[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en América Latina el 21/07/2023

# [Medicina y seguridad digital: sus beneficios y peligros](http://www.notasdeprensa.es)

## Según DigiCert los dispositivos médicos conectados crean superficies de ataque para amenazas cibernéticas

Los dispositivos médicos conectados, también conocidos como IoMT (Internet of Medical Things), pueden mejorar drásticamente la salud del paciente y minimizar el potencial de daño. Impulsado por los avances tecnológicos, el IoT en el mercado de la salud en América Latina se valoró en USD 6510 millones en 2021 y se espera que crezca rápidamente a una tasa de crecimiento anual compuesta del 24,30% durante 2023-2028. Según Fortune Business Insights, el mercado global de IoMT aumentará a casi $ 188 mil millones para 2028, cuadruplicando su valor desde 2020. El lado peligroso de la tecnología médicaLos dispositivos médicos conectados crean superficies de ataque para amenazas cibernéticas. Esta posibilidad ya ha sido explorada en la cultura popular, ya que según Marc Goodman autor del libro Future Crimes, describe lo difícil que puede ser investigar un ataque a dispositivos médicos conectados: "es posible que la evidencia de manipulación de dispositivos médicos ni siquiera esté ubicada en el cuerpo, donde el forense está acostumbrado a encontrarla, sino más bien podría estar a miles de kilómetros de distancia, al otro lado del océano en un servidor informático extranjero". Para Dean Coclin, director comercial senior de Desarrollo en DigiCert: "hay muchas otras formas, aunque menos espectaculares, en que los actores de amenazas pueden infiltrarse en IoMT. El ransomware puede bloquear las redes de los hospitales, evitando que los datos de los pacientes lleguen a las bombas de infusión. Infiltrarse en un dispositivo médico conectado puede causar estragos en otros dispositivos que dependen de ellos, ya que los datos del paciente pueden verse comprometidos". Un informe del FBI de 2022 citó investigaciones que muestran que el 53% de los dispositivos IoT y conectados en hospitales tenían vulnerabilidades conocidas, que hay un promedio de 6,2 vulnerabilidades por dispositivo médico y que el 40% de los dispositivos médicos al final de su vida útil ofrecen poco o nada actualizaciones o parches de seguridad. Dadas las innumerables conexiones entre diferentes dispositivos y redes, es esencial proteger y monitorear los dispositivos médicos conectados con una infraestructura de seguridad actualizable. Los lados positivos son innegablesLa confianza digital garantiza que los usuarios puedan confiar en que las interacciones, los procesos y las transacciones que llevan a cabo son seguras, como se analiza en el informe de IDC, Confianza digital: la base para la libertad digital. Para los dispositivos médicos conectados, la incorporación de la confianza digital en una estrategia de seguridad de dispositivos que pueden abarcar lo siguiente: Establecimiento de la autenticidad del dispositivo y prevención de la falsificación: los certificados digitales pueden autenticar de forma segura la identidad del dispositivo, lo que evita que los dispositivos se inicien o funcionen si están comprometidos. Cifrado de datos privados de pacientes que se transmiten de forma inalámbrica o a través de una red: los certificados digitales pueden garantizar tanto el cifrado como la integridad de los datos, lo que impide el robo o la manipulación de datos por parte de malos actores. Mejorar la confianza del usuario en la seguridad del dispositivo: la identidad y las operaciones seguras del dispositivo pueden proporcionar a los usuarios la confianza para incorporar dispositivos que mejoren los resultados del paciente. Integración segura con otras tecnologías que mejoran la precisión de la atención al paciente: los dispositivos médicos conectados pueden integrarse de forma segura en sistemas protegidos que automatizan la entrega precisa y oportuna de medicamentos. Brindando confianza digitalNo es sorprendente que implementar estrategias de confianza digital para dispositivos IoT rara vez sea sencillo. Pero es posible abordarlos con éxito con las siguientes herramientas: Conectividad intermitente en los centros de fabricación: las conexiones de fábrica inconsistentes imponen estrategias que permiten la entrega continua de certificados digitales a partes o dispositivos terminados para el funcionamiento continuo de la línea, incluso durante cortes de Internet. Diversas líneas de productos con diferentes factores de forma y necesidades de seguridad: las soluciones de confianza de DigiCert IoT permiten enfoques centralizados para la gestión de confianza digital, gobernando múltiples tipos de necesidades de inscripción y autenticación de certificados. Esto garantiza la coherencia en la arquitectura y la política al tiempo que reduce la necesidad de expertos en PKI altamente capacitados para crear aplicaciones de seguridad personalizadas. Integración con servicios en la nube: los proveedores de la nube ofrecen servicios de valor agregado para la gestión de IoT sin embargo, muchos requieren el desarrollo de código de integración de API. Esto puede conducir eventualmente a un nivel insostenible de mantenimiento. Las soluciones de confianza de DigiCert IoT automatizan las integraciones con IoT Hub de Azure y otros recursos en la nube, para que los equipos de desarrollo puedan concentrarse en su trabajo en lugar de en la integración del sistema. "A medida que aumenta la cantidad de ataques a los proveedores de atención médica, se vuelve más importante que nunca que los fabricantes de dispositivos IoMT encuentren una manera de consolidar la confianza digital en todas sus líneas de productos", agregó Dean Coclin. En países como Estados Unidos, organizaciones como la Administración de Alimentos y Medicamentos ahora requiere que las aplicaciones de dispositivos médicos brinden una garantía razonable para que los dispositivos estén protegidos, lo que incluye proporcionar a la FDA una factura de software o los materiales utilizados por los dispositivos, y realizar actualizaciones de seguridad y parches periódicamente y en situaciones críticas. Las arquitecturas y estrategias de confianza digital ayudan a los fabricantes de dispositivos IoMT a cumplir con estos requisitos reglamentarios y del mercado.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/medicina-y-seguridad-digital-sus-beneficios-y](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Medicina Innovación Tecnológica Servicios médicos

[notasdeprensa.jpg](http://www.mexicopress.com.mx)

[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)