %** en 2024. Entre sus usos, se incluye el procesamiento de datos médicos, la actualización de recursos, la personalización de tratamiento y el diagnóstico de afecciones.

A pesar de que el uso haya aumentado, solo el **36 %** de las organizaciones cuentan con medidas de seguridad específicas para la IA, lo que plantea preocupaciones sobre la privacidad de los pacientes. Es por eso que modernizar los sistemas es fundamental para garantizar la privacidad de los pacientes.

El informe de 2025 presenta un panorama claro: el recorrido tecnológico de la atención sanitaria está en ascenso, pero de manera desigual. Para poder convertir la adopción en una verdadera integración, la industria debe encargarse de los sistemas legacy, reforzar la seguridad de los datos y lograr que los recursos de TI no tengan problemas constantes.

Sistemas Legacy

Las organizaciones de atención sanitaria no logran integrar los sistemas interconectados y las soluciones de telemedicina, sobre todo porque es desafiante administrar los sistemas legacy obsoletos de manera remota.

Estos sistemas presentan riesgos de seguridad: el **83 %** de las organizaciones han informado violaciones de datos, fugas o ataques de ransomware desde 2023. Además, dificultan la integración del Registro Médico Electrónico (RME), que afecta al **79 %** de las organizaciones.

Como resultado, cuando las organizaciones intentan adoptar nuevas tecnologías, los obstáculos suelen persistir, lo que dificulta la innovación y afecta de manera negativa la experiencia de los pacientes. En definitiva, las limitaciones que imponen estos sistemas obsoletos tienen una influencia directa sobre los resultados de la atención a los pacientes, por lo que es fundamental que las organizaciones inviertan en tecnología moderna y sistemas interconectados para mejorar la eficiencia, seguridad y calidad general de la atención.

Gestión de dispositivos móviles + Gestión de la movilidad empresarial

Las organizaciones de atención sanitaria confían cada vez más en una variedad de dispositivos móviles, como computadoras portátiles, teléfonos inteligentes, tabletas y equipo especializado, como lectores de RFID. La gestión de estos dispositivos presenta grandes desafíos en la seguridad y la resolución remota de problemas si cuenta con soluciones de gestión de dispositivos móviles (GDM) obsoletas.

Sin embargo, el panorama actual debe evolucionar más allá de la GDM tradicional a fin de incluir un enfoque de gestión de la movilidad empresarial (GME) integral.

A medida que evoluciona la tecnología en el ámbito sanitario, el foco debe orientarse hacia una plataforma integrada que incluya diagnósticos, análisis de datos e inteligencia operativa avanzados. Este enfoque permite que las organizaciones aborden los problemas de manera proactiva y aprovechen la información para tomar decisiones informadas y optimizar los flujos de trabajo. Mediante la digitalización de los procesos y la automatización de las tareas administrativas, los proveedores de atención sanitaria pueden mejorar la eficiencia operativa y brindar una mejor atención a los pacientes.

Las soluciones efectivas de gestión móvil también requieren una gestión completa del ciclo de vida para promover la sostenibilidad. Las organizaciones deben tener el objetivo de maximizar la vida útil de sus dispositivos, mediante el uso de información sobre el estado de la batería y los patrones de uso para desarrollar estrategias de reemplazo sostenibles. Esta gestión proactiva no solo ayuda a mantener un estado óptimo del dispositivo, sino que reduce las vulnerabilidades y protege los datos del paciente.

EL PANORAMA CAMBIANTE DE LA ATENCIÓN SANITARIA:

PROGRESO Y AVANCES DESDE 2020

SOTI lleva realizando investigaciones sobre el ámbito sanitario desde 2020. Las encuestas y la cantidad de países y encuestados evolucionaron de la misma manera. Entre las tendencias de los últimos cinco años, se incluye la siguiente información:

2020/2021

- Seguridad: el **81 %** tiene preocupaciones sobre la seguridad de los registros del paciente
- Problemas técnicos: el **63 %** experimentan fallos del dispositivo o del sistema cada semana
- Impacto de la tecnología en la atención al paciente: el **81 %** tiene problemas con los sistemas y la tecnología durante la atención a los pacientes

475 trabajadores de atención domiciliaria y otros profesionales de atención sanitaria en siete países de todo el mundo

2022

- Seguridad: el **73 %** de las organizaciones han experimentado una violación o fuga de datos desde 2020
- IoT o telemedicina: el **98 %** ha implementado capacidades de dispositivos médicos de IoT o telemedicina
- Impacto en la inactividad del dispositivo: el **53 %** afirma que experimentan tiempos de inactividad habituales, lo que retrasa la atención al paciente y provoca una pérdida de 3,4 horas por semana, por empleado

1300 profesionales de TI que trabajan en organizaciones de atención sanitaria en ocho países de todo el mundo

2023

- Seguridad de los datos del paciente: el **97 %** tiene preocupaciones con respecto a la seguridad de los registros de datos de los pacientes
- Seguridad de red: el **55 %** sufrió una fuga de datos accidental o planificada desde fuentes internas, mientras que un **53 %** no puede detectar la conexión de nuevos dispositivos porque los sistemas están obsoletos, lo que provoca vulnerabilidades
- Sistemas legacy: el **52 %** afirma que los sistemas legacy no les permiten resolver problemas a tiempo y el **37 %** cree que los sistemas legacy los deja vulnerables ante violaciones de seguridad
- Tiempo de inactividad: pérdida de 3,4 horas en una semana normal por dificultades técnicas o del sistema

1450 profesionales de TI que trabajan en organizaciones de atención sanitaria en nueve países de todo el mundo

2024

- IA: el **85 %** considera que la IA podría ayudar a simplificar las tareas, pero solo el 23 % la está usando ampliamente en la actualidad
- Seguridad: el **71 %** transfiere datos a discos duros externos o de respaldo cuando se deshace de dispositivos antiguos. El **23 %** considera que la seguridad de los datos es su principal preocupación de TI
- IoT/telemedicina: el **67 %** experimenta problemas regulares con dispositivos de IoT o telemedicina que tienen como resultado retrasos en la atención al paciente.
- Sistemas heredados: el **63 %** confirma que usa tecnología obsoleta y el **45 %** ha experimentado una violación de datos o fuga de datos accidental en el último año
- Tiempo de inactividad: pérdida de 3,9 horas por semana, por empleado debido al tiempo de inactividad

1450 profesionales de TI o responsables de decisiones que trabajan en organizaciones de atención sanitaria en nueve países de todo el mundo

2025

- IA: el **81 %** ahora utiliza la IA para atender a los pacientes, cifra que aumentó del 61 % en 2024
- Seguridad: el **83 %** experimentó una fuga de datos accidental, una violación de datos externa o un ataque de ransomware de DDoS en los últimos 12 meses. El **30 %** considera que la seguridad de los datos es su principal preocupación de TI
- IoT/telemedicina: el **96 %** se enfrenta a desafíos a la hora de implementar dispositivos médicos de IoT o telemedicina
- Sistemas legacy: el **45 %** afirma que la vulnerabilidad de las redes ante los ataques es responsabilidad de la legacy
- Gestión de dispositivos móviles: el **47 %** afirma que las soluciones de gestión de dispositivos móviles son fundamentales para resolver problemas de manera remota

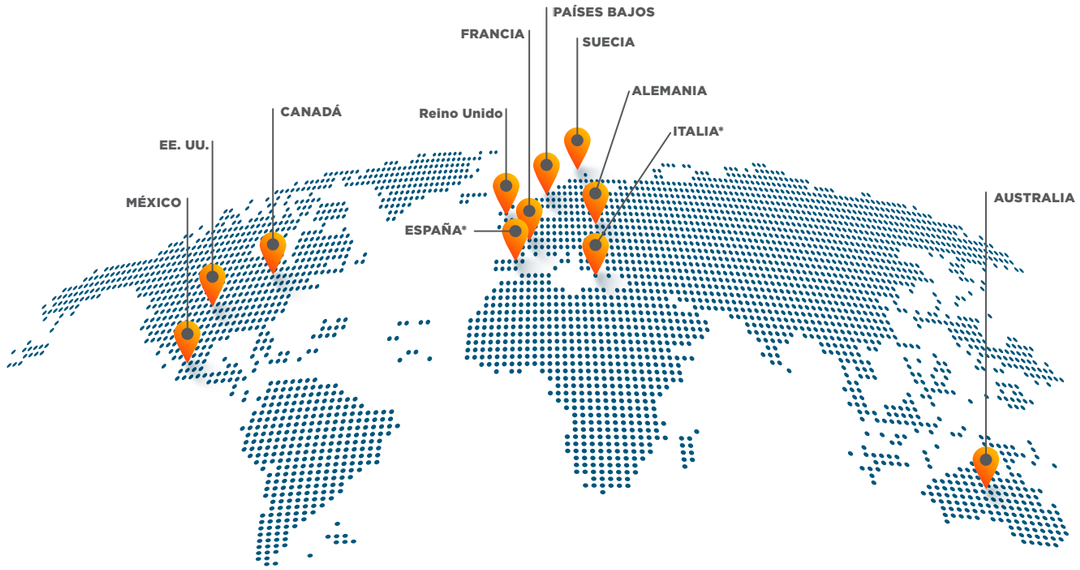
1750 profesionales de TI o responsables de decisiones que trabajan en organizaciones de atención sanitaria en nueve países de todo el mundo

CONTENIDOS

METODOLOGÍA

Este año, SOTI amplió el alcance de su investigación a **1750 encuestados en 11 países**: Estados Unidos (200), Canadá (150), México (150), Reino Unido (200), Alemania (150), Francia (150), Suecia (150), Países Bajos (150), Italia* (150), España* (150) y Australia (150). Entre enero y marzo de 2025, los responsables de la toma de decisiones de TI de organizaciones de atención sanitaria completaron la encuesta.

*Se incluyeron nuevas regiones en el informe de atención sanitaria de 2025.



DESGLOSE GLOBAL

Para este informe, las organizaciones de atención sanitaria se refieren a lo siguiente:

Un hospital que presta servicios de emergencia.

Una práctica médica general o clínica en distintas especialidades, p. ej., en el consultorio, médico de familia o práctica médica.

Una clínica que brinda atención de emergencia a pacientes en una o más especialidades, p. ej., salud mental, neurología y fisioterapia, entre otros.

Un proveedor de atención médica que brinda atención remota directa o de telemedicina a los pacientes.

Las organizaciones de atención sanitaria tenían entre 50 y más de 5000 empleados. Si bien todos los encuestados pertenecen al área de toma de decisiones de TI en una organización de atención sanitaria, sus funciones varían desde profesionales de TI a cargos gerenciales y de primera línea.

HALLAZGOS GLOBALES

96 %

de las organizaciones se enfrentan a desafíos a la hora de implementar dispositivos médicos de IoT o telemedicina, de los cuales la integración de sistemas es el mayor.

83 %

de los incidentes de seguridad siguen siendo muchos, con fugas de datos accidentales, violaciones de datos externas y ataques de ransomware de DDoS que no parecen reducirse.

47 %

de los responsables de la toma de decisiones de TI afirma que las soluciones de gestión de dispositivos móviles son fundamentales para resolver problemas de manera remota.

45 %

afirma que la vulnerabilidad de las redes ante los ataques es responsabilidad de la TI heredada.

81 %

tiene preocupaciones sobre la seguridad de los registros del paciente cuando se deshace de dispositivos móviles.

81 %

ahora utiliza la IA de alguna manera para mejorar la eficiencia y eficacia de la atención a los pacientes, un aumento del 61 % en 2024.

40 %

de las organizaciones reemplazan dispositivos antiguos cuando hay nuevas versiones disponibles.

30 %

considera que la seguridad de los datos es su principal preocupación de TI, cifra que aumentó del 23 % en 2024.

LOS AVANCES:

INTELIGENCIA ARTIFICIAL EN LA ATENCIÓN AL PACIENTE EN AUMENTO

En los últimos años, la industria de la atención sanitaria ha sido testigo de avances transformativos, en particular con la integración de la tecnología en la atención a los pacientes. El crecimiento de la IA está cambiando la forma en que los proveedores de atención sanitaria prestan servicios e interactúan con los pacientes.

Aprovechar la IA para mejorar los diagnósticos, personalizar planes de tratamiento y optimizar las operaciones llamó la atención de las organizaciones de atención sanitaria de todo el mundo. Según nuestra encuesta de este año, la IA se utiliza para atender a los pacientes en el **81 %** de las organizaciones de atención sanitaria, un tercio más que en 2024 (**61 %**).

La mayoría de las organizaciones que no utilizan la IA para atender a los pacientes están, al menos, considerándolo (**16 %** a nivel mundial), mientras que el **3 %** de los responsables de la toma de decisiones de TI afirman que su organización no planea utilizarla.

El Reino Unido es el país que más utiliza la IA, en el que el **94 %** de los responsables de la toma de decisiones de TI afirma que su organización la utilizó para atender a los pacientes. Esta cifra aumentó del **47 %** en 2024. En Australia, el **93 %** afirma que utiliza IA, que aumentó del **70 %**.

Porcentaje de organizaciones que utilizan la IA para atender pacientes en 2025 en comparación con 2024

	2025	2024		2025	2024
	81 %	**61 %**		81 %	45 %
	80 %	72 %		71 %	53 %
	87 %	72 %		70 %	43 %
	82 %	80 %		74 %	-
	94 %	47 %		83 %	-
	77 %	71 %		93 %	70 %

IA: ALIVIANAR LA CARGA ADMINISTRATIVA

Si bien la cantidad de organizaciones que usan IA aumentó, la forma en que aplican la tecnología sigue igual en su mayoría desde el año pasado. En 2025, el uso más común de la IA era el procesamiento o análisis de datos médicos (el **60 %** de los responsables de decisiones de TI declararon este uso), seguido de la actualización de registros de los pacientes (un **59 %**). Apenas menos de la mitad (**46 %**) usa la IA para planear el mejor tratamiento, mientras el **45 %** lo hace para personalizar tratamientos y el **40 %** para diagnosticar afecciones.

¿En cuál de las siguientes formas su organización utiliza la IA en este momento para atender a los pacientes? (Pregunta para quienes usan la IA en la atención de los pacientes)

Hallazgos globales	2025	2024
Procesamiento o análisis de datos médicos	60 %	60 %
Actualización de registros de pacientes	59 %	56 %
Planificación del mejor tratamiento	46 %	47 %
Personalización de tratamientos	45 %	44 %
Cumplimiento de otros objetivos administrativos	45 %	20 %
Diagnóstico de afecciones	40 %	38 %
RED: Actualización de registros u otras tareas administrativas	79 %	63 %

Un cambio significativo este año es el aumento del uso de la IA para otros objetivos administrativos. En 2024, el **20 %** de los responsables de decisiones de TI informaron que usaron la TI con este propósito, que aumentó al **45 %** en 2025.

Mediante la delegación de tareas pesadas a la IA, el personal de atención sanitaria se puede enfocar en aspectos importantes de la atención a los pacientes que van surgiendo en el momento. Si tenemos esto en cuenta, además del uso de la IA por parte de las organizaciones para actualizar registros médicos, vemos que un **79 %** utiliza la IA con fines administrativos de algún tipo.

El Reino Unido y Estados Unidos son los usuarios principales de la IA para la personalización de tratamientos (el **57 %** y el **55 %**, respectivamente), mientras que el Reino Unido es pionero en el diagnóstico de afecciones con IA (el **52 %**). Suecia (**53 %**) y Canadá (**52 %**) informaron el mayor uso de IA para otros fines administrativos.

En la investigación del año pasado, se descubrió que más de la mitad (**57 %**) de los profesionales de TI tenían algunas dudas sobre el uso de la IA para atender pacientes y les preocupaba las posibles amenazas a la privacidad de los pacientes. Este año, descubrimos que todas las organizaciones han implementado al menos algunas medidas de seguridad con respecto a los dispositivos móviles, pero solo el **36 %** cuentan con medidas específicas de seguridad. Debido al gran aumento del uso de la IA el año pasado, esta área parece ser un aspecto que más organizaciones de atención sanitaria deberían investigar.

¿Qué medidas de seguridad prioriza con respecto a los dispositivos móviles?

Actualizaciones frecuentes	**51 %**
Formación y educación de los empleados sobre amenazas específicas y prácticas recomendadas de seguridad	**45 %**
Garantía de cumplimiento de las normativas y leyes de protección de datos (p. ej., RGPD, EHDS)	**45 %**
Límite el acceso a datos confidenciales de ciertas funciones y responsabilidades	**45 %**
Autenticación multifactorial	**44 %**
Cifrado	**42 %**
Auditorías de seguridad frecuentes	**42 %**
Implementación de medidas de seguridad específicas de la IA	**36 %**
Implementación de anonimización de los datos	**34 %**
Plan de respuesta ante incidentes listo para usar	**33 %**
Borrado remoto	**23 %**

El año pasado, más de ocho de cada diez (**83 %**) profesionales de TI afirmaron que la IA es una estrategia económica fundamental para las organizaciones de atención sanitaria. Este año, aumentó el uso en la atención a los pacientes. Con los problemas que los sistemas legacy presentan a la adopción de la tecnología emergente y los desafíos con respecto a la seguridad de los datos que persisten en toda la industria, la gestión de los dispositivos que la utilizan requieren una monitorización cuidadosa a fin de garantizar que despliegue todo su potencial con seguridad.

EL DESAFÍO:

LOS SISTEMAS HEREDADOS LIMITAN EL VALOR DE LA TECNOLOGÍA EMERGENTE

LA ADOPCIÓN DE LA IOT Y TELEMEDICINA ES UNIVERSAL, PERO LOS PROBLEMAS PERSISTEN

La integración de las tecnologías interconectadas está modificando el panorama de la atención sanitaria, sobre todo con respecto a la telemedicina, que combina dispositivos y sistemas en las instalaciones y de manera remota. Este año, casi todos los responsables de decisión de TI (**99 %**) indicaron que sus organizaciones utilizan algún tipo de dispositivo conectado o solución de telemedicina.

A pesar del alto nivel de adopción, la eficiencia operativa de estos sistemas está a la altura de las expectativas.

96 %

de los líderes de TI informaron que se enfrentan a desafíos con respecto a estas tecnologías.

Uno de los problemas principales es la falta de integración entre los sistemas que se utilizan para los dispositivos conectados y las aplicaciones de telemedicina. Este problema se refleja en las siguientes estadísticas en distintas regiones.

Los sistemas que se utilizan para los dispositivos médicos de IoT/ telemedicina no están integrados:

- **65 %** GLOBAL
- **69 %** EE. UU.
- **71 %** CANADÁ
- **66 %** MÉXICO
- **73 %** REINO UNIDO
- **60 %** ALEMANIA
- **60 %** FRANCIA
- **72 %** SUECIA
- **58 %** PAÍSES BAJOS
- **58 %** ESPAÑA
- **58 %** ITALIA
- **53 %** AUSTRALIA

El desafío más grande al que se enfrenta el **65 %** de las organizaciones este año es la falta de integración entre estos sistemas. Este problema incluye desafíos de interoperabilidad, como la incapacidad de acceder a toda la información de salud de un paciente desde una única ubicación (informado por el **43 %** de los encuestados) y la falta de actualizaciones automáticas en todos los sistemas (**40 %**). Además, el **65 %** de los responsables de decisiones de TI expresaron su frustración con respecto a que su organización es incapaz de brindar datos relevantes a las personas correctas cuando más los requieren.

Estos desafíos son evidentes a nivel mundial, pero son notables sobre todo en Australia (**77 %**), el Reino Unido (**73 %**) y Canadá (**71 %**). Los problemas de integración también son comunes en las organizaciones de atención sanitaria que abarcan distintas especialidades. Entre las que experimentan dichas dificultades, el **69 %** pertenece a prácticas médicas generales o clínicas, mientras que el **67 %** pertenecen a clínicas que prestan servicios de una o más especialidades. De manera similar, el **62 %** de los responsables de decisiones de TI en los hospitales que ofrecen atención de emergencias y las organizaciones orientadas a la prestación de servicios remotos o telemedicina informaron que se enfrentan a desafíos de integración similares (**60 %**).

SISTEMAS LEGACY QUE CAUSAN PROBLEMAS DE INTEGRACIÓN E INTEROPERABILIDAD

El porcentaje de responsables de la toma de decisiones de TI cuyas organizaciones usan tecnología obsoleta disminuyó del **63 %** en 2024 al **55 %** este año. Sin embargo, el **97 %** de los responsables de la toma de decisiones de TI informaron que su organización cuenta con tecnología legacy. Alrededor de la mitad de quienes cuentan con tecnología legacy no la consideran obsoleta, pero está afectando la facilidad con la que las organizaciones se pueden adaptar a las nuevas formas de trabajo.

Cuatro de cada diez (**38 %**) responsables de la toma de decisiones de TI afirmaron que una TI legacy no les permite implementar ni gestionar impresoras o dispositivos nuevos, y la misma proporción manifiesta que no pueden ofrecer asistencia remota a los dispositivos ni obtener información detallada sobre problemas técnicos.

¿En qué afecta una tecnología legacy a sus operaciones diarias?

Imposibilidad de implementar y gestionar impresoras y dispositivos nuevos	**38 %**	39 %	46 %	37 %	47 %	37 %	37 %	31 %	33 %	29 %	36 %	43 %
Imposibilidad de ofrecer asistencia remota a dispositivos u obtener información detallada sobre los problemas del dispositivo	**38 %**	38 %	43 %	37 %	53 %	35 %	35 %	38 %	29 %	29 %	33 %	43 %
Demasiado tiempo solucionando problemas	**39 %**	38 %	47 %	39 %	41 %	43 %	36 %	43 %	41 %	29 %	33 %	39 %

Con el aumento del Registro Médico Electrónico (RME) para permitir el intercambio continuo de datos de pacientes dentro de las organizaciones de salud y el creciente uso de los dispositivos de telemedicina, la integración y la interoperabilidad nunca han sido tan críticas. Sin embargo, los resultados de este año revelan que los problemas de integración que causan los sistemas legacy siguen siendo un obstáculo.

Más de tres cuartos (**79 %**) de los responsables de la toma de decisiones de TI afirmaron que la adopción de los RME fue un gran desafío para su organización, mientras que el **36 %** se lo atribuyen directamente a que poseen una TI legacy. El impacto de la tecnología legacy sobre la adopción o integración de RME se siente con mayor intensidad en el Reino Unido (**44 %**), Australia (**42 %**), Estados Unidos y Canadá (**41 %** cada uno).

La adopción o integración de RME fue un desafío/fue afectada por la TI legacy

La adopción o integración de del Registro Médico Electrónico fue un gran desafío para nuestra organización	**79 %**	74 %	78 %	71 %	92 %	73 %	87 %	66 %	77 %	82 %	84 %	80 %
Una TI legacy afectó la adopción o integración del Registro médicos electrónicos	**36 %**	41 %	41 %	35 %	44 %	33 %	31 %	33 %	27 %	27 %	37 %	42 %

Los datos sugieren que la adaptación humana es fundamental para usar la nueva tecnología con eficacia. El **30 %** de los encuestados afirma que los cambios en los sistemas son tan frecuentes que la organización no puede ponerse al día. Otro **33 %** afirma que capacitar a los usuarios sobre nuevos sistemas ralentiza los procesos y afecta la atención a los pacientes. Pero el mayor desafío de que los dispositivos médicos de IoT y telemedicina funcionen sin problemas proviene de los sistemas obsoletos dentro de la industria de atención sanitaria:

90 % **de las organizaciones requieren que se invierta más en mejores o nuevas tecnologías para optimizar la atención a los pacientes, y**

89 % **para más dispositivos interconectados.**

SISTEMAS LEGACY QUE PROVOCAN RIESGOS DE SEGURIDAD

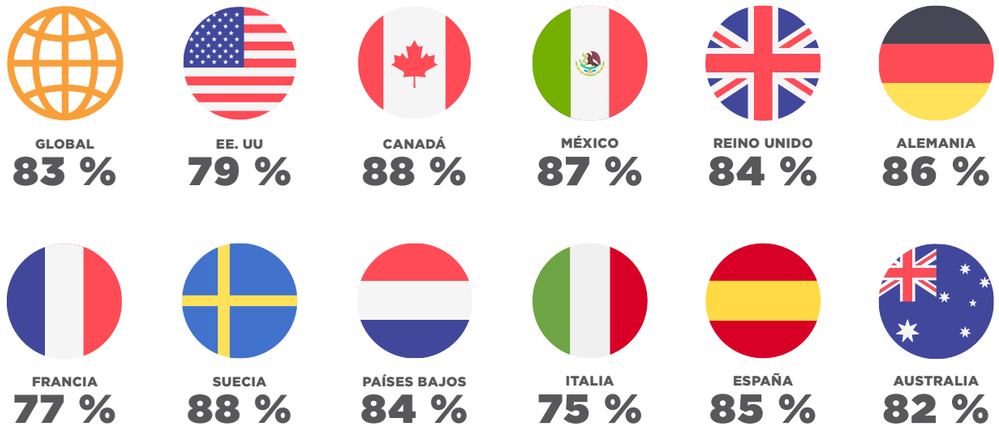
Más de ocho de cada diez (83 %)
responsables de decisione de TI afirman que su organización ha experimentado al menos una o más **violaciones de datos, fugas o ataques de ransomware** desde 2023.

Esto coincide con las cifras de 2024 (**85 %**), lo que indica que las amenazas prevalecen y no se están gestionando de manera efectiva.

Es posible que haya pocos cambios respecto al año anterior en el porcentaje general de las organizaciones que sufren incidentes, pero ahora, casi la mitad ha experimentado una fuga de datos accidental (**48 %** en comparación con 2022, que era del **33 %**) y dos tercios ha experimentado una violación de datos de una fuente externa o un ataque de ransomware (**65 %**, que corresponde con el 2024, pero aumentó del **48 %** de 2022 y del **52 %** de 2023).

El único tipo de incidente que tuvo un cambio significativo este año es el porcentaje de responsables de la toma de decisiones de TI que informaron una fuga de datos de empleados planificada, que disminuyó del **34 %** en 2024 al **24 %** en 2025.

Experimentaron uno o más incidentes de seguridad en los últimos 12 meses:



Con la caída de las violaciones de datos de los empleados planificadas este año, es posible que el elemento humano de las preocupaciones sobre la seguridad de los datos empiece a estar bajo control, pero las fuentes impulsadas por la tecnología están lejos de desaparecer.

Este año, casi la mitad de los responsables de decisiones de TI (**45 %**) afirma que la TI legacy provoca que las redes sean vulnerables frente a ataques de seguridad, que aumentó del **36 %** en 2024.

Es un problema que afecta a las organizaciones de todo el mundo, pero en algunos países la preocupación es mayor: a más de la mitad de los responsables de decisiones de TI en Suecia (**55 %**), Francia (**54 %**), Australia (**53 %**) y Canadá (**51 %**) le preocupa que su red sea vulnerable frente a ataques de seguridad por su TI legacy.

Las preocupaciones sobre la TI legacy crecen respecto al año anterior, como ha sucedido en todos los países encuestados. Si las organizaciones no abordan los problemas del sistema legacy, corren el riesgo de exponerse a amenazas de seguridad, ineficacias operativas y atención al paciente comprometida.

"La TI legacy hace que nuestras redes sean vulnerables a ataques de seguridad"

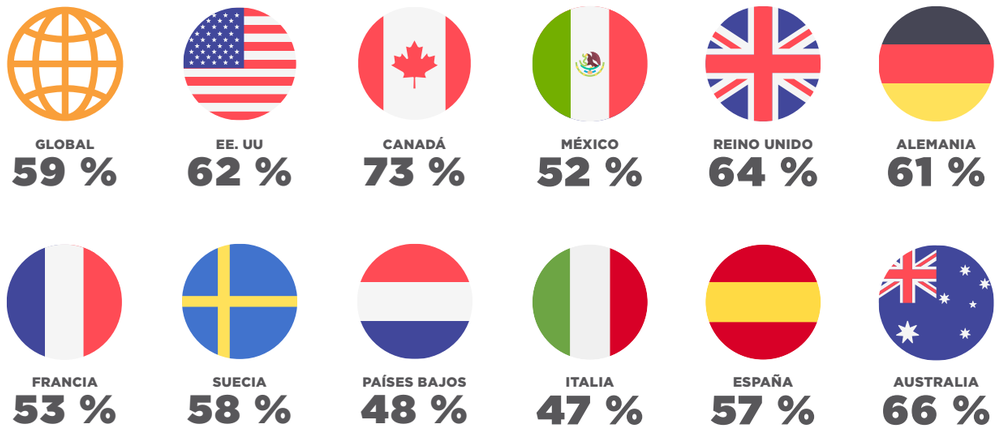
	2025	2024		2025	2024
Global	45 %	36 %	Francia	54 %	27 %
EE. UU	44 %	39 %	Suecia	55 %	25 %
Canadá	51 %	43 %	Países Bajos	40 %	37 %
México	39 %	35 %	Italia	37 %	-
Reino Unido	43 %	40 %	España	41 %	-
Alemania	45 %	33 %	Australia	53 %	39 %

Cuatro de cada diez (**38 %**) no admiten dispositivos remotos ni obtienen información detallada sobre los problemas del dispositivo, y uno de cada cinco (**20 %**) afirma que no logra detectar los nuevos dispositivos que se conectan al sistema. El **97 %** de las organizaciones de TI utilizan la TI legacy. Según la investigación de este año, lo siguiente son problemas de integración, mantenimiento y seguridad.

LOS SISTEMAS HEREDADOS GENERAN MÁS TRABAJO PARA LOS EQUIPOS DE TI

Los problemas técnicos y el tiempo de inactividad frecuentes presentan otro desafío a la hora de usar dispositivos interconectados y dispositivos médicos de telemedicina: afecta al **59 %** de las organizaciones este año, que aumentó del **52 %** de 2022.

¿Su organización experimentó problemas técnicos o tiempos de inactividad de manera frecuente con dispositivos médicos de IoT o telemedicina?



El tiempo de inactividad técnico en el ámbito de la atención sanitaria puede interrumpir la atención a los pacientes y afectar la eficiencia general de las operaciones. Las organizaciones enfrentan desafíos relacionados con la actualización y el mantenimiento del sistema, lo que provoca que los flujos de trabajo sean ineficientes y la calidad de la atención sanitaria disminuya.

Si bien los desafíos se presentan a nivel mundial, los siguientes países experimentan problemas técnicos y tiempo de inactividad en mayor medida: Canadá (**73 %**), Australia (**66 %**) y el Reino Unido (**64 %**).

Mientras se centran en proyectos estratégicos, los equipos de TI suelen verse agobiados por las tareas demandantes relacionadas con la solución de problemas técnicos menores, como arreglo de impresoras, problemas de conectividad y otras tareas de soporte repetitivas. Gran parte de este problema proviene de una TI legacy, con el **39 %** de los responsables de la toma de decisiones de TI que afirman que, por esto, pasan mucho tiempo solucionando problemas. Esta ineficiencia desvía la atención de la capacidad de concentrarse en iniciativas con mayor impacto que impulsen mejoras organizativas. Las organizaciones de atención sanitaria deben considerar implementar soluciones que ayuden a integrar la tecnología existente con la nueva.

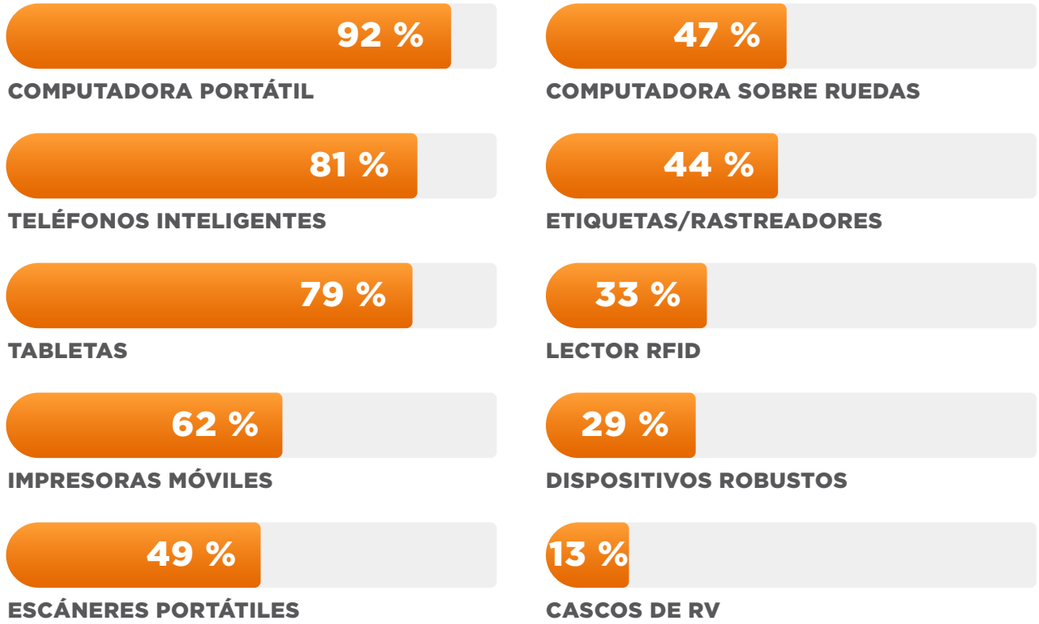
EL CAMINO A SEGUIR:

LA GESTIÓN DE LA MOVILIDAD EMPRESARIAL REEMPLAZÓ LA GESTIÓN DE DISPOSITIVOS MÓVILES

La creciente integración de distintos dispositivos móviles, un mayor uso de impresoras y una amplia gama de aplicaciones en las operaciones diarias de salud requiere una sólida solución de gestión de dispositivos.

¿Cuál de los siguientes tipos de dispositivos móviles se utiliza en su organización?

Hallazgos globales



Con una flota de dispositivos tan diversa, las organizaciones de atención sanitaria se enfrentan al desafío de mantener la seguridad, solucionar problemas de manera remota y asegurarse de que todos los dispositivos funcionen correctamente. Para los responsables de la toma de decisiones de TI, es fundamental que la conexión con estos dispositivos sea óptima. Para satisfacer estas demandas, las organizaciones de atención sanitaria deben ir más allá de la gestión de dispositivos móviles tradicional y adoptar un enfoque más amplio e integrado.

LA NECESIDAD CRECIENTE DE SOLUCIONES DE GESTIÓN DE MOVILIDAD EMPRESARIAL

Sin dudas, hay lugar para la tecnología móvil, ya que el **86 %** de los responsables de decisiones de TI afirma que acelera su trabajo. Sin embargo, la cantidad en circulación sugiere que hay muchos dispositivos móviles que se deben rastrear, mantener y gestionar, y la mayoría utiliza la GDM por cuestiones de seguridad (**90 %**). Esto incluye la gestión de políticas de seguridad, la protección contra las amenazas cibernéticas y la identificación de dispositivos no autorizados que acceden a la red: todos son aspectos fundamentales para minimizar las vulnerabilidades y reducir el riesgo de filtraciones.

¿Qué característica de una solución de GME es fundamental para sus operaciones?

Gestión de la seguridad	63 %
Protección contra amenazas cibernéticas o identificación de dispositivos externos que acceden a la red	56 %
Maneras de reducir vulnerabilidades ante amenazas externas o reducir la oportunidad de los hackers	48 %
Solución remota de problemas	47 %
Gestión de aplicaciones	47 %
Rastreo de Dispositivo	45 %
Cumplimiento y aplicación de políticas	44 %
Restringir el acceso a las funciones del dispositivo en ciertos entornos	38 %
RED: Relacionado con la seguridad (gestión de la seguridad o protección ante amenazas cibernéticas o identificación de dispositivos externos que acceden a la red, o formas de reducir las vulnerabilidades ante amenazas externas o reducir la oportunidad de los hackers)	90 %

Muchas organizaciones de atención sanitaria confían en las soluciones de GDM para la gestión básica de dispositivos y seguridad, pero eso es solo el punto de partida. En los arriesgados y acelerados entornos de atención sanitaria de hoy en día, la GDM básica ya no es suficiente.

Con la creciente complejidad de la atención al paciente y la cantidad en aumento de dispositivos conectados, las organizaciones deben pasar de estrategias reactivas a proactivas que detecten y prevengan problemas antes de que afecten a la prestación de servicios. Esto significa ir más allá de lo básico para implementar un monitoreo en tiempo real y mantenerse a la vanguardia de las fallas de seguridad y las interrupciones operativas.

Dos tercios (**65 %**) de los responsables de decisiones de TI informa que su organización experimentó una violación de datos de una fuente externa o un ataque de ransomware de DDoS en los últimos 12 meses. Esto destaca la necesidad de dejar atrás los aspectos básicos y aplicar medidas de seguridad más avanzadas y exhaustivas.

La seguridad de los datos es un aspecto que menciona el **30 %** de los responsables de decisiones de TI, por lo que sigue ocupando el primer lugar en la lista de problemas de TI. El porcentaje que lo coloca como la principal preocupación sigue aumentando significativamente, de un **16 %** en 2023 y el **23 %** en 2024. A esto se le agrega el **13 %** que afirma que la gestión de la seguridad de dispositivos compartidos es su preocupación principal este año; al mismo tiempo, se observa cómo casi la mitad (**43 %**) menciona que un problema relacionado con la seguridad es la preocupación principal a la que se enfrenta el sector de TI dentro de su organización.

¿Cuál es el área de mayor preocupación para el sector de TI dentro de su organización?

La preocupación por la seguridad de los datos o la gestión de la seguridad de dispositivos compartidos

	2025	2024		2025	2024
	43 %	**35 %**		51 %	25 %
	41 %	43 %		39 %	33 %
	53 %	39 %		31 %	28 %
	43 %	32 %		36 %	-
	39 %	43 %		50 %	-
	41 %	24 %		53 %	39 %

La seguridad de los datos es la principal preocupación de todos los países este año, y algunos países experimentan un aumento particularmente fuerte:

en **Francia**, el **25 %** clasificó un problema relacionado con la seguridad como la principal preocupación en 2024 y el **51 %** en 2025,

en **Canadá**, aumentó del **39 %** el año pasado al **53 %**,

en **Australia**, aumentó del **39 %** al **53 %**

y en **Alemania** del **24 %** al **41 %**.

La naturaleza de los dispositivos móviles requiere que múltiples usuarios los manejen. Por lo que es de esperar que la gestión de la seguridad de dispositivos compartidos siga siendo una de las principales preocupaciones de TI. A esto se la suma el desafío de que la tecnología legacy vuelve casi imposible la gestión remota de estos dispositivos y, por lo tanto, los dispositivos móviles se convierten en un arma de doble filo.

Las funciones “básicas” de la GDM ya no son suficientes en el mundo de la tecnología moderna y para todos los dispositivos y sistemas complejos existentes. Las capacidades históricas de la GDM llegaron a su límite. Hoy en día, la necesidad de soluciones tecnológicas avanzadas es más esencial que nunca. Las herramientas modernas de GME brindan a las organizaciones de atención sanitaria una mayor visibilidad de todo su ecosistema de dispositivos, lo que les permite monitorear mejor las operaciones, mejorar la seguridad de los datos y responder a las amenazas emergentes con mayor rapidez.

PRIORIDAD DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES: CUBRIR TODAS LAS BASES

Las organizaciones están priorizando medidas para garantizar la seguridad de los dispositivos móviles. Algunas organizaciones se centran en un enfoque orientado al ser humano: el **45 %** capacita a los empleados sobre amenazas de seguridad, prácticas recomendadas, y leyes de protección de datos, mientras que un número similar restringe el acceso a datos confidenciales según roles y responsabilidades. Sin embargo, solo un tercio (**33 %**) tiene un plan de respuesta ante incidentes por si algo sale mal.

Con el **51 %**, la implementación de actualizaciones regulares es la medida de seguridad más utilizada. Un porcentaje significativamente mayor que los que no habían experimentado ningún incidente de seguridad de datos en los últimos 12 meses emplean este enfoque (**60 %**) (en comparación con el **49 %** que ha sufrido un incidente). El **44 %** prioriza el uso de la autenticación multifactorial, mientras que el **42 %** utiliza el cifrado.

Está claro que todas las organizaciones están tomando medidas para proteger los dispositivos móviles, pero pocas están haciendo todo lo posible.

LA NECESIDAD DE MEJORES ESTRATEGIAS DE GESTIÓN DE DISPOSITIVOS MÓVILES

La seguridad no es el único ámbito en el que las soluciones de GDM obsoletas no están alcanzando. Muchas organizaciones de atención sanitaria se encuentran con inconsistencias a la hora de aplicar estas soluciones en distintos dispositivos, lo que complica su rastreo y soporte. Por lo general, esta inconsistencia conduce a reemplazos innecesarios de dispositivos e ineficiencias en las operaciones generales.

Casi la mitad (**47 %**) de los responsables de la toma de decisiones de TI afirman que una solución de GDM es fundamental para que su organización solucione problemas de manera remota y el **45 %** manifiesta que es esencial para rastrear dispositivos, pero el **38 %** de las organizaciones no puede implementar ni gestionar impresoras y dispositivos nuevos con facilidad por los sistemas legacy. Además, el **38 %** no puede ofrecer asistencia remota a los dispositivos ni obtener información detallada sobre problemas técnicos por la misma razón.

En la investigación, se destaca la necesidad de que las organizaciones de atención sanitaria adopten soluciones de GME sólidas y centralizadas que garanticen que los dispositivos estén seguros y cumplan con los requisitos básicos. Además, las soluciones deben ser compatibles con la resolución remota de problemas, optimizar la configuración y proporcionar información factible.

Las herramientas avanzadas que ofrecen análisis e inteligencia operativa en todos los dispositivos permiten que los equipos de TI identifiquen de manera proactiva los problemas de rendimiento del dispositivo. Además, pueden rastrear tendencias de uso y ofrecer a las organizaciones la información necesaria para tomar decisiones informadas. Este enfoque reduce el tiempo de inactividad, minimiza las ineficiencias y mejora la calidad general de la atención.

TECNOLOGÍA MÉDICA DESECHABLE

Las preocupaciones no desaparecen cuando un dispositivo móvil ya no está en uso, por el contrario, suelen aumentar. De hecho, al **81 %** de los responsables de la toma de decisiones de TI le preocupa la seguridad de los datos de los pacientes cuando se desechan dispositivos.

Las organizaciones de atención sanitaria manejan volúmenes gigantes de datos confidenciales, y sin los procesos de eliminación estandarizados, los dispositivos desechados plantean riesgos graves de violaciones de datos e incumplimiento de normas. Si bien la mayoría de las organizaciones toman medidas para proteger los datos cuando desechan dispositivos, el porcentaje de inconsistencias sigue siendo elevado: este año, ocho de cada diez responsables de decisiones de TI aún muestran preocupación.

Las actualizaciones frecuentes agravan el problema. El **31 %** de las organizaciones reemplazan los dispositivos cuando los usuarios lo solicitan, el **40 %** lo hace cuando hay nuevos modelos disponibles, el **41 %** lo hace según los términos del contrato y el **31 %** cuando la garantía se acaba. Esto plantea grandes preocupaciones con respecto a la seguridad y la sostenibilidad.

A fin de reducir los riesgos, las organizaciones deben implementar protocolos estandarizados, lo que incluye la eliminación remota de datos y una gestión sólida del ciclo de vida para garantizar que el rastreo y la eliminación sean correctos. El personal también debería recibir capacitación regular sobre las prácticas seguras de eliminación. Si las organizaciones priorizan los procesos seguros y sostenibles, pueden proteger mejor los datos de los pacientes y cumplir las normas de cumplimiento.

¿Cuál es la política de su organización para actualizar, renovar o reemplazar dispositivos como los mencionados anteriormente, p. ej., teléfonos inteligentes, tabletas, dispositivos robustos, etc.?

	Se realiza en algún momento por el plazo de su contrato, sin importar si sigue funcionando o no	Se realiza cuando un modelo nuevo o más avanzado está disponible	Se realiza a petición de los usuarios	Se realiza cuando la garantía se acaba	Se realiza solo para aquellos dispositivos que dejaron de funcionar
	41 %	**40 %**	**31 %**	**31 %**	**5 %**
	38 %	48 %	37 %	38 %	6 %
	41 %	47 %	33 %	32 %	5 %
	50 %	37 %	26 %	30 %	8 %
	49 %	43 %	43 %	49 %	2 %
	45 %	39 %	39 %	25 %	6 %
	34 %	41 %	25 %	23 %	7 %
	39 %	35 %	20 %	31 %	5 %
	37 %	27 %	27 %	25 %	6 %
	39 %	37 %	18 %	31 %	4 %
	41 %	41 %	28 %	21 %	6 %
	40 %	47 %	35 %	29 %	4 %

Estados Unidos, Canadá y Australia tienen el mayor porcentaje de reemplazo de dispositivos cuando una nueva versión está disponible. Aunque es importante destacar que esta tendencia es común a nivel mundial. Es fundamental encontrar un equilibrio entre la sostenibilidad y el rendimiento del dispositivo. Si los dispositivos se desechan solo cuando dejan de funcionar, los equipos de TI pasarán aún más tiempo solucionando problemas pequeños.

GESTIÓN DEL ESTADO DE LA BATERÍA: MÁS VALE PREVENIR QUE CURAR

El monitoreo ineficiente del estado de las baterías también puede ser una de las razones de los fallos inesperados de los dispositivos en la industria sanitaria. Es común que los costos aumenten debido a reemplazos anticipados, que causan restricciones financieras y preocupaciones ambientales sobre la eliminación de desechos electrónicos. El **97 %** de las organizaciones monitorean de manera activa el estado de la batería del dispositivo, pero solo un tercio (**31 %**) afirma que hacen controles cuando se presentan problemas.

En el **41 %** de los casos, la política es reemplazar las baterías según un cronograma establecido sin importar el estado. De manera más alentadora, la mitad realiza pruebas manuales habituales, el **44 %** emplea un sistema de monitoreo automático del estado de la bateria y el **41 %** cuenta con un sistema de mantenimiento predictivo.

Finalmente, los resultados sugieren que, si bien los dispositivos móviles ofrecen beneficios innegables, se debe optimizar su gestión mediante la implementación de soluciones de GME para consolidar prácticar recomendadas con respecto al rastreo de dispositivos, el monitoreo del estado de la batería y las estrategias sostenibles de reemplazo. De esa forma, no solo se optimizarían las operaciones diarias, sino que se sentarían las bases para iniciativas de TI más estratégicas en todo el ámbito de la atención sanitaria.

CONCLUSIÓN

El sector de la atención sanitaria está avanzando rápidamente en su viaje de transformación digital, pero el camino sigue siendo complejo. A pesar del uso generalizado de los dispositivos de IoT y telemedicina, un sistema legacy obsoleto presenta problemas tales como la consolidación incompleta de datos y problemas técnicos frecuentes, lo que impide que los equipos de TI vean los beneficios de su viaje de transformación digital.

Al mismo tiempo, los problemas relacionados con la seguridad es la principal preocupación del **43 %** de los responsables de decisiones de TI, impulsada por amenazas que van desde la gestión de dispositivos compartidos hasta el aumento de las violaciones de datos. Si bien las fugas de datos de empleados planificadas disminuyeron ligeramente, las fugas accidentales y los ataques externos sofisticados aún exponen vulnerabilidades. Casi la mitad de los líderes de TI afirman que los sistemas legacy son la razón principal de que las redes sean vulnerables ante los ataques, lo que enfatiza la necesidad urgente de modernizar las tecnologías fundacionales. Parece que la cuestión es menos acerca de la tecnología emergente en sí misma y más acerca de los sistemas que la respaldan.

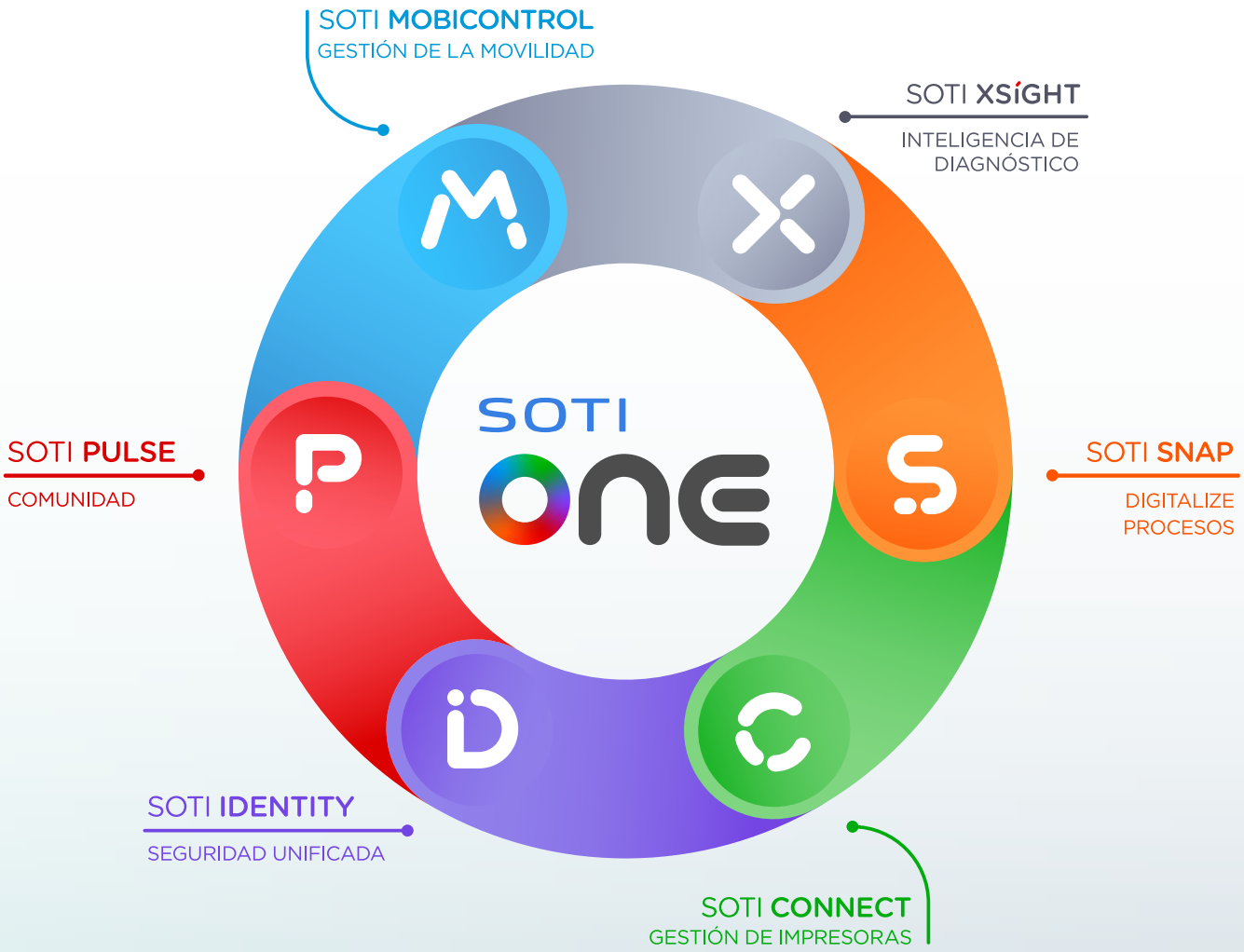
La adopción de la IA aumentó a nivel mundial y se utiliza un tercio más en las organizaciones este año, con regiones como el Reino Unido y Australia marcando el camino. La IA se está integrando al análisis de datos médicos, la planificación de tratamientos, la atención personalizada de los pacientes y más. Es un sustento para la sobrecargada industria sanitaria, pero no se debe ignorar la necesidad de monitorear y asegurar su uso.

Además, se está demostrando que la gestión de dispositivos móviles es una carga importante para los recursos de TI y que la gran cantidad de dispositivos en uso complica el monitoreo efectivo y la gestión remota. La insuficiencia de las soluciones existentes de GDM y las políticas de sustitución inconsistentes implican más presiones, lo que aumenta las preocupaciones con respecto a la seguridad y la sostenibilidad.

En definitiva, alcanzar la verdadera transformación digital en la industria sanitaria requiere que las organizaciones retrocedan y consideren el panorama general. Se requiere una estrategia que combine la continua adopción generalizada de tecnologías innovadoras con inversiones específicas en la modernización e integración de infraestructuras de TI y una solución adecuada para la GME. Este enfoque equilibrado permitirá que las organizaciones protejan los datos, optimicen el uso de dispositivos móviles y, en última instancia, mejoren la atención a los pacientes.

ACERCA DE SOTI

SOTI es una reconocida empresa innovadora y líder de la industria en la simplificación de la movilidad empresarial por hacerlas más inteligentes, más rápidas y más confiables. Con su innovadora cartera de soluciones, las organizaciones pueden confiar en SOTI para mejorar y agilizar sus operaciones móviles, maximizar el retorno de sus inversiones y reducir el tiempo de inactividad de los dispositivos. A nivel mundial, con más de 17 000 clientes, SOTI ha demostrado ser el proveedor de plataforma móvil de referencia para administrar, asegurar y dar soporte a dispositivos críticos para los negocios. Con el soporte de primera categoría que brinda SOTI, las empresas pueden llevar la movilidad a posibilidades infinitas.



PARA OBTENER MÁS DETALLES:

Para obtener más información sobre cómo SOTI puede preparar su negocio para el éxito, **haga clic aquí**.
Para obtener más información sobre la plataforma SOTI ONE, **haga clic aquí**.
Para descubrir cómo SOTI puede contribuir a sus inversiones móviles, póngase en contacto con nosotros hoy a través de **sales@soti.net**.

SOTI es una reconocida empresa innovadora y líder de la industria en la simplificación de la movilidad empresarial por hacerlas más inteligentes, más rápidas y más confiables. SOTI ayuda a las empresas de todo el mundo a llevar la movilidad a posibilidades infinitas.

soti.es

© 2025, SOTI Inc. Todos los derechos reservados. Todos los nombres de productos y empresas son marcas comerciales™ o marcas registradas® de sus respectivos propietarios. El uso de estas marcas comerciales no implica ninguna afiliación con SOTI ni la aprobación por parte del titular de la marca. Las ofertas están sujetas a cambios o cancelación sin previo aviso. SOTI se reserva el derecho de modificar productos, servicios o precios en cualquier momento. La información se proporciona "TAL CUAL" sin ninguna garantía. Los productos y servicios se rigen por los términos y condiciones aplicables.
052925